ADİL KATILIM BANKASI A.Ş.

Corporate Policy on the Prevention of Money Laundering and Financing of Terrorism

CONTENTS

1. PURPOSE AND SCOPE

The objective of the Anti-Money Laundering and Counter-Terrorist Financing Policy (the "Policy") is to establish the general procedures and principles for Adil Katılım Bankası A.Ş. (the "Bank") to fulfill its obligations arising from the legislation on preventing money laundering and terrorist financing, as well as relevant international regulations and agreements. This includes, primarily, compliance with Law No. 5549 on the Prevention of Money Laundering and the Regulation on the Compliance Program for Obligations Related to the Prevention of Money Laundering and Terrorist Financing, published in the Official Gazette No. 26999 dated September 16, 2008. The Policy aims to ensure customer identification, risk-based analysis of customers and transactions, development of strategies to mitigate potential risks, internal controls, audits, preventive measures, reporting obligations, and raising awareness among Bank employees on these matters.

2. DEFINITIONS

In this policy, the following terms are used:

Article 282 of the Turkish Penal Code No. 5237 (Money Laundering of Proceeds from Crime): The offense of processing assets derived from criminal activities, which is punishable by a minimum of six months or more imprisonment as regulated by Article 282 of the Turkish Penal Code, to various transactions with the intent of disguising their illicit origin and presenting them as if acquired through legal means.

Law No. 5549: Law No. 5549 on the Prevention of Laundering of Proceeds of Crime.

Law No. 6415: Law No. 6415 on the Prevention of the Financing of Terrorism.

Law No. 7262: Law No. 7262 on the Prevention of the Financing of the Proliferation of Weapons of Mass Destruction.

FATF (Financial Action Task Force): An international organization that combats money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction.

Ultimate Beneficial Owner (UBO): The natural person or persons who ultimately control or have ultimate influence over a legal entity or an unincorporated organization on whose behalf a transaction is conducted.

Enhanced Approval Mechanism: Approval obtained from the Bank’s compliance unit or higher-level managers.

Politically Exposed Person (PEP): High-level natural persons vested with prominent public functions domestically or in a foreign country through election or appointment, as well as board members and senior executives of international organizations, or other persons in equivalent positions.

Institutional Policies and Procedures: Internal regulations and instructions prepared by the Bank, detailing the provisions outlined in the institutional policy for preventing money laundering and terrorist financing, and communicated to the entire Bank.

Asset: Funds and income owned, possessed, or directly or indirectly controlled by a natural or legal person.

Freezing of Assets: The prevention of disposal, consumption, transfer, or other transactions involving assets by removing or restricting the authority to dispose of them.

MASAK: The Financial Crimes Investigation Board Presidency.

Proceeds from Crime: Assets or values derived from the commission of a crime.

Ongoing Business Relationship: A business relationship established between an obligated party and a client due to services involving continuity, such as account opening, credit, or financing provision.

Suspicious Transaction: Any transaction conducted or attempted at the entities subject to obligations, where there is any information, suspicion, or circumstance that raises suspicion that the assets involved were obtained through illegal means or used for unlawful purposes by terrorist acts, terrorist organizations, terrorists, or those financing terrorism.

Compliance Officer: The officer appointed in accordance with Article 3 of the Compliance Regulation, who is equipped with the necessary authority and employed to ensure compliance with the obligations imposed by the law and relevant legislation.

Deputy Compliance Officer: The person defined in Article 3 of the Compliance Regulation, to whom the compliance officer has delegated, in writing, part or all of the authority and responsibilities imposed by legislation, and who is employed and equipped with the necessary authority to ensure compliance with obligations.

Compliance Program: The set of measures specified in Article 5 of the Compliance Regulation.

Compliance Regulation: The Regulation on the Compliance Program for Obligations Related to the Prevention of Money Laundering and the Financing of Terrorism, published in the Official Gazette No. 26999 dated September 16, 2008.

Obligated Entity: The institutions responsible for implementing mandatory measures, such as identity verification and suspicious transaction reporting, to prevent money laundering within the scope of Law No. 5549.

3. GENERAL PRINCIPLES

At Adil Participation Bank Inc., the Board of Directors is ultimately responsible for ensuring that the compliance program is executed in a manner consistent, adequate, and effective for the Bank's activities, within the scope of regulations concerning the prevention of money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction.

Within this responsibility, the Board of Directors is obligated to appoint a Compliance Officer and Deputy. The Board of Directors defines the duties and authorities of the compliance officer and compliance personnel in writing, approves institutional policies and training programs, and reviews changes to these programs. The Board of Directors is also authorized to evaluate the results of risk management, monitoring, control, and internal audit activities carried out under the compliance program, to take necessary measures to address identified errors and deficiencies, and to ensure that all activities are conducted effectively and in a coordinated manner.

Details regarding authority, responsibility, processes, and practices related to matters regulated under this Policy are determined by the "PRO-13 Prevention of Money Laundering and Terrorist Financing Procedure" (the Procedure). The preparation, updating, and implementation of this Procedure fall under the authority and responsibility of the Compliance Officer or Deputy.

In the preparation and implementation of this Policy, the Procedure, and other internal Bank regulations, the "National Risk Assessment Report" published by MASAK is taken into account, in line with compliance with the FATF standard and as required by the Strategy Document.

All activities carried out at the Bank shall be conducted in accordance with this Policy and Procedure. All employees must comply with this Policy, the Procedure, and relevant legal provisions while performing their duties.

Failure to comply with this Policy or the Procedure, or any violation thereof, may result in disciplinary penalties, up to and including termination of employment, depending on the severity of the incident.

The Policy is communicated to employees through methods determined by MASAK. Changes to the Policy will be published via the Bank's internal systems and shall be deemed notified.

4. RISK MANAGEMENT

Non-compliance with laws and related sub-regulations, or the use of provided services for purposes such as money laundering, terrorist financing, or financing the proliferation of weapons of mass destruction, exposes the Bank to financial and reputational risks.

As part of this policy, a comprehensive risk management policy has been established to identify, rate, monitor, assess, and mitigate potential risks, taking into account the Bank's size, transaction volume, and the unique nature of its activities.

Risk identification, classification, and rating methodologies are continuously reviewed retrospectively based on actual transactions and case studies. This ensures the consistency and effectiveness of the methods, with results reassessed

according to changing conditions. Additionally, risk monitoring and assessment outcomes are regularly reported to the Audit Committee and/or the Board of Directors.

The Bank's Risk Management framework consists of minimum components, including Customer Acceptance Principles, Customer Due Diligence Guidelines, Customer Risk, Country Risk, and Product/Service Risk.

4.1 Customer Acceptance Principles

Customer Acceptance Principles are established to ensure compliance with the "Know Your Customer" principle, which is a cornerstone of national and international regulations and FATF recommendations aimed at preventing money laundering, terrorist financing, and the financing of weapons of mass destruction proliferation. In this context, the Bank pays attention to the following:

- Before any transaction is conducted and throughout the ongoing business relationship, the accuracy of customers' valid identification and address information, as recognized by legal authorities, is verified, and necessary additional measures are taken.

- As part of the customer due diligence process, information is obtained regarding whether the individual holds a public position, their profession, the sector they operate in, and their source of income.

- To the extent possible, information and documentation regarding the source of assets involved in the transaction are requested; a reasonable level of investigation is conducted to verify the provided information and documents.

- Detailed information is gathered about the customer's business history and the duration of their declared business activities.

- Information is obtained on why a ongoing business relationship with the Bank is desired, which products and services are requested, and the expected transaction volume.

- Information is gathered about the geographical area where the declared business operates.

- It is determined whether the customer or the ultimate beneficial owner is involved, or suspected to be involved, in known or alleged financial or other serious crimes, through reviews of lists provided by reputable commercial entities (e.g., Dow Jones).

4.2 Principles Regarding Customer Identification

In accordance with the law and other subordinate regulations, it is essential to identify customers and verify this information. Compliance with the "know your customer" principle, which is one of the most important recommendations of the FATF and has been integrated into our national legislation, holds significant importance for the Bank.

4.2.1 Identity Verification

In accordance with Article 5 of the Regulation on Measures Regarding the Prevention of Money Laundering and Terrorist Financing, it is mandatory to obtain and verify the identity information of customers and those acting on their behalf, as well as to take necessary measures to reveal the actual beneficial owner in all transactions conducted at the Bank. This obligation applies in the following cases:

- When establishing a ongoing business relationship, regardless of the amount.

- When the total amount of a transaction or multiple interconnected transactions reaches or exceeds the amount specified in paragraph (b) of the first subparagraph of Article 5 of the Regulation.

- In electronic transfers, when the transaction amount or the total of interconnected transactions reaches or exceeds the amount specified in paragraph (c) of the first subparagraph of Article 5 of the Regulation.

- In cases requiring suspicious transaction reporting, regardless of the amount.

- When there is doubt about the accuracy or adequacy of previously obtained customer identity information, regardless of the amount.

Identity verification must be completed before establishing a business relationship or conducting a transaction. When establishing a ongoing business relationship, information about the purpose and nature of the relationship must be obtained.

4.2.2 Identity Verification for Individuals

For the identity verification of individuals, the following information is collected: the person's name, surname, date of birth, nationality, type and number of the identity document, address, signature sample, information related to job and profession, and, if available, telephone number, fax number, and email address. For Turkish citizens, in addition to these, the Turkish Republic identification number is collected, and for non-Turkish nationals, the place of birth information is collected.

The accuracy of this information is confirmed through the Turkish Republic identity card, national identity card, driver's license, or passport for Turkish nationals; and through passport, residence permit, or other identity documents approved by the Ministry for non-Turkish nationals. If requested by the authorized authorities, the originals or notarized copies of the identity documents, or readable photocopies or electronic images, are obtained, or the identity information is recorded.

When a ongoing business relationship is established, the accuracy of the declared address is verified through the Address Sharing System (APS). If this information is incomplete or different, it must be confirmed with a residence certificate requested from the customer, a bill issued within the last three months, a public institution document, or other documents approved by the Presidency.

A readable photocopy or electronic image of the documents used for verification should be obtained, or distinctive information about the document should be recorded.

4.2.3 Identity Verification for Legal Entities Registered in the Trade Registry

For the identity verification of legal entities registered in the trade registry, the following information is collected: the entity's name, trade registry number, tax identification number, field of activity, physical address, telephone and email address, along with the name, surname, date of birth, nationality, type and number of the identity document of the person authorized to represent the legal entity, and a signature sample. For Turkish citizens, the Turkish Republic identity number is additionally collected, and for non-Turkish nationals, the place of birth information is obtained.

The legal entity's name, trade registry number, field of activity, and address are verified through documents related to trade registry registration; the tax identification number is verified through documents issued by the relevant unit of the Revenue Administration.

The accuracy of the identity information of persons authorized to represent the legal entity is confirmed through the identity documents specified in the Identity Verification for Natural Persons section; their authorization is confirmed through registration documents.

Upon request by the authorities, after presenting the original identity documents or notarized copies, a readable photocopy or electronic image should be taken, or the identity information should be recorded.

For establishing a ongoing business relationship, the validity and accuracy of the information in the registration documents should be confirmed by consulting the relevant trade registry office records or by querying the database of the Union of Chambers and Commodity Exchanges of Turkey.

Within the scope of an existing ongoing business relationship, when a transaction is requested on behalf of a legal entity through the written instruction of a person authorized to represent the legal entity, the identity information of the authorized representative is verified via a notarized signature circular containing the details from their identification documents, provided it is confirmed that the instruction originates from a company official.

4.2.4 Remote Identity Verification for Individuals and Legal Entities Registered in the Trade Registry

If legislation related to the Bank's core business area permits contract execution using identity verification methods without face-to-face interaction, remote identity verification methods may be used when establishing ongoing business relationships with individuals or legal entities registered in the trade registry. As soon as the Ministry issues instructions regarding the methods to be applied in remote identity verification, other measures for customer identification, and the types of other transactions that can be conducted through this means, work will commence to implement the necessary measures.

4.2.5 Identity Verification for Associations and Foundations

For identity verification of associations, the following information is collected: the association's name, purpose, registration number, tax identification number, full address, telephone number, fax number (if available), and email

address, along with the name, surname, date of birth, nationality, type and number of the identity document, and a signature sample of the authorized representative. For Turkish citizens, the Turkish Republic ID number is added; for non-Turkish nationals, the place of birth is included. The association's name, purpose, registration number, and address are verified using the association's charter and registration records; the tax identification number is confirmed with documents from the Revenue Administration; the identity details of authorized representatives are verified with the identity documents specified in the "Identity Verification for Individuals" section; and the authority to represent is confirmed through documents demonstrating such authority.

For identity verification of foundations, the following information is collected: the foundation's name, purpose, central registration number, tax identification number, full address, telephone number, fax number (if available), and email address, along with the identity details and a signature sample of the authorized representative. For Turkish citizens, the Turkish Republic ID number is added; for non-Turkish nationals, the place of birth is included. The foundation's name, purpose, central registration number, and address are verified using the foundation deed and records from the General Directorate of Foundations; the tax identification number is confirmed with documents from the Revenue Administration; the identity details of authorized representatives are verified with the documents in the "Identity Verification for Individuals" section; and the authority to represent is confirmed through documents demonstrating such authority. Identity verification for branches and representative offices of foreign associations and foundations in Turkey is conducted based on records held by the Ministry of Interior.

Upon request by authorities, after presenting the original documents or notarized copies used for verification, a readable photocopy or electronic image should be taken, or the identity-related information should be recorded.

4.2.6 Identity Verification for Trade Unions and Confederations

For the identity verification of trade unions and confederations, the following information is collected: name, purpose, registration number, tax identification number, physical address, telephone and email details, along with the full name, date of birth, nationality, type and number of identity documents of authorized representatives, and a signature sample. For Turkish citizens, the Turkish Republic ID number is added; for non-Turkish nationals, place of birth information is included. The collected information is verified against these organizations' statutes and the registry records held by the Ministry of Family, Labor, and Social Services; the tax identification number is verified against documents from the Revenue Administration; the identities of authorized representatives are verified using the documents specified in the "Identity Verification for Individuals" section; and the authority to represent is confirmed through registration documents or other documents demonstrating authorization.

Upon request by the authorities, after presenting the original documents or notarized copies used for verification, a readable photocopy or electronic image should be taken, or identity-related information should be recorded for submission.

4.2.7 Identity Verification in Political Parties

For identity verification of political party organizations, the following information is collected: the name of the relevant unit, full address, telephone, fax, and email details, as well as the name, surname, date of birth, nationality, type and number of identity document of the authorized representative, along with a signature sample. For Turkish citizens, the Turkish Republic ID number is added; for non-Turkish nationals, the place of birth information is included. The name and address of the relevant unit of political parties are confirmed from their bylaws; the identity of the authorized representative is verified using the documents specified in the Identity Verification for Individuals section; and their authorization status is confirmed through documents demonstrating authority. Upon request by authorities, after presenting the original documents or notarized copies used for verification, a readable photocopy or electronic image should be taken, or identity-related information should be recorded.

4.2.8 Identity Verification for Legal Entities Residing Abroad and Trust Agreements Established Abroad

Identity verification for legal entities residing abroad is conducted through documents corresponding to those required in Turkey, which are certified by the consulates of the Republic of Turkey or by the authorities of countries party to the Convention Abolishing the Requirement of Legalisation for Foreign Public Documents. Based on a risk-based approach, identity information may also be confirmed via notarized Turkish translations of these documents when necessary.

For assets constituting the subject of a trust agreement established abroad, when a trustee (natural or legal person) specified in the agreement requests a transaction from the Bank requiring identity verification, in order to proceed with such transactions, it must be notified in writing to the Bank that the transaction pertains to the asset account created under the trust agreement, in accordance with Article 15 of the Law.

Identity verification under a trust agreement established abroad is carried out through written copies of the agreement certified by the consulates of the Republic of Turkey or bearing an apostille by the competent authority of a country party to the Convention Abolishing the Requirement of Legalisation for Foreign Public Documents. Within the framework of a risk-based approach, identity information is confirmed via notarized Turkish translations of these documents when required. Additionally, the identity information obtained for the trustee under identity verification is confirmed in accordance with Article 6 or 7. For the purpose of identifying the ultimate beneficial owner, identity information is collected from the settlor, beneficiary or beneficiary groups, and any person designated as an auditor, and reasonable measures are applied to verify them. Necessary measures are also taken to uncover the natural person or persons ultimately controlling the relevant assets.

In the application of the above section, a trust agreement shall be understood as a legal relationship whereby the settlor, who owns an asset, places it under the control of a trustee executing the agreement for the management, use, or other dispositions specified in the agreement, with the aim of benefiting a specific beneficiary or beneficiary group.

4.2.9 Identity Verification for Unincorporated Entities

For transactions conducted on behalf of unincorporated entities, such as apartment, residential complex, or office building management, the following information is collected: the entity's name, full address, and, if available, telephone, fax, and email address, along with the name, surname, date of birth, nationality, type and number of the identity document, and a signature sample of the person authorized to represent the entity. For Turkish citizens, the Turkish Republic ID number is added; for non-Turkish nationals, the place of birth is included. The identity information of the person acting on behalf of the entity is verified using the identity documents specified in the "Identity Verification for Individuals" section, while the entity's information and the person's authorization status are confirmed through a notarized decision log.

For identity verification of entities such as unincorporated partnerships, the following information is collected: the partnership's name, purpose, field of activity, tax identification number, full address, telephone and email address, along with the name, surname, date of birth, nationality, type and number of the identity document, and a signature sample of the person authorized to represent the partnership. For Turkish citizens, the Turkish Republic ID number is added; for non-Turkish nationals, the place of birth is included. The accuracy of the partnership's name, purpose, field of activity, and address is verified through a notarized partnership agreement; the tax identification number is verified using documents from the Revenue Administration; the identity of the person requesting the transaction on behalf of the partnership is verified using the identity documents specified in the "Identity Verification for Individuals" section; and authorization statuses are confirmed through documents demonstrating authority.

Upon presentation of the original documents or notarized copies required for verification, a readable photocopy or electronic image should be taken, or identity-related information should be recorded, to be submitted when requested by the authorities.

4.2.10 Identity Verification in Public Institutions

According to Law No. 5018 on Public Financial Management and Control, in transactions where public administrations within the scope of general administration and professional organizations with public institution status are clients, the identity of the person acting on their behalf is determined in accordance with the Identity Verification for Individuals section. The authorization status is confirmed through a duly issued authorization document in compliance with the legislation.

4.2.11 Identity Verification for Persons Acting on Behalf of Others

When a transaction is requested by persons authorized by individuals representing legal entities or entities without legal personality, the following steps are taken:

- Identity verification of legal entities or entities without legal personality is conducted in accordance with the section on Identity Verification for Legal Entities Registered in the Trade Registry or Identity Verification for Entities Without Legal Personality.

- Identity verification of individuals authorized to represent the legal entity or entity, as well as the persons they have authorized, is performed according to the procedure specified in the Identity Verification for Natural Persons section. If identity verification of the authorized representative cannot be completed using the documents outlined in the Identity Verification for Natural Persons section, it may be conducted based on a notarized power of attorney or signature circular containing the information from the identity documents.

- The authorization status of persons authorized by the representatives is confirmed through a notarized power of attorney or written instructions provided by the authorized representatives. The signatures of the authorized representatives on the written instructions are verified against their notarized signature circulars.

When a person acts on behalf of a natural person customer, the identity verification of the person acting on behalf of the customer is conducted in accordance with the Identity Verification for Natural Persons section. Additionally, the authorization status of the person acting on behalf of the customer is confirmed through a notarized power of attorney. If identity verification of the customer on whose behalf the action is taken cannot be performed according to the Identity Verification for Natural Persons section, it is conducted based on a notarized power of attorney. If identity verification of the customer on whose behalf the action is taken has been previously completed, the requested transaction may be carried out with the written instruction of the customer, provided the customer’s signature on the written instruction is verified against the signature on file with the Bank.

For transactions conducted by legal representatives on behalf of minors or persons under guardianship, the authority of guardians appointed by court order, as well as custodians and trustees, is confirmed through the original or notarized copy of the relevant court order. When parents request transactions on behalf of their minor children, identity verification of both the child and the parent requesting the transaction, in accordance with the Identity Verification for Natural Persons section, is sufficient.

Upon presentation of the original or notarized copies of the documents required for verification, a readable photocopy or electronic image should be taken, or identity-related information should be recorded, to be submitted when requested by the authorities.

4.2.12 Verification of the Authenticity of Supporting Documents

When doubts arise regarding the authenticity of documents used during identity verification, the Bank, within its capabilities, confirms the document's authenticity by contacting the issuer, institution, or other authorized authorities.

4.2.13 Identity Verification in Subsequent Transactions

For a customer whose identity has been previously verified in accordance with the procedures, in subsequent transactions requiring identity verification conducted face-to-face within the scope of an ongoing business relationship, identity-related information is collected and compared with the existing information at the Bank. Following this comparison, the name, surname, and signature sample of the person carrying out the transaction are added to the relevant document. If there is doubt regarding the accuracy of the information obtained, it is verified by comparing the information on the original identification documents or their notarized copies, presented for confirmation, with the information held at the Bank.

In subsequent transactions requiring identity verification conducted using systems that enable non-face-to-face transactions, necessary measures are taken to ensure the accuracy of the customer's identity and the currency of the identity information.

4.2.14 Identification of Persons Acting on Behalf of Others

The bank takes necessary measures to determine whether transactions are conducted on behalf of another person. In establishing a ongoing business relationship, a written declaration is obtained from the customer regarding whether they are acting on behalf of another person's account. This declaration may be appended to the customer agreement or obtained using special forms.

When the person requesting the transaction declares that they are acting on behalf of another person, both the identity and authorization status of the requester and the identity of the person on whose behalf they are acting are verified. If the individual claims not to be acting on behalf of another person's account but doubts arise, necessary measures are implemented to identify the actual beneficial owner.

4.2.15 Identification of the Ultimate Beneficial Owner

In accordance with the customer identification principle, necessary measures are taken to reveal the ultimate beneficial owner of a transaction. When establishing a ongoing business relationship with legal entities registered in the trade registry, the identity of natural person partners holding more than twenty-five percent of the legal entity's shares is determined according to the section on Identification of Natural Persons.

If it is suspected that a natural person partner holding more than twenty-five percent of the shares of the legal entity is not the ultimate beneficial owner, or if no natural person holds shares at this rate, necessary measures must be taken to identify the natural person or persons who ultimately control the legal entity. The natural person or persons identified in this manner are considered the ultimate beneficial owner.

In cases where the ultimate beneficial owner cannot be identified, the natural person or persons with the highest level of executive authority registered in the trade registry are considered the ultimate beneficial owner in the capacity of senior management.

Within the scope of a ongoing business relationship, necessary measures must be taken to identify the natural person or persons who ultimately control other legal entities or unincorporated associations. If the ultimate beneficial owner cannot be identified, the natural person or persons with the highest level of executive authority within them are considered the ultimate beneficial owner in the capacity of senior management.

The identity information of the identified ultimate beneficial owner must be obtained, and necessary measures must be applied to confirm this information. In this context, notarized signature circulars containing identity information may be used.

4.2.16 Transactions Requiring Special Attention

The bank pays special attention to transactions that are complex, unusually large, lack an apparent economic or visible lawful purpose. All necessary measures are taken to obtain sufficient information about the purpose of such transactions, and the information, documents, and records obtained are preserved for submission to the authorities.

4.2.17 Monitoring of Customer Status and Transactions

The bank is obligated to continuously monitor, throughout the ongoing business relationship, whether the transactions conducted by its customers are commensurate with their professional profile, commercial activities, business history, financial status, risk profile, and sources of funds, and to keep customer information up to date. Additionally, the accuracy of information concerning the telephone and fax numbers, as well as email addresses obtained for the identification of these customers, is confirmed, within the framework of a risk-based approach, by contacting the relevant party using these means when necessary. Our bank takes the necessary measures to monitor transactions conducted outside of an ongoing business relationship with a risk-based approach as well. Our bank establishes an appropriate risk management system for these purposes.

4.2.18 Measures Against Technological Risks

Within the scope of digital banking, special attention is given to the risk of new and emerging technologies, new distribution channels, and products being used for money laundering and terrorist financing. The compliance of new services to be offered by the Bank and existing products restructured as a result of technological developments with laws and regulations is continuously monitored, and the suspension of implementation is ensured when necessary. Particular attention is paid to transactions such as establishing ongoing business relationships through non-face-to-face methods or systems, deposits/withdrawals, and electronic transfers. In this context, effective measures are taken, such as closely monitoring transactions that do not align with the customer's financial profile and activities, and setting limits on amounts and transaction numbers.

4.2.19 Reliance on Third Parties

The Bank may establish a business relationship or conduct transactions by relying on the measures taken by another financial institution regarding the identification of the customer, the person acting on their behalf, and the ultimate beneficial owner, as well as obtaining information about the purpose of the business relationship. In such cases, in accordance with the Law and relevant regulations, ultimate responsibility lies with Adil Participation Bank, which conducts the transaction by relying on this third party.

This principle may be applied provided that it is ensured that the third party complies with identification, record-keeping, and customer recognition rules, and if it is based abroad, is subject to regulations and supervision consistent with international standards in the fight against money laundering and terrorist financing. The Bank that establishes a business relationship or conducts transactions by relying on a third party shall promptly obtain the customer's identification information from the third party.

The principle of reliance on third parties does not apply if the third party is based in high-risk countries.

4.2.20 Rejection of Transactions and Termination of Business Relationships

If customer identification cannot be completed or sufficient information about the purpose of the business relationship cannot be provided, no business relationship will be established with these individuals or institutions, and the requested transactions will not be carried out. Opening accounts under anonymous or fictitious names is strictly prohibited. If there are doubts regarding the adequacy and accuracy of previously obtained identification information, and these concerns cannot be resolved, the business relationship will be terminated. Additionally, it will be assessed whether the specified circumstances constitute suspicious transactions.

4.2.21 Correspondent Banking Relationship

The bank pays attention to the following matters in its overseas correspondent banking relationships:

- Obtains accurate information from publicly available sources regarding whether the correspondent financial institution has undergone any money laundering or terrorist financing investigations, received any penalties or warnings, and its business nature, reputation, and level of supervision.

- Evaluates the correspondent financial institution's system for combating money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction, and ensures that this system is adequate and effective.

- Obtains approval from senior management before establishing new correspondent relationships.

- Clearly defines the responsibilities of both itself and the correspondent financial institution through a contract, ensuring compliance with the Customer Due Diligence obligations stipulated in relevant legislation.

- If the correspondent relationship involves the use of payable-through accounts, takes necessary measures to ensure that the correspondent financial institution has implemented adequate precautions within the framework of Customer Due Diligence principles and can provide identity information of relevant customers upon request.

Financial institutions cannot establish correspondent relationships with "shell banks" or financial institutions that they cannot confirm do not allow their accounts to be used by shell banks. For this purpose, specific customer acceptance rules and workflows requiring senior management approval are established, including requesting a questionnaire form containing the above-mentioned information from other financial institutions applying to open correspondent accounts.

Accurate information is obtained regarding the regulatory adequacy of the country where the financial institution for which a correspondent relationship is to be established is located, and the adequacy of its system for preventing proceeds of crime is examined. A contract specifying responsibilities and obligations is drawn up between the bank and the correspondent financial institution. The Wolfsberg Anti-Money Laundering Principles for Correspondent Banking may also be considered for additional measures.

4.2.22 Electronic Transfers

In domestic and international electronic transfer messages at or above the amount specified in the first paragraph of Article 24 of the Regulation on Measures Regarding the Prevention of Laundering Proceeds of Crime and Financing of Terrorism, it is mandatory to include at least one of the following pieces of information that help identify the sender:

• The full name of the natural person or the title of the legal entity.

• Account number or reference number.

• Information such as address, place and date of birth, national ID number, passport number, tax identification number.

The accuracy of this information is additionally confirmed. The same information must also be provided for the recipient; however, confirmation of this information is not mandatory. For transfer messages below the amount specified in the

second paragraph of Article 24 of the Regulation, only the name/title and account number or reference number are required for the sender and recipient, and there is no obligation for confirmation.

Transfers between banks themselves and transfers where credit or bank card numbers are used in the messages are excluded from this scope.

A financial institution receiving an electronic transfer message with incomplete information must either return the transfer or request the sending institution to complete the missing information. If messages from the sending bank consistently contain incomplete information and are not completed despite requests, the receiving financial institution should consider steps such as rejecting transfers from this sender, limiting relationships, or terminating the business relationship.

Special attention is paid to ensuring that the necessary information about the sender is transmitted at every stage throughout the entire message chain, from the initial financial institution where the transfer order is given to the final financial institution that will execute the payment.

4.2.23 Terminal Services

In payment services conducted via terminals provided under the payment instrument acceptance service to be offered by our Bank in accordance with Article 12 of Law No. 6493 on Payment and Securities Settlement Systems, Payment Services, and Electronic Money Institutions (terminal services), the following measures are applied in establishing business relationships with customer merchant members and in other transactions requiring identity verification:

- Customer acceptance, entering into a business relationship, maintaining an existing business relationship, or executing transactions within the scope of terminal services of a specified amount or type are approved by the Board of Directors upon the suitability of the Compliance Officer.

- Detailed information is obtained to determine the ultimate beneficial owner regarding terminal service customers, and customers are requested to update their identity information by repeating the customer acquisition process every three months.

- Additional explanations and declarations are obtained from the customer regarding the nature of the business relationship within the scope of terminal services.

- Additional explanations and declarations are obtained regarding the source of the assets subject to the transaction and the funds belonging to the customer within the scope of terminal services.

- Additional explanations and declarations are obtained regarding the purpose of the transaction within the scope of terminal services.

- The Compliance Department examines transactions within the scope of terminal services and establishes additional controls for transactions and related customers deemed necessary.

- If deemed necessary, customers may be requested to provide additional supporting documents for the explanations and declarations obtained within the scope of terminal services.

- Transactions found to pose compliance risks in any way are immediately halted, and if necessary, contracts with the customer are terminated. Decisions regarding transaction halting and contract termination practices are made by the Board of Directors upon notification by the Compliance Officer.

4.2.24 Relations with High-Risk Countries

Our bank is obligated to exercise special caution in establishing business relationships and conducting transactions with individuals and legal entities based in high-risk countries. For transactions lacking a reasonable legal or economic purpose, as much information as possible regarding their purpose and nature is collected and recorded. Necessary measures regarding high-risk countries, including those designated as such by international organizations of which Turkey is a member, are initiated immediately upon notification by the Ministry.

4.2.25 Simplified Measures

The Ministry of Treasury and Finance may permit the implementation of simplified measures in specific situations where the risk of money laundering and terrorist financing is assessed as low, within the framework of customer identification principles. These situations include:

- Transactions conducted between financial institutions.

- Transactions where the customer is a public administration entity under Law No. 5018 or a professional organization with public institution status.

- Business relationships established through bulk customer acceptance under salary agreements.

- Transactions related to plans and contracts providing retirement benefits to employees through salary deductions.

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

Measures to be determined by the Ministry for application within this scope, as well as other low-risk transaction types not listed above, are taken into consideration. However, if there is a possibility of money laundering or terrorist financing risk in a transaction, simplified measures are not applied, and the transaction is handled with consideration that it may be suspicious.

4.2.26 Enhanced Measures

Our bank applies all or part of the following measures, proportionate to the risk, in transactions covered by Articles 18, 20, and 25 of the Regulation and in high-risk situations identified within the framework of a risk-based approach:

- Obtains additional information about the customer and the actual beneficial owner and updates their identification details more frequently.

- Collects supplementary information regarding the nature of the business relationship.

- Gathers as much information as possible about the source of the assets and funds involved in the transaction.

- Determines the purpose of the transaction.

- Makes the establishment of a new business relationship, the continuation of an existing relationship, or the execution of a transaction subject to senior management approval.

- Increases the number and frequency of applied controls, identifies transaction types requiring additional control, and maintains the business relationship under strict supervision.

- In the case of establishing a ongoing business relationship, requires that the initial financial transaction be conducted through another financial institution where customer identification principles have been applied.

Work begins as soon as the relevant instruction is issued by the Ministry for the application of additional enhanced measures beyond those specified above and for high-risk situations to be determined under this article.

4.3 Activities Related to Risk Management

Risk management activities include at least the following steps:

- Developing risk identification, rating, classification, and assessment methods based on customer, service, and country risks.

- Rating and classifying services, transactions, and customers according to their risk levels.

- Monitoring and controlling risky customers, transactions, or services; taking necessary measures to mitigate risks; providing warning reports to relevant units; establishing appropriate operational and control rules for high-level approval and, when necessary, auditing of transactions.

- Reviewing risk identification and assessment methods, as well as risk rating and classification methodologies, for consistency and effectiveness through case studies and past transactions; reassessing and updating them in light of results and changing conditions.

- Tracking national legislation and the recommendations, principles, standards, and guidelines of international organizations on risk-related topics and conducting necessary improvement work.

- Regularly reporting risk monitoring and assessment results to the Board of Directors.

4.3.1 Customer Risk

A customer's business line requiring intensive cash usage, involving the trade of high-value goods, or enabling international fund transfers increases the Bank's risk of being exploited for money laundering or terrorist financing. To mitigate such risks, customer acceptance principles and risk profiles are established under the "Know Your Customer" principle. This allows for the identification of individuals or entities with whom business relationships should not be established or for whom additional measures are required.

4.3.2 Product / Service Risk

Certain products and services are more vulnerable to money laundering due to their facilitation of fund transfers. In this context, non-face-to-face transactions, correspondent banking, technology-based products, safe deposit boxes, prepaid cards, private banking products, and other products and services deemed risky under published procedures are classified as high-risk.

4.3.3 Country Risk

Country risk refers to risks associated with countries that, according to the Ministry of Treasury and Finance, lack sufficient regulations on money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction, do not cooperate in combating these crimes, or are considered risky by international organizations.

4.3.4 Risk Categories, Customer Risk Classification, and Continuous Monitoring

The Bank adopts a risk-based approach to determine risk assessment criteria and performs a systematic risk rating by considering customer, service, and country risks as a whole. Customer risk classification is based on factors such as the sector and profession in which they operate, their country of citizenship, frequency of cash usage, individuals and organizations with whom they have business relationships, the scale of the business relationship, and the financial services they use.

Customer risk classification must be conducted before the business relationship begins. The purpose of this classification is to enhance customer due diligence, monitoring, and control activities to minimize the risks the Bank may be exposed to. Risk classification consists of at least three categories:

- Low risk

- Medium risk

- High risk

For customers, transactions, or services identified as high risk, approval from the Internal Control and Compliance Presidency must be obtained. When deemed necessary, approval from the Compliance Officer or Deputy is also required. The risk status of customers is reviewed at periodic intervals specified in the relevant guidelines.

Table 1: Risk Rating Matrix and Applicable Measures

Risk Level	**Measures Actions to be Taken**
Low Risk	Standard Customer Due Diligence (CDD) is applied. Transactions are monitored with routine checks.
Medium Risk	Standard CDD is applied. Customer and transaction profiles are reviewed at more frequent intervals.
High Risk	Enhanced Customer Due Diligence (EDD) is applied. Additional information and documentation regarding the purpose of the transaction and the source of funds are obtained to the extent possible. Transactions may be carried out with the approval of a higher authority.

4.3.5 Additional Measures for High-Risk Groups

For customers classified as high-risk based on the Bank's risk assessment, one or several, or all of the following measures are applied proportionally to the risk, with the aim of risk reduction:

- Additional information is obtained about the customer and the ultimate beneficial owner, and identification details are updated more frequently.

- Additional information is obtained regarding the nature of the business relationship.

- As detailed information as possible is obtained about the source of the assets involved in the transaction and the customer's funds.

- The purpose of the transaction is determined.

- The initiation, continuation of the business relationship, or execution of the transaction is subject to approval by a senior manager.

- The number and frequency of controls are increased, and types of transactions requiring additional control are identified, keeping the business relationship under strict supervision.

- When establishing a ongoing business relationship, it is mandatory for the initial financial transaction to come from another financial institution where customer due diligence principles have been applied.

4.3.6 Additional Precautions Required When Establishing Business Relationships with Certain Persons and Organizations

4.3.6.1 Customer Transactions Involving High-Risk Geographical Areas or Connections

Additional measures are taken when accepting customers who operate in countries that do not cooperate with FATF, of which our country is a member, or that lack adequate supervision mechanisms, or who have business relationships with individuals/organizations in these countries. Reasonable research is conducted using external sources to gather information, and a ongoing business relationship is established following an enhanced approval mechanism.

4.3.6.2 Correspondent Banks Located in or Connected to High-Risk Geographical Areas

Additional measures are also applied in relationships with correspondent banks operating in countries outside the European Union that do not cooperate with FATF or have insufficient supervision mechanisms. Information is collected as a result of reasonable research, and a ongoing business relationship is established through an enhanced approval mechanism.

4.3.6.3 Free Zones and Financial Centers

Maximum caution and diligence are exercised in transactions with customers related to free zones and other financial centers where regulatory and supervisory functions are minimal or non-existent. Decisions are made following an enhanced approval mechanism.

4.3.6.4 Situations Involving Politically Exposed Persons (PEPs), Their Relatives, or Cases Where They Are the Ultimate Beneficial Owners

It is determined whether the customer or the ultimate beneficial owner is a politically exposed person or a relative of one. A reasonable investigation is conducted to ascertain the source of funds and assets, and the decision to establish a business relationship is made through an enhanced approval mechanism.

For business relationships and transactions with politically exposed persons appointed or elected by a foreign country, or with their spouses, first-degree relatives, or close associates, the following measures are applied:

- The establishment, continuation, or execution of the business relationship is subject to approval by a senior-level official.

- Reasonable measures are taken to determine the source of assets and funds belonging to these persons or involved in the transaction.

- The business relationship is closely monitored by increasing the number and frequency of applied controls and identifying transaction types that require additional scrutiny.

The above measures are applied if a business relationship with politically exposed persons appointed or elected by Turkey or serving in international organizations, or with their relatives, is assessed as high-risk. Even if these persons are not assessed as risky, the Bank may decide to implement all or part of these measures.

4.3.6.5 Sensitive Sectors and Professional Groups

For individuals and organizations with high cash transaction volumes or those generating high-value cash flows due to their activities, a comprehensive review is conducted prior to establishing a business relationship, and "Enhanced Customer Due Diligence Measures" are applied. The decision to work with such customers is subject to a strengthened approval mechanism. In this context, based on a customer-specific risk assessment conducted by the Internal Control and Compliance Presidency, the business relationship is established upon approval from the Head of Internal Control and Compliance. The Head of Internal Control and Compliance may submit the decision to establish a business relationship to the General Manager or, upon the General Manager's recommendation, to the Board of Directors for approval.

Similarly, electronic money institutions, payment service providers, and Crypto Asset Service Providers (CASPs) are also considered within the scope of "Sensitive/High-Risk Sectors." Due to the specific risks arising from their operational structures, these entities are subject to additional regulations, supplementary control processes, and restrictive application principles.

4.3.6.6 Special Provisions Regarding Electronic Money and Payment Service Institutions

Electronic money and payment service institutions are always classified as "High-Risk Customers," regardless of their ownership structure. The following additional measures apply to these institutions:

- Identification of Beneficial Owners: The institution's ownership structure is examined to identify individuals holding more than 25% of shares and those in control. At a minimum, the institution's ownership structure and beneficial owners are reviewed annually, and records are updated accordingly.

- Pre-Approval Mechanism: Before establishing a business relationship with electronic money and payment service institutions, a detailed analysis is conducted by the Compliance Unit. Account openings cannot proceed without the Compliance Officer's favorable opinion and the Board of Directors' approval.

- License Verification: During the customer identification process, the institution's operating permit and license scope obtained from the Central Bank of the Republic of Turkey are verified.

- Compliance Program Assessment: The adequacy of the institution's own Compliance Program or other obligations, such as the appointment of a compliance officer, is analyzed. Accounts cannot be opened, and no business relationship may be established with institutions that do not fully meet their obligations under the Compliance Regulation.

- Nature of the Business Relationship: The sectors served by the institution are thoroughly investigated. The institution is required to disclose the nature of its business relationships with its own customers.

- Source of Funds: The source of the institution's assets held with the Bank is determined in writing, as well as whether it segregates its own assets from customer funds (safeguarding accounts) and which accounts held with the Bank belong to whom.

- Purpose of Transactions: For transactions conducted by the institution through the Bank or by Bank customers with the institution via the Bank, explanations are required on a transaction-by-transaction basis. Transactions are not permitted to proceed without such explanations.

- Transaction Approval: The Bank may require that transactions involving the institution be approved by the Compliance Officer or the Board of Directors, based on amounts and types determined by the Bank.

- Risk Management and Control Practices: Within the scope of compliance risk management activities, the number and frequency of controls for electronic money and payment service institutions are increased, taking into account the volume and size of the institution's transactions. Details of these practices are outlined in "PRO-013 Prevention of Money Laundering and Terrorist Financing Procedure."

4.3.6.7 Special Provisions Regarding Crypto Asset Service Providers

Crypto Asset Service Providers (CASPs) are always classified as "High-Risk Customers," regardless of their ownership structure. The following "Enhanced Customer Due Diligence Measures" apply to these entities:

- Beneficial Ownership Identification: The partnership structure of the entity is examined to identify natural persons holding 25% or more of the capital and those with ultimate control. The entity’s partnership structure and beneficial ownership information are reviewed and updated at least annually.

- Pre-Approval Mechanism: A detailed risk analysis is conducted by the Compliance Unit before establishing a business relationship with Crypto Asset Service Providers. Account opening cannot proceed without the "suitability opinion" of the Compliance Officer and the approval of the Board of Directors.

- License Verification: During the customer identification process, the entity's operating permit and license scope from the Capital Markets Board (CMB) are confirmed through official sources.

- Compliance Program Assessment: The effectiveness of the entity's own Compliance Program and the adequacy of its legal obligations, such as the appointment of a Compliance Officer, are analyzed. Accounts cannot be opened, and business relationships cannot be established with entities that do not fully meet their obligations under the Compliance Regulation.

- Nature of the Business Relationship: The sectors served by the entity are thoroughly scrutinized. The entity is required to provide transparent disclosure regarding the nature and purpose of the business relationships it establishes with its own customers.

- Purpose of Transactions: Explanations are requested on a transaction basis for transfers made by the entity through the Bank or by Bank customers through the entity. Transactions without satisfactory explanations are not permitted.

- Transaction Approval: The Bank may require transactions involving the entity to be submitted for approval by the Compliance Officer or the Board of Directors, based on predetermined amount limits and transaction types.

- Risk Management and Control Practices: As part of compliance risk management activities, the frequency of controls on Crypto Asset Service Providers is increased. The entity's transaction count, volume, and fund flow traffic are closely monitored.

4.3.7 Countries, Individuals, and Institutions with Whom Business Relationships Will Not Be Established or Whose Financial Transactions Will Not Be Facilitated

4.3.7.1 Individuals and Entities Listed on Authorized Organizations' Sanction Lists

Under regulations for preventing money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction, no ongoing business relationships are established, and no transactions are facilitated with individuals or entities included in sanction lists published by authorized organizations. If an existing customer or entity is found to be on a blacklist, the relevant authorities are notified accordingly. The termination of any ongoing business relationship is also evaluated by the Internal Control and Compliance Directorate.

4.3.7.2 Embargoed Countries Listed on Authorized Organizations' Sanction Lists

Under regulations for preventing money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction, transactions related to countries on embargo lists published by authorized organizations are not facilitated.

4.3.7.3 Shell Banks

No direct or indirect business relationships are established, and no transactions are facilitated with shell banks that lack a physical presence, are not subject to supervision, and do not have adequate regulations for preventing money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction.

4.3.7.4 Offshore Banking

No direct or indirect business relationships are established, and no transactions are facilitated with offshore banks where regulatory and supervisory functions are minimal or nonexistent.

4.3.7.5 Other Individuals and Entities with Whom Business Relationships Will Not Be Established

In addition to the above, other individuals and entities with whom business relationships will not be established are communicated to all Bank employees through procedures and regulations issued by the Internal Control and Compliance Directorate. These include individuals and associated entities listed on local or international (e.g., U.S./OFAC, EU, UN, UK) sanction lists due to involvement in financial crimes, corruption, or terrorism.

4.4 Screening of Customers and Payments through Lists

In cases involving all new customers, authorized representatives, company owners, and other related individuals are monitored against the following lists:

- European Union Financial Sanctions List.

- US/OFAC List.

- United Nations Security Council List.

- United Kingdom Sanctions List.

- Local sanctions lists (lists published by MASAK, the Ministry of Internal Affairs' Wanted for Terrorism List, etc.).

- Politically Exposed Person (PEP)/Close Associate lists provided by reputable commercial organizations such as Dow Jones or Worldcheck.

- Bank internal monitoring list.

- Sanctions lists published under Law No. 6415 on the Prevention of the Financing of Terrorism.

- Sanctions lists published under Law No. 7262 on the Prevention of the Financing of the Proliferation of Weapons of Mass Destruction.

For existing customers, these checks are repeated periodically based on updates to the lists.

5. MONITORING AND CONTROL

Continuous monitoring and control are essential to ensure that customer activities are conducted in compliance with the Law, relevant legislation, and Bank policies and procedures. Monitoring and control activities are carried out under the responsibility of the Compliance Officer, and the results are reported to them for evaluation in terms of suspicious transactions.

Within this scope, systematic arrangements are made and monitoring-control activities are carried out, taking into account the following matters:

- Tracking of customers and transactions in the high-risk group.

- Monitoring of transactions conducted with high-risk countries.

- Tracking of complex and unusual transactions.

- Control of transactions inconsistent with the customer profile.

- Monitoring of linked transactions exceeding the threshold requiring identity verification.

- Verification of mandatory information in electronic transfer messages.

- Continuous monitoring of whether customer transactions are consistent with their profession, activities, and risk profile.

- Control of non-face-to-face transactions.

- Tracking of new products and technological developments for potential misuse risks.

6. SUSPICIOUS TRANSACTIONS

During monitoring and control activities or during non-face-to-face transactions, if any suspicion arises that the assets involved in the transaction were obtained through illegal means or are being used for illegal purposes, a suspicious transaction report must be filed without any threshold limit. All necessary information and documents must be provided immediately upon request to support the Compliance Officer in this matter.
Bank units cannot report directly to MASAK. Reports must first be submitted to the Internal Control and Compliance Directorate. After review, transactions deemed suspicious by the Compliance Officer are reported to MASAK.
Suspicious transaction reports and related information are subject to confidentiality provisions under the relevant Law. Sharing this information with third parties is prohibited under the applicable legislation.
The deadline for reporting a suspicious transaction to the Compliance Officer is a maximum of three business days from the date the transaction is detected.
The period between the detection of the suspicious transaction and its submission to MASAK by the Compliance Officer, including the Compliance Officer's assessment of the matter, is a maximum of 10 business days.

7. INTERNAL AUDIT

The effectiveness and adequacy of the institution's policies and procedures, risk management, monitoring, control, and training activities are annually reviewed and audited by the Inspection Board's Internal Audit Management using a risk-based approach. Deficiencies, errors, and abuses identified as a result of internal audits, along with opinions and recommendations to prevent their recurrence, are reported by the Inspection Board to the Board of Directors through the Audit Committee, and measures taken by the relevant unit managements are monitored.
Within the scope of internal audit activities, statistics containing information such as the Bank's annual transaction volume, total number of personnel and affiliated units, number of audited units, dates of audits conducted in these units, total audit duration, personnel involved in audits, and number of transactions audited are reported to the Presidency by the Compliance Officer by the end of March of the following year.

8. TRAINING

One of our Bank's fundamental priorities is combating illicit activities such as money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction. To foster a strong corporate awareness in this area and keep our employees' knowledge up to date, specialized training programs are organized in line with our Bank's dynamic structure and changing conditions.
Training content is primarily determined to encompass internal Bank policies and procedures, risk management, monitoring and control processes, and information sharing. These programs are conducted jointly by the Human Resources Department under the coordination of the Compliance Officer. Our annual training plan includes at least the following topics:
- Concepts, stages, and current methods of money laundering and terrorist financing (explained with real-life examples).
- Relevant legal legislation and regulations.
- Identification of financial risk areas.
- Our Bank's specific policies and operational rules.
-Legal obligations:
  • Customer due diligence processes.
  • Reporting of suspicious transactions.
  • Retention and presentation of documents.
  • Obligation to provide information and documents.
  • Sanctions to be applied in case of legal non-compliance.
- International regulations on combating money laundering and terrorist financing.
Trainings are provided in classroom or remote formats based on the employee's experience and role. Newly hired staff are required to complete these trainings within 90 days. To ensure information remains current, regular interim exams are conducted, and trainings are repeated for employees who do not achieve sufficient success.
To enhance training effectiveness, various methods are used, such as seminars, panels, visual and auditory materials, and computer-assisted interactive programs. Training personnel must hold a "Train the Trainer" certificate.
The outcomes of training activities (date, duration, number of participants, etc.) are recorded, employees' knowledge levels are regularly assessed, and steps are taken to address any gaps.

9. MONITORING OF LEGISLATION

Ensuring that our bank's activities comply with laws, regulations, and internal procedures is one of our fundamental principles. Therefore, we closely monitor all changes in legal regulations, assess their impact on our business processes, and promptly implement necessary updates. This ensures that our control systems remain up-to-date.

10. OBLIGATION TO PROVIDE INFORMATION AND DOCUMENTS

All requests for information and documents from legally authorized institutions and officials are meticulously fulfilled in accordance with the legal framework.

11. RECORD KEEPING

In compliance with laws and regulations aimed at preventing money laundering, all information and documents held by our bank are stored in an easily accessible format for the periods specified by law. This retention obligation includes suspicious transaction reports submitted to MASAK, internal notifications, written justifications for decisions not to report suspicious transactions, and all other relevant documents.

12. MANAGEMENT REPORTING

The Compliance Officer periodically reports the bank's risk profile and the effectiveness of implemented controls to Senior Management, the Audit Committee, and the Board of Directors. Additionally, urgent notifications are provided as needed regarding significant events.

13. OBLIGATIONS TO PREVENT THE FINANCING OF TERRORISM AND WEAPONS OF MASS DESTRUCTION

Our bank adopts a "risk-based" approach in accordance with laws and regulations aimed at preventing the financing of terrorism and weapons of mass destruction. This includes implementing freezing decisions communicated to us, managing related assets, and addressing risks associated with non-compliance with obligations.

13.1 Freezing of Assets

The fundamental principles for managing risks related to the freezing of assets, as well as monitoring and mitigating these risks, are outlined below:

13.2 Risks Associated with Freezing Asset

The primary risks encountered in asset freezing processes are classified under three main categories:

- Breach Risk: Allowing an asset subject to a freezing decision to be used, transferred, or released (disposed of) in violation of the decision.

- Non-Implementation Risk: Delayed reflection of the decision in the system, failure to block relevant accounts in a timely manner, or incomplete or non-fulfillment of notification obligations.

- Evasion Risk: Prohibited individuals or organizations attempting to circumvent or nullify freezing decisions by concealing their true identities (through front companies, third parties, or complex financial structures).

13.3 Assessment and Monitoring of Asset Freezing Risks

13.3.1 Risk Assessment Criteria

- Customer Risk: The customer’s direct or indirect connections with individuals or entities listed on sanction lists, such as the UN Security Council Lists or Presidential Decrees.

- Geographic Risk: Commercial and financial relationships with sanctioned regions or countries considered high-risk.

- Product and Service Risk: The use of products that enable high-speed fund transfers or provide anonymity (e.g., crypto assets, cash-like instruments, and similar).

13.3.2 Monitoring Mechanisms

- Automated Screening: Real-time comparison of customer databases and transactions with current sanction lists.

- Retroactive Screening: When a new freezing decision or sanction list is published, the existing customer portfolio is screened retrospectively based on these updates.

- Transaction Monitoring: Detection of unusual transaction patterns and suspicious activities (e.g., sudden asset outflows prior to a freezing decision).

13.3.3 Risk Mitigation

The following control processes are applied to minimize identified risks:

- Enhanced Customer Due Diligence Policies: It is essential to clearly identify not only the legal name of the person or entity but also the "beneficial owner" information.

- Staff Training: Regular training is provided to relevant operational units on the legal consequences and implementation methods of freezing decisions.

- Technological Infrastructure: Effective use of AML software's "fuzzy matching" capability to detect spelling errors or variations in names.

- Internal Audit: The effectiveness and compliance of freezing processes are regularly audited and evaluated by our Bank's Internal Control and Compliance Directorate and the Inspection Board Directorate.

13.3.4 Our Bank's Responsibilities and Process for Implementing Decisions

The process of asset freezing in Turkey is primarily conducted within the framework of Law No. 6415 on the Prevention of the Financing of Terrorism and Law No. 7262 on the Prevention of the Financing of the Proliferation of Weapons of Mass Destruction. Our bank takes all necessary measures for the continuous monitoring of customers whose assets are frozen and their transactions. The steps of the process applied within this scope are as follows:

- Implementation of Decisions: Following the announcement or notification by MASAK, our bank freezes the relevant assets forthwith and, in any case, within 24 hours at the latest.

- Notification to MASAK: Details regarding the frozen assets (such as business relationship, account number, balance, etc.) are reported to MASAK as soon as possible and within 7 days at the latest.

- Digital Access Block: Credit and bank cards belonging to individuals and organizations subject to freezing decisions are deactivated; access to all digital channels, including internet and mobile banking, is blocked.

- Freezing of Joint Accounts: Freezing procedures are applied to all joint accounts of individuals and organizations whose assets are frozen. Transactions by other rights holders in these accounts are only considered within the framework of applications made to MASAK and permissions obtained.

- Increase in Assets: Any increase in a frozen asset due to profit shares or similar reasons is subject to the provisions of the freezing. Access to these amounts cannot be granted without MASAK's permission.

Access to Frozen Assets: Disposal authority over frozen assets can only be exercised with MASAK's permission. Without permission, the disposal, transfer, or assignment of assets is strictly prohibited and not facilitated.

- Prohibition of Disclosure: It is prohibited to inform the customer or third parties about the freezing of assets or the notification made to MASAK. If a customer cannot complete a transaction, standard expressions such as "System Error" or "Awaiting Head Office Approval" are used.

- Lifting of Freezing Decisions: When a freezing decision is lifted, blocks and access restrictions on accounts are removed as soon as possible.

Details regarding the process and procedures for asset freezing are included in PRO-013 Procedure for the Prevention of Money Laundering and the Financing of Terrorism.

14. MONITORING OF CONTROLS

To ensure that the bank's activities comply with laws and internal policies, second-level controls are carried out by the Internal Control and Compliance Directorate. It is essential that this control system is designed in the most appropriate manner for the bank's business strategy and corporate structure.

15. EFFECTIVENESS

This document becomes effective on the date it is approved by the Board of Directors.

ADİL KATILIM BANKASI A.Ş.

Procedure for the Prevention of Money Laundering and Financing of Terrorism

CONTENTS

1. PURPOSE AND SCOPE

The purpose of the Anti-Money Laundering and Counter-Terrorist Financing Procedure (the "Procedure") is to ensure Adil Katılım Bankası A.Ş.'s ("the Bank") compliance with legal requirements under "Law No. 5549 on Prevention of Laundering of Proceeds of Crime" (Law No. 5549) and the "Regulation on Compliance with Obligations Regarding Prevention of Laundering of Proceeds of Crime and Financing of Terrorism" (Compliance Regulation) published in the Official Gazette No. 26999 dated September 16, 2008, concerning the prevention of money laundering and terrorist financing. This includes assessing customers, products, transactions, and services through a risk-based approach to identify strategies for mitigating potential risks, establishing internal controls, operational rules, and responsibilities within the Bank, and defining procedures and principles for raising awareness among Bank employees on these matters.
This Procedure applies to all units, employees, and activities of the Bank.

2. DEFINITIONS

In this policy, the following terms are used:
Law No. 5549: Law No. 5549 on the Prevention of Laundering of Proceeds of Crime,
Law No. 6415: Law No. 6415 on the Prevention of the Financing of Terrorism,
Law No. 7262: Law No. 7262 on the Prevention of the Financing of the Proliferation of Weapons of Mass Destruction,
Ministry: The Ministry of Treasury and Finance of the Republic of Turkey,
Presidency: The Presidency of the Financial Crimes Investigation Board,
Audit Committee: A committee established under the Law and Regulation, consisting of two members selected by the Board of Directors from among its members to assist in carrying out oversight and supervision activities,
Electronic Notification: Notifications made electronically by the Presidency within the scope of Article 9/A of Law No. 5549,
Electronic Transfer: The process of transferring a specified amount of money or securities from one financial institution to a recipient at another financial institution using electronic means on behalf of the sender,
FATF: The Financial Action Task Force, established in 1989 by G-7 countries within the OECD to develop national legal systems, harmonize legislation, strengthen the role of the financial system, and ensure continuous cooperation among member countries in preventing money laundering and the financing of terrorism,
Financial Institution: Banks, institutions authorized to issue bank cards or credit cards other than banks, authorized establishments specified in foreign exchange legislation, financing and factoring companies, capital market intermediary institutions and portfolio management companies, payment institutions and electronic money institutions, investment partnerships, insurance, reinsurance and pension companies, insurance and reinsurance brokers, financial leasing companies, institutions providing clearing and custody services within the framework of capital markets legislation, precious metals intermediary institutions, and the Postal and Telegraph Organization Joint Stock Company limited to banking activities,
Funds: Money or any movable or immovable, tangible or intangible asset, right, receivable, or any document representing them, whose value can be represented by money,
Beneficial Owner: The natural person(s) who ultimately controls or has ultimate influence over the natural persons, legal entities, or entities without legal personality on whose behalf a transaction is conducted with the obligated party,
Trust Agreement: A legal relationship whereby the owner of an asset, as the settlor, places the asset under the control of a trustee for the benefit of a specific beneficiary or group of beneficiaries, for the purpose of managing, using, or exercising other dispositions specified in the agreement.
Account: Any instrument or arrangement by which a financial institution accepts deposits of money or valuable securities, permits withdrawals or transfers, pays check values or payment orders, performs check collections, accepts traveler's checks, payment orders, or electronic money in the name of a natural person, or provides safe deposit box services.
Transaction: Any purchase, sale, credit, mortgage, tax, financing, transfer, delivery, deposit, withdrawal, remittance, or any form of saving of funds, use of safe deposit boxes or any type thereof, or any other form of saving of funds as specified in the arrangements, conducted in cash, checks, payment orders, stocks, bonds, or any other financial instrument, in any currency.

Suspension of Transactions: The suspension or prevention of a transaction from taking place.
Complex and Unusual Transactions: Transactions that, within the framework of previously acquired information about the customer and additional information obtained during the transaction request process, lead to the conclusion that there is a discrepancy between the customer's financial capacity and the transactions they conduct regarding risk profile or fund sources, or that are not consistent with the apparent economic, commercial, or legal purpose of the business.
Assets: The funds and income owned or possessed, in whole or in part, by a natural or legal person, or directly or indirectly under their control, and the benefits and value derived from them or resulting from their conversion, as well as the funds and income owned or possessed, in whole or in part, by a natural or legal person acting on their behalf or account, and the benefits and value derived from them or resulting from their conversion.
Freezing of Assets: The removal or restriction of the authority to dispose of assets to prevent their elimination, consumption, conversion, transfer, assignment, and other disposal transactions.
MASAK: Financial Crimes Investigation Board.
Legislation: The current laws, regulations, and communiqués related to the prevention of money laundering and terrorist financing, as well as MASAK decisions.
MRZ: (Machine Readable Zone) A fixed-size area on an identity document, formatted for machine reading using optical character recognition methods, containing mandatory and optional data.
Customer Risk: The risk of the Bank being exploited due to the nature of the customer's business, which involves intensive cash usage, trading of high-value goods, or facilitating international fund transfers; or due to the customer or those acting on behalf of or for the account of the customer engaging in activities aimed at money laundering or terrorist financing.
OFAC: (Office of Foreign Assets Control) The financial intelligence and enforcement agency of the U.S. Department of the Treasury.
Risk: Under the Compliance Program Regulation, the potential for financial or reputational damage that the Bank or its employees may face due to the misuse of the Bank's services for money laundering or terrorist financing, or failure to fully comply with obligations imposed by relevant laws and regulations issued pursuant to such laws.
Politically Exposed Person (PEP): Individuals who currently or previously hold prominent public positions in Turkey or abroad, such as heads of state or government, senior politicians, high-ranking officials in public institutions, judicial or military authorities, senior executives of state-owned enterprises, senior officials of political parties, as well as executives, deputy executives, board members, and similar officials in international organizations, along with their family members up to the second degree, close associates, and individuals for whom they are the ultimate beneficial owner.
SMS OTP: (Short Message Service - One Time Password) A one-time password transmitted via the short message service provided by electronic communication operators.
Criminal Proceeds: Money, any negotiable instruments and assets acquired through the commission of crimes punishable by a minimum sentence of six months or more of imprisonment, and all benefits derived therefrom.
Money Laundering: The act of subjecting funds or proceeds obtained from crimes punishable by a minimum sentence of more than six months of imprisonment to various transactions with the intent to conceal their true source or create the impression that they were obtained through legitimate means.
Ongoing Business Relationship: A business relationship established between an obligated party and a customer due to services such as account opening, provision of credit or credit cards, safe deposit boxes, financing, factoring, financial leasing, life insurance, or private pension plans, which inherently involves an element of continuity by nature.
Suspicious Transaction: Any information, suspicion, or circumstance giving rise to suspicion that the assets subject to a transaction conducted or attempted to be conducted at or through obligated parties were obtained through illegal means, used for illegal purposes, used for terrorist acts or by terrorist organizations, terrorists, or terrorist financiers, or are related or connected to them.
Suspicious Transaction Report: The notification to be made to the Presidency in case there is any information, suspicion, or circumstance giving rise to suspicion that the assets subject to transactions conducted or attempted to be conducted at or through the Bank were obtained through illegal means or used for illegal purposes.
Shell Bank: A bank that does not have a physical service office in any country, does not employ full-time staff, and is not subject to the supervision and authorization of an official authority regarding banking operations and records.

Measures Regulation: The Regulation on Measures Regarding the Prevention of Money Laundering and the Financing of Terrorism, published in the Official Gazette dated 9.1.2008 and numbered 26751.

Terrorist: A natural person residing in Turkey or abroad who directly or indirectly commits a terrorist act; acts as an accomplice in a terrorist act; organizes or directs others to carry out a terrorist act; or intentionally assists an individual or a group acting for a common purpose in carrying out a terrorist act.
Terrorism: According to Law No. 3713 on the Fight Against Terrorism, acts carried out using methods of coercion, intimidation, suppression, or threat through the use of force and violence, with the aim of altering the characteristics of the Republic, its political, legal, social, secular, or economic order; undermining the indivisible unity of the state with its territory and nation; endangering the existence of the state and the Republic; weakening, destroying, or seizing state authority; abolishing fundamental rights and freedoms; disrupting the internal and external security of the state; or disturbing public order or general health; or acts intended to intimidate a population or compel a government or international organization to perform or refrain from performing an action.
Terrorism Financing Offense: Under Article 3 of Law No. 6415 on the Prevention of the Financing of Terrorism, the provision or collection of funds to or for a terrorist or terrorist organization, knowingly and intentionally, for the purpose of being used in the commission of acts listed in the law, which are prohibited.
Terrorist Organization: A terrorist group, whether located in Turkey or abroad, that carries out the acts defined within the concept of terrorism.
Compliance Department: The department within the Bank, directly reporting to the Compliance Officer, responsible for implementing the compliance program. It is established to ensure the Bank effectively fulfills its obligations under anti-money laundering and counter-terrorism financing legislation, taking into account factors such as the Bank's size, transaction volume, number of personnel, or the level of risks it may face.
Compliance Officer: The officer appointed within the Bank in accordance with the Law on the Prevention of Money Laundering and related legislation enacted thereunder, vested with the necessary authority to ensure the Bank's compliance with obligations arising from this legislation.
Deputy Compliance Officer: Personnel appointed within the Bank, possessing the same qualifications as the Compliance Officer, who will act on behalf of the Compliance Officer during temporary absences due to leave, illness, or similar reasons.
Compliance Regulation: Regulation on Obligations Regarding the Prevention of Money Laundering and Terrorist Financing,
Compliance Program: The set of measures established within the Bank within the framework of relevant legislation aimed at preventing money laundering and terrorist financing,
Country Risk/Geographic Risk: The risk to which the Bank may be exposed due to business relationships and transactions with citizens, companies, and financial institutions of countries announced by the Ministry that lack adequate regulations on preventing money laundering and terrorist financing, do not cooperate sufficiently in combating these crimes, or are considered risky by competent international organizations,
Product/Service Risk: The risk that may be exposed within the scope of services such as non-face-to-face transactions, private banking, correspondent banking, or new products offered using emerging technologies,
Senior Management: The Bank's board of directors and top-level management,
Top-Level Management: The General Manager and Deputy General Managers, managers of units within internal systems, and managers of units other than consultancy units, regardless of their titles, who hold positions equivalent to or higher than a deputy general manager in terms of authority and responsibilities,
Near Field Communication (NFC): A short-range wireless technology used for reading and writing data, enabling electronic devices to perform secure, contactless transactions and access digital content and/or electronic devices,
Obliged Party: The parties referred to in Article 4 of the Regulation on Measures Regarding the Prevention of Money Laundering and Terrorist Financing, along with their branches, agencies, representatives, commercial agents, and similar affiliated business units.

3. DUTIES, AUTHORITIES, AND RESPONSIBILITIES

All employees, including the Bank's senior management, are responsible for performing their duties, authorities, responsibilities, and activities in compliance with the legislation and this Procedure, as well as other internal Bank regulations, within the scope of preventing money laundering and combating the financing of terrorism.

3.1 Duties and Responsibilities of the Board of Directors

The duties and responsibilities of the Board of Directors are as follows:

- Ensure the entire compliance program is established and operated in a manner that is appropriate, adequate, and effective, considering the scope and nature of the Bank's activities.
- Establish the compliance department and appoint a compliance officer and deputy compliance officer.
- Ensure the authority and responsibilities of the compliance officer and the legal and compliance department are clearly and formally defined in writing.
- Ensure Bank personnel participate in relevant training programs and approve any changes to these programs based on regulatory developments.
- Evaluate the results of risk management, monitoring, control, and internal audit activities conducted under the compliance program.
- Take necessary measures to promptly address any identified errors or deficiencies in this context.

The Board of Directors fulfills its authority in this area through one or more board members it designates. Such delegation of authority does not absolve the Board of Directors of its responsibility in this matter.

3.2 Duties, Authorities, and Responsibilities of the Compliance Officer and Assistant Compliance Officer

Under this Procedure, the Compliance Officer is responsible for:

- Preparing and submitting the Bank's internal regulations on preventing money laundering and combating the financing of terrorism to the Board of Directors for approval, in accordance with this Procedure and legal regulations, and monitoring their implementation.
- Monitoring national and international regulations on preventing money laundering and the financing of terrorism, communicating them across the Bank, and ensuring that this Procedure and its amendments are accessible to all personnel.
- Establishing risk management, monitoring, and control policies for the operations covered by this Procedure, and conducting improvement initiatives based on findings from audits and controls.
- Evaluating transactions reported to them or identified independently that may be suspicious, and ensuring that transactions deemed suspicious are reported to the Presidency within the periods specified by legislation.
- Taking necessary measures to ensure the confidentiality of reports and other matters within their scope of responsibility.
- Conducting necessary work to ensure the Bank's compliance with published regulations under relevant legislation and maintaining necessary communication and coordination with the Presidency.
- Submitting work related to the training program on preventing money laundering and the financing of terrorism to the Board of Directors for approval and monitoring the effective implementation of the approved training program.
- Regularly maintaining information and statistics on internal audit and training activities and submitting them to the Presidency within the periods specified by legislation.
- Preparing reports to be submitted to MASAK and other official institutions as required by legislation, or ensuring their preparation by relevant units.
- Acting in good faith, reasonably, honestly, impartially, and with independent judgment while performing their duties and responsibilities.

The details of the duties and responsibilities of the Compliance Officer and Assistant Compliance Officer are outlined in "YON-015 Internal Control and Compliance Presidency Directive."

3.3 Duties, Authorities, and Responsibilities of the Compliance Department

Under this Procedure, the Compliance Department is tasked and responsible for:

- Monitoring legislative applications within the scope of this Procedure,
- Responding to questions from Bank employees regarding legislation,
- Notifying relevant Bank departments to assess risks that may arise in connection with legislative changes,
- Tracking the compliance of all activities, new services, and products carried out or planned by the Bank with relevant legislation,
- Announcing notifications and legislative changes from official institutions concerning legislation within the scope of this Procedure across the Bank.

The details of the Compliance Department’s duties and responsibilities are outlined in “Directive YON-015 on Internal Control and Compliance Presidency.”

3.4 Duties, Authorities, and Responsibilities of the Inspection Board Presidency

Within the scope of this Procedure, the Inspection Board Presidency is tasked and responsible for:

- Annually reviewing and reporting on the adequacy and effectiveness of the Bank's internal regulations, risk management, monitoring, control, and training activities related to preventing money laundering and combating the financing of terrorism, using a risk-based approach.
- Considering high-risk customers, services, transactions, and units to be audited, as well as deficiencies identified in monitoring and control activities, when preparing the annual audit plan, in accordance with relevant legislation.
- Providing data related to internal audit activities conducted under the compliance program to the Compliance Officer.

3.5 Duties, Authorities, and Responsibilities of Bank Employees

Under this Procedure, bank employees are responsible for:

- Participating in training activities organized for the prevention of money laundering and terrorist financing,
- Learning, understanding, and complying with relevant laws, related legal regulations, and internal bank policies,
- Reporting any suspicious situations related to money laundering or terrorist financing encountered during banking operations to the Compliance Officer,
- Acting in accordance with the principles of customer identification and verification, as outlined in this Procedure and internal bank regulations, in all banking transactions, especially customer transactions.

4. GENERAL APPLICATION PROCEDURES AND PRINCIPLES

4.1 Risk-Based Approach and Risk Management Activities

Within the framework of this Procedure, the purpose and scope of risk management activities are to ensure the identification, rating, classification, monitoring, and assessment of risks to which the Bank may be exposed, as well as the implementation of necessary measures to mitigate these risks.

The Bank's fundamental principle is to implement a proactive risk-based approach regarding the prevention of money laundering and terrorist financing. Establishing a risk-based approach means defining a risk management process to combat money laundering and terrorist financing. This process involves identifying and assessing risks, and developing strategies to manage and mitigate them.

Through the established compliance risk methodology, the Bank aims to create an indicator of the overall risk level within the framework of risk factors related to money laundering and terrorist financing for customers with whom ongoing business relationships are maintained. Thus, while standard customer acceptance procedures are applied to lower-risk customers, the necessary due diligence can be exercised in the acceptance processes for higher-risk customers.

Through the compliance risk methodology, a risk-based approach is followed in customer acceptance; for high-risk customers, enhanced customer acceptance practices and additional approval and control processes are implemented.

The Bank classifies the risks it may be exposed to in relation to money laundering and terrorist financing due to its customers, activities, products, and transactions into the following categories:

- Country Risk,
- Service Risk,
- Customer Risk.

Within the framework of relevant legislation, when conducting risk assessments, the Bank's customers, products/services, and transactions are rated as:

- High Risk
- Medium Risk
- Low Risk.

Based on the results of risk assessments, the Bank may decide to accept, mitigate, or avoid risks according to their determined level.

To protect against risks related to the prevention of money laundering and terrorist financing, and to continuously monitor, control, and report that activities are conducted in accordance with legislation and internal regulations, the Bank establishes monitoring, control, and reporting activities, taking into account the Bank's size, transaction volume, and the nature of the transactions carried out.

The Bank's activities related to risk management under this procedure are structured as follows:

- Developing risk identification, rating, classification, and assessment methods based on customer risk, service risk, and country risk,
- Rating and classifying services, transactions, and customers according to risks,

- Ensuring the monitoring and control of risky customers, transactions, or services; taking necessary measures to mitigate risks; reporting in a manner that alerts relevant departments; developing appropriate operational and control rules for transactions to be carried out with senior management approval and, when necessary, audited,
- Following national legislation and recommendations, principles, standards, and guidelines introduced by international organizations on matters within the scope of risk, and conducting necessary development work,
- Regularly reporting the results of risk monitoring and assessments to the board of directors.

4.1.1 Identification and Classification of Risks

The Bank identifies risks related to money laundering and terrorist financing that may arise from its customers, activities, products, and transactions, and classifies them according to the following risk categories within the regulatory framework:

- Country Risk: Risks that may arise from business relationships and transactions with citizens, companies, and financial institutions of countries announced by the Ministry of Treasury and Finance, which lack sufficient regulations to prevent money laundering and terrorist financing, do not cooperate adequately in combating these crimes, or are considered risky by authorized international organizations.
- Service Risk: Risks that may arise from non-face-to-face transactions at the Bank or new products offered using emerging technologies.
- Customer Risk: Risks arising from the customer's business sector, which may involve intensive cash usage, trade in high-value goods, or facilitate international fund transfers; or risks of misuse due to the customer or those acting on behalf of or for the customer engaging in money laundering or terrorist financing activities.

4.1.2 Risk Rating

The Bank conducts risk assessments for each customer. In performing this assessment, at a minimum, the following risk factors are considered:

- Customer profile (information such as occupation/sector, business history/commercial history/sector experience, relationship duration, nationality)
- Areas of activity,
- Products and services,
- Beneficial owner information,
- Country/region of operation,
- Whether the customer is a Politically Exposed Person (PEP).

For the aspects mentioned above—specifically the country of operation, areas of activity, and products—pre-prepared and continuously updated lists of high-risk countries/regions and products are used. Bank customers, products/services, and transactions are categorized as:

- High Risk
- Medium Risk
- Low Risk

Based on current information and indicators such as occupation, business history, activities, financial status, account and transaction details, and the country of residence/operation, customers' risk profiles for money laundering and terrorist financing are determined as high, medium, or low. Monitoring and control activities are then applied according to these risk profiles.

All new high-risk customer acceptances require approval from the Head of Internal Control and Compliance. If deemed necessary by the Head of Internal Control and Compliance, high-risk customer acceptance may be submitted for approval to the General Manager or, upon the General Manager's recommendation, to the Board of Directors. The acceptance of customers rated as high risk involves a more comprehensive onboarding process and a different approval mechanism compared to other risk categories. Enhanced measures, including continuous monitoring and annual updates of customer information, are applied to high-risk customers.

4.1.3 Risk Assessment

Risk assessment studies aim to determine the Bank's risk profile within the framework of existing operations, customers, products, and transaction structures, in line with applicable regulations and sectoral developments. Based on these assessments, the allocation of appropriate resources for identified risks is ensured. The minimum considerations to be taken into account in risk assessment studies are listed below:

- Changes in risks arising from service channels used and technological capabilities employed in the delivery of products and services,

- Changes in the Bank's target market, products, and customer segments,
- Variations in the number of high-risk customers according to the risk rating model,
- Findings from the Bank's Inspection Board Presidency and Internal Control Presidency, independent audits, and official regulatory audit reports regarding obligations related to money laundering and terrorist financing,
- Increases in the Bank's transaction volume, either overall or specific to certain products,
- The Bank's country risk status in relation to its existing customer portfolio,
- Changes in legal regulations and best practices,
- Changes in the Bank's operational structure.

Customer risk assessment also determines how frequently accepted customers will undergo re-identification processes. To mitigate risks associated with customers identified as high-risk following risk assessment, the Bank applies one or more of the following enhanced measures, proportionate to the identified risk:

- Requiring the initial financial transaction for establishing a ongoing business relationship to be conducted through another financial institution where customer identification principles have been applied,
- Obtaining as much information as possible about the source of assets involved in transactions and funds belonging to the customer,
- Gathering additional information about the nature of the business relationship,
- Maintaining the business relationship under close supervision by increasing the number and frequency of controls and identifying transaction types requiring additional scrutiny,
- Making the establishment of a business relationship, continuation of an existing relationship, or execution of a transaction subject to approval by a higher-level authority,
- Acquiring additional information about the customer and updating identification details of the customer and the ultimate beneficial owner more frequently,
- Gathering additional information about the nature of the business relationship.

4.1.4 Risk Management

Within the scope of preventing money laundering and combating the financing of terrorism, the Bank ensures that necessary measures are taken to reduce existing risks and prevent potential risks. Based on risk assessments, the Bank may decide to accept, mitigate, or avoid risks according to their severity. As a principle, the Bank ensures that all employees approach money laundering and terrorism financing risks with high sensitivity and take reasonable measures to mitigate these risks.

For groups identified as high-risk based on risk assessments, the Bank applies one or more of the following measures, proportionate to the identified risk, to reduce the assumed risk:

- Obtain additional information about the customer and update the identity details of the customer and the beneficial owner more frequently,
- Gather additional information about the nature of the business relationship,
- Obtain as much information as possible about the source of the assets involved in the transaction and the customer’s funds,
- Inquire about the purpose of the transaction,
- Require approval from a senior officer for establishing a business relationship, continuing an existing relationship, or executing a transaction,
- Increase the number and frequency of applied controls and identify transaction types requiring additional controls to maintain the business relationship under close supervision,
- Mandate that the initial financial transaction for establishing a ongoing business relationship be conducted through another financial institution where customer identification principles are applied.

The bank takes necessary measures against situations that may lead to non-compliance with its obligations and does not establish business relationships, terminates existing business relationships, or refuses to conduct transactions in cases where the risk of money laundering, terrorist financing, or sanctions violations is high or unmanageable. Within this framework, the bank acts in accordance with the following principles to limit risk:

- It does not open accounts in anonymous or fictitious names.
- It does not establish business relationships with individuals operating in areas that could be potential sources of money laundering, such as casinos, online lotteries, lottery draws, or betting transactions.
- It does not establish business relationships with individuals listed on sanctions lists.
- It does not conduct transactions related to countries subject to sanctions or that violate sanctions.
- It does not establish relationships with shell banks or banks that use shell banks for their accounts.

- It does not establish business relationships with entities whose ultimate beneficial owner cannot be identified or verified.
- It does not establish business relationships with those engaged in activities that could harm the bank's reputation, such as illegal arms and ammunition trade, drugs, narcotics, human trafficking, adult entertainment, or gambling.
- It checks the customer, the ultimate beneficial owner of the account, and persons related to the account (partners/shareholders, agents, authorized persons, etc.) against sanctions lists.

4.1.5 Monitoring and Control Activities

The Bank conducts monitoring, control, and reporting activities to protect against risks related to preventing money laundering and terrorist financing, and to continuously monitor, control, and report whether its operations are conducted in accordance with legislation and internal regulations, taking into account the Bank's size, business volume, and the nature of transactions carried out.

Personnel responsible for monitoring and control activities within the Bank are ensured access to internal information sources. Results of risk monitoring and assessments are regularly reported to the Board of Directors. The monitoring and control activities conducted within the Bank include, at a minimum, the following:

- Monitoring and control of high-risk customers and transactions,
- Monitoring and control of transactions conducted with high-risk countries,
- Monitoring and control of complex and unusual transactions,
- Sampling-based control to determine whether transactions exceeding the amount set by the Bank according to its risk policy are consistent with the customer profile,
- Monitoring and control of linked transactions exceeding the threshold requiring identity verification,
- Control of information and documents that must be retained electronically or in writing regarding customers, as well as mandatory information in electronic transfer messages, ensuring deficiencies are addressed and updates are made,
- Continuous monitoring during the business relationship to determine whether the customer's transactions are consistent with information about their business, risk profile, and fund sources,
- Control of transactions conducted using systems that enable non-face-to-face transactions,
- Risk-focused control of services that may become vulnerable to abuse due to newly offered products and technological developments.

Within this framework, monitoring and control activities are carried out by the Compliance Department. In the context of centralized monitoring and control activities conducted by the Compliance Department, technological resources are also utilized for monitoring customers and transactions, as well as detecting suspicious transactions.

The supervision of the implementation of the compliance program in accordance with current legislation and the Bank's internal regulations is carried out by the Inspection Board. Deficiencies identified as a result of these controls related to ensuring compliance with obligations are reported to the Compliance Officer, the Audit Committee, and the Board of Directors.

4.2 Compliance Officer and Compliance Unit

The Compliance Unit within the bank is the "Compliance Department," positioned under the Internal Control and Compliance Presidency within the organizational chart. It operates under the Board of Directors. The Compliance Officer and the Assistant Compliance Officer, who meets the required conditions and qualifications for the compliance officer role and whose appointment follows the same procedures and duration as that of the Compliance Officer, are designated to have sufficient seniority, knowledge, and authority to carry out their responsibilities independently. The bank submits these appointments to the Presidency within ten days at the latest from the appointment date. Matters related to the appointment, dismissal, delegation of authority, and acting roles of the Compliance Officer and Assistant Compliance Officer are conducted in accordance with the conditions specified in the Compliance Regulation and the procedures and timelines outlined in "Directive YON-015 on Internal Control and Compliance Presidency."

4.3 General Procedures and Principles Regarding Customer Recognition and Identification

4.3.1 Know Your Customer Principle

Customer recognition is achieved by the Bank obtaining sufficient information about its customers and their activities. The Know Your Customer Principle also aims to raise awareness of complex and unusual transactions or activities that are disproportionate to the customer's known business.

The Compliance Officer is authorized to demand the rejection of a natural or legal person as a customer or the termination of an ongoing business relationship with an existing customer in any case, due to the risks related to money laundering and terrorist financing, within the framework of the Bank's customer acceptance policy.

Within the scope of the Know Your Customer Principle, the following measures are taken in establishing ongoing business relationships and executing requested transactions, in accordance with current legislation and the Bank's internal regulations:
- Obtaining sufficient information about the purpose and nature of the requested transaction,
- Conducting identity verification,
- Verifying the identity of those acting on behalf of others,
- Checking the authenticity of documents used for verification,
- Conducting identity verification in subsequent transactions,
- Determining whether actions are taken on behalf of others and verifying the identity of those acting on behalf of others,
- Recognizing the actual beneficial owner,
- Taking necessary measures for customers, activities, and transactions requiring special attention,
- Monitoring the customer's status and transactions during the business relationship,
- Implementing measures against technological risks,
- Reliance on third parties,
- Transaction rejection and termination of the business relationship,
- Correspondent relationships,
- Electronic transfers,
- Relationships with high-risk countries,
- Application of simplified measures, and
- Application of enhanced measures.

4.3.2 Principles Regarding Customer Acceptance and Recognition

When establishing a new business relationship, the bank obtains information for customer identification. Additionally, it applies enhanced measures for customers classified as high-risk based on risk assessment.

4.3.2.1 Standard Customer Identification Measures

Customer identification minimally includes the following:
- Complete and accurate verification of the customer’s identity,
- Complete and accurate verification of identity information for persons related to the customer,
- Identification of the beneficial owner and confirmation of identity information through reliable documents and data,
- Obtaining information about the purpose and nature of the business relationship,
- Gathering information within the scope of customer profiling (e.g., the customer’s profession/sector of activity, main source of income, source of wealth, expected transaction volume),
- Obtaining a declaration from the customer confirming that they are the beneficial owner of the account,
- Conducting checks on sanction lists for the customer and related persons,
- Acquiring additional information deemed necessary, including the source of funds,
- Continuous monitoring of the account,
- Updating customer identification information based on the customer’s risk profile.

4.3.2.2 Simplified Measures

Provided the customer's risk score is low, the Bank may apply simplified measures for customer identification in the following cases:
- Transactions between financial institutions,
- Transactions where the customers of non-financial obligated parties are banks,
- Transactions where the customer is a public administration or a professional organization with public institution status,
- Transactions where the customer is an international organization or an embassy or consulate located in Turkey,
- Transactions establishing a business relationship through bulk customer acceptance under a Salary Payment Agreement,
- Transactions related to salary payments for units of international organizations resident in Turkey, or for embassy or consulate staff,
- Transactions where the customer is a company whose shares are listed on the stock exchange, and
- Transactions related to prepaid cards.

Simplified measures must be consistent with the risk factors in the Bank's internal regulations. These measures are not limited to the items above and include the following:
- The ability to verify the identity of the customer and the beneficial owner after establishing the business relationship,
- The ability to update customer data at intervals longer than the standard information update frequency,
- The application of simplified and periodic monitoring and verification,
- Not obtaining detailed information to understand the purpose and nature of the business relationship, or not applying specific measures, if the existing business relationship and transactions provide sufficient information.

The Bank does not apply simplified measures in cases where there is a risk of money laundering or terrorist financing due to the transaction, and considers that the transaction may be suspicious.

4.3.2.3 Enhanced Measures

The bank applies all or part of the following measures, proportionate to the identified risk, in transactions falling under "Transactions Requiring Special Attention," "Measures Against Technological Risks," and "Relationships with High-Risk Countries," as well as in high-risk situations identified within the framework of a risk-based approach:
- Obtains additional information about the customer and updates the identification details of the customer and the actual beneficiary more frequently.
- Obtains additional information about the nature of the business relationship.
- Gathers as much information as possible about the source of the assets involved in the transaction and the customer's funds.
- Obtains information about the purpose of the transaction.
- Makes the establishment of a business relationship, the continuation of an existing business relationship, or the execution of a transaction subject to approval by a senior officer.
- Increases the number and frequency of controls applied; keeps the business relationship under close supervision by identifying transaction types requiring additional controls.
- Requires that the initial financial transaction for establishing a ongoing business relationship be conducted through another financial institution where customer identification principles have been applied.

4.3.3 Identity Verification

The primary focus in combating money laundering and terrorist financing is the customer, who is the source of suspicious transactions.

Therefore, verifying customer identity is crucial in the fight against proceeds from these illegal activities. According to the "Principles Regarding Customer Identification" under the third section of the Measures Regulation, the obligation for customer identification begins with the identity verification step. Identity verification is conducted in the following cases, as stipulated by relevant legislation:
- When establishing a ongoing business relationship, regardless of the amount,
- When the transaction amount or the total amount of multiple related transactions meets or exceeds the threshold specified in the legislation,
- In electronic transfers, when the transaction amount or the total amount of multiple related transactions meets or exceeds the threshold specified in the legislation,
- In cases requiring suspicious transaction reporting, regardless of the amount,
- When there are doubts about the adequacy or accuracy of previously obtained customer identity information, regardless of the amount.

A ongoing business relationship can also be established using remote identity verification methods, to the extent permitted by legislation, or through identity verification via a notarized power of attorney.

The bank takes necessary measures to identify its customers and those acting on their behalf or for their accounts by obtaining identity-related information and confirming its accuracy, as well as to uncover the actual beneficial owner of the transaction.

Identity verification is completed before establishing a business relationship or conducting a transaction. The obligation for customer identification is not limited to identity verification alone. In cases where the bank cannot verify identity, it shall refrain from establishing a business relationship or fulfill requested transactions. For ongoing business relationships, additional information is obtained regarding the purpose and nature of the relationship.

As a general rule, no business relationship is established, and no transactions requested by the parties are carried out until the potential customer's identity is properly verified or sufficient information about the purpose of the business relationship is obtained. Similarly, if identity verification and confirmation cannot be performed due to doubts about the adequacy or accuracy of previously obtained customer identity information, the business relationship is terminated.

The procedures and principles for customer identity verification are outlined in the Customer Acquisition Procedure, the Electronic Banking Channels Authentication and Transaction Security Procedure, and the Remote Customer Acquisition Security Procedure, all prepared based on MASAK legislation.

4.3.3.1 Identity Verification Methods

The Bank conducts identity verification processes in accordance with relevant legislation and remote identity verification methods. However, the Bank may use in-person identity verification methods through services it obtains in cases where current technological or operational capabilities and integrations are insufficient to meet regulatory requirements via remote identity verification, or when procedures and principles for the relevant individual or customer type are not yet established in the legislation.

4.3.3.2 Identification of Persons Acting on Behalf of Others

When transactions are requested by persons authorized by representatives of legal entities or unincorporated associations, by other natural persons on behalf of natural person clients, or by legal representatives on behalf of minors or persons under guardianship, the identification of these persons shall be carried out in accordance with the Measures Regulation.

Upon presentation of the original documents or notarized copies serving as the basis for verification, to be submitted when requested by authorities, a legible photocopy or electronic image is taken, or identity-related information is recorded.

4.3.3.3 Verification of the Authenticity of Documents Serving as the Basis for Verification

If there is doubt about the authenticity of documents used to verify information obtained within the scope of identification, the authenticity of the document shall be confirmed by contacting the issuer of the document or other competent authorities to the extent possible.

4.3.3.4 Identification in Subsequent Transactions

Within the scope of an ongoing business relationship, necessary measures are taken to verify the customer's identity in subsequent transactions requiring identification and to keep the information within the scope of identification up to date.

4.3.3.5 Identification of Persons Acting on Account of Others

The Bank takes necessary measures to determine whether a person is acting on account of another. Persons conducting transactions requiring identification must legally notify the Bank if they are acting on account of another. However, in all cases when establishing an ongoing business relationship, a declaration must be obtained from customers regarding whether they are acting on account of another.

If a person declares that they are acting on account of another or if this is determined by the Bank, the identity of the person on whose account the transaction is conducted must be properly identified, along with the person conducting the transaction. If a person declares that they are not acting on account of another but there is suspicion that they are acting in their own name on account of another, measures are applied to identify the actual beneficial owner.

4.3.3.6 Identification of the Ultimate Beneficial Owner

Measures are taken to identify the ultimate beneficial owner of a transaction. The ultimate beneficial owner refers to the natural person(s) who ultimately own or control the natural persons conducting the transaction with the Bank, or on whose behalf the transaction is carried out, whether they are natural persons, legal entities, or unincorporated organizations.

The Bank is obligated to take necessary measures to determine whether someone is acting on behalf of another party and to identify the ultimate beneficial owner of the transaction. Based on the definition, the ultimate beneficial owner must be a natural person. For legal entities, the determination of the ultimate beneficial owner focuses on ownership (shareholding relationships), senior management representation, and ultimate control.

In some clients, the ultimate beneficial owner is a natural person holding a majority stake in the company, while in other companies, holding a majority stake may not necessarily confer ultimate control or influence over the company. Therefore, relevant Bank officials must consider each client individually when identifying the ultimate beneficial owner of legal entities registered in the trade registry, adhering to the following regulatory rules, and focus on uncovering the individuals who truly control or exert influence over the company.

In this context, the following points must also be observed in accordance with the relevant regulations:

- For establishing ongoing business relationships with legal entities registered in the trade registry, the identity of natural person shareholders holding more than 25% of the shares is determined to identify the ultimate beneficial owner.
- If there is suspicion that a natural person shareholder holding more than 25% of the shares is not the ultimate beneficial owner, or if no such natural person shareholder exists, measures are taken to identify the natural person(s) who ultimately control the legal entity. The identified natural person(s) are considered the ultimate beneficial owner.
- For ongoing business relationships, measures are taken to identify the natural person(s) who ultimately control other legal entities or unincorporated organizations. The identity information of the identified ultimate beneficial owner is obtained, and necessary measures are applied to verify this information. In this context, notarized signature circulars containing identity information may be used. Additionally, for establishing ongoing business relationships with legal entities registered in the trade registry, the identity of legal entity shareholders holding more than 25% of the shares is determined.
- If the ultimate beneficial owner cannot be identified, no business relationship is established, existing business relationships are restricted or terminated, the requested transaction is refused, and it is evaluated whether a suspicious transaction report needs to be filed.

In addition to the above, for the verification of identity information required for the identification of legal entity shareholders residing abroad, confirmation is carried out through officially certified documents.

4.3.3.7 Reliance on Third Parties

The bank may establish a business relationship or conduct a transaction by relying on measures taken by another financial institution regarding the customer for the identification of the customer, the person acting on behalf of the customer, and the ultimate beneficial owner, as well as for obtaining information about the purpose of the business relationship or transaction. In such cases, under the Law and relevant regulations, the ultimate responsibility shall belong to the financial institution that conducts the transaction by relying on a third party. Reliance on a third party is possible provided that:

- The third party has taken the necessary measures to fulfill the requirements for identification, record-keeping, and customer due diligence, and if it is based abroad, it is also subject to regulations and supervision in line with international standards for the prevention of money laundering and terrorist financing;
- All necessary information within the scope of customer due diligence can be promptly obtained from the third party upon request;
- Certified copies of identification documents and other documents within the scope of customer due diligence can be promptly obtained from the third party upon request;
- The third party is subject to regulations, supervised, and implements adequate measures to comply with the requirements for identification, record-keeping, and customer due diligence;
- Sufficient assurance is provided regarding confidentiality in the exchange of information with the third party.

If a business relationship is established by relying on a third party, the customer's identification information is promptly obtained from the third party. Transactions conducted by the bank on behalf of customers with other banks, as well as the bank's relationships with agents and similar units, or persons providing services that are extensions or complements of its main service units, are not within the scope of the reliance on third parties principle. The reliance on third parties principle does not apply if the third party is based in high-risk countries.

4.3.4 Transactions Requiring Special Attention

The bank pays special attention to transactions that are complex or unusually large in size, as well as transactions and activities that lack an apparent legitimate legal or economic purpose, or are suspected or attempted to be linked to money laundering or terrorist financing. It takes necessary measures to obtain sufficient information about the purpose of the requested transaction and retains the information, documents, and records obtained within this scope to present to authorities upon request.

4.3.5 Monitoring Customer Status and Transactions

The bank takes necessary measures to monitor, on a risk-based approach, whether transactions conducted by customers are consistent with information regarding their profession, commercial activities, business history, financial status, risk profile, and sources of funds, and to keep this information up to date. For this purpose, it establishes an appropriate risk management system. It defines the procedures and principles for suspicious transactions within the scope of customer and transaction categories that involve higher-risk activities or operate under unusual conditions. Additionally, the accuracy of contact information, such as telephone and fax numbers and email addresses obtained

for customer identification, is confirmed as needed within the framework of a risk-based approach by contacting the relevant parties using these means.

4.3.6 Measures Against Technological Risks

The Bank pays special attention to the risks that the use of new and emerging technologies, including new distribution channels, as well as existing and new products and business practices, may be exploited for money laundering and terrorist financing, and takes appropriate measures to prevent such exploitation.

In this context, the Bank exercises particular caution over transactions conducted through electronic banking channels, such as deposits, withdrawals, and electronic transfers. It closely monitors transactions that are inconsistent with or unrelated to the customer's financial profile and activities, and implements suitable and effective measures, including setting limits on transaction amounts and frequencies.

4.3.7 Customer Acceptance/Transaction Rejection and Termination of Business Relationship

If customer identification cannot be performed or sufficient information about the purpose of the business relationship cannot be obtained, no business relationship is established with the customer. On the other hand, if there are doubts about the accuracy of a previously conducted identification and the customer refuses to provide new identification despite being requested, the Bank terminates the business relationship within legal limits, in accordance with the Bank's internal regulations and MASAK regulations. In cases where the business relationship cannot be terminated due to reasons such as liens on credit relationships, new transaction requests from the customer are not accepted. If necessary, the Compliance Officer is consulted on the matter. Due to risks related to money laundering and terrorist financing, if a request to establish a business relationship with a potential customer is rejected, the Compliance Officer is informed.

The Bank does not establish a new business relationship, restricts or terminates an existing business relationship, and refuses to carry out the requested transaction in the following cases, and notifies the Compliance Officer of this situation:

- Inability to conduct the customer due diligence process for the customer,
- Failure to obtain information and documents for identification and customer due diligence during the customer acceptance phase or as part of information updates during the continuation of the business relationship,
- Inability to identify or verify the customer or the ultimate beneficial owner,
- Unwillingness of the customer to provide requested information regarding business and transactions,
- Non-compliance by the customer with the terms and conditions in agreements signed with the Bank,
- Unmanageable or unacceptable money laundering risks associated with the customer.

The Bank separately evaluates the above-mentioned situations in terms of suspicious transactions.

4.3.8 Correspondent Banking Relationship

In the process of establishing correspondent banking relationships abroad, the Bank implements the following measures. Before establishing new correspondent relationships, approval is obtained from the Treasury and the Deputy General Managers responsible for financial affairs.

- Obtain reliable information from publicly available sources regarding whether the counterpart financial institution has been investigated for money laundering or terrorist financing, whether it has received any penalties or warnings, the nature and subject of its business, its reputation, and the adequacy of supervision over it.
- Evaluate the counterpart financial institution's anti-money laundering and counter-terrorist financing system to ensure it is appropriate and effective.
- Clearly define the responsibilities of the Bank and the correspondent institution through a contract, ensuring they meet the obligations outlined in the General Procedures and Principles for Customer Due Diligence and Identification section of this Regulation.
- In cases where the correspondent relationship involves the use of pass-through correspondent accounts, ensure that the counterpart financial institution has taken adequate measures in accordance with the procedures and principles under the General Procedures and Principles for Customer Due Diligence and Identification section of this Regulation and can provide the identity information of relevant customers upon request.

The Bank does not enter into correspondent relationships with shell banks or financial institutions that it cannot confirm do not allow their accounts to be used by shell banks.

4.3.9 Electronic Transfers

- In domestic and international electronic transfer messages requiring identification, the sender must include:

1. Full name, or the registered title of a legal entity in the trade registry, or the complete name of other legal entities and organizations without legal personality,

2. Account number, or in the absence of an account number, a reference number related to the transaction,
3. At least one piece of information to identify the sender, such as address, place and date of birth, customer number, citizenship number, passport number, or tax identification number.

The accuracy of this information is additionally confirmed. For the recipient in electronic transfer messages, the information specified in items 1 and 2 above is also included; confirmation of this information is not mandatory.

- In domestic and international electronic transfer messages not requiring identification, the information specified in items 1 and 2 above is included for both the sender and recipient. Confirmation of this information is not mandatory.

-Transfers conducted between banks in their own names and accounts, as well as transfers made using credit and bank cards, provided that card numbers are used in the messages, are outside the scope specified in the above paragraph.

- A bank receiving an electronic transfer message that does not contain the information specified in items 1, 2, and 3 returns the transfer or ensures that the sending financial institution completes the missing information.

- If sent messages consistently contain incomplete information and this information is not completed upon request, the receiving bank may consider rejecting electronic transfers from the sending financial institution, limiting transactions with that institution, or terminating the business relationship.

- In the message chain from the financial institution issuing the transfer order to the financial institution executing the payment, all intermediary financial institutions include the required sender information in electronic transfer messages and take special care to ensure this information is transmitted at every stage of the transfer.

4.3.10 Relations with High-Risk Countries

The Bank exercises special caution in business relationships and transactions with individuals and legal entities, as well as unincorporated organizations and citizens residing in high-risk countries. It makes every effort to ascertain and record the purpose and nature of transactions that lack an apparent reasonable legal or economic basis. High-risk countries are defined as those that lack adequate regulations for preventing money laundering and terrorist financing, do not cooperate in combating these crimes, or are designated as risky by competent international organizations.

High-risk countries are determined by the Compliance Officer. The Compliance Officer may add or remove countries from the list of high-risk countries or adjust their risk levels as necessary, taking into account evaluations by international organizations active in combating money laundering and terrorist financing. This includes raising the risk level of a low-risk country or reducing it, provided it does not fall below the threshold established in the Bank's written policies.

Customers residing or operating in high-risk countries designated by the Compliance Officer are directly classified as high-risk. Individuals residing abroad without reasonable and customary explanations for conducting banking transactions or opening accounts in different countries are not accepted as customers. Country risk is assessed based on the customer's place of residence and nationality for individuals, and the country of operation and residency status for legal entities. During customer onboarding, this information is collected from the customer and recorded in relevant systems.

The following countries and regions, as well as customers residing or associated with them, are closely monitored under the high-risk category from a country risk perspective:

- Countries listed on the FATF black and gray lists,
- Countries included in the high-risk country list announced by the Ministry,
- Countries subject to sanctions by the United Nations Security Council, the European Union, or OFAC due to policies and practices related to money laundering or terrorist financing,
- Countries considered high-risk under international regulations for preventing money laundering and terrorist financing.

4.3.11 High-Risk Customers

Within the framework of the customer identification principle, it is essential to obtain complete and accurate information regarding the natural person customer's occupation, the legal entity customer's field of activity, and fundamentally, the source of their income.

Beyond planning marketing activities related to the customer, significant emphasis is placed on accurately monitoring and evaluating customer transactions.

When assessing which activity area a natural or legal person with multiple activities operates in, the activity area that stands out in terms of time spent and share of generated income is taken into account.

Priority is given to evaluating activity areas and professions that are more risky in terms of money laundering and terrorist financing.

Additional due diligence is exercised before establishing business relationships with customers from these sectors and professional groups; customer identification and introductory documents, as well as sector information, are recorded carefully and comprehensively.
Establishing business relationships with high-risk customers is subject to approval by a higher-level official, and these accounts are additionally monitored with care.
Within this scope, customers considered High Risk are listed below:
- Non-Profit Civil Society Organizations,
- Politically Exposed Persons or Companies Owned by Them,
- Foreign Correspondent Banks, Shell Banks, Offshore Banks, and Financial Institutions,
- Currency Exchange Offices,
- Customers Operating in Sanctioned or High-Risk Regions,
- Foreign-Resident Customers,
- Embassies/Consulates,
- Jewelers, Precious Stone and Metal Traders,
- Weapons and Military Ammunition Manufacturers and Traders,
- Real Estate Agents and Car Dealers,
- Legal Entities with Complex Partnership or Control Structures Involving Multiple Countries/Regions,
- Antique and Art Galleries,
- Natural/Legal Persons Operating in Countries Subject to Financial Sanctions,
- Casino, Gambling Hall, and Lottery Operators,
- Individuals Without a Specific Job/Activity,
- Automotive Spare Parts Manufacturers and Traders,
- Businesses Operating in Cash-Intensive Industries,
- Travel Agencies, Passenger and Cargo Transporters.

4.3.12 Controls Regarding Electronic Money and Payment Service Institutions

Within the scope of "enhanced measures," at least the following controls are applied to electronic money and payment service institutions:
- Customer Acquisition Process: In addition to standard identity verification, the following documents are required:
    - Partnership Structure and Ultimate Beneficial Owner Declaration: The organization must provide official documents verifying its partnership structure, along with a declaration regarding the ultimate beneficial owner. The declaration is cross-checked by the Bank's Compliance Unit using information obtained from open sources. Accounts cannot be opened or business relationships established based on declarations deemed suspicious.
    - Compliance Program Declaration: A written declaration is required regarding whether the organization has prepared a Compliance Program, appointed an internal Compliance Officer, and uses risk-based monitoring software.
    - Representative List: A list of representatives (agent network) authorized to conduct transactions on behalf of the organization, along with information on the oversight mechanisms applied by the organization to these representatives, is requested.
    - Segregation of Funds: It must be confirmed that the organization strictly segregates "client accounts" (where customer funds are held) from "operational accounts" (used for administrative expenses). Documentation must also be provided to clarify under which category the account opened with the Bank falls.
- Transaction Monitoring and Scenario Analysis: As part of transaction monitoring activities, the following scenarios are added to the monitoring system for electronic money and payment service providers:
    - Excessive Volume Increase: A sudden increase of 50% or more in the institution's declared monthly expected turnover.
    - Split Transactions: Detection of consecutive, small-amount transactions conducted by the same or related sub-customers to avoid reporting thresholds.
    - Reverse Fund Flow: Continuous transfer of funds to the same individuals or to high-risk countries/regions.
    - Monitoring Outside Business Hours: Tracking unusual concentration and activity in the institution's accounts during weekends or nighttime hours.
- Contract Terms:

- Information and Document Sharing Obligation: A provision is added to the contract to be made with the Institution, stating that any information and document requests that may be requested by the Bank within the scope of compliance activities during or after the customer acquisition process will be met by the Institution without raising any objections.
- Suspicious Transaction Clause: A provision is added to the contract to be made with the Institution, stating: "The Institution undertakes to share, upon request by the Bank, the identity information of the ultimate sender and recipient (sub-customer) of transactions deemed suspicious, along with the invoice/contract and other relevant documents forming the basis of the transaction, with the Bank within a maximum of 2 (two) business days."

- Termination of Relationship: In the following cases, upon the Compliance Officer's suitability opinion and the approval of the Board of Directors, procedures are initiated to terminate or restrict the business relationship with the Institution, or to close all or part of the accounts held at the Bank.

- License Revocation: The cancellation or suspension of the Institution's license by the Central Bank of the Republic of Turkey (CBRT).
- Non-compliance with Obligations: Detection, as a result of Financial Crimes Investigation Board (MASAK) examinations, that the institution systematically facilitates "money laundering" activities.
- Failure to Fulfill Information and Documentation Obligations: Failure to provide the information and documents requested by the Bank within a reasonable time and in a consistent manner.

4.3.13 Persons and Institutions Not Acceptable as Customers

Our bank, as a fundamental principle, does not provide banking services to individuals and entities whose "Know Your Customer" (KYC) and identification processes are incomplete. Business relationships cannot be established with those who refuse to provide the information and documents required by legislation. Information pertaining to individuals and institutions whose business relationship establishment or transaction request is denied is retained for the legally mandated storage periods.

Our bank does not accept the following types of persons and institutions as customers:

- Individuals whose true identity and address cannot be verified or who avoid declaring a physical address,
- Persons who refuse to provide information and documents required by legal regulations or avoid signing necessary documents,
- Individuals and organizations listed in the "Money Laundering and Terrorism Financing" sanction lists (prohibited lists) published by official authorities,
- Persons from whom sufficient information cannot be obtained regarding the purpose of the business relationship or the intended transaction, or who avoid meeting reasonable information requests in this regard,
- Institutions suspected of being shell companies or providing shell banking services,
- Individuals trading crypto assets on their own behalf or on behalf of third parties, and Crypto Asset Service Providers (CASP),
- Banks and institutions without a physical address and establishment,
- Those operating in an area subject to licensing, special authorization, or permits without possessing the necessary permit/license/authorization document,
- Persons and institutions (organizations) engaged in gambling and illegal betting activities, including those operated over the internet,
- Those with adverse records in our bank's internal intelligence and monitoring systems regarding money laundering, terrorism financing, and related financial crimes.

Business relationships established with individuals and organizations later found to be in a prohibited status (listed on the Unacceptable Customers list) are terminated immediately. The relevant business unit promptly reports the situation to the Compliance Officer to initiate the necessary exit procedures.

Refusal to provide the information and documents requested by the Bank within the framework of this Procedure and other relevant internal regulations constitutes a reasonable and valid justification for rejecting the establishment of a business relationship or declining transaction requests from existing customers.

The Bank does not permit the use of "Hold-mail" addresses (where mail is held by the service provider on behalf of the recipient without being returned to the sender) or "Poste Restante" addresses (delivered to a post office branch) as the sole communication address. Individuals and organizations declaring only such addresses as their communication address are not accepted as customers.

In the customer acceptance process for individuals and institutions where there is suspicion that their wealth and funds were obtained through illegal means, as well as for individuals with negative intelligence (social reputation risk), "Enhanced Customer Due Diligence" measures are applied, and maximum care and diligence are exercised.

4.3.14 High-Risk Products and Services

In the context of risks related to money laundering and terrorist financing, it is essential to consider the purpose of the business relationship to be established with the customer as a risk factor, particularly for transactions that are riskier than others, such as cash transactions, money transfers involving high-risk countries, or transactions with associations and foundations.

During the customer acceptance phase, fields related to the purpose of the business relationship are included in the relevant forms used for customer acceptance to determine why the customer wishes to establish a business relationship. The purpose of the business relationship to be established with the customer may be declared by the customer. However, even if no declaration is made, it is recorded in the relevant fields of the forms used for customer acceptance by the relevant bank officials, depending on the transaction on which the customer identification is based.

Customer funds and transactions arising from activities of unknown origin that cannot be directly linked to the customer's line of business, typically stemming from cash transactions and electronic fund transfers, are subject to enhanced due diligence measures.

The following products are considered high-risk products/services by the Bank:

- Transactions of Customers Establishing Business Relationships Through Electronic Banking Channels
- Electronic Transfers
- Cash Transactions

4.3.15 Cash Transactions

Cash transactions for customers at our bank can be conducted via ATMs owned by other banks with which our bank has agreements or through ATMs jointly used by multiple banks. In this context, the following situations are considered risky, requests requiring in-person transactions are not accepted, and similar transactions conducted via ATMs are periodically monitored by the surveillance system:

- The customer frequently and regularly transferring money to the same or different individuals via ATM without a reasonable and valid reason for depositing cash into their own account.
- Continuous inflows of small amounts from numerous sources into the customer’s bank account, which are then withdrawn by the customer via ATM or transferred to other accounts through ATM.
- The customer frequently requesting cash withdrawals or deposits via call center that exceed the established ATM limits without reasonable justification.
- Our bank and credit card customers consistently making high-value expenditures that could be aimed at obtaining cash from the same locations.

If deemed necessary, systemic restrictions may be imposed on the transactions listed above or similar ones, or suspicious transaction reports may be filed regarding the transactions that have occurred.

4.3.16 Updating Customer Information

To ensure that relationships with customers are conducted in a healthy manner and that the level of customer identification established during customer onboarding is maintained throughout the duration of the customer relationship, the bank regularly reviews customer identification, verification, and onboarding information based on a risk-based approach. The frequency of review varies depending on customer risk assessments, last update dates, and customer activity. The following aspects are considered during review activities:

- If there are changes in customer onboarding/assessment criteria or required information/documents due to modifications in bank practices or regulations, a review shall be conducted regardless of the customer’s risk level. For example, if it is decided to request information or documents not previously required, the content of such information/documents, the content of the legal regulation necessitating it, and similar factors are evaluated, and decisions on how to proceed for existing customers are made on a case-by-case basis.
- In accordance with the customer acceptance policy, a ongoing business relationship cannot be established without obtaining mandatory documents from customers.
- For compliance risk levels: high-risk customers are reviewed and controlled annually, medium-risk customers every two years, and low-risk customers every three years. If a customer has been reviewed within the six months prior to the month in which a review is required for another reason, a new review is not necessary, and the next review date is determined based on the last review date.

Category No	Customer Risk Level	Information Update Frequency
1	Customers categorized as "High Risk" according to the risk assessment	Once a Year
2	Customers categorized as "Medium Risk" according to the risk assessment	Once Every 2 Years
3	Customers categorized as "Low Risk" according to the risk assessment	Once Every 3 Years

Customer information is reviewed in cases of "significant changes" in customer activity, risk level, administrative structure, and other similar areas.

A dormant customer becoming active, an increase in a customer's risk level, significant changes in the company's management or control structure (such as a change in ownership control or comprehensive changes in company management), or a change in the company's field of activity are considered "significant change situations."

All review activities mentioned above are carried out by relevant bank personnel or systems under the coordination of the Compliance Officer. During the review process, any outdated information or documents are updated and recorded.

The Compliance Department ensures that necessary corrections are made regarding any deficiencies identified in the review records submitted to it.

4.4 Compliance with Sanctions

The Bank is committed to adhering to legal and regulatory requirements concerning sanctions and ensures that no business relationships are established with individuals listed on UN, OFAC, EU, or local sanctions lists.

Whenever possible, the Bank terminates existing business relationships with individuals listed on OFAC or other sanctions lists.

The Bank verifies whether the parties involved in domestic and international money transfers are listed on sanctions-related lists. For domestic transfers, the responsibility for checking that the originator is not on the list of individuals with frozen assets and for not proceeding with the transaction lies with the sending bank, while the responsibility for verifying that the beneficiary is not on the list of individuals with frozen assets and for not proceeding with the transaction rests with the receiving bank.

4.4.1 Relations with Sanctioned Countries

In accordance with its risk appetite framework for preventing money laundering and the financing of terrorism and chemical weapons, risk assessments, and the principles established by relevant national and international organizations, the Bank does not conduct any banking transactions (including incoming and outgoing transfers), commercial, or financial transactions with sanctioned countries.

4.4.2 Freezing of Assets

The Bank promptly implements asset freezing decisions announced or reported by the Presidency of the Financial Crimes Investigation Board (MASAK) under Law No. 6415 on the Prevention of the Financing of Terrorism ("Law No. 6415") and related regulations, within the scope of implementing United Nations Security Council Resolutions.

Accordingly, it is checked whether any assets exist at our Bank belonging to individuals, institutions, or organizations named in decisions published in the Official Gazette or sent to our Bank's Registered Electronic Mail (KEP) address. If assets are identified, the freezing process is immediately applied, and transaction details are reported to the Presidency within seven days following the notification date.

The management of frozen assets belongs to the relevant natural or legal person. However, our Bank does not permit or facilitate activities related to the disposal, consumption, conversion, transfer, assignment, or other dealings of such assets, subject to the provisions of Law No. 6415.

Notifications regarding the lifting of freezing decisions are also carried out in the same manner and without delay.

4.4.2.1 Roles and Responsibilities in Asset Freezing Processes

The Internal Control and Compliance Presidency is responsible for monitoring asset freezing decisions, managing scanning systems, examining whether there is an asset record at the Bank, coordinating the freezing process, and executing the necessary MASAK notifications.

The Digital Product Management and Business Development Deputy General Manager is responsible for establishing necessary controls during customer onboarding and related banking operations; blocking access to accounts based on asset freezing decisions; and performing blocking transactions within its authority.
The Individual, SME, and Commercial Banking Deputy General Manager is responsible for taking necessary measures regarding participation and financing accounts of customers subject to asset freezing decisions and implementing blocking transactions on these accounts.

4.4.2.2 Key Risk Areas and Controls

Regarding Asset Freezing Processes
- Delayed Screening (Timing Latency): This occurs when the time between the publication of a freezing decision in the Official Gazette or notification by MASAK and the execution of internal bank screening exceeds legal limits. All freezing decisions and MASAK notifications are tracked daily; screening and blocking processes are ensured to be completed within the legal timeframe (24 hours).
- Exact Match Control Error: This arises when AML software only searches for exact name matches, causing oversight of typographical errors, abbreviations, or different spelling variations. "Fuzzy matching" algorithms are actively used in AML software. For identifying existing customers, systematic queries are primarily conducted via Turkish ID number or passport number.
- Risk of Not Screening Existing Customer Base: When a new freezing decision is issued, screening may be limited to new customer acquisitions, and the existing customer portfolio may not be retrospectively screened. With each new list update or freezing decision, all existing customer records in the system are subjected to comprehensive (retroactive) screening.
- Insufficient Beneficial Owner Identification: This refers to failure to detect cases where an individual on the sanctions list is not a direct customer but is the ultimate owner or controlling person (e.g., holding 25% or more shares) of a corporate customer. In corporate customer acquisitions, the ownership structure chain is analyzed until the topmost natural person is reached. Identified "Beneficial Owners" are also included in sanctions list screening.

4.4.2.3 Notifications Regarding the Freezing of Assets

All communication and notification processes with MASAK are conducted through the MASAK Online 2.0 system.
The Asset Freezing Notification Form includes the following information regarding the assets subject to the freezing:
- Asset Type: (e.g., demand deposit, blocked amount, stock, crypto asset wallet address, safe deposit box, etc.)
- Amount and Currency: The current balance at the time the decision is implemented.
- Transaction Records: Account transaction statements for the period prior to the freezing (typically the last 6 months or 1 year).
- Related Persons: A list of proxies, representatives, or authorized signatories with access to the customer's accounts.

4.4.3 Bank Activities Regarding the Prevention of the Financing of the Proliferation of Weapons of Mass Destruction

The Bank implements the United Nations Security Council (UNSC) sanction resolutions aimed at preventing the financing of the proliferation of weapons of mass destruction, as well as the provisions of the Law on the Prevention of the Financing of the Proliferation of Weapons of Mass Destruction and related regulations.
In this context, the Bank does not:
- Collect or provide funds in any way for the benefit of, or engage in business partnerships or other business relationships in Turkey with, individuals, entities, or organizations related to nuclear or ballistic missile programs or other activities specified in these resolutions, or individuals or entities directly or indirectly controlled by them, or those acting on their behalf or account.
- Establish business partnerships, capital partnerships, or correspondent banking relationships with their banks.

Except as permitted by the UNSC, depending on the scope of the relevant resolutions, the Bank does not contribute to or support the import, export, transit, or technology transfer of items, materials, and equipment specified in these resolutions, or activities related to nuclear programs or the development of nuclear weapon delivery systems.
If information or documents are requested by the Monitoring and Cooperation Commission established for the implementation of the Law on the Prevention of the Financing of the Proliferation of Weapons of Mass Destruction, the Bank is obligated to provide such information and documents within the requested timeframe and format.
The Bank is obligated to monitor the lists published on the Presidency’s website regarding individuals, entities, or organizations subject to asset freeze decisions and to take action in accordance with notifications made by the Presidency.

4.5 Training and Awareness Programs

In accordance with national and international regulations on preventing money laundering and terrorist financing, as well as the Bank's internal regulations, training is provided to all new and existing employees, including the Board of Directors and Senior Management. Bank employees must participate when invited to these training programs and are obligated to read documents published for training purposes.

The Bank conducts training activities within the framework of relevant legislation, aiming to prevent money laundering and terrorist financing, in a manner suitable to the size of the business, transaction volumes, and changing conditions. These activities are carried out under the supervision and coordination of the Compliance Officer and within the scope of the annual training program approved by the Board of Directors.

Training activities aim to ensure compliance with obligations under relevant legislation, foster an institutional culture by enhancing employees' sense of responsibility regarding this Procedure, the Bank's internal regulations, and risk-based approaches, and keep employees' knowledge up to date.

The training program is prepared by the Compliance Officer with the participation of relevant units. Training sessions can be conducted face-to-face through seminars, panels, conferences, and similar methods, or online via electronic platforms such as the internet or intranet.

The effective implementation of the training program is monitored by the Compliance Officer. Training activities are carried out within a specific training program and plan, covering the training topics detailed below:

- Concepts of money laundering and terrorist financing,
- Concepts of financing the proliferation of weapons of mass destruction,
- Stages and methods of money laundering, along with case studies on the topic,
- Legislation related to the prevention of money laundering and terrorist financing,
- International regulations in the fight against money laundering and terrorist financing,
- Institutional policies and procedures,
- Risk areas,
- Principles regarding customer due diligence,
- Obligations for identity verification,
- Detection and prevention of money laundering and terrorist financing activities,
- Typologies and trends in money laundering and terrorist financing,
- Principles for reporting suspicious transactions,
- Obligations for record-keeping and disclosure,
- Obligations to provide information and documents,
- Penalties and sanctions applied in case of non-compliance with obligations.

The bank reports the results of its training activities, including the information and statistics specified in the relevant regulations, to MASAK through the Compliance Officer by the end of March of the following year.

4.6 Internal Audit Activities

The purpose of internal audit activities related to the prevention of money laundering and combating the financing of terrorism is to provide assurance to the Board of Directors regarding the effectiveness and adequacy of the compliance program.

It is regularly reviewed and audited each year using a risk-based approach to determine whether the Bank’s internal regulations, risk management, monitoring and control activities, and training activities are sufficient and efficient, as well as the adequacy and effectiveness of the Bank’s risk policy, and whether transactions are conducted in accordance with relevant legislation and the Bank’s compliance policies. Internal audit activities within this scope are carried out by the Bank’s Inspection Board Presidency.

The internal audit conducted by the Inspection Board Presidency includes the following activities:

- Significant deficiencies, errors, and abuses related to money laundering and terrorist financing identified as a result of internal audit activities, along with opinions and recommendations to prevent their recurrence, are reported to the Board of Directors through the Audit Committee, including periodic reporting.
- When determining the scope of the audit, shortcomings identified in monitoring and control activities, as well as customers, services, and transactions posing risks, are included in the audit scope.
- When selecting departments and transactions to be audited, the Bank’s operational size and transaction volume are taken into account. In this context, it is ensured that departments and transactions audited are representative in quantity and quality of all transactions conducted by the Bank.

- The Bank reports the results of audit activities, including information and statistics specified in relevant regulations, to MASAK (Financial Crimes Investigation Board) through the Compliance Officer by the end of March of the following year.

4.7 Other Provisions

4.7.1 Deferral of Transactions

If the Bank identifies serious indications that a transaction is linked to money laundering or terrorist financing offenses, it will submit a suspicious transaction report to MASAK (Financial Crimes Investigation Board) requesting deferral of the transaction, along with the reasons, and will act in accordance with the decision communicated by MASAK regarding the transaction.

4.7.2 New Products and Services

Before offering new or revised products or services to customers, relevant departments must obtain approval from the Compliance Department to ensure compliance with AML/CFT requirements.

4.7.3 Outsourcing

The Bank may engage external firms for customer due diligence matters, such as identifying the customer and beneficial owner and obtaining information about their activities. In such cases, the following conditions must be met:
- All necessary information for customer due diligence must be immediately obtainable from the outsourced firm upon request.
- Certified copies of identification documents and other customer due diligence records must be immediately obtainable from the outsourced firm upon request.
- It must be ensured that the outsourced firm is subject to regulations, audited, and implements adequate measures to comply with identification, record-keeping, and customer due diligence requirements.
- The outsourced firm must not be based in high-risk countries.
- The outsourced firm must provide sufficient guarantees regarding confidentiality in information exchange.
- The duties and responsibilities of the outsourced firm, and the transactions and services to which customer due diligence requirements will apply, must be clearly defined in a contract signed between the Bank and the outsourced firm.

In all cases, the ultimate responsibility for identification and verification lies with the Bank.

4.7.4 Preservation and Presentation

The bank is obligated to preserve all documents related to its obligations and transactions in any environment for a period of eight years from the date of issuance, and its books and records from the date of the last entry; it must also preserve documents and records related to identity verification for eight years from the date of the last transaction and present them to the authorities upon request. The starting date for the preservation period of identity verification documents related to accounts held by the obligor is the date the account is closed.

Documents and records pertaining to suspicious transaction reports submitted to MASAK or internal reports made to the compliance officer, documents attached to the report, and written justifications for suspicious transactions for which the compliance officer decided not to report are also subject to the preservation and presentation obligation.

4.8 Information Sharing and Notification Obligations

4.8.1 Information Sharing with Legal and Regulatory Authorities

If public authorities directly request information or documents, the Compliance Officer is informed about the matter as soon as possible, and a copy of the request is forwarded to the Compliance Officer. Such information and document requests are submitted to the relevant public authorities through the Compliance Officer.

The Bank facilitates, under the coordination of the Compliance Officer, the provision of all necessary information, documents, and records in any medium, along with the required access and passwords to make them readable, to the Presidency and audit personnel appointed by the Presidency, in a complete and accurate manner.

In investigations related to potential money laundering, terrorism, terrorist financing, or other illegal activities, the Bank cooperates with legal and regulatory authorities through official communication channels such as email, reports, and SWIFT messages, without violating obligations arising from laws concerning customer confidentiality and privacy. The Bank fulfills information requests within this scope in a timely manner.

Requests from regulatory bodies or state institutions (written or verbal) are directed to the Compliance Department to ensure necessary actions are taken. Such information and document requests are submitted through the Compliance Officer.

4.8.2 Suspicious Transaction Reporting

If there is any information, suspicion, or circumstance that raises suspicion that the assets involved in a transaction conducted or attempted to be conducted at or through the Bank have been obtained illegally or are being used for illegal purposes—including for terrorist acts, by terrorist organizations, terrorists, or those financing terrorism, or are related or connected to such activities—the transaction shall be reported to MASAK by the Compliance Officer within the period and according to the principles specified in the legislation, after conducting necessary investigations to the extent possible. Suspicious transactions shall be reported to the Presidency no later than ten business days from the date the suspicion arises.

Additionally, the Bank regularly reports to the Presidency transactions in which it is a party or acts as an intermediary that exceed the threshold determined by the Ministry. Customers and transactions for which the Compliance Officer decides to file a suspicious transaction report following additional investigation and evaluation are sent to the Presidency along with supplementary information and documents.

If new information or findings are later obtained regarding a reported transaction, a new Suspicious Transaction Reporting Form is completed and submitted to MASAK without delay, indicating that it supplements the previous report.

The Bank is committed to fostering an open and transparent working environment that encourages employees to report suspicious transactions or matters that violate the Bank's internal regulations to the Compliance Department without fear of any sanctions.

Employees are required to immediately report all matters they know or believe to be in violation of this Procedure to the Compliance Department using the banking system, email, or other appropriate channels. The Bank confirms that such reports made in good faith and in accordance with relevant legislation will protect employees from criminal, legal, and administrative liability.

Bank personnel are prohibited from disclosing other employees, customers, or any third party about the existence of a suspicious situation, ongoing investigation, close monitoring, suspicious transaction reporting, or the likelihood of such reporting regarding a customer or transaction at any stage of the transaction, or from disclosing any information within their knowledge. However, this prohibition shall not prevent information sharing among employees involved in such transactions or with authorized authorities.

4.8.3 Other Notifications

The Bank reports the results of its internal audit activities conducted within the framework of the internal audit policy established under this Procedure, as well as the results of its training activities carried out within the scope of its training policy, along with relevant information and statistics, to the Presidency through the Compliance Officer by the end of March of the following year.

5. REVIEW AND UPDATE

The Compliance Officer and deputy, together with the Digital Product Management and Business Development Group, conduct a comprehensive review of the adequacy of this Procedure and related processes at least once a year. The Procedure is updated by implementing necessary changes either as a result of periodic reviews or in the event of any significant developments that may affect activities related to the prevention of money laundering and terrorist financing.

6. EFFECTIVENESS

This document enters into force on the date it is approved by the Board of Directors.