THE DEVELOPMENT AND INVESTMENT BANK OF TÜRKİYE

COMPLIANCE POLICY ON ANTI-MONEY LAUNDERING, COUNTERING THE FINANCING OF TERRORISM, AND THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION

RESTRICTED

NOVEMBER 2025

TABLE OF CONTENTS

1. PURPOSE

The purpose of this policy is to ensure the Development and Investment Bank of Türkiye's compliance with obligations concerning the prevention of money laundering, terrorism financing, and the financing of the proliferation of weapons of mass destruction, established within the scope of the "Compliance Program" created under the "Regulation on Program for Compliance with Obligations Regarding Anti-Money Laundering and Countering the Financing of Terrorism" to develop create strategies to mitigate potential risks by evaluating customers, transactions, and services through a risk-based approach, to define internal controls, preventive measures, internal audit activities, and respective roles and responsibilities, to raise awareness among Bank and to establish training policies.

2. SCOPE

This Policy encompasses all branches, departments, and personnel within the Bank, as well as all transactions, activities, and services conducted by or through the Bank.

The Bank has established a "Compliance Program" to carry out the necessary control activities in order to comply with national legislation and international standards and regulations regarding anti-money laundering, countering the financing of terrorism, and the prevention of the proliferation of weapons of mass destruction.

The Bank's Compliance Program consists of the following functions:

- Establishment of institutional policies and procedures,
- Execution of risk management activities,
- Execution of monitoring and control activities,
- Appointment of a Compliance Officer and establishment of a Compliance Unit,
- Execution of training activities, and
- Execution of internal audit activities.

The scope of this Policy covers risk management activities, customer due diligence and customer acceptance processes, monitoring/control activities, as well as policies regarding training and internal audit related to anti-money laundering, the prevention of the financing of terrorism, and the proliferation of weapons of mass destruction.

The procedures detailing the duties, responsibilities, and implementation of compliance processes within the Bank are presented in "Compliance Program Procedures – Table 1".

3. DEFINITIONS AND ABBREVIATIONS

Hereinafter, the following terms shall have the meaning ascribed to them below:

Pass-Through Account: A type of account opened by a foreign financial institution with a financial institution established in Türkiye under a correspondent banking relationship, which also allows the customers of the foreign financial institution to issue checks.

The Ministry: The Ministry of Treasury and Finance of the Republic of Türkiye.

The Bank: Development and Investment Bank of Türkiye.

UNSC: The United Nations Security Council.

Audit Committee: The Audit Committee of the Bank.

Electronic Transfer: A transaction conducted through electronic means to transfer a specific amount of funds or securities from a financial institution on behalf of a sender to a recipient at another financial institution.

Financial Group: A group consisting of financial institutions established in Türkiye, including their branches, agents, representatives, commercial attorneys, and similar affiliated units, which are attached to or controlled by a parent company headquartered in Türkiye or abroad.

Financial Institution: The obliged parties listed in subparagraphs (a) through (h), (m), and (ü) of the first paragraph of Article 4 of the Regulation on Measures, as well as the Post and Telegraph Organization, limited to its banking activities.

FATF: The Financial Action Task Force.

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

MASAK: Financial Crimes Investigation Board

Risk Management Policy: The entire set of activities aimed at identifying, rating, monitoring, evaluating, and mitigating the risks the Bank may be exposed to regarding money laundering and the financing of terrorism/proliferation of weapons of mass destruction, and ensuring that necessary measures are taken and managed.

SKY: Core Banking System of the Bank.

Suspicious Transaction: Any transaction conducted or attempted through or within the Bank, where there is any information, suspicion, or reason for suspicion that the assets involved are obtained through illegal means or used for illegal purposes; including being used for terrorist acts, or by terrorist organizations, terrorist, or those who finance terrorism, or being related to or associated with them.

Shell Bank: A bank that does not have a physical presence or service office in any country, does not employ full-time staff, and is not subject to the supervision and licensing of an official authority regarding its banking transactions and records.

Regulation on Measures: The Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism.

Compliance Officer: An officer vested with the necessary authorities, appointed by the obliged parties to ensure compliance with the obligations introduced by the Law and the legislation enacted pursuant to the Law.

Senior Management: The General Manager and Deputy General Managers of the Bank, managers of units within the scope of internal systems, and managers who – even if employed under different titles – hold positions equivalent to or higher than a Deputy General Manager in terms of authorities and duties, excluding consultancy units.

Board of Directors: The Board of Directors of the Bank.

4. LEGAL FRAMEWORK

The legal framework of this Policy is established by Law No. 5549 on the Prevention of Laundering Proceeds of Crime, Law No. 6415 on the Prevention of the Financing of Terrorism, Law No. 7262 on the Prevention of Financing the Proliferation of Weapons of Mass Destruction, and the regulations and communiques issued pursuant to these laws.

Furthermore, the recommendations and standards published by the FATF, which set binding international standards for member countries to enhance national legal systems in combating money laundering, the financing of terrorism, and proliferation of weapons of mass destruction, and other financial crimes, along with UNSC decisions, are taken into consideration. Additionally, recommendations, principles, standards, and guidelines issued by international organizations, such as the Council of the European Union, are also observed. The Bank conducts its operations in full compliance with the aforementioned laws, the respective regulations and communiques, as well as the international standards.

5. RISK MANAGEMENT POLICY

The Bank's Risk Management Policy encompasses activities aimed at identifying, rating, monitoring, evaluating, and mitigating the risks that the Bank may be exposed to regarding money laundering and the financing of terrorism/proliferation of weapons of mass destruction, as well as ensuring the implementation and management of measures required for these purposes.

The Risk Management Policy, at a minimum, covers the internal Bank rules regarding the measures set forth in the third section of the Regulation on Measures, titled "Principles Regarding Customer Due Diligence".

Risk Management activities include the following:

- Methods for identifying, rating, classifying, and assessing the risks within the frameworks of customer risk, service risk, and country risk;
- Methods for the rating and classification of services, transactions, and customers based on their respective risk profiles;
- Methods for monitoring and controlling high-risk customers, transactions, or services, and for reporting these to warn relevant units, and establishing appropriate operational and control rules for executing the respective transactions through Senior Management approval and conducting audits when necessary;

- Retrospective review of the consistency and effectiveness of risk identification, assessment, rating, and classification methods through case studies or historical transactions, and the re-evaluation and updating of these methods based on findings and evolving conditions;
- Continuous monitoring of national legislation as well as recommendations, principles, standards, and guidelines introduced by international organizations regarding risk-related matters, and conducting any developments as needed; and
- Regular reporting of risk monitoring and assessment results to the Audit Committee and the Board of Directors.

The measures and implementation methods envisaged by the Bank for the identification, rating, monitoring, evaluation, and mitigation of risks associated with money laundering and the financing of terrorism/proliferation of weapons of mass destruction are detailed in the "UYM.03-P Procedure on Compliance Risk Management Activities".

5.1. Customer Due Diligence and Customer Acceptance Principles

Under the framework of the "Customer Due Diligence" principle, it is fundamental for the Bank to identify customers and persons acting on their behalf, and to implement necessary controls and measures to identify the Ultimate Beneficial Owner of the transaction. In this context, the following matters are taken into consideration:

- Identification of the customer and verification of identification information using reliable and valid documents or data;
- Obtaining detailed information regarding the purpose and intended nature of the business relationship;
- Establishing a customer financial profile by obtaining information such as the customer's profession, sector, field of activity, income, and source of funds; and monitoring subsequent transactions for consistency with this profile;
- Taking necessary measures for customers, activities, and transactions that require enhanced due diligence;
- Taking necessary measures for the identification of the Ultimate Beneficial Owner;
- Obtaining information regarding the geographic location/jurisdiction where the declared line of business or activity is conducted;
- Conducting adverse media screenings, as well as checks against prohibited/sanctioned lists and intelligence databases.

Based on the customer evaluation conducted within the scope of the criteria mentioned above, the Bank ensures that:

- Customer risk categories are identified;
- Customers are monitored according to their respective risk levels; and
- Appropriate actions are taken regarding the establishment, rejection, and/or termination of the business relationship with the customer.

At the bank, during the onboarding of new customers (opening accounts and similar transactions where the relationship is intended to be ongoing), the roles, authorities, and responsibilities for identifying customers, recording declared addresses, obtaining additional identifying information and documents required by legislation and/or internal Bank policies, verifying this information, and storing records in physical and/or electronic media are clearly defined. All duties and responsibilities assigned within the Bank are detailed in the "UYM.01-P Procedure on Duties and Responsibilities within the Scope of the Compliance Program."

Customer risk classification is performed based on criteria determined by the Internal Control and Compliance Department. The principles regarding risk criteria are detailed in the "UYM.03-P Procedure on Compliance Risk Management Activities".

5.2. Principles for Identification

The Bank shall identify the customer in a timely, complete, and accurate manner, in accordance with the legislation in force and the internal regulations, prior to the establishment of a permanent business relationship and before any transaction is executed.

Identification shall be carried out by obtaining the identity information of customers and those acting on behalf of or for the account of customers, and by verifying the accuracy of such information under the following circumstances:

- Regardless of the amount upon the establishment of a permanent business relationship;
- Regardless of the amount, whenever there is a suspicion regarding the adequacy or accuracy of previously obtained customer identification data;
- Regardless of the amount, in cases requiring a suspicious transaction report;
- When the transaction amount, or the total amount of multiple linked transactions, exceeds the threshold determined by the Regulation on Measures; and
- In electronic transfers, when the transaction amount, or the total amount of multiple linked transactions, exceeds the threshold determined by the Regulation on Measures.

The implementation of the customer due diligence and acceptance processes, along with the detailed components of identification specified in this policy, are further elaborated in the "UYM.02-P Procedure on Customer Due Diligence and Identification".

5.2.1. Identification of Natural Persons

During the identification processes of natural persons, the following information is obtained: full name, date of birth, nationality, type and number of the identity document, address, signature specimen, information regarding business and occupation, and, if available, telephone number, fax number, and e-mail address. For Turkish citizens, the T.R. ID Number is required in addition to this information; for non-Turkish citizens, the place of birth is also required.

In accordance with the Regulation on Measures, the accuracy of information regarding the customer's full name, date of birth, T.R. ID Number, and the type and number of the identity document is verified through T.R. Identity Card, T.R. Driver's License, Passport, or other identity documents expressly stated as official identity documents in specialized laws and

containing the T.R. ID number, for Turkish citizens; and through a passport, a residence permit, or identity documents deemed appropriate by the Ministry, for non-Turkish citizens.

Upon the presentation of the original documents or notarized copies thereof, a legible photocopy or an electronic image of the document is captured and recorded in the SKY.

5.2.2. Identification of Legal Entities

During the identification process of legal entities registered with the Trade Registry, the following information is obtained: the legal entity's title, trade registry number, tax identification number, field of activity, full address, telephone number, and, if available, fax number and e-mail address. Additionally, the full name, date of birth, nationality, type and number of identity document, and signature specimen of the authorized signatories are obtained. For Turkish citizens, the T.R. ID number is required, while for non-Turkish citizens, the place of birth information is also obtained.

The legal entity's title, trade registry number, field of activity, and address are verified through the Trade Registry registration documents, while the Tax Identification Number is verified through documents issued by the relevant unit of the Revenue Administration.

The identity information of the persons authorized to represent the legal entity is verified through the identity documents specified in the Identification of Natural Persons section above, while their representation authority is verified through the official registration documents.

Upon the presentation of the original documents or notarized copies thereof, a legible photocopy or an electronic image of the document is captured and recorded in the SKY.

5.2.3. Remote Identification of Natural Persons and Trade Registry-Recorded Legal Entities

In cases where the legislation governing the Bank's primary field of activity permits the establishment of a contract through methods that allow identity verification without a face-to-face meeting with the customer, remote identification methods may be utilized to verify customer identity when establishing a permanent business relationship with natural persons or legal entities registered with the trade registry.

Currently, the Bank does not have an active practice for establishing contracts through methods that permit identity verification without a physical face-to-face meeting.

5.2.4. Identification of Association and Foundations

In the identification process of associations, the following information is obtained: the association's name, purpose, registry number, tax identification number, full address, telephone number, and, if available, fax number and e-mail address, as well as the full name, date of birth, nationality, type and number of identity document, and signature specimen of the authorized representative. For Turkish citizens, the T.R. ID number is required, while for non-Turkish citizens, the place of birth information is also obtained. The association's name, purpose, registry number, and address are verified through the association's charter and documents related to the registration in the association registry, while the tax identification number is verified through documents issued by the relevant unit of the Revenue Administration, and the

identity information of the authorized representative is verified through the documents specified in the "Identification of Natural Persons" section above, with their representation authority verified through official documents confirming their authorization.

In the identification process of foundations, the following information is obtained: the foundation's name, purpose, central registry number, tax identification number, full address, telephone number, and, if available, fax number and e-mail address, as well as the full name, date of birth, nationality, type and number of identity document, and signature specimen of the authorized representative. For Turkish citizens, the T.R. ID number is required, while for non-Turkish citizens, the place of birth is also obtained. The foundation's name, purpose, central registry number, and address are verified through the foundation deed of trust and records held by the General Directorate of Foundations, while the tax identification number is verified through documents issued by the relevant unit of the Revenue Administration, and the identity information of the authorized representative is verified through the documents specified in the "Identification of natural Persons" section above, with their representation authority verified through official documents confirming their authorization.

Upon the presentation of the original documents or notarized copies thereof, a legible photocopy or an electronic image of the document is captured and recorded in the SKY.

5.2.5. Identification of Labor Unions and Confederations

In the identification process of labor unions and confederations, the following information is obtained: the organization's name, purpose, registry number, tax identification number, full address, telephone number, and, if available, fax number and e-mail address, as well as the full name, date of birth, nationality, type and number of identity document, and signature specimen of the authorized representatives of the union or confederation. For Turkish citizens, the T.R. ID number is required, while for non-Turkish citizens, the place of birth information is also obtained. The obtained information is verified through the constitutions of these organizations and other registration documents held by the regional labor directorates of the Ministry of Family, Labor and Social Security, while the tax identification number is verified through documents issued by the relevant unit of the Revenue Administration, and the identity information of the authorized representatives is verified through the documents specified in the "Identification of Natural Persons" sections above, with their representation authority verified through official registration or authorization documents.

Upon the presentation of the original documents or notarized copies thereof, a legible photocopy or an electronic image of the document is captured and recorded in the SKY.

5.2.6. Identification of Political Parties

In the identification of political party organizations, the following information is obtained: the name of the relevant unit of the political party, its full address, telephone number, and, if available, fax number and e-mail address, as well as the full name, date of birth, nationality, type and number of identity document, and signature specimen of the authorized representative of the political party. For Turkish citizens, the T.R. ID number is required, while for non-Turkish citizens, the place of birth information is also obtained. The name and address of the relevant unit of the political party are verified through their constitutions, while the identity of the authorized representative is verified through the identity documents specified in the

"Identification of Natural Persons" sections above, with their representation authority verified through official registration or authorization documents.

Upon the presentation of the original documents or notarized copies thereof, a legible photocopy or an electronic image of the document is captured and recorded in the SKY.

5.2.7. Identification of Non-Resident Legal Entities and Foreign Trusts

The identification of non-resident legal entities is conducted through the equivalents of the documents required for legal entities resident in Türkiye, as either certified by the consulates of the Republic of Türkiye or bearing an Apostille issued by the competent authority of a party state within the framework of the Convention Abolishing the Requirement of Legalization for Foreign Public Documents. Furthermore, within the scope of a risk-based approach, identity information shall be verified through notary-certified Turkish translations of these documents, as deemed necessary.

In cases where a trustee, whether a natural or legal person as specified in the agreement, requests the execution of a transaction requiring identification from obliged parties on behalf of an asset account governed by a trust agreement established abroad, a written declaration must be provided to the obliged parties indicating that the transaction is being requested for the account associated with the assets created under the aforementioned trust agreement prior to the execution of such transactions, pursuant to Article 15 of the Law. Identification related to a trust agreement established abroad is conducted based on written copies of the trust agreement approved by the consulates of the Republic of Türkiye, or that bear an Apostille from the authorities of a contracting state within the framework of the "Convention Abolishing the Requirement of Legalization of Foreign Public Documents". Within the scope of a risk-based approach, the identification details shall be verified through notary-certified Turkish translations of these documents, as deemed necessary.

Furthermore, the identity information acquired as a part of the trustee's identification process is verified in accordance with Article 6 or 7 of the Regulation on Measures. In the context of identifying the beneficial owner, the identity information of the settlor, the beneficiary or group of beneficiaries, and, where applicable, the individuals appointed as auditors under the agreement shall be obtained, and reasonable measures shall be taken to verify this information. Furthermore, necessary actions shall be taken to identify the natural person(s) who ultimately exercise control over the assets in question.

5.2.8. Identification of Entities Without Legal Personality

In transactions conducted on behalf of entities without legal personality, such as apartment, housing estate, or business center managements, the following information shall be obtained: the name of the entity, its full address, and, if available, its telephone number, fax number, and e-mail address, as well as the full name, date of birth, nationality, type and number of the identity document, and a signature specimen of the authorized representative of the entity. For Turkish citizens, the T.R. ID number is required, while for non-Turkish citizens, the place of birth is obtained. The identity information of the authorized representative of the entity is verified through the identity documents specified in the "Identification of Natural Persons"

section above, while the information about the entity and the authorization of the representative are verified via the notarized resolution book.

In the identification process of entities such as joint ventures without legal personalities, the following information is obtained: the joint venture's name, purpose, field of activity, tax identification number, full address, telephone number, and, if available, fax number and e-mail address, as well as the full name, date of birth, nationality, type and number of identity document, and signature specimen of the authorized representatives of the joint venture. For Turkish citizens, the T.R. ID number is required, while for non-Turkish citizens, the place of birth information is also obtained. The joint venture's name, purpose, field of activity, and address is verified through the notary-certified partnership agreement, while the tax identification number is verified through documents issued by the relevant unit of the Revenue Administration, and the identity information of the authorized representatives is verified through the documents specified in the "Identification of Natural Persons" sections above, with their representation authority verified through official registration or authorization documents.

Upon the presentation of the original documents or notarized copies thereof, a legible photocopy or an electronic image of the document is captured and recorded in the SKY.

5.2.9. Identification of Public Institutions

In transactions involving public administrations operating under the general management pursuant to the Public Financial Management and Control Law No. 5018, as well as professional organizations designated as public institutions, the identity of the person acting on their behalf shall be identified in accordance with the "Identification of Natural Persons" section above. Their authorization status shall be verified through a power of attorney issued in compliance with the relevant legislation.

5.2.10. Identification of Persons Acting on Behalf of Others

In cases where a transaction is initiated by individuals authorized by those possessing the representative authority for legal entities or entities without legal personality, it is mandatory to establish the scope of the representative authority and identify the individuals authorized to represent.

In cases where a transaction is initiated by authorized representatives, they shall be identified via a power of attorney or signature circular, provided that these documents contain identity information and are certified by a notary public. In cases where the transaction is initiated by third parties authorized by representative authorities, the authorization status shall be determined by a power of attorney or written instructions issued by the authorized representative. These authorized third parties shall also be identified in the manner prescribed for natural persons.

5.2.11. Verification of the Authenticity of Supporting Documents

In instances where there is doubt concerning the authenticity of documents used for the verification of information obtained during the identification process, the authenticity of the document shall be verified, to the extent possible, by contacting the issuing individual or institution, or other competent authorities. Subsequent to the necessary investigations, any

transactions deemed suspicious shall be reported to the Presidency of MASAK (Financial Crimes Investigation Board) by the Bank Compliance Officer, in accordance with the timeframes and principles outlined in the relevant law and regulations.

5.2.12. Identification in Subsequent Transactions

In subsequent face-to-face transactions that require identification within the context of an ongoing business relationship, where the individual's identity has been duly established, identity information shall be collected and cross-referenced against the data maintained by the bank. Following this cross-verification, the name and surname of the natural person executing the transaction shall be documented on the relevant record, and a signature specimen shall be obtained. If there is any doubt concerning the accuracy of the information provided, such information shall be validated by comparing it with the records held by the Bank, upon the presentation of supporting identity documents or notarized copies thereof.

5.2.13. Identification of Persons Acting on Behalf of Others

Necessary measures shall be taken to ascertain whether a transaction is executed on behalf of another individual. In this context, to remind those acting in their own capacity yet on behalf of others of their legal obligations, appropriate notices shall be prominently displayed in service branches, ensuring visibility to customers. Furthermore, during the establishment of an ongoing business relationship, a written declaration shall be obtained from the customer affirming whether they are acting on behalf of another person. This declaration shall be collected via the "Customer Due Diligence Form" and shall be duly recorded within the SKY system upon receipt.

Should the individual initiating the transaction indicate that they are acting on behalf of another party, the identity and authorization status of the individual making the request, along with the identity of the person on whose behalf the transaction is conducted, shall be verified.

In the event of any suspicion that an individual is acting in their own name but on behalf of another party, despite contrary declarations, necessary measures shall be taken to identify the ultimate beneficial owner.

5.3 Identification of the Ultimate Beneficial Owner

The ultimate beneficial owner is defined as the natural person(s) who ultimately control a natural individual, legal entity, or an unincorporated entity on whose behalf a transaction is executed, or who possess significant influence over the accounts or transactions associated therewith. In accordance with the principles of Customer Due Diligence, it is imperative to undertake necessary measures to accurately identify the ultimate beneficial owner involved in the transaction.

In the establishment of an ongoing business relationship with legal entities registered in the trade registry, it is essential to identify and verify the identity of natural person shareholders holding more than twenty-five percent of the legal entity. In instances where there is a reasonable suspicion that the natural person shareholder holding more than twenty-five percent of the shares is not the ultimate beneficial owner, or in cases where no natural person possesses such a percentage, necessary measures shall be implemented to identify the natural person(s)

exercising ultimate control over the legal entity. The natural person(s) identified through this process shall be regarded as the ultimate beneficial owner.

In cases where the ultimate beneficial owner cannot be identified, the natural person(s) holding the highest level of executive authority as recorded in the trade registry shall be recognized as the ultimate beneficial owner in their capacity as senior management.

5.4. Customer Risk and Classification Principles

The Bank categorizes customers into three primary classifications based on evaluations performed during the customer onboarding process:

1. Persons/entities deemed unacceptable as customers
2. High-risk customers
3. Medium and low-risk customers

5.4.1 Persons and Entities Deemed Unacceptable as Customers

In order for an individual or legal entity to be accepted as a customer, they must meet the criteria established in accordance with this Policy. In this context, the Bank shall refrain from entering into a business relationship with, or accepting as customers, the following categories:

- Individuals or entities that abstain from providing the required information and documentation;
- Customers for whom true identities and addresses cannot be determined;
- Those who are unable to furnish satisfactory information regarding their transactions and the source of their funds;
- Individuals or entities engaged in activities related to the financing of terrorism, as defined by the United Nations and Presidential Decrees, and those listed on other national and international sanctions/terrorism lists;
- Casinos and individuals or entities involved in illegal betting operations;
- Illegitimate constructs such as pyramid or Ponzi schemes;
- Shell banks;
- Shell companies (entities that generally exist only on paper and are established in offshore jurisdictions);
- Those involved in alternative remittance (hawala) systems;
- Individuals or entities offering unlicensed payment services or intermediating electronic fund transfers.

A business relationship shall not be initiated with natural or legal entities whose identities cannot be verified in accordance with applicable legislation, or for whom adequate information regarding the purpose of the business relationship cannot be obtained. Any relationships with customers identified as engaging in or permitting their accounts to be utilized for the laundering

of proceeds of crime or for the financing of terrorism and the proliferation of weapons of mass destruction shall be terminated.

In the event that identity information and verification cannot be performed due to concerns regarding the adequacy and accuracy of previously acquired customer identification data, it shall be necessary to terminate the business relationship. Furthermore, in instances where the nature of a transaction requested by the customer is unclear, or when the ultimate beneficial owner of the transaction cannot be identified and remains concealed, consideration shall be given to rejecting the requested transaction and terminating the business relationship.

Upon the establishment of an account relationship with the Bank, any business relationship shall be terminated with customers subsequently included on the sanction lists specified in Article 8, titled "Provisions Regarding the Management of Sanctions." In cases where customers monitored through screening programs fail to provide the necessary information and documentation regarding their requested transactions, such transactions shall not be executed, and the consideration of terminating the business relationship shall ensue.

Prior to establishing a correspondent relationship, it is imperative to ascertain whether the counterparty financial institution functions as a shell bank; otherwise, a correspondent relationship shall not be established. Furthermore, accounts opened with correspondent banks shall not be employed as pass-through accounts, and any accounts identified as utilized for such purposes shall be subject to closure.

For transactions categorized as suspicious following the completion of necessary due diligence, the measures detailed under the heading "Suspicious Transactions" shall be enacted.

5.4.2. High-Risk Customers

Based on the risk assessment conducted by the Bank, customers will be classified as high-risk as per the following criteria:

- Those residing in high-risk countries and jurisdictions;
- Those engaged in high-risk sectors, business activities, or professions;
- Those executing a significant volume of transactions or engaging in complex and unusual transaction patterns;
- Politically Exposed Persons; and
- Those residing in or associated with free zones and other financial centers where regulatory and supervisory oversight is minimal or absent.

Those Residing in High-Risk Countries and/or Jurisdictions: Citizens, companies, and financial institutions from countries and offshore centers identified by the Ministry as having inadequate regulations for the prevention of money laundering and financing of terrorism, characterized by insufficient cooperation in combating such crimes, or are categorized as high-risk by relevant international organizations.

Those Engaged in High-Risk Sectors, Business Activities, or Professions: Criminal organizations often seek to acquire businesses that are cash-intensive or can be easily converted

into cash as a means to obscure proceeds of crime. The sectors and business lines identified as high-risk in this context are as follows:

- Authorized exchange offices;
- Authorized payment institutions and electronic money institutions;
- Jewelers and traders in precious stones and metals such as gold/diamond;
- Travel agencies, passenger and freight transporters;
- Casinos, gambling operators, and lottery agents (official representatives of authorized firms);
- Dealers of luxury vehicles;
- Antique dealers, art galleries, and retailers of carpets;
- Large-scale real estate agents and all types of their associated agencies, representatives, and commercial attorneys;
- Lessors of aircraft and marine vessels;
- Manufacturers and traders engaged in leather goods;
- Manufacturers and traders of automotive spare parts;
- Those operating in cash-intensive business sectors (including parking lot operators, restaurants, fuel stations, lottery and newsstands, distribution companies, and traders of toys and stationery);
- Factoring companies;
- Foundations and associations (voluntary donation and aid institutions);
- Non-residents or foreign nationals;
- Manufacturers, sellers, and intermediaries within the defense industry and weaponry;
- Companies intermediating the trading of cryptocurrencies; and
- Savings finance companies.

Politically Exposed Persons (PEPs): Senior natural persons who are entrusted with prominent public functions, whether at the domestic or international level, by means of election or appointment, including board members, senior executives, and other individuals holding equivalent positions in international organizations.

To effectively mitigate risks associated with customers identified as high-risk through a risk assessment, one, several, or all of the measures specified under Section 5.15, titled “Enhanced Due Diligence Measures, shall be implemented in proportion to the level of risk. Furthermore, the monitoring and control activities applicable to customers classified as high-risk are detailed under Section 6.

5.4.3. Medium and Low-Risk Customers

Customers who do not fall within the specified categories outlined above shall be classified by the Bank as low and medium-risk customers.

The “Monitoring and Control Activities” applicable to customers identified as low or medium-risk, as determined through risk management processes, are detailed in Section 6.

5.5. Transactions Requiring Special Attention

It is imperative to exercise heightened scrutiny with respect to transactions that are complex or unusually large, as well as those that do not exhibit a clear and justifiable legal or economic purpose. Requisite measures shall be undertaken to acquire sufficient information regarding the intent behind the requested transaction, and all relevant information, documentation, and records obtained in this context shall be preserved for future submission to authorities upon request.

5.6. Monitoring of Customer Status and Transactions

The monitoring of customer status and transactions involves the systematic tracking of a customer’s financial activities and their business relationship, the timely updating of any alterations in their information and documentation, and the periodic reassessment of the customer’s risk profile in relation to the nature of the business relationship. The specifics of monitoring and control activities, which are executed utilizing a risk-based approach that takes into account the nature of customers’ financial activities, are detailed in Section 6, titled “Monitoring and Control Activities.”

5.7. Product/Service Risk

Product/Service Risk encompasses non-face-to-face transactions, correspondent banking, and offerings facilitated through emerging technologies, as well as products and services classified as inherently risky.

Given the Bank’s product and service structure, which does not permit cash transactions and ensures that all monetary transactions are executed electronically by the Bank’s operations teams in accordance with customer instructions, there are no alternative distribution channels available for customers to perform monetary transactions on their accounts independently. Consequently, the assessment of product and service risk specifically focuses on electronic fund transfer operations, as well as products and services offered through emerging technologies and those inherently identified as high-risk.

5.8. Mitigation of Technological Risks

The Bank exercises diligent oversight regarding the risks associated with leveraging the opportunities presented by both existing and emerging products, as well as innovative business practices, which may include new distribution channels, if established, for the purpose of laundering illicit proceeds. Furthermore, the Bank implements risk-focused controls over services that may be susceptible to misuse.

Within the Financial Group’s subsidiaries, rigorous controls are enacted to ensure that newly introduced services and existing products, which have been restructured due to ongoing

technological advancements, comply with applicable legislation, and the process of implementation is subject to strict monitoring.

5.9. Reliance on Third Parties

The Bank may establish a business relationship or execute a transaction by relying on the measures taken by another financial institution in relation to the identification of the customer, the person acting on behalf of the customer, and the ultimate beneficial owner, as well as the acquisition of information concerning the purpose of the business relationship or the transaction.

Reliance on a third party is permissible provided that:

- It is ensured that the third party has implemented adequate measures for identity verification, record-keeping, and all other requisites related to Customer Due Diligence, and in instances where the third party is based abroad, that it adheres to regulations and supervisory frameworks that align with international standards aimed at combating money laundering and the financing of terrorism;
- It is ensured that certified copies of documents related to identification (or digital images thereof, when the relied-upon institution has established a business relationship through remote identification) shall be promptly provided by the third party upon request;
- It is ensured that the identification of the customer whose information is shared was not conducted by the third party under simplified due diligence measures.

When establishing a business relationship or executing a transaction based on reliance on a third party, information and documentation regarding the customer's identification shall be promptly obtained from the third party. In any event, prior to the execution of any such transaction, it is essential to secure approval from the Internal Control and Compliance Department.

The principle of relying on third parties shall not be applied if the third party is resident in a high-risk country.

5.10. Rejection of Transactions and Termination of Business Relationship

In circumstances where customer identification cannot be completed or where customers fail to provide sufficient information regarding the purpose of the business relationship, no business relationship shall be established with such individuals or entities, and their requested transactions shall not be executed. Within this scope, no accounts shall be opened under anonymous or fictitious names.

In the event that the required identification and verification cannot be performed due to doubts concerning the adequacy and accuracy of previously obtained customer identification information, the business relationship shall be terminated. Furthermore, the Bank shall independently evaluate whether the aforementioned circumstances constitute a suspicious transaction.

5.11. Correspondent Banking Relationships

In cross-border correspondent banking relationships, the following procedures shall be implemented:

- The relevant institution's policy and questionnaire documents shall be obtained and reviewed to assess the Anti-Money Laundering and Countering the Financing of Terrorism systems of the correspondent financial institution, ensuring the adequacy and effectiveness of their systems.
- Questionnaires and publicly available resources shall be employed to ascertain whether the correspondent financial institution has been subjected to any investigations related to money laundering or the financing of terrorism, whether it has incurred any penalties or warnings, and to assess its business activities, reputation, and the level of supervision it receives.
- The initiation of new correspondent relationships or the termination of existing correspondent relationships at the Bank's discretion shall proceed only with the explicit approval of senior management.
- Particular attention shall be directed toward complex and unusually large transactions, as well as transactions that lack a reasonable legal or economic purpose; necessary measures shall be taken to procure sufficient information regarding the objectives and nature of the proposed transaction.

5.12. Electronic Transfers

The Bank shall implement necessary measures to ensure the inclusion of the full name, title, account number, address, and identification numbers of the ordering parties in all domestic and cross-border transfer messages, including national identification numbers (T.R. ID Number, Foreign ID Number, Tax ID Number), passport numbers, or their equivalents.

In relation to the aforementioned measures, special attention shall be exercised for incoming transfer messages that do not contain the required information concerning the ordering party and the beneficiary. Such transactions shall undergo thorough scrutiny as part of the assessment of suspicious transactions. The unit responsible for executing payments to beneficiaries shall ensure that the identity and address of the individual or entity are accurately verified, identified, and documented.

In the event that the Bank receives an electronic transfer message lacking essential information regarding the sender, the missing details shall be requested from the originating financial institution. Should the originating financial institution fail to provide the missing information, the electronic transfer shall be rejected. In instances where an institution consistently submits messages that are missing information despite repeated requests for completion, the Bank shall consider the rejection of incoming electronic transfers from that institution, the imposition of transaction restrictions, or the potential termination of the business relationship.

5.13. High-Risk Countries

Enhanced due diligence is required for transactions involving citizens, companies, and financial institutions from jurisdictions identified by the FATF as non-cooperative, as well as for entities based in tax havens and offshore financial centers, including individuals/entities that maintain

business relationships with them. The Bank shall implement enhanced monitoring activities for transactions associated with these jurisdictions. The Bank shall not intermediate any transactions related to countries subject to comprehensive economic or financial sanctions imposed by international organizations or institutions.

The classification to be taken as the basis for determining country risk is detailed in "UYM.03-P Procedure on Compliance Risk Management Activities."

5.14. Simplified Due Diligence

Within the framework of Customer Due Diligence principles, simplified measures may be implemented regarding the identification of customers under the following circumstances:

- Transactions conducted exclusively between financial institutions;
- Transactions in which the customer is a public administration within the scope of general management or a professional organization classified as a public institution pursuant to Law No. 5018;
- Establishment of business relationships through bulk customer onboarding as part of salary payment agreements;
- Transactions related to pension plans and pension contracts that facilitate retirement benefits for employees via wage deductions; and
- Transactions involving customers that are publicly traded companies with shares listed on a stock exchange.

Simplified measures shall not be applicable in situations where there exists a risk of money laundering or the financing of terrorism due to the specific nature of the transaction in question.

5.15. Enhanced Due Diligence

In transactions falling within the scope of Articles 18, 20, and 25 of the Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism, as well as in high-risk scenarios identified within the context of a risk-based approach, one or more, or all, of the following measures shall be implemented in proportion to the identified risk:

- Obtaining supplementary information regarding the customer and increasing the frequency of updates to identity information for both the customer and the ultimate beneficial owner;
- Obtaining additional details concerning the nature of the business relationship;
- Obtaining, to the extent possible, information regarding the source of the assets and the source of funds associated with the customer;
- Securing information regarding the intended purpose of the transaction;
- Requiring approval from senior management for the establishment of a business relationship, the continuation of an existing relationship, or the execution of any transaction;

- Enhancing the number and frequency of applied controls while maintaining the business relationship under strict supervision, specifically identifying transaction types that require additional oversight; and
- Mandating that the initial financial transaction in a permanent business relationship be conducted through another financial institution where Customer Due Diligence principles are strictly adhered to.

6. MONITORING AND CONTROL ACTIVITIES

The Bank engages in monitoring and control activities utilizing a risk-based approach, which considers the nature of the transactions executed by its customers. The primary objective of these activities is to safeguard the Bank against various risks while ensuring that operations are conducted in compliance with the Law, regulations, and communiques as mandated by the Law, in addition to the institution's own policies and procedures. In this context, the Bank develops and implements monitoring and control methodologies that are tailored to align with the nature and level of risks associated with its customers, transactions, and services.

Monitoring and control activities include the following:

- Monitoring and control of customers and transactions within the high-risk group;
- Monitoring and control of transactions conducted with high-risk countries;
- Monitoring and control of complex and unusual transactions that do not demonstrate a reasonable legal or economic purpose;
- Controlling transactions that surpass designated thresholds to ensure alignment with customer profiles;
- Monitoring and control of linked transactions that collectively exceed the threshold requiring identification;
- Verifying and ensuring the completion and updating of necessary information and documentation, both electronically and in writing, alongside compliance with mandatory information stipulated in electronic transfer messages;
- Continuous monitoring of customer transactions throughout the business relationship to ensure alignment with information related to the customer's business, risk profile, and source of funds;
- Monitoring and control of linked transactions that exceed the specified thresholds requiring identification;
- Verifying the adequacy, accuracy, and currency of existing information and documentation pertaining to the customer, ensuring that any deficiencies are adequately addressed;
- A risk-oriented approach to the control of services that may become susceptible to financial crimes, sanctions risk, or misuse due to emerging products and technological developments; and
- Monitoring media reports related to the laundering of proceeds from crime, the financing of terrorism, and the proliferation of weapons of mass destruction, including

investigations to ascertain whether individuals mentioned in such reports are customers of the Bank.

In the context of a permanent business relationship, customer transactions are systematically monitored to ensure alignment with their commercial activities, business history, financial standing, and source of funds. Additionally, customer information, documentation, and records are maintained in an up-to-date manner.

As a result of risk management activities, customer information and documents are reviewed every year for customers classified within the high-risk category; every three years for those in the medium-risk category, and every five years for those in the low-risk category.

7. SUSPICIOUS TRANSACTIONS

In instances where monitoring and control measures reveal information or circumstances that raise suspicions regarding the legality of the assets involved in a transaction, or their use for illicit purposes, including terrorist acts or support for terrorist organizations, terrorists, or those who finance terrorism, or that the transaction is linked or associated with the laundering of proceeds of crime or the financing of terrorism, or if transactions are inconsistent with the established customer profile or if the customer refrains from providing required information and documentation, a Suspicious Transaction Report shall be filed, irrespective of the transaction amount.

Transactions identified as suspicious, following the necessary investigation, shall be reported to the Presidency of MASAK by the Compliance Officer within the timeframes and principles specified by applicable law and regulations. The Compliance Officer is authorized to request any information or documentation from all departments within the respective fields of duty in relation to the suspicious transaction. Departments requested to provide such information and documentation shall comply fully and provide the necessary cooperation to the Compliance Officer.

In accordance with the regulations governing the confidentiality of suspicious transaction reports and the safeguarding of whistleblowers, the Bank personnel who become aware, in any manner, of a submitted suspicious transaction report are prohibited from disclosing any information regarding the existence of such a report to any parties, including those involved in the transaction, except for disclosure made to audit officials responsible for liability inspections and to judicial authorities during legal proceedings.

It is imperative to exercise maximum diligence with respect to the confidentiality and security of internal reports filed within the Bank and to ensure the protection of the parties involved in such reporting.

In cases where documentation or serious indications exist that suggest the assets involved in an attempted or ongoing transaction may be associated with the crime of money laundering or the financing of terrorism, the Suspicious Transaction Report shall be submitted to MASAK, accompanied by a request for the suspension of the transaction and the necessary justifications thereof. In such cases, the Bank shall refrain from executing the transaction for a period of seven (7) business days, as stipulated by relevant legislation.

8. PROVISIONS REGARDING THE MANAGEMENT OF SANCTIONS

The Bank undertakes all necessary measures to ensure that its products and services are not employed for the purposes of laundering proceeds of crime, the financing of terrorism, or the proliferation of weapons of mass destruction, and strictly adheres to sanctions imposed by both national and international bodies, as well as those that are specific to certain countries. To this end, all incoming and outgoing transfer transactions are monitored in real-time through a dedicated filtering program.

In addition to adhering to national sanctions, the Bank guarantees full compliance with, at a minimum, the sanctions established by the UNSC, the European Union, the United States, and the United Kingdom.

Sanction risks are carefully evaluated during the onboarding process of new customers, the updating of customer information, and the execution of customer transactions. In this context;

- Customers, shareholders, guarantors, individuals acting on behalf of or for the account of customers, and ultimate beneficial owners are screened against sanctions lists.
- Transactions executed by the customer with or through the Bank are analyzed to ascertain whether they directly or indirectly involve Comprehensively Sanctioned Countries/Regions, or any person or entity subject to sanctions.
- The onboarding of customers or the execution of transactions shall not proceed until authorized personnel, appointed for this purpose, have completed the evaluations of the screening results.
- For existing customers, regular screenings are conducted to ensure ongoing compliance with sanction lists.

Furthermore, the Bank adheres to supplementary sanction regulations established within the context of agreements made with international financing institutions concerning resources received from overseas.

9. OBLIGATIONS REGARDING THE PREVENTION OF THE FINANCING OF TERRORISM/THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION

The Bank adopts a risk-based approach in its operations, considering the regulations established under 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.

9.1. Freezing of Assets

Decisions concerning the freezing or prohibition of assets, as well as the revocation of such decisions related to individuals or entities subject to UNSC resolutions, or entities directly or indirectly controlled by them, or individuals/entities acting on their behalf or for their account, shall be executed without delay following the Presidential Decision published in the Official Gazette.

Upon the publication of an asset-freezing decision in the Official Gazette, the Bank shall take the necessary actions in accordance with the procedures outlined in the relevant provisions of

Article 128 of the Criminal Procedure Code No. 5271, regarding the freezing of existing assets, including jointly held accounts, of the designated individuals, entities, and organizations.

The Bank prioritizes the establishment of controls designed to identify, assess, monitor, and mitigate risks associated with the violation, non-implementation, or evasion of asset-freezing decisions. In this regard, measures are taken for the continuous monitoring of customers and transactions, taking into account asset-freezing decisions and potential matching criteria.

Upon the request of the Presidency of MASAK, the Bank is required to report within seven (7) days following the receipt of the official request, providing affirmation that no asset records exist, should none be found, or a confirmation of the execution of the asset freezing process, accompanied by detailed information regarding any frozen assets, if such records are present.

The procedures and principles governing the implementation are outlined in the "UYM.05-P Implementation Procedure for the Freezing of Assets," which has been developed in accordance with applicable legislation.

10. OBLIGATION TO PROVIDE INFORMATION AND DOCUMENTATION

Requests regarding notifications within the scope of the continuous obligation to provide information and documentation, as well as all types of information, documents, and records in any medium received from institutions and officials authorized to request such information, shall be fulfilled with maximum care and diligence. This includes providing all necessary information, passwords, and access protocols required to ensure full accessibility or to render these records legible, ensuring they are provided completely and accurately.

11. RETENTION

In accordance with the Law and its secondary regulations, the Bank ensures to present to the authorities upon request and to retain for a period of eight (8) years:

- from the date of issuance, for documents;
- from the date of the last entry, for books and records; and
- from the date of the last transaction, for identification documents, in any medium related to its transactions and the obligations imposed by the aforementioned Law.

Suspicious Transaction Reports, their annexes, and the written justifications related to suspicious transactions for which the Compliance Officer has decided not to file a report, are strictly subject to the obligations for retention and presentation.

12. INTRA-GROUP INFORMATION SHARING

Entities within the Development and Investment Bank of Türkiye Financial Group are permitted to share information pertaining to customer due diligence, accounts, and transactions to ensure the effective implementation of compliance measures at the group level. Confidentiality provisions stipulated in specific laws shall not be applicable to such intra-group information sharing.

Employees of subsidiary entities within the group are strictly prohibited from disclosing information related to customer identification, accounts, and transactions, and they are not authorized to utilize such information for their personal gain or for the benefit of third parties.

In this context, individuals who breach confidentiality obligations shall be subject to sanctions as prescribed in the relevant legal frameworks.

The Board of Directors of the parent financial institution, along with the Financial Group Compliance Officer, is responsible for implementing necessary measures to ensure the secure sharing of the information within the group. This obligation also extends to compliance officers and the boards of directors of the subsidiary financial institutions within the group.

Financial institutions affiliated with the group are strictly prohibited from sharing any information regarding the filing of a Suspicious Transaction Report.

13. INTERNAL AUDIT

The Board of Inspectors shall conduct an annual examination and audit, through a risk-based approach, of the adequacy and effectiveness of institutional policies and procedures, risk management, monitoring and control activities, training programs, as well as the sufficiency and efficacy of the Bank's risk policy, and to ascertain whether operations are conducted in compliance with the Law, regulations, and communiques issued pursuant to the Law, in addition to institution's own policies and procedures.

In defining the scope of the audit, deficiencies identified through monitoring and control activities, along with high-risk customers, services, and transactions, shall be taken into account. The Bank shall ensure that a sufficient quantity and quality of units and transactions are audited to accurately represent the entire operation, considering the total volume of transactions.

Deficiencies, errors, and instances of misconduct identified through internal audit activities, together with corresponding opinions and recommendations aimed at preventing their recurrence, shall be reported to the Board of Directors.

In the context of internal audit operations, the Bank shall report statistics to MASAK through the Compliance Officer by the end of March of the subsequent year, including but not limited to, information concerning annual transaction volume, total personnel count, the number of branches, agents, and affiliated units, the number of audited units, the dates of such audits, the overall duration of each audit, the personnel assigned to the audits, and the number of transactions audited.

14. TRAINING POLICY

14.1. Training Activities

The Bank executes training activities aimed at preventing the laundering of proceeds of crime, financing of terrorism, and proliferation of weapons of mass destruction, ensuring that such activities are commensurate with the Bank's size, business volume, and changing conditions.

The objective of these training activities is to ensure compliance with the obligations imposed by the Law and other relevant regulations, to foster a corporate culture by enhancing the sense of responsibility among personnel concerning the Bank's policies and procedures and its risk-based approach, and to maintain current knowledge among staff. In this context, it is ensured that employees participate in training at least once a year.

While the Bank's training policy encompasses the operational aspects of training activities, the designation of responsible parties, the identification and development of participants and trainers, and the selection of training methods, it specifically stipulates that:

- Training activities shall be conducted under the supervision and coordination of the Compliance Officer;
- The Bank shall carry out training activities within the scope of an annual training program;
- The training program shall be prepared by the Compliance Officer with the participation of the Human Resources and Legal Affairs departments and submitted to the Board of Directors for approval;
- The effective implementation of the training shall be overseen by the Compliance Officer; and
- Measurement and evaluation shall be conducted following training activities; and the results shall be reviewed with the participation of relevant departments, and training shall be repeated at regular intervals based on identified needs.

To ensure the dissemination of training activities across the organization, the Bank may employ various methods such as seminars, panels, working groups, visual and auditory materials, and computer-based training via the internet or intranet.

Information and statistics regarding the training activities implemented by the Bank shall be reported to the Presidency of MASAK via the Compliance Officer by the end of March of the following year.

The duties, responsibilities, and measures required for the effective implementation of the training program are further detailed in the "UYM.08-P Compliance Procedure for Training Activities."

14.2. Training Topics.

The training to be provided to personnel by the Bank shall include the following topics:

- Concepts of laundering proceeds of crime and the financing of terrorism;
- Stages and methods of money laundering, supported by case studies;
- Legislation regarding money laundering and the financing of terrorism;
- Risk areas;
- Institutional policy and procedures;
- Within the framework of the Law and related legislation:
- Principles regarding Customer Due Diligence;
- Principles regarding Suspicious Transaction Reporting;
- Obligations of retention and presentation;
- Obligation to provide information and documentation;
- Sanctions to be applied in the event of non-compliance with obligations;

- International regulations in the field of combating money laundering and the financing of terrorism;
- Prevention of bribery of foreign public officials in international commercial transactions; and
- Prevention of the financing of the proliferation of weapons of mass destruction.

15. DUTIES AND RESPONSIBILITIES

The Board of Directors is responsible for the effective and adequate implementation of this Policy and the Compliance Program prepared within the scope of the legislation.

In this context, the Board of Directors is obliged to appoint a Compliance Officer and at least one Assistant Compliance Officer. The Board of Directors is authorized and responsible for clearly and in writing defining the authorities and responsibilities of the Compliance Officer and the Compliance Department, approving institutional policies, annual training programs, and any amendments thereto based on ongoing developments, evaluating the results of risk management, monitoring, control, and internal audit activities conducted within the scope of the compliance program, taking necessary measures for the timely remediation of identified errors and deficiencies, and ensuring that all activities under the compliance program are carried out effectively and in a coordinated manner.

The Internal Control and Compliance Department, under the supervision, audit and responsibility of the Board of Directors, shall ensure that the Bank complies with the obligations concerning the prevention of laundering proceeds of crime, the financing of terrorism, and the proliferation of weapons of mass destruction, and shall implement all activities and measures within the Bank under this policy, as well as risk management, Suspicious Transaction Reporting, monitoring, and control activities within the scope of the compliance program. Internal audit activities, on the other hand, shall be executed by the Board of Inspectors.

To ensure the effective execution of the Compliance Program, all duties and responsibilities assigned within the Bank are detailed in the "UYM.01-P Procedure on Duties and Responsibilities within the Scope of the Compliance Program."

16. MISCELLANEOUS AND FINAL PROVISIONS

16.1. Repealed Regulations

Upon the approval of this Policy, the "Regulation on Combating Laundering Proceeds of Crime and the Financing of Terrorism", which was approved by the Board of Directors' Resolution dated 07.03.2025, and numbered 2025-03-20/052, is hereby repealed.

16.2. Entry into Force

This Policy shall enter into force upon the approval of the Board of Directors. The Policy shall be renewed at least once a year to ensure continued compliance with legislation and international standards; any necessary updates shall be prepared and submitted to the Board of Directors for approval.

Subsequent amendments and updates to the Policy shall also become effective upon the approval of the Board of Directors.

16.3. Execution

The Board of Directors is responsible for the execution of the provisions of this Policy. In instances where this Policy contains no applicable provision, operations shall be conducted in accordance with the aforementioned Law, the regulations and communiques published pursuant to these Laws, and international standards.

DOCUMENT HISTORY

Revision Date	Subject of Revision	Revision No.	Revised By	Approved By
07.11.2025	Preparation of the Document	R-00	Initial Release	Board of Directors

Procedures within the Scope of the Compliance Program - Table 1
UYM.01-P Procedure on Duties and Responsibilities within the Scope of the Compliance Program
UYM.02-P Procedure on Customer Due Diligence and Identification
UYM.03-P Procedure on Compliance Risk Management Activities
UYM.04-P Procedure on Transactions of Politically Exposed Persons
UYM.05-P Implementation Procedure for the Freezing of Assets
UYM.06-P Procedure on Suspicious Transaction Reporting
UYM.07-P Compliance Procedure for the Management of Sanctions
UYM.08-P Compliance Procedure for Training Activities