

 Dünya Katılım	Policy on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism	Page 1 / 37
Doc. No.: UYB.POL.01	Date/Rev. No. 22.09.2025/02	

POLICY ON PREVENTION OF LAUNDERING PROCEEDS OF CRIME AND FINANCING OF TERRORISM

Prepared By:	Cemile Aytar Bulut
Document Owner:	Compliance Department

Revision Article:	Reason for Revision
3.1.	"Duties and Responsibilities of the Board of Directors" has been updated.
3.2.	The clause "Duties, Authorities, and Responsibilities of the Compliance Officer and Assistant Compliance Officer" has been updated.
3.5.	"Duties and Responsibilities of Bank Employees" has been updated.
4.1.1.	The clause "Risk Management" has been updated.
4.1.2.	The clause "Monitoring and Control Activities" has been updated.
4.2.	The clause "Compliance Officer and Compliance Unit" has been updated.
4.3.2.2.	The clause "Simplified Due Diligence" has been updated.
4.3.3.7.	The clause "Reliance on Third Parties" has been updated.
4.4.	The clause "High-Risk Customers" has been updated.
4.22.	The clause "Notification" has been updated.

Revoked/Revised Document	
Name:	Policy on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism
Reason for Revocation:	Revision
Document Number:	UYB.POL.01
Document Date / Rev. No:	Date/Rev. No. 19.08.2024/01

I have read this policy and its annexes, consisting of 37 pages and 7 articles, and I fully accept it as is.

Compliance Dept.	Talent and Culture Dept.	Legal Consultancy Department	Participation Banking Compliance
			
Deputy General Manager of Internal Systems	Audit Committee Resolution	Resolution of the Board of Directors	
			22.09.2025 Resolution No. 1068

 Dünya Katılım	Policy on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism	Page 2 / 37
Doc. No.: UYB.POL.01	Date/Rev. No. 22.09.2025/02	

TABLE OF CONTENTS

1. PURPOSE, BASIS AND SCOPE	3
2. DEFINITIONS	3
3. DUTIES, AUTHORIZATIONS AND RESPONSIBILITIES.....	ERROR! BOOKMARK NOT DEFINED.
3.1. DUTIES AND RESPONSIBILITIES OF THE BOARD OF DIRECTORS	8
3.2. DUTIES, POWERS AND RESPONSIBILITIES OF THE COMPLIANCE OFFICER AND ASSISTANT COMPLIANCE OFFICER.....	8
3.3. DUTIES, POWERS AND RESPONSIBILITIES OF THE COMPLIANCE UNIT.....	9
3.4. DUTIES, POWERS AND RESPONSIBILITIES OF THE INSPECTION BOARD DIRECTORATE	ERROR! BOOKMARK NOT DEFINED.
3.5. DUTIES AND RESPONSIBILITIES OF BANK EMPLOYEES	ERROR! BOOKMARK NOT DEFINED.
4. GENERAL APPLICATION PROCEDURES AND PRINCIPLES.....	10
4.1. RISK-BASED APPROACH AND RISK MANAGEMENT ACTIVITIES	10
4.1.1. Risk Management	12
4.1.2. Monitoring and Control Activities	14
4.2. COMPLIANCE OFFICER AND COMPLIANCE UNIT.....	15
4.3. GENERAL PRINCIPLES AND PROCEDURES ON CUSTOMER DUE DILIGENCE AND CUSTOMER IDENTIFICATION.....	16
4.3.1. Know Your Customer Principle	16
4.3.2. Principles on Customer Acceptance and Customer Due Diligence	17
4.3.3. Identification	19
4.3.4. Transactions Requiring Special Attention	22
4.3.5. Monitoring of Customer Status and Transactions	22
4.3.6. Taking measures against technological risks	23
4.3.7. Customer Acceptance/Rejection of Transaction and Termination of Business Relationship	23
4.3.8. Correspondent Banking Relationship	24
4.3.9. Electronic Transfers.....	24
4.3.10 Relations with Risky Countries	25
4.4. HIGH-RISK CUSTOMERS	26
4.5. PERSONS AND INSTITUTIONS NOT ACCEPTABLE AS CUSTOMERS	27
4.6. HIGH-RISK PRODUCTS AND SERVICES	28
4.7. UPDATING CUSTOMER INFORMATION	28
4.8. COMPLIANCE WITH SANCTIONS.....	30
4.8.1. Relations with Sanctioned Countries.....	30
4.9. FREEZING OF ASSETS	30
4.10. BANK ACTIVITIES ON PREVENTING THE FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION.....	31
4.11. POSTPONEMENT OF TRANSACTIONS	31
4.12. NEW PRODUCTS AND SERVICES	31
4.13. OUTSOURCING	31
4.14. SUSPICIOUS TRANSACTION REPORT (STR)	32
4.15. PROVIDING INFORMATION AND DOCUMENTS	33
4.16. PERIODICALLY REPORTING.....	ERROR! BOOKMARK NOT DEFINED.
4.17. TRAINING AND AWARENESS PROGRAMS	33
4.18. INTERNAL AUDIT ACTIVITIES	34
4.19. RETENTION AND SUBMISSION	35
4.20. ADMINISTRATIVE AND JUDICIAL FINES IN FAILURE TO COMPLY WITH THE OBLIGATIONS	35
4.21. EXCHANGE OF INFORMATION WITH LEGAL AND REGULATORY AUTHORITIES.....	35
4.22. NOTIFICATION	36
5. VIOLATION OF THE POLICY.....	36

 Dünya Katılım	Policy on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism	Page 3 / 37
Doc. No.: UYB.POL.01	Date/Rev. No. 22.09.2025/02	

6. ENTRY INTO FORCE ERROR! BOOKMARK NOT DEFINED.
7. REVIEW AND UPDATE 36

1. PURPOSE, BASIS AND SCOPE

This Policy has been formulated to ensure the Bank's compliance with legal requirements within the framework of the Law on the prevention of laundering proceeds of crime and financing of terrorism and the relevant legislation; to determine the strategies, internal controls and measures, operating rules and responsibilities for reducing the risks that may be exposed by analyzing customers, products, transactions and services with a risk-based approach; and to raise awareness of the Bank's employees on these issues.

This Policy has been prepared under the "Law on the Prevention of Laundering Proceeds of Crime", "Law on the Prevention of Financing of Terrorism", "Law on Prevention of Financing the Proliferation of Weapons of Mass Destruction", "Regulation On Measures Regarding Prevention Of Laundering Proceeds Of Crime And Financing Of Terrorism" and "Regulation on the Program for Compliance with the Obligations Regarding the Prevention of Laundering Proceeds of Crime and Financing of Terrorism" and "Regulation on Remote Identification Methods to be Used by Banks and Establishment of Contractual Relations in Electronic Environment" and other relevant legislation.

2. DEFINITIONS

Bank:	Dünya Katılım Bankası A.Ş.,
Ministry:	Republic of Türkiye Ministry of Treasury and Finance,
Presidency:	Presidency of Financial Crimes Investigation Board,
MASAK:	Financial Crimes Investigation Board
Board of Directors:	Dünya Katılım Bankası A.Ş. Board of Directors,
Audit Committee:	Committee established within the scope of the Law and the Regulation on Banks' Internal Systems and Internal Capital Adequacy Assessment Process, consisting of two members selected by the Board of Directors to assist in carrying out the oversight and monitoring activities of the Board,
Senior Management:	Bank's Board of Directors and Executive Management,
Upper Level Management:	Dünya Katılım Bankası A.Ş. General manager and assistant general managers, managers of the units within the scope of internal systems and managers of the units other than consulting units that are equivalent to assistant general manager or higher in aspect of their authorities and duties even if they are recruited under different titles,
Legislation:	Laws, Regulations, Communiqués, and other MASAK (Financial Crimes Investigation Board) regulations in force regarding the prevention of laundering proceeds of crime, the financing of terrorism, and the financing of the proliferation of weapons of mass destruction
Law No. 5549:	Law No. 5549 on the Prevention of Laundering 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
Regulations on Measures:	Regulation on Measures Regarding the Prevention of Laundering Proceeds of Crime and the Financing of Terrorism,

 Dünya Katılım	Policy on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism	Page 4 / 37
Doc. No.: UYB.POL.01	Date/Rev. No. 22.09.2025/02	

Regulations on the Program for Compliance:

Regulation on Compliance Programs for Obligations Related to the Prevention of Laundering Proceeds of Crime and the Financing of Terrorism,

Policy: Regulation on Prevention of Laundering Proceeds of Crime and Financing of Terrorism of the Bank,

Compliance Officer: An officer appointed within the Bank under the Law on the Prevention of Laundering Proceeds of Crime and the relevant legislation enacted based on the Law, authorized with the necessary powers to ensure the Bank's compliance with the obligations arising from this legislation,

Assistant Compliance

Officer: Employee appointed within the Bank with the same qualifications as the Compliance Officer to act as proxy for the Compliance Officer in case the Compliance Officer temporarily vacates his/her position due to leave, illness or similar reasons,

Compliance

Department: Department directly reporting to the compliance officer and in charge of the execution of the compliance program, taking into account factors such as the size, transaction volume, number of branches and personnel or the level of risks that the Bank may encounter to ensure that the Bank can effectively fulfill its obligations within the framework of the legislation on the prevention of laundering proceeds of crime and financing of terrorism,

Compliance Officer

Registry: The electronic database in which the records of individuals who have obtained a Compliance Officer License are maintained,

Compliance Officer License: The certificate that demonstrates the professional competence required to work as a compliance officer or an assistant compliance officer, which is issued by MASAK provided that the candidate succeeds in the qualification exam administered by MASAK and fulfills the other conditions specified in the legislation,

Compliance Program: Entire set of measures created within the Bank to prevent laundering proceeds of crime and financing of terrorism within the framework of the relevant legislation,

Obligated Party: Parties referred to in Article 4 of the Regulation Regarding Measures to Prevent Laundering Proceeds of Crime and Financing of Terrorism and their branches, agencies, representatives and commercial agents and similar affiliated business units,

FATF: The Financial Action Task Force (FATF) is an OECD organization established in 1989 by the G-7 countries to take measures to improve national legal systems, harmonize legislation, strengthen the role of the financial system and ensure continuous cooperation among member countries to prevent laundering proceeds of crime and financing of terrorism,

Risk: Possibility of financial or reputational damage suffered by the Bank or the Bank's employees due to reasons such as the utilization of the services provided by the Bank for the purpose of laundering proceeds of crime or financing of terrorism within the framework of the Compliance Program Regulation, or failure to fully comply with the

 Dünya Katılım	Policy on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism	Page 5 / 37
Doc. No.: UYB.POL.01	Date/Rev. No. 22.09.2025/02	

	obligations imposed by the Bank with the relevant Law and the regulations and communiqués issued in accordance with the Law,
Customer Risk:	The risk of abuse of the Bank as a result of enabling intensive use of cash, the purchase or sale of high value goods or the easy transfer of international funds for the business line in which the client operates; and actions of the client or those acting on behalf or account of the client for the purpose of laundering proceeds of crime or financing of terrorism,
Country Risk/	
Geographic Risk:	Risk that the Bank may be exposed to arising from its business relations and transactions with the citizens, companies and financial institutions of those announced by the Ministry from countries without adequate regulations on the prevention of laundering and financing of terrorism, that do not cooperate sufficiently in combating these crimes or that are considered risky by authorized international organizations,
Product/Service Risk:	Risk exposure in the context of non-face-to-face transactions, services such as private banking, correspondent banking or new products offered using emerging technologies,
Electronic Notification:	Notification electronically made by the Presidency within the scope of Article 9/A of Law No. 5549,
Electronic Transfer:	The transaction carried out to transfer a certain amount of money and securities from a financial institution on behalf of the originator to the beneficiary persons in another financial institution by using electronic means,
Financial Institution:	Banks, institutions other than banks authorized to issue debit cards or credit cards, authorized institutions specified in the foreign exchange legislation, financing and factoring companies, capital market intermediary institutions and portfolio management companies, payment institutions and electronic money institutions, investment trusts, insurance, reinsurance and pension companies and insurance and reinsurance brokers, financial leasing companies, institutions providing settlement and custody services within the framework of capital markets legislation, precious metals intermediary institutions, and Posta ve Telegraf Teşkilatı Anonim Şirketi (PTT) limited to banking activities,
Fund:	Any kind of goods, rights, receivables, tangible or intangible, movable or immovable the value of which can be represented by money or equivalent of money, and all kinds of documents representing them,
Account:	Any means and arrangement through which a financial institution accepts deposits of money or negotiable instruments, permits withdrawals or transfers, pays check values or payment orders, collects checks, accepts traveler's checks, payment orders, or electronic money on behalf of a natural person, or provides safe deposit box services,
Transaction:	Any purchase, sale, loan, mortgage, tax, financing, transfer, delivery, deposit, withdrawal, remittance, or disposition of funds in any currency, whether by cash, check, money order, stock, bond, or any other financial instrument, the use of a safe deposit box or any form of safe deposit box or other disposition of funds as specified in the regulations,

 Dünya Katılım	Policy on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism	Page 6 / 37
Doc. No.: UYB.POL.01	Date/Rev. No. 22.09.2025/02	

Postponement of

Transactions: Suspending or not allowing the transaction to take place,

Transactions of Complex

and Unusual Magnitude: Transactions that, within the framework of the information previously obtained about the customer and additional information obtained during the transaction request process, lead to the conclusion that there is a disproportion between the customer's financial power and the transactions made by the customer in the assessment of the risk profile or fund sources, or that the business is not compatible with the apparent economic, commercial or legal purpose of the business,

Assets: Funds and income wholly or partly owned or possessed, or directly or indirectly controlled, by a natural or legal person, and the interest and value derived therefrom or derived from the conversion thereof, and funds and income wholly or partly owned or possessed by a natural or legal person acting on its behalf or account, and the interest and value derived therefrom or derived from the conversion thereof,

Freezing of Assets: Removal or restriction of the power of disposition over the assets in order to prevent the disposal, consumption, conversion, transfer, assignment, transfer and assignment of the assets and other dispositive transactions,

Proceeds of Crime: Money, all kinds of negotiable instruments and goods and all benefits obtained by committing crimes that require a lower limit of six months or more imprisonment,

Laundering Proceeds

of Crime: Activity of subjecting funds or revenues obtained from crimes punishable with a lower limit of imprisonment of more than six months to various transactions in order to conceal their true source or to give the impression that they were obtained through legitimate means,

Suspicious Transaction: Presence of any information, suspicion or reason for suspicion that the assets subject to the transaction made or attempted to be made in or through the obliged entities were obtained illegally or used for illegal purposes, used for acts of terrorism or used by terrorist organizations, terrorists or terrorist financiers, or related or connected to them,

Suspicious Transaction

Report (STR): Notification to be made to the Presidency in the event that there is any information, suspicion or suspicion that the assets subject to the transactions made or attempted to be made in or through the Bank have been obtained illegally or used for illegal purposes.

Permanent Business

Relationship: A business relationship established between the obliged party and the customer due to services such as account opening, credit or credit card issuance, safe deposit box, financing, factoring, financial leasing, leasing, life insurance or private pension, which is continuous in nature,.

Politically Exposed Person (PEP):

Persons holding senior public positions in Türkiye or in a foreign country, currently or in the past, such as heads of state or government, senior politicians, senior officials of public institutions, judicial authorities or military authorities, senior executives of state-owned enterprises, senior executives of political parties, persons holding important positions in international organizations (managers, deputy

 Dünya Katılım	Policy on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism	Page 7 / 37
Doc. No.: UYB.POL.01	Date/Rev. No. 22.09.2025/02	

	managers, board members, etc.), their family members, including second-degree family members and persons with whom they are closely related, and persons who are their beneficial owners,
Real Beneficiary:	Real person or persons having ultimate control over, or ultimate influence over, the natural person or natural persons, legal entities or unincorporated entities on whose behalf transactions are carried out before the obliged party,
Shell Bank:	The bank which does not have any physical office in any country, does not employ full time staff and is not subject to control and authorization of an official authority in terms of banking transactions and registrations,
Terrorist:	A natural person residing in Türkiye or abroad who commits a terrorist act directly or indirectly; who is complicit in a terrorist act; who organizes or directs others to commit a terrorist act; who intentionally helps a person or a group acting with a common purpose to commit a terrorist act,
Terrorism:	Acts carried out with the aim of intimidating a population or forcing a government or an international organization to perform or refrain from performing an act. The Law No. 3713 on Anti-Terrorism defines terrorism as the use of coercion, intimidation, suppression, deterrence and threats by force and violence in order to "change the characteristics of the Republic, political, legal, social, secular, economic order, to disrupt the indivisible integrity of the State with its country and state, to endanger the existence of the State and the Republic, to weaken, destroy or seize the state authority, to destroy fundamental rights and freedoms, to disrupt the internal and external security of the state, to disrupt public order or public health".
Crime of Financing of Terrorism:	Providing or collecting funds to a terrorist or terrorist organizations, knowing and willing that they will be used or will be used in the performance of the acts prohibited in Article 3 of the Law No. 6415 on the Prevention of Financing of Terrorism,
Terrorist Organization:	Terrorist group in Türkiye or abroad that commits the acts included in the definition of terrorism,
OFAC:	(Office of Foreign Assets Control) The US Treasury Department's Office of Financial Intelligence and Sanctions

 Dünya Katılım	Policy on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism	Page 8 / 37
Doc. No.: UYB.POL.01	Date/Rev. No. 22.09.2025/02	

3. DUTIES, POWERS AND RESPONSIBILITIES

All employees, including the Bank's Senior Management, are responsible for fulfilling their duties, powers and responsibilities and carrying out their activities in compliance with the legislation and this Policy and other internal regulations of the Bank within the scope of preventing laundering of proceeds of crime 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 within the scope of this Policy are as follows:

- Ensure that the entire compliance program is established and executed in an adequate and effective manner in accordance with the scope and characteristics of the Bank's activities,
- Establish the Compliance Department, appoint the Compliance Officer and the Assistant Compliance Officer,
- Ensure that the powers and responsibilities of the Compliance Officer and Compliance Directorate are clearly defined in writing,
- Approve the Bank's policies
- Ensure that the Bank's personnel participate in the training programs within this scope and approve the changes to be made in these programs according to the developments in the legislation,
- Assess the results of risk management, monitoring and control and internal audit activities carried out within the scope of the compliance program,
- Take the necessary measures to eliminate the identified errors and deficiencies in a timely manner,
- Ensure that all activities within the scope of the compliance program are conducted effectively and in coordination,
- Monitor the activities and effectiveness of the Compliance Department.

3.2. Duties, Powers and Responsibilities of the Compliance Officer and Assistant Compliance Officer

The duties, powers and responsibilities of the Compliance Officer within the scope of this Policy are as follows:

- Formulate the Bank's regulations and procedures regarding the prevention of laundering proceeds of crime and combating the financing of terrorism within the framework of this Policy and legal regulations, submit the regulations to the Board of Directors for approval and monitor their implementation,
- Monitor and announce national and international regulations on the prevention of laundering proceeds of crime and financing of terrorism to the Bank, and ensure that this Policy and its amendments are accessible to all personnel,

 Dünya Katılım	Policy on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism	Page 9 / 37
Doc. No.: UYB.POL.01	Date/Rev. No. 22.09.2025/02	

- Create risk management, monitoring and control policies for the business and transactions within the scope of this Policy and carry out studies to improve the process by evaluating the findings identified in the audits and controls carried out,
- Evaluate potentially suspicious transactions communicated to him/her or which he/she learns ex officio, and ensure that the transactions deemed to be suspicious are reported to the Presidency within the periods specified in the legislation,
- Take necessary measures to ensure the confidentiality of notifications and other matters falling within the scope of its duties,
- Conduct the necessary studies to ensure the Bank's compliance with the published regulations within the scope of the relevant legislation and ensure the necessary communication and coordination with the Presidency,
- Present the work on the training program for the prevention of laundering proceeds of crime and financing of terrorism to the Board of Directors for approval and monitor the effective implementation of the approved training program,
- Keep information and statistics on internal audit and training activities on a regular basis and send them to the Presidency within the periods specified in the legislation,
- Prepare the reports to be made to MASAK and other official institutions in accordance with the legislation or ensure that they are prepared by the relevant units,
- Act in good faith, reasonably and honestly, with an impartial and independent will while fulfilling its duties and responsibilities,
- Be registered in the Compliance Officer Registry and to meet the licensing conditions specified in the legislation regarding the non-revocation or non-suspension of the Compliance Officer License,
- Notify MASAK in writing, together with the reasons thereof, within ten days from the date of resignation or dismissal, in the event of removal from office or resignation as the compliance officer or assistant compliance officer.

3.3. Duties, Powers and Responsibilities of the Compliance Department

The duties, powers and responsibilities of the Compliance Directorate within the scope of this Policy are as follows:

- Follow up the legislative practices within the scope of this Policy, respond to the questions submitted by the Bank's employees regarding the legislation, and notify the relevant departments of the Bank in order to evaluate the risks that may arise in connection with legislative changes,
- Follow up the compliance of all activities, new services and products that the Bank performs and plans to perform with the relevant legislation,
- Announce the notifications made by official institutions regarding the legislation within the scope of this Policy and legislative amendments to the Bank in electronic environment,

 Dünya Katılım	Policy on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism	Page 10 / 37
Doc. No.: UYB.POL.01	Date/Rev. No. 22.09.2025/02	

3.4. Duties, Powers and Responsibilities of the Audit Department

The duties, powers and responsibilities of the Inspection Board Directorate within the scope of this regulation are as follows:

- Review and report on the adequacy and effectiveness of the Bank's internal regulations, risk management, monitoring, control and training activities for the prevention of laundering proceeds of crime and combating the financing of terrorism annually and with a risk-based approach,
- Consider, within the framework of the relevant legislation, the customers, services, transactions and units to be audited that involve risk and the deficiencies identified in monitoring and control activities in the preparation of the annual audit plan,
- Forward the data regarding the internal audit activities carried out within the scope of the compliance program to the Compliance Officer.

3.5. Duties, Powers and Responsibilities of Bank Employees

The duties, powers and responsibilities of the Bank's employees within the scope of this Policy are set out below:

- Participate in training activities to be organized for the prevention of laundering proceeds of crime and financing of terrorism,
- Learn, understand and comply with the relevant laws and legal regulations related to these laws and the relevant internal regulations of the Bank,
- Notify the Compliance Officer in case of any suspicious situation within the scope of laundering crime and terrorist financing while performing banking transactions,
- Act within the framework of the principles of customer due diligence and customer identification described in this Policy and the Bank's internal regulations in all Banking transactions, particularly customer transactions.
- Provide the necessary support to the Compliance Department staff while performing their duties, and to submit all kinds of information and documents requested within the scope of the legislation on the prevention of laundering proceeds of crime, the financing of terrorism, and the financing of the proliferation of weapons of mass destruction in a timely, complete, and accurate manner.

4. GENERAL APPLICATION PROCEDURES AND PRINCIPLES

4.1. Risk-Based Approach and Risk Management Activities

The purpose and scope of risk management activities within the framework of this Policy is to ensure that necessary measures are taken to identify, rate, classify, monitor, evaluate and mitigate the risks that the Bank may be exposed to. The core principle of the Bank is to implement a proactive risk-based approach to the prevention of money laundering and financing of terrorism.

Determining a risk-based approach implies defining a risk management process for combating the laundering proceeds of crime and the financing of terrorism. This process includes identifying and assessing risks and developing strategies to manage and mitigate those risks. The Bank aims, with the compliance risk methodology, to establish an indicator of the general risk level of customers with

 Dünya Katılım	Policy on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism	Page 11 / 37
Doc. No.: UYB.POL.01	Date/Rev. No. 22.09.2025/02	

whom the Bank has a continuous business relationship within the framework of risk factors related to laundering of the proceeds of crime and the financing of terrorism. In this way, standard customer acceptance procedures are applied to less risky customers, while more risky customers are given due attention. Using the compliance risk methodology, a risk-based approach to customer acceptance is followed, with additional approval and control processes applied to the acceptance of high-risk customers, using enhanced customer acceptance practices for higher-risk customers. Risks related to the laundering of proceeds of crime and financing of terrorism to which the Bank may be exposed as a result of its customers, activities, products, and transactions are classified according to the following categories;

- Country Risk,
- Service Risk,
- Customer Risk

Country Risk: refers to the risk that the Bank may be exposed to arising from its business relations and transactions with the citizens, companies, and financial institutions of those announced by the Ministry from countries without adequate regulations on the prevention of laundering and financing of terrorism, that do not cooperate sufficiently in combating these crimes or that are considered risky by authorized international organizations.

Service Risk: refers to the risk that the Bank may be exposed to within the scope of transactions that are not carried out face-to-face or new products to be offered using developing technologies.

Customer Risk: refers to the risk of abuse of the obliged entities due to the fact that the line of business in which the customer operates allows for the intensive use of cash, the purchase and sale of high-value goods or the easy realization of international fund transfers; the customer or those acting on behalf or account of the customer act for the purpose of laundering proceeds of crime or financing of terrorism.

While making risk assessment within the framework of the relevant legislation, the Bank's customers, products/services and transactions are rated as follows:

- High Risk
- Medium Risk
- Low Risk

Taking into account the customer's profession, business history, activities, financial status, accounts, and transactions, as well as the country where they are domiciled or operate, and other similar relevant up-to-date information and indicators, customers' risk profiles are determined as high, medium, and low in terms of the laundering of proceeds of crime and the financing of terrorism, and they are subjected to monitoring and control activities based on these risk profiles.

The acceptance of high-risk customers to the Bank is governed by both a more rigorous customer acceptance process and a different approval mechanism than other rating types. Strengthened measures, including ongoing monitoring and annual updates of customer information, are implemented for high-risk customers.

The Bank may decide to accept, mitigate or avoid risks depending on the degree of risks identified as a result of risk assessments.

 Dünya Katılım	Policy on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism	Page 12 / 37
Doc. No.: UYB.POL.01	Date/Rev. No. 22.09.2025/02	

In order to protect against risks related to prevention of laundering proceeds of crime and prevention of financing of terrorism and to continuously monitor, control and report the execution of activities in accordance with the legislation and internal regulations; the Bank establishes monitoring, control and reporting activities by taking into account the size of the Bank, the volume of business and the nature of the transactions performed.

The Bank's risk management activities within the scope of this Policy are shaped as follows:

- Developing methods for risk identification, rating, classification, and assessment based on customer risk, service risk, and country risk,
- Rating and classification of 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 way to alert the relevant units; developing appropriate operating and control rules to carry out the transaction with the approval of the higher authority and to audit it when necessary,
- A retrospective review of the consistency and effectiveness of risk identification and assessment methods, risk rating and classification methods, using case studies or actual transactions, and the re-evaluation and updating of these methods based on the results obtained and changing circumstances
- Carrying out the necessary development activities by following the recommendations, principles, standards and guidelines introduced by national legislation and international organizations regarding the issues falling within the scope of risk,
- Reporting of risk monitoring and evaluation results to the Board of Directors on a regular basis,

The Bank adopts a risk-based approach within the scope of the relevant legislation and internal regulations. Risk management activities reveal the Bank's fundamental approach to measures against activities regarding the laundering of the proceeds of crime and financing of terrorism.

4.1.1. Risk Management

The necessary measures are taken to mitigate existing risks and prevent potential risks within the Bank within the scope of preventing the laundering proceeds of crime and combating the financing of terrorism. The Bank may decide to accept, mitigate or avoid risks depending on the degree of risks identified as a result of risk assessments. The Bank, as a principle, provides that risks related to the laundering proceeds of crime and financing of terrorism are approached with high sensitivity by all employees and reasonable measures are taken to mitigate these risks. With the aim of reducing the risk to be undertaken for groups with a risk profile determined as high risk as a result of the risk assessment, the Bank implements one or more or all of the following measures in proportion to the risk identified:

- a) Obtaining additional information about the customer and update the credentials of the customer and the beneficial owner more frequently,
- b) Obtaining additional information about the nature of the business relationship,
- c) Obtaining as much information as possible about the source of the assets subject to the transaction and the funds belonging to the customer,

 Dünya Katılım	Policy on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism	Page 13 / 37
Doc. No.: UYB.POL.01	Date/Rev. No. 22.09.2025/02	

- d) Obtaining information about the purpose of the transaction,
- e) Making the entry into a business relationship, the continuation of an existing business relationship or the execution of a transaction subject to the approval of a senior official,
- f) Increasing the number and frequency of controls applied and keeping the business relationship under close supervision by identifying the types of transactions that require additional controls,
- g) Requiring that in the establishment of a permanent relationship the first financial transaction is carried out through another financial institution subject to customer due-diligence principles.

In the establishment of business relationships and other transactions requiring identification with crypto asset service providers, the measures specified in paragraphs (c), (d), and (e) of the first paragraph shall be applied at a minimum; furthermore, appropriate measures aimed at determining thresholds for amounts and the number of transactions shall be taken. At the same time, the establishment of business relationships with crypto asset service providers by the Bank shall be subject to the approval of a senior management official.

In the event that there is a payment service executed through a terminal provided within the scope of paragraphs (a) and (b) of the first paragraph of Article 12, and the payment instrument acceptance service specified in paragraph (c) thereof, of the Law No. 6413 on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions dated 20/6/2013 (terminal service); the measures specified in paragraphs (a) to (g) among the above-mentioned measures shall be applied at a minimum in the establishment of business relationships with the customer (merchant) and other transactions requiring identification. The measure specified in paragraph (g) may not be applied by the Bank. It shall be regularly controlled whether the subject terminals are used in accordance with the purpose of the business relationship or whether they are made available to other persons except in cases permitted by the relevant legislation; within this scope, in the event that any non-compliance is detected, necessary measures shall be taken, including the termination of the business relationship.

Taking into account the risks identified within the scope of the national risk assessment, risk management activities also cover efforts directed towards the risks of violation, non-implementation, and evasion of asset freezing decisions within the scope of Law No. 6415 and Law No. 7262, as well as enhanced controls for the implementation of the subject sanctions. Within this scope, measures aimed at the continuous monitoring of customers and transactions are taken by taking into consideration the asset freezing decisions and potential matching criteria.

The Bank takes the required measures against circumstances that may create incompatibility with its obligations and in cases where the risk of laundering proceeds of crime, financing of terrorism and violation of sanctions is high or unmanageable, the Bank does not establish a business relationship, terminates the existing business relationship or refuses to carry out the transaction. Within this framework, the Bank acts in line with the following principles in order to limit the risk:

- Does not open accounts with anonymous or imaginary names.
- Does not establish a business relationship in cases where identity verification cannot be performed or sufficient information about the purpose of the business relationship cannot be obtained,

 Dünya Katılım	Policy on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism	Page 14 / 37
Doc. No.: UYB.POL.01	Date/Rev. No. 22.09.2025/02	

- Does not establish business relationships with persons operating in fields such as casinos, online lotteries, lottery draws, betting operations, which may be a potential source of laundering of the proceeds of crime.
- Does not establish business relations with persons included in the sanction lists.
- Does not perform transactions that are related to sanctioned countries and that are contrary to sanctions.
- Does not establish a relationship with banks that are shell banks or banks that lend their accounts to shell banks.
- Does not engage in business relations with organizations where the beneficial owner cannot be identified and confirmed.
- Does not enter into business relationships with those who are engaged in activities that may damage the Bank's reputation, such as illegal arms and ammunition trade, drugs, narcotics, human trafficking, adult entertainment, gambling.
- Screening the customer, the actual beneficiary of the account, persons associated with the account (partner/shareholder, proxy, authorized person, etc.) against sanctions lists.

4.1.2. Monitoring and Control Activities

The Bank performs monitoring, control and reporting activities, by taking into account the Bank's size, business volume and the nature of the transactions carried out, for the purpose of protecting the Bank from risks related to the prevention of laundering proceeds of crime and financing of terrorism and continuously monitoring, controlling and reporting whether its activities are carried out in accordance with the legislation and internal regulations.

The personnel who will carry out monitoring and control activities at the Bank are provided with access to the Bank's internal information sources. Risk monitoring and assessment outcomes are reported to the Board of Directors at regular intervals. Monitoring and control activities carried out within the Bank cover the following issues at a minimum level:

- Monitoring and control of high risk customers and transactions,
- Monitoring and control of transactions with risky countries,
- Monitoring and control of complex and unusual transactions,
- Controlling whether the transactions above the amount to be determined by the Bank according to the risk policy are compatible with the customer profile through sampling method,
- Monitoring and control of connected transactions exceeding the amount requiring identification (including transactions made independently of the account),
- Checking mandatory information and documents that must be kept electronically or in writing about customers, as well as information that must be included in electronic transfer messages, and ensuring that deficiencies are completed and updated,

 Dünya Katılım	Policy on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism	Page 15 / 37
Doc. No.: UYB.POL.01	Date/Rev. No. 22.09.2025/02	

- Monitoring whether the customer's transactions are in line with information about the customer, its business, risk profile and funding sources on an ongoing basis throughout the business relationship,
- Control of transactions carried out using systems that enable non-face-to-face transactions,
- Risk-oriented control of services vulnerable to abuse due to new products and technological developments.

In context, monitoring and control activities are executed within the Compliance department. Within the framework of central monitoring and control activities conducted by Compliance department, technological opportunities shall be utilized in the monitoring and control of the customers and transactions and detection of suspicious transactions.

Monitoring and control activities, by taking into account the risks identified within the scope of the national risk assessment, also cover efforts directed towards the risks of violation, non-implementation, and evasion of asset freezing decisions within the scope of Law No. 6415 and Law No. 7262, as well as enhanced controls for the implementation of the subject sanctions. Within this scope, measures aimed at the continuous monitoring of customers and transactions are taken by taking into consideration the asset freezing decisions and potential matching criteria.

The Inspection Board Directorate supervises the execution of the compliance program within the framework of the applicable legislation and the Bank's internal regulations. Deficiencies detected as a result of these controls conducted for compliance with the obligations shall be notified to the Compliance Officer. Data containing information on the activities carried out within this scope are reported to MASAK by the Compliance Officer.

4.2. Compliance Officer and Compliance Department

The Compliance Department of the Bank is structured as the Internal Control and Compliance Directorate and reports to the Board of Directors. The Compliance Officer and the Assistant Compliance Officer, bearing the conditions and qualifications required for the Compliance Officer and subject to the same term and procedures as the Compliance Officer in terms of appointment, shall be determined to have sufficient seniority, knowledge and power to fulfill their responsibilities independently. The Bank shall send such appointments to the Presidency within ten days at the latest from the date of appointment.

The appointment, dismissal, delegation of authority and deputization of the Compliance Officer and Assistant Compliance Officer shall be carried out in accordance with the conditions, procedures and periods sought in the Compliance Program Regulation. The Bank checks through the Compliance Officer Registry whether the persons to employ as compliance officers or assistant compliance officers are registered in the registry and that their licenses are not suspended, prior to signing the employment contract and throughout the period of service.

The Compliance Unit is audited by various independent parties, including internal and external auditors and regulators.

 Dünya Katılım	Policy on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism	Page 16 / 37
Doc. No.: UYB.POL.01	Date/Rev. No. 22.09.2025/02	

4.3. General Principles and Procedures on Customer Due Diligence and Customer Identification

4.3.1. Know Your Customer Principle

Customer due diligence is ensured when the Bank has sufficient information about its customers and their activities and obtains this information. The Know Your Customer Principle also aims to recognize complex and unusual transactions or activities that are not commensurate with the customers' known business.

The Compliance Officer is authorized to request the refusal to accept a real or legal person as a customer or the termination of a continuous business relationship with an existing customer in any case due to the risks of laundering and terror financing within the framework of the Bank's customer acceptance policy. Within the scope of the Know Your Customer Principle, necessary measures are taken within the framework of the legislation in force and the Bank's internal regulations on;

- Providing sufficient information about the purpose and nature of the requested transaction
- Identification
- Identification of those acting on behalf of others
- Verification of the authenticity of the confirmation documents
- Identification in subsequent operations
- Identification of whether someone else is acting on behalf of someone else and identification of those acting on behalf of someone else
- Identification of the real beneficiary
- Taking necessary measures for customers, activities and transactions that require special attention
- Monitoring the status and transactions of the customer throughout the business relationship
- Taking measures against technological risks
- Trust in the third party
- Refusal of the transaction and termination of the business relationship
- Correspondent relationship
- Electronic transfers
- Relations with risky countries
- Implementation of simplified measures
- Implementation of enhanced measures

in establishing a continuous business relationship and realizing the transactions requested.

 Dünya Katılım	Policy on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism	Page 17 / 37
Doc. No.: UYB.POL.01	Date/Rev. No. 22.09.2025/02	

4.3.2. Principles on Customer Acceptance and Customer Due Diligence

The Bank provides information to get to know the customer when establishing a new business relationship. It also imposes enhanced measures on customers classified as high-risk based on risk assessment.

4.3.2.1 Measures for Standard Customer Due Diligence

Customer due diligence includes, at a minimum, the following aspects:

- Complete and accurate identification and confirmation of the customer,
- Full and accurate realization of the identity information of the persons associated with the customer,
- Determining the real beneficiary and confirming their identity through reliable documents and information,
- Obtaining information about the purpose and nature of the business relationship
- Obtaining information about the customer's profession/sector of activity, main income generating business, source of wealth, expected transaction volume, etc. within the scope of know your customer,
- Obtaining a declaration from the customer that he/she is the beneficial owner of the account,
- Checking sanction lists of customers and the persons associated with the customer,
- Providing any required additional information, including the fund source,
- Constant account monitoring,
- Updating the customer's diagnostic information based on the customer's risk profile.

 Dünya Katılım	Policy on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism	Page 18 / 37
Doc. No.: UYB.POL.01	Date/Rev. No. 22.09.2025/02	

4.3.2.2. Simplified Measures

Provided that the customer's risk score is low, the Bank may apply simplified customer due diligence measures with a risk-based approach in the following cases:

- Transactions Performed by Financial Institutions Amongst Themselves
- Transactions where Banks are the Customers of the Obligated Parties other than Financial Institutions
- Transactions where the Customer is a Public Administration or a Professional Organization Qualified as a Public Institution
- Transactions where the Customer is an International Organization or an Embassy or Consulate Resident in Türkiye
- In Establishing a Business Relationship within the Scope of Salary Payment Agreement By Accepting a Batch of Customers
- Transactions Regarding Salary Payments of Members of Embassies or Consulates of International Organizations in Türkiye:
- Transactions where the Customer is a Listed Company
- Transactions Regarding Prepaid Cards

Simplified measures should be consistent with the risk factors in the Bank's internal regulations. These measures include, but are not limited to, the following:

- Being able to verify the customer's and the beneficial owner's identity after the establishment of a business relationship,
- Updating customer data at longer intervals than the standard information update frequency,
- Implementation of simplified and periodic monitoring and verification,
- Not obtaining detailed information or applying specific measures to understand the purpose and nature of the business relationship when the existing business relationship and transactions provide sufficient information.

Where a transaction may pose a risk of laundering or financing of terrorism, the Bank shall not apply simplified measures and considers that the transaction may be a suspicious transaction.

4.3.2.3 Enhanced Due Diligence (Enhanced Measures)

The Bank implements one, more, or all of the following measures in a proportionate manner to the identified risk in transactions within the scope of Transactions Requiring Special Attention, Taking Measures Against Technological Risks, Relations with Risky Countries, and high-risk situations identified within the framework of the risk-based approach. The bank also takes reasonable measures to determine whether the beneficial owner is a politically exposed person (PEP) and implements one or more, or all of the following measures, including those specified in the MASAK General Circular No. 21:

 Dünya Katılım	Policy on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism	Page 19 / 37
Doc. No.: UYB.POL.01	Date/Rev. No. 22.09.2025/02	

- Obtaining additional information about the customer and update the credentials of the customer and the beneficial owner more frequently,
- Obtaining additional information about the nature of the business relationship,
- Obtaining as much information as possible about the source of the assets subject to the transaction and the funds belonging to the customer,
- Obtaining information about the purpose of the transaction,
- Making the entry into a business relationship, the continuation of an existing business relationship or the execution of a transaction subject to the approval of a senior official,
- Increasing the number and frequency of controls applied and keeping the business relationship under close supervision by identifying the types of transactions that require additional controls,
- Requiring that in the establishment of a permanent business relationship, the first financial transaction must be made from another financial institution to which the principles of customer due diligence apply/

4.3.3. Identification

The customer, as the source of the suspicious transaction, is the key focus in laundering proceeds of crime and the financing of terrorism. Therefore, customer identification is very important in the fight against proceeds of illegal activity. Pursuant to the third section of the Regulation on Measures under the heading "Principles Regarding Customer Due Diligence", the obligation to recognize customers starts with the identification step. Identification is carried out in the following cases as regulated in the relevant legislation:

- Regardless of the monetary amount in establishing an ongoing business relationship,
- When the amount of a single transaction or the total amount of multiple linked transactions is at or above the amount specified in the legislation,
- When the amount of a single transaction or the total amount of multiple linked transactions in electronic transfers is at or above the amount specified in the legislation,
- Regardless of the monetary amount in cases requiring suspicious transaction reporting,
- Regardless of the monetary amounts when there is doubt about the adequacy and accuracy of previously obtained customer identification information.

A permanent employment relationship may also be established by using remote identification methods to the extent permitted by the legislation or by identification through a notarized power of attorney.

By obtaining identity information, verifying its accuracy, and revealing the real beneficiary of the transaction, the Bank takes the necessary steps to identify its customers and those acting on their behalf or on their behalf of its customers. Identification shall be completed prior to the establishment of a business relationship or transaction. The obligation of customer due diligence is not limited to the identification of the customer. In cases where the Bank is unable to establish identification, no business relationship shall be established and the Bank shall not fulfill the transactions requested.

 Dünya Katılım	Policy on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism	Page 20 / 37
Doc. No.: UYB.POL.01	Date/Rev. No. 22.09.2025/02	

In establishing a permanent employment relationship, information is also obtained about the purpose and nature of the employment relationship.

The general rule is that no business relationship shall be established and no transactions requested by the parties shall be carried out until the identity of the potential customer has been duly established or until sufficient knowledge of the purpose of the business relationship has been obtained. Similarly, the business relationship is terminated in the event that the required identification and verification cannot be made due to doubts about the adequacy and accuracy of the customer identification information previously obtained.

The procedures and principles regarding the identification of the customer are set out in the Identification Application Principles based on MASAK legislation.

4.3.3.1 Identification Methods

The Bank performs identification procedures in compliance with face-to-face or remote identification methods in accordance with the relevant legislation.

4.3.3.2 Identification of Those Acting on behalf of Others

In the event that a transaction is requested on behalf of legal entities or entities without legal personality by persons authorized by persons authorized to represent them, on behalf of natural person customers by other natural persons, on behalf of minors and restricted persons by their legal representatives, the identification of these persons shall be carried out in accordance with the Regulation on Measures.

Upon the submission of the originals or notarized copies of the documents to be presented when requested by the authorities, a readable photocopy or electronic image is taken or information regarding the identity is recorded.

4.3.3.3. Verification of The Authenticity of the Confirmation Documents

In case of doubt about the authenticity of the documents used to confirm the information received within the scope of identification to the extent possible, the authenticity of the document shall be verified by contacting the person or institution that issued the document or other competent authorities.

4.3.3.4. Customer Identification in Subsequent Transactions

In order to maintain the accuracy of the information within the scope of identification and to verify the customer's identification in subsequent transactions requiring identification during the course of an ongoing business relationship, necessary steps are performed.

4.3.3.5. Customer Identification of Those For the Benefit of Others

The Bank takes the necessary measures to determine whether a person is acting for the benefit of other persons. In case that persons making a transaction requiring identification are acting for the benefit of another person, they are legally required to notify the Bank. However, in the establishment of a permanent business relationship, in all cases, a declaration must be obtained as to whether the customers are acting for the benefit of others. In the event that the person declares acting for the benefit of others or this is determined by the Bank, the person on whose account the transaction is made must be duly identified along with the person who made the transaction. Where a person is suspected of acting in his or her own behalf but for the benefit of another person, despite the person's

 Dünya Katılım	Policy on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism	Page 21 / 37
Doc. No.: UYB.POL.01	Date/Rev. No. 22.09.2025/02	

declaration that he or she is not acting for the benefit of another person, measures to identify the real beneficiary are implemented.

4.3.3.6. Identification of The Real Beneficiary (Ultimate Beneficial Owner)

Necessary measures are taken to identify the beneficial owner of the transaction.

The real beneficiary refers to the natural person or persons who ultimately control individuals transacting with the Bank, the individual on whose behalf transactions is conducted, or the natural person or persons who ultimately control or have ultimate influence over legal entities or unincorporated entities without legal personality. The Bank is obliged to take the necessary measures to determine whether the transaction was made on behalf of someone else and the identity of the real beneficiary of the transaction. The real beneficiary must be a real person according to its definition. In determining the real beneficiary for legal entities, the concepts of ownership (shareholding relationship), senior representation, and ultimate control come to the fore.

In some customers, a real beneficiary is a real person holding a majority stake in the company, while in other companies, holding a majority stake may not actually confer ultimate control or influence over the company. Therefore, in determining the real beneficiary in the case of legal entities registered in the commercial register, Customer Representatives should focus on identifying the persons who actually control or have influence over the company and consider each customer on an individual basis, while adhering to the following regulatory rules. In this scope, the following issues should also be complied with in accordance with the relevant regulations. In addition to the issues listed below, the verification of the identity information required to be obtained within the scope of the identification of legal entity shareholders residing abroad is carried out by confirming it through officially approved documents.

- In establishing a permanent business relationship with legal entities registered in the trade registry, the identification of the real person partners of the legal entity with shares exceeding twenty-five percent is determined in order to identify the real beneficiary.
- In case it is suspected that the natural person partner of the legal entity with a shareholding exceeding twenty-five percent is not the real beneficiary or there is no natural person partner with such a shareholding, necessary measures are taken to identify the real person or persons who ultimately control the legal entity. The identified real person or persons are considered as real beneficiaries.
- Necessary measures are taken to reveal the real person or persons who ultimately control other legal entities and unincorporated entities within the scope of permanent business relationship. Identification information about the identified real beneficiary is obtained, and necessary measures are taken to confirm this information. In this scope, notarized signature circulars containing identity information can be used. In establishing a permanent business relationship with legal entities registered in the trade registry, the identity of the legal entity's legal entity partners with shares exceeding twenty-five percent shall also be determined.
- In cases where the real beneficiary cannot be identified, the business relationship is not established, the existing business relationship is restricted or terminated, the desired transaction is refused and whether a suspicious transaction reporting is required is evaluated.

4.3.3.7. Trust for Third Party

The Bank may establish a business relationship or conduct a transaction in reliance on the measures taken by another financial institution in relation to the customer in order to determine the identity of

 Dünya Katılım	Policy on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism	Page 22 / 37
Doc. No.: UYB.POL.01	Date/Rev. No. 22.09.2025/02	

the customer, the person acting on behalf of the customer and the real beneficiary and to obtain information about the purpose of the business relationship or transaction. In this situation, the ultimate responsibility within the scope of the Law and the relevant regulations will rest with the financial institution that performs the transaction by relying on the third party. Being able to trust a third party depends on the following:

- Ensuring that the third party has taken the necessary measures to ensure the requirements of identification, retention of records, and customer due diligence, and in the case of a non-resident, that it is also subject to regulations and inspections in accordance with international standards on the prevention of laundering proceeds of crime and financing of terrorism,
- Ensuring that all necessary information within the scope of knowing the customer can be obtained immediately from the third party when requested,
- That certified copies of documents regarding identification and other documents within the scope of customer due diligence, and their digital images in the event that an ongoing business relationship is established via remote identification by a trusted institution, shall be immediately obtained from the third party upon request,
- Ensuring that the third party is regulated and audited for compliance with requirements relating to the identification, record retention, and customer due diligence and that adequate measures are in place to comply with these requirements,
- Ensuring that there are adequate measures taken for confidentiality in the exchange of information by the third party,
- Ensuring that the identification of the customer, whose information is shared, has not been performed under simplified measures by the third party.

In the event that a business relationship is established by relying on a third party, the customer's identification information is immediately obtained from the third party. The Bank's transactions with other banks on behalf of its customers, and the relations between the Bank's agencies and similar units and the persons to whom they have services rendered as extensions or complements of the main service units are not within the scope of the principle of trust in third parties.

The trust on third party principle does not apply if the third party is resident in risky countries.

4.3.4. Transactions Requiring Special Attention

The Bank pays special attention to complex and unusually large transactions, transactions and activities without any apparent reasonable legal and economic purpose, and transactions or activities that are believed to be linked to laundering proceeds of crime and financing of terrorism or that are actually intended or attempted to be carried out for this purpose. The Bank takes the necessary measures to obtain sufficient information about the purpose of the requested transaction and keeps the information, documents, and records obtained within this scope to be submitted to the authorities upon request.

4.3.5. Monitoring of Customer Status and Transactions

The Bank takes the necessary measures to monitor and update whether the transactions carried out by the customers are compatible with the information on the customers' profession, commercial activities, business history, financial status, risk profile and fund sources with a risk-based approach. In addition, the accuracy of the information regarding the telephone and fax numbers and e-mail

 Dünya Katılım	Policy on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism	Page 23 / 37
Doc. No.: UYB.POL.01	Date/Rev. No. 22.09.2025/02	

addresses received for the identification of these customers is verified by contacting the relevant person using these tools when necessary within the framework of a risk-based approach. It establishes an appropriate risk management system for this purpose.

4.3.6. Taking measures against technological risks

The Bank exercises special care and takes appropriate measures to prevent the risk that the use of new and emerging technologies, existing and new products and new business practices, including new distribution channels, may be used for laundering proceeds of crime and financing of terrorism.

Within this framework, the Bank pays special attention to transactions such as deposits into and withdrawals from and electronic transfers made through electronic banking channels, closely monitors transactions incompatible with or unrelated to the customer's financial profile and activities, and takes appropriate and effective measures, including setting limits on the amount and number of transactions.

4.3.7. Customer Acceptance/Rejection of Transaction and Termination of Business Relationship

In cases where customer identification cannot be made or sufficient information cannot be obtained about the purpose of the business relationship, a business relationship is not established with the customer. However, in case of a situation where the accuracy of a previous identification is in doubt, if a new identification is requested from the customer but the request is rejected, the Bank terminates the business relationship within the legal limits and in accordance with the Bank's regulations and MASAK regulations.

In cases where the business relationship cannot be terminated due to a credit relationship, existence of a lien, attachment or similar legal restriction, or similar reasons, the customer's new transaction requests shall not be accepted. The Compliance Officer is consulted on the matter when necessary. In the event that the request to establish a business relationship with a potential customer is rejected due to risks related to laundering proceeds of crime and terrorist financing, the Compliance Officer is informed about the matter.

In the following cases, the Bank does not establish a new business relationship, restricts or terminates the existing business relationship and refuses to perform the transaction requested to be performed and notifies the Compliance Officer:

 Dünya Katılım	Policy on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism	Page 24 / 37
Doc. No.: UYB.POL.01	Date/Rev. No. 22.09.2025/02	

- Failure to operate a customer due diligence and identification process about the customer,
- Failure to provide information and documents for customer due diligence and identification within the scope of information updates at the customer acceptance stage or during the continuation of the business relationship,
- Failure to identify and confirm the identity of the customer or real beneficiary,
- The customer's unwillingness to provide the requested information about the business and transactions,
- Failure of the Customer to comply with the terms and conditions in the agreements signed with the Bank,
- Risk of unmanageable or unacceptable laundering of proceeds of crime related to the customer.

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

4.3.8. Correspondent Relationship

In the process of establishing foreign correspondent relations, the Bank implements the following measures. Approval from the Deputy General Manager under which the financial institution department operates, is obtained before initiating new correspondent relationships.

- Obtaining reliable information from publicly available sources on whether the respondent financial institution is under investigation for laundering or financing of terrorism and whether the financial institution has been fined or warned, the nature and subject matter of its business, its reputation, and the adequacy of its supervision,
- Evaluating the systems employed by the respondent financial institution for combating laundering proceeds of crime and financing of terrorism, and ensuring that the systems are appropriate and effective,
- Explicitly define the responsibilities of the Bank and the correspondent institution in a contract to meet the obligations in the General Procedures and Principles for Customer Recognition and Customer Identification section of this Policy,
- In cases where the correspondent relationship includes the use of direct correspondent accounts, ensuring that the addressee financial institution takes adequate measures within the framework of the procedures and principles in the General Procedures and Principles on Customer Due Diligence and Customer Identification of this Policy and that it can provide the identity information of the relevant customers when requested

The Bank does not enter into a correspondent relationship with shell banks and financial institutions with which there is no certainty that they do not make their accounts available to shell banks.

4.3.9. Electronic Transfers

In domestic and international electronic transfer messages requiring identification of the sender; providing the following information is mandatory:

1. Name and surname, the title of the legal entity registered in the trade register, the full name of other legal entities and non-legal entities,

 Dünya Katılım	Policy on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism	Page 25 / 37
Doc. No.: UYB.POL.01	Date/Rev. No. 22.09.2025/02	

2. Bank account number, the reference number related to the transaction in case the account number is not available,
3. At least one of the identifying information such as address or place and date of birth, customer number, nationality number, passport number, tax identification number must be included to determine the sender, and the accuracy of this information is additionally verified. Regarding the recipient of electronic transfer messages, the information specified in Articles 1 and 2 above is included, confirmation of this information is not obligatory.

Domestic and international electronic transfer messages not requiring identification shall include the information specified in Articles 1 and 2 regarding the sender and recipient. Confirmation of this information is not obligatory.

Transfers made by banks on behalf of their own accounts and transfers made using credit and debit cards, provided that the card numbers are used in the messages, are excluded from the scope specified in the paragraph above.

Upon receiving the electronic transfer message that does not contain the information specified in Articles 1.2 and 3, the Bank returns the electronic transfer in question or ensures that the missing information is completed by the financial institution that sent this message.

In the event that the messages sent include short-coming information permanently and they may not be completed although they are required, either the wire transfers received from the originator financial institution may be refused or transactions carried out with related financial institution may be restricted or business relationship with related financial institution may be ceased.

In the message chain from the financial institution where the transfer order is placed to the financial institution that will make the payment, all financial institutions intermediating the transfer shall include the information regarding the sender that should be included in the electronic transfer messages and pay special attention to transfer this information at every stage of the transfer.

4.3.10 Relations with Risky Countries

The Bank exercises special care in business relations and transactions with natural and legal persons, unincorporated entities and citizens of risky countries, obtains and records information to the extent possible about the purpose and nature of transactions that do not have a reasonable legal and economic purpose.

Countries that do not have adequate regulations on the prevention of laundering proceeds of crime and financing of terrorism, do not cooperate in the fight against these crimes, or are considered risky by authorized international organizations are defined as risky countries.

Risky countries are determined by the Compliance Officer. The Compliance Officer may add or remove new countries among risky countries or change the risk levels of countries when necessary, taking into account the country's assessments of international organizations operating in the field of money laundering and terrorist financing. The Compliance Officer can increase the risk level of a low-risk country or reduce it so that it does not fall below the risk level set in the Bank's written regulations.

 Dünya Katılım	Policy on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism	Page 26 / 37
Doc. No.: UYB.POL.01	Date/Rev. No. 22.09.2025/02	

Customers that reside or conduct business in high-risk nations as determined by the Compliance Officer are regarded as such. Customers cannot be accepted from non-residents who do not have legitimate, customary justifications for wanting to conduct banking transactions and open accounts abroad.

Country risk is taken into account according to the residence and nationality of the customer for real persons, and according to the country of operation and residency status for legal entities. During customer acceptance, this information is taken from the customer and transferred to the associated records.

The following countries and regions and customers residing in or associated with these countries and regions are closely monitored within the high-risk category in terms of country risk:

- Countries included in the black and gray list announced by FATF,
- Countries included in the list of risky countries announced by the Ministry,
- Countries sanctioned by the United Nations Security Council, the European Union, United Kingdom or OFAC for policies and practices related to the laundering of proceeds of crime or financing of terrorism,
- Countries considered risky in international regulations on the prevention of laundering proceeds of crime and financing of terrorism,

4.4. High-Risk Customers

One of the most important steps in customer due diligence and identification is obtaining complete and accurate information about what the natural person customer is engaged in, the field in which the legal entity customer operates, and basically what the source of income is.

This is essential not only for the planning of customer-related marketing activities but also for the accurate monitoring and evaluation of customer transactions. When evaluating which field of activity, a natural or legal person with more than one activity is engaged in, the field of activity that stands out in terms of the share of time spent and revenues generated should be taken into account. Some fields of activity and professions are riskier than others in terms of money laundering and financing of terrorism.

Before entering into business relations with the following sectors and occupational groups, extra care is taken, customer due diligence and identification documents, sector information are carefully and completely recorded. Engaging in business relationships with high-risk customers is subject to the approval of a higher level official and these accounts are also carefully monitored. In this context, customers deemed High Risk are listed below:

- Non-Profit Non-Governmental Organizations
- Politically Exposed Persons or Their Companies,
- Foreign Correspondent Banks, Shell Banks, Offshore Banks and Financial Institutions
- Exchange Offices
- Customers Operating in Sanctioned or High-Risk Areas

 Dünya Katılım	Policy on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism	Page 27 / 37
Doc. No.: UYB.POL.01	Date/Rev. No. 22.09.2025/02	

- Resident Customers Abroad
- Embassies/Consulates
- Jewelers, Precious Stones and Metals Traders
- Manufacturers and Traders of Arms and Military Ammunition
- Real Estate Agents and Automobile Dealers
- Legal Entities with a Complex Partnership Structure or Control Structure Involving Many Countries/Regions
- Antique and Art Galleries
- Real/legal persons operating in countries subject to financial sanctions
- Operators of Casinos and Games of Chance Halls
- Those with No Specific Job/Activity
- Those Engaged in Production and Trading of Auto Spare Parts
- Those Operating in Cash Intensive Business Lines
- Travel Agencies, Passenger and Freight Carriers
- Crypto Asset Service Providers
- Payment Institutions and Electronic Money Institutions

4.5. Persons and Institutions Not Acceptable as Customers

As a fundamental principle, the Bank refrains from providing banking services to individuals and institutions that have not gone through the customer due diligence and identification stages. No business relationship can be established with persons and organizations that refuse to submit the information and documents required to be submitted in accordance with the legislation. The Bank retains information on the persons and institutions denied the establishment of a business relationship or a transaction request. The Bank cannot accept the following persons and institutions as customers:

- Persons with unknown identities and addresses or persons who refuse to provide a physical address,
- Persons refraining from providing the information and documents required to be submitted or signing the necessary documents in accordance with legal regulations,
- Persons and entities named in blacklists published by public authorities on laundering proceeds of crime and financing of terrorism,
- Persons for whom sufficient information cannot be obtained about the purpose of the business relationship or the transaction to be realized in line with the existing legal regulations, and who refrain from meeting the information requests in this direction,
- Shell companies or institutions suspected of providing shell banking services

 Dünya Katılım	Policy on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism	Page 28 / 37
Doc. No.: UYB.POL.01	Date/Rev. No. 22.09.2025/02	

- Persons or entities trading cryptocurrencies on behalf of third parties,
- Persons refraining from providing the information and documents required to be submitted or signing the necessary documents in accordance with legal regulations,
- Banks and institutions that do not have a physical address,
- Those operating in an area subject to a license, special authorization or permit, but without the required permit/license/authorization,
- Persons and institutions engaged in gambling and illegal betting activities, including those operated over the Internet,
- Those who are registered in the bank's internal list for laundering proceeds, financing of terrorism and related financial crimes.

The relevant unit shall forward the situation to the Compliance Officer for the immediate termination of the business relationship established with persons and institutions subsequently understood to hold this status, and for taking the necessary actions.

On the other hand, refusal to submit the information and documents required to be obtained within the framework of this Policy and the Bank's internal regulations constitutes a reasonable and customary justification for the establishment of a business relationship or the rejection of requests to conduct transactions for existing customers.

The Bank prohibits its customers from using hold-mail addresses (addresses held by organizations that provide this service, where mail sent to individuals for a temporary period of time is held on behalf of the owner of the address without returning it to the sender) or postrestant addresses (showing a PTT branch as address information) as the only address information. Persons and institutions that only declare such addresses as address information are not accepted as customers.

Maximum care and diligence are exercised to accept as clients individuals and institutions whose wealth and funds are suspected to have been acquired legally, as well as those whose social reputation is in question.

4.6. High-Risk Products and Services

Considering the risks related to laundering proceeds of crime and financing of terrorism, certain product groups may be riskier than others. For example, it is recognized that cash transactions or money transfers with risky countries, and transactions with associations and foundations are riskier in terms of laundering proceeds of crime and financing of terrorism. Therefore, purpose of the business relationship to be established with the customer is an important risk factor. Therefore, at the customer acceptance stage, it is important to know the purpose for which the customer wants to establish a business relationship. The relevant forms used in customer acceptance include fields for the purpose of the business relationship. The purpose of the business relationship to be established with the customer may be declared by the customer. In the absence of a declaration, depending on which transaction the customer identification is based on, it is also received by the Customer Representatives by recording it in the relevant fields of the forms used in customer acceptance.

Customer funds and transactions arising from activities of unknown origin and not directly attributable to the nature of the business, typically cash transactions and electronic fund transfers, are subject to enhanced measures. The following products are considered high risk products/services by the Bank:

 Dünya Katılım	Policy on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism	Page 29 / 37
Doc. No.: UYB.POL.01	Date/Rev. No. 22.09.2025/02	

- Customer Transactions Established through Electronic Banking Channel
- Electronic transfers
- Cash Transactions

4.7. Updating Customer Information

The Bank periodically reviews the information within the scope of customer due diligence, customer identification and customer acceptance using a risk-based approach in order to ensure that customer relations are conducted in a healthy manner and that the level of customer due diligence provided at the time of customer acceptance is maintained throughout the duration of the customer relationship. The frequency of reviews depends on customer risk assessments, last update dates, and customer activity. The following issues are taken into consideration during the review process:

- It is essential to make a review regardless of the risk level of the customer in case of changes in customer acceptance/evaluation criteria or information/documents required to be obtained due to changes in the Bank's practices or legislation. For example, upon deciding to obtain information or documents that have not been requested before, the content of this information/document, the content of the legal regulation that makes it necessary, etc. are evaluated and the action to be taken for existing customers is decided separately on a case-by-case basis.
- In accordance with this Policy, an ongoing business relationship shall not be established without obtaining the mandatory documents required to be obtained from customers.
- For customers classified as high-risk in terms of compliance risk level, review and control activities are carried out every year, every two years for medium-risk customers, and every three years for low-risk customers. If for some other reason, the customer has already been reviewed in the six months preceding the month in which the review is due, it does not need to be reviewed again and the new review date is determined according to the date of the last review.

Customer Risk Rating	Update Frequency
Customers in the "High-Risk" category based on the risk assessment	Annual
Customers in the "Medium-Risk" category based on the risk assessment	2 years
Customers in the "Low-Risk" category based on the risk assessment	3 years

Customer information is reviewed in case of significant changes in customer assets, risk level, administrative structure, etc. Significant changes can be defined as the activation of an inactive customer, an increase in the customer's risk level, significant changes in the management or control structure of the company (change in control ownership, comprehensive changes in the management of the company), change in the company's field of activity.

All above mentioned review activities are carried out by the relevant Customer Representatives or the system under the coordination of the Compliance Officer. Any outdated information and

 Dünya Katılım	Policy on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism	Page 30 / 37
Doc. No.: UYB.POL.01	Date/Rev. No. 22.09.2025/02	

documents are updated and recorded during the review process. The Compliance Unit ensures that the necessary corrections are made regarding the issues deemed deficient in the review records submitted to it.

4.8. Compliance with Sanctions

The Bank undertakes to comply with legal and regulatory regulations related to sanctions and ensures that no business relationship is established with persons on UN, OFAC, EU and local sanctions lists:

- Lists published pursuant to UN Security Council resolutions,
- The U.S. SDN List,
- The U.S. Entity List or Denied Persons List,
- The U.S. Foreign Sanctions Evaders List,
- The EU Consolidated List,
- The UK Consolidated List of Asset Freeze Targets,
- Lists determined by the Turkish Presidency, Ministry of the Interior, or MASAK.

In case the Bank's existing customers subsequently enter the above lists, what risk-reducing measures (for example, limiting transactions or terminating the customer relationship) can be taken in compliance with the Banking Law No. 5411 and relevant legislation are evaluated separately on a case-by-case basis and relevant actions are taken immediately.

The Bank checks whether the parties to the transaction are included in the sanctions lists for domestic and international money transfer transactions. In domestic transfers, the bank sending the transfer is responsible for checking that the supervisor is not on the list of those whose assets are frozen and not executing the transaction. However, the Bank, which is the recipient of the transfer, is responsible for checking that the beneficiary is not included in the list of those whose assets are frozen and not executing the transaction.

4.8.1. Relations with Sanctioned Countries

The Bank shall not conduct any banking transactions (including incoming and outgoing transfers), commercial and financial transactions with countries subject to sanctions in line with the principles determined by the risk appetite structure, risk assessment, and relevant national and international organizations regarding the prevention of laundering proceeds of crime and the financing of terrorism and chemical weapons.

4.9. Freezing of Assets

The Bank implements the decisions of freezing of assets announced or notified by the Presidency of MASAK in relation to the implementation of the UN Security Council Resolutions without delay in accordance with the Law No. 6415 on the Prevention of Financing of Terrorism ("**Law No. 6415**") and the relevant regulation.

Pursuant thereto, the Bank reviews whether or not there are any asset records of the persons, institutions or organizations for which an order to freeze assets has been issued, and if so, it takes the necessary actions and notifies the Presidency within seven days from the date of notification of the information regarding the frozen assets.

The relevant real or legal person may manage the frozen assets. Notwithstanding the provisions of Law No. 6415, the Bank does not provide or facilitate the disposal, consumption, conversion,

 Dünya Katılım	Policy on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism	Page 31 / 37
Doc. No.: UYB.POL.01	Date/Rev. No. 22.09.2025/02	

transfer, and assignment of such assets or the execution of transactions for other disposals. In addition, decisions to revoke orders to freeze assets shall also be implemented without delay.

4.10. Bank Activities on Preventing the Financing of the Proliferation of Weapons of Mass Destruction

The Bank implements the sanctions resolutions of the United Nations Security Council (UNSC) to prevent the financing of the proliferation of weapons of mass destruction and the provisions of the Law on the Prevention of the Financing of the Proliferation of Weapons of Mass Destruction and the relevant regulations. In this context, the Bank shall not;

- Raise or provide funds for the benefit of, or enter into business partnerships or other business relationships in Türkiye with, any of the persons, entities, or organizations related to nuclear, ballistic missile programs or other activities specified in these decisions, or persons or entities directly or indirectly controlled by them, or persons or entities acting on their behalf or account;
- Establish business partnerships, capital partnerships or correspondent bank relationships with such banks.

Contribute to or support the import, export, transit, or transfer of materials, supplies, and equipment, or the transfer of technology, nuclear activities, or the development of nuclear weapon delivery systems, depending on the scope of the relevant resolutions, except as authorized by the UNSC.

If requested by the Audit and Cooperation Commission established in relation to the implementation of the Law on the Prevention of Financing the Proliferation of Weapons of Mass Destruction, the Bank is obliged to provide such information and documents within the time and in the manner requested.

The Bank must follow the lists published on the website of the Presidency regarding the persons, institutions or organizations for which an asset freezing decision has been issued and take action in line with the notifications made by the Presidency.

4.11. Postponement of Transactions

The Bank sends a suspicious transaction reporting to MASAK with a request for postponement of the transaction together with the reasons, if there is a serious indication that the transaction is related to the crime of laundering or financing of terrorism, and acts according to the decision notified to them by MASAK about the transaction. However, the postponement of transactions cannot exceed seven business days from the date of suspicious transaction notification by the Bank. If the decision regarding the transaction is not notified to the Bank within the said period, the transaction subject to the postponement request may be carried out according to the evaluation conducted.

4.12. New Products and Services

The relevant departments must obtain the approval of the Compliance Unit before offering new or derivative products or services to customers, to ensure that they comply with AML/CFT requirements.

4.13. Outsourcing

The Bank may seek outsourcing services for customer due diligence, such as identifying the customer and the beneficial owner and obtaining information about their activities. In this case, the following conditions must be met:

 Dünya Katılım	Policy on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism	Page 32 / 37
Doc. No.: UYB.POL.01	Date/Rev. No. 22.09.2025/02	

- All information required for customer identification can be obtained immediately from the outsourcing company upon request,
- Ensuring that certified copies of identification documents and other customer identification documents are promptly available from the third party upon request,
- Ensuring that the outsourcing firm is regulated and audited for compliance with requirements relating to due diligence, retention of records and customer identification, and that adequate measures are in place to ensure compliance with these requirements,
- Outsourcing company not being based in risky countries,
- Adequate assurance of confidentiality in the exchange of information by the outsourcing company,
- A clear definition of the duties and responsibilities of the outsourcing company and the transactions and services to which the customer due diligence requirements will be applied in the contract to be signed between the Bank and the outsourcing company.

In any event, the ultimate responsibility for identification and confirmation of identity belongs to the Bank.

4.14. Suspicious Transaction Report (STR)

In the event that there is any information, suspicion, or reason for suspicion that the assets subject to the transaction made or attempted to be made in or through the Bank have been obtained illegally or used for illegal purposes, used for terrorist acts, or used by terrorist organizations, terrorists or those financing terrorism, or related or connected to them, the transactions that are concluded to be suspicious are reported to MASAK by the compliance officer within the framework of the time and principles specified in the legislation, by conducting the necessary investigations to the extent possible. Suspicious transactions are reported to the Presidency within ten business days at the latest from the date of suspicion regarding the transaction.

If new information and findings are subsequently obtained in relation to the notified transaction, the Suspicious Transaction Notification Form is filled out again and sent to MASAK without delay, indicating that it is in addition to the previous notification.

Bank personnel executing the suspicious transaction reporting obligation in the specified manner and within the specified period shall not be held legally or criminally liable in any way.

Except for the information provided to the auditors assigned with the audit of liability and to the courts during the proceedings, it cannot provide information to anyone, including the parties to the transaction, that a suspicious transaction report has been or will be made to MASAK.

The Bank undertakes to create 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 sanctions.

Employees have the obligation to immediately notify the compliance unit of all matters that they know or assess to be in violation of this Policy by using the banking system, e-mail or other appropriate

 Dünya Katılım	Policy on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism	Page 33 / 37
Doc. No.: UYB.POL.01	Date/Rev. No. 22.09.2025/02	

channels. The Bank confirms that such notifications made in good faith and in compliance with the relevant legislation will protect employees from criminal, legal and administrative liability.

Customers and transactions that the Compliance Officer decides to report suspicious transactions as a result of additional research and evaluation are sent to MASAK together with additional information and documents.

Maximum care and diligence shall be exercised by all relevant persons involved in or aware of the subject matter with respect to the confidentiality and security of suspicious transaction reports and internal notifications made within the Bank within this scope and the protection of the parties to the notifications, within the framework of the legislation.

Bank personnel are prohibited from informing other employees, the customer or any third party about a customer or transaction, or disclosing matters within their knowledge, at any stage of the transaction, that a suspicious situation exists, is being investigated, is being closely monitored, a suspicious transaction has been reported or is likely to be reported. Such prohibition should not, however, prevent the sharing of information about such transactions among employees or with the competent authorities.

4.15. Providing Information and Documents

Upon direct request for information and documents by the relevant public institutions, the Compliance Officer shall be informed as soon as possible and a copy of the letter shall be forwarded to the Compliance Officer. Such requests for information and documents are sent to the relevant public institutions through the Compliance Officer.

The Bank has the obligation to provide all kinds of information, documents and related records in all kinds of media to be requested by the Presidency and the audit staff assigned by the Presidency, all information and passwords necessary to access and make these records readable, in full and accurately and to provide the necessary convenience.

The bank is obliged to keep its books and records available for inspection during on-site audits; to provide full access to its information systems to auditors for the purposes of the audit; and to ensure the security of its data.

4.16. Periodically Reporting

The Bank shall report the transactions to which it is a party or intermediary, exceeding the amount to be determined by the Ministry to the Presidency.

4.17. Training and Awareness Programs

All new and existing employees, including the Board of Directors and Senior Management, are provided with training within the framework of national and international regulations on the prevention of laundering of proceeds of crime and financing of terrorism and the Bank's internal regulations. Bank employees should participate in these training programs upon invitation and read the documents published for training purposes.

The Bank executes the training activities within the framework of the relevant legislation within the annual training program approved by the Board of Directors, in accordance with the needs of the unit/branch in which they work and the risks they encounter in their activities under the supervision

 Dünya Katılım	Policy on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism	Page 34 / 37
Doc. No.: UYB.POL.01	Date/Rev. No. 22.09.2025/02	

and coordination of the Compliance Officer in accordance with the size of the business, business volumes and changing conditions to prevent laundering proceeds of crime and financing of terrorism.

The training program is drafted by the Compliance Officer with the participation of the relevant units. Training can be organized face-to-face through seminars, panels, conferences, etc. or online through training platforms on electronic media such as the internet and intranet. The Compliance Officer monitors the effective implementation of the training program. Training activities are carried out within a specific training program and plan, including the training topics detailed below:

- The concepts of laundering proceeds of crime and financing of terrorism
- Concepts of financing the proliferation of weapons of mass destruction
- Stages and methods of laundering proceeds of crime and case studies on this subject
- Legislation regarding the prevention of laundering proceeds of crime and financing of terrorism
- International regulations on combating money laundering and financing of terrorism
- Corporate policy and procedures
- Risk areas
- Principles on customer due diligence
- Identification obligation
- Detection and prevention of activities of laundering proceeds of crime and financing of terrorism
- Typologies and trends in laundering proceeds of crime and financing of terrorism
- Principles on suspicious transaction reporting
- Preservation and submission obligation
- Obligation to present information and documents
- Sanctions for non-compliance with obligations
- Sanctions

The training activities aim to ensure compliance with the obligations within the framework of the relevant legislation, to create a corporate culture by increasing the awareness of responsibility of the personnel on this Policy and the Bank's internal regulations and risk-based approach, and to update the knowledge of the personnel.

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

4.18. Internal Audit Activities

The internal audit activities performed in relation to the prevention of laundering proceeds of crime and combating the financing of terrorism aim to provide assurance to the Board of Directors on the effectiveness and adequacy of the compliance program.

The Bank's internal regulations, risk management, monitoring and control activities, adequacy and efficiency of training activities, the adequacy and effectiveness of the Bank's risk policy, and whether transactions are carried out in accordance with the relevant legislation and the Bank's compliance policies are regularly examined and audited every year with a risk-based approach. Internal audit activities within this scope are executed by the Bank's Inspection Board Directorate.

Internal audit conducted by the Inspection Board Directorate covers the activities listed below:

 Dünya Katılım	Policy on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism	Page 35 / 37
Doc. No.: UYB.POL.01	Date/Rev. No. 22.09.2025/02	

- Major shortcomings, errors and misconduct uncovered in relation to money laundering and terrorist financing as a result of internal audit activities, as well as opinions and suggestions for preventing their re-emergence, are reported to the Board of Directors through the Audit Committee within the scope of periodic reports.
- While determining the scope of audit, the faults detected during the monitoring and controlling workings and the customers, services and transactions containing risk shall be included within the scope of audit.
- The Bank's business size and transaction volume are taken into consideration when determining the units and transactions to be audited. In this scope, supervision of departments and transactions in a quantity and quality that can represent all of the transactions carried out by the Bank is ensured,

The Bank shall submit the results of its audit activities to MASAK through the Compliance Officer by the end of March of the following year, including the information and statistics specified in the relevant regulations.

4.19. Retaining and Submitting

The Bank shall retain documents relating to its obligations and transactions in all kinds of media for a period of eight years from the date of issuance, books and records from the date of the last record, and documents and records relating to identification shall be retained for a period of eight years from the date of the last transaction and shall be submitted to the authorities upon request. The date of the beginning of the preservation period of the documents related to the identification of the accounts held by the obligor is the date the account is closed.

Documents and records for suspicious transactions reporting submitted to MASAK or internal suspicious transaction reporting submitted to the compliance officer, documents attached to suspicious transaction report, the written reasons for suspicious transactions which are decided not to be reported by compliance officers, are in the scope of retaining and submitting obligation.

4.20. Administrative and Judicial In Failure to Comply with The Obligations

Pursuant to Article 14 of Law No. 5549, in case of breach of the obligation stipulated in the second paragraph of Article 4 of the same law stating that "obliged entities shall not disclose the fact that a suspicious transaction report was made to anyone other than the auditors assigned to audit the obligation and the courts during the proceedings" and in case of breach of the obligations to provide information and documents specified in Article 7 and to preserve and present information and documents specified in Article 8; one to three years imprisonment and a judicial fine up to five thousand days shall be imposed.

In addition, administrative penalty fines are applied on the basis of the lump sum amounts set forth in Articles 13 and 16 of Law No. 5549. These monetary amounts are applied by increasing them by the revaluation rate determined in accordance with the Tax Procedure Law dated 04.01.1961 and numbered 213 for the previous year, effective from the beginning of each year.

4.21. Exchange of Information with Legal and Regulatory Authorities

The Bank cooperates with legal and regulatory authorities through official communication channels such as e-mails, reports, SWIFT messages, etc. in examinations and investigations related to possible laundering of proceeds of crime, terrorism, financing of terrorism or other illegal activities,

 Dünya Katılım	Policy on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism	Page 36 / 37
Doc. No.: UYB.POL.01	Date/Rev. No. 22.09.2025/02	

provided that it does not contradict its obligations arising from laws on customer confidentiality and privacy. The Bank complies with such information requests in a timely manner.

Relevant requests (written or verbal) from regulatory authorities or government agencies shall be directed to the Compliance Department in order to take necessary actions. Such requests for information and documents shall be sent through the Compliance Officer.

The Bank has the obligation to provide all kinds of information, documents and related records in all kinds of media to be requested by the Presidency and the audit staff assigned by the Presidency, all information and passwords necessary to access and make these records readable, in full and accurately and to provide the necessary convenience.

4.22. Notification

The commitment forms, established by the Presidency in relation to the Bank policy formulated through this Policy, will be signed by the Board of Directors and submitted to the Presidency within a thirty-day period starting from the approval date. If there are modifications to the Bank policy, the said forms will be revised and sent to the Presidency.

In the event that the Compliance Officer or the deputy compliance officer loses the qualifications required by this Policy, or it is subsequently understood that they do not possess these qualifications, or they resign from their position, or are dismissed from office by the Bank, the situation shall be notified in writing by the Bank to the Presidency within ten days from the date of departure, together with its reasons. The compliance officer and the deputy compliance officer shall also notify the situation in writing to the Presidency, together with its reasons, within ten days from the date of departure in the event of their dismissal or resignation from office. The new appointment shall be made within a maximum of thirty days from the date of separation. The commitment form, created by the Presidency regarding the appointment, is signed by the Board of Directors and sent to the Presidency within ten days from the date of appointment.

The Bank notifies the Presidency through the Compliance Officer until the end of March of the following year of the results, relevant information and statistics regarding the internal audit activities carried out within the scope of the internal audit policy established within the framework of this Policy and the training activities carried out within the scope of the training policy.

5. VIOLATION OF THE POLICY

All employees of the Bank are obliged to act within the framework of the principles of customer recognition and identification explained in this Policy and the internal regulations of the Bank, primarily in customer transactions and in all banking transactions. In the event that this Policy and its sub-regulations are violated by a Bank employee, actions shall be taken within the framework of the Discipline Regulations.

Employees who suspect or know that the Policy has been violated are required to report the situation in accordance with the Ethics Reporting Policy.

3. ENTRY INTO FORCE

This document shall enter into force on the date of publication.

4. REVIEW AND UPDATE

This Policy is reviewed every year and updated when necessary.

 Dünya Katılım	Policy on the Prevention of Laundering Proceeds of Crime and Financing of Terrorism	Page 37 / 37
Doc. No.: UYB.POL.01	Date/Rev. No. 22.09.2025/02	

I have read this policy and its annexes, consisting of 37 pages and 7 articles, and I fully accept it as is.

Compliance Dept.	Talent and Culture Dept.	Legal Consultancy Department	Participation Banking Compliance
			
Deputy General Manager of Internal Systems	Audit Committee Resolution		Resolution of the Board of Directors
			22.09.2025 Resolution No. 1068