

№ 1866

(Seal of Notary)  
(Seal of Türk Eximbank)

(Seal of Türk Eximbank)

(Logo of Türk Eximbank)

RESOLUTION OF BOARD OF DIRECTORS

DATE OF MEETING : 30.12.2021  
PLACE OF MEETING : ISTANBUL

NUMBER OF MEETING : 21/13  
RESOLUTION NO : 165

REF : Attached minutes related to the "Policy and Codes of Practice on Prevention of Laundering Crime Revenues and Financing of Terrorism" dated 14.12.2021 and numbered 43049449.050.02-67 received from Legislation Compliance Unit with approval of Audit Committee.

RESOLUTION

In the meeting of our Board dated 30.12.2021, it is resolved for the "Policy and Codes of Practice on Prevention of Laundering Crime Revenues and Financing of Terrorism", which is prepared for full compliance to the provisions of "Law No 5549 on Prevention of Laundering Crime Revenues", "Law No 6415 on Prevention of Financing of Terrorism", "Law No 7262 on Preventing the Financing of Proliferation of Weapons of Mass Destruction", the regulations/communiqués introduced within the scope of these laws, international liabilities of our country, and the arrangements regarding prevention of laundering crime revenues and financing of terrorism within the generally accepted banking practices, to be accepted as annexed hereto; for the "Policy and Codes of Practice on Prevention of Laundering Crime Revenues and Financing of Terrorism", which was accepted with the Resolution of Board of Directors dated 25.12.2020 and numbered 194, and Appendices thereto to be repealed; and for the Audit Committee to be authorized to perform the necessary updates and amendments to the Appendices of the Policy within the given period.

(Signature)

Rıza Tuna TURAGAY  
Vice-Chairman

(Signature)  
Ali Güney  
Member

(Signature)  
Nail OLPAK  
Member

(Signature)  
İsmail GÜLLE  
Member

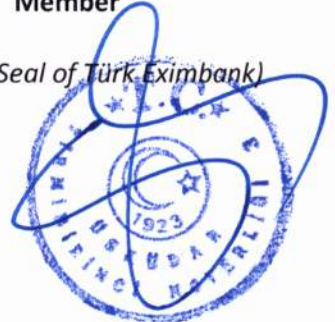
(Signature)  
Fahriye Alev ARKAN  
Member

(Signature)  
Duygu GÜVEN  
Member

(Seal of Türk Eximbank)

(Seal of Türk Eximbank)

I hereby certify that  
this text was translated by  
me from TR to ENG...  
as true to its original  
Sworn Translator



13 Ocak 2022



13 Ocak 2022

**TÜRKİYE İHRACAT KREDİ BANKASI A.Ş.**  
**Policy and Codes of Practice on Prevention of Laundering Crime Revenues**  
**and Financing of Terrorism**

REGULATORY COMPLIANCE DEPARTMENT  
DECEMBER 2021, ISTANBUL



Policy and Codes of Practice on Prevention of Laundering Crime Revenues and Financing of Terrorism

Document: POL\_AML\_03

Page: 1 of 24

I hereby certify that  
this text was translated by  
me from TR to ENG...  
as true to its original  
Sworn Translator

Document Name	Türkiye İhracat Kredi Bankası A.Ş. Policy and Codes of Practice on Prevention of Laundering Crime Revenues and Financing of Terrorism
Document No	POL_AML_04
Version No	V1.3
Issued By	REGULATORY COMPLIANCE DEPARTMENT

## Revision History

Version No	Date	Prepared By	Responsible Department
V1.0	12.10.2006	Internal Control Department	Teoman ŞENER
V1.1	24.11.2016	Regulatory Compliance Department	Regulatory Compliance Department
V1.2	25.12.2020	Regulatory Compliance Department	Regulatory Compliance Department
V1.3	27.12.2021	Regulatory Compliance Department	Regulatory Compliance Department

13 Ocak 2022

## Revision Details

Version No	Revision Details
V1.0	First Release
V1.1	Reflection of Changes in National and International Legislation
V1.2	Reflection of Changes in National and International Legislation
V1.3	Reflection of Changes in National and International Legislation

## Document Structure

Related Principal Document	Regulation of Regulatory Compliance Department
Related Sub-Documents	APPENDIX-1 Identification Procedures APPENDIX-2 Prevention of Money Laundering Questionnaire APPENDIX-3 Types of Suspicious Transaction and Suspicion Categories Reference Table APPENDIX-4 Suspicious Transaction Reporting Form

## Distribution and Announcement

Distribution	All Bank Units
Announcement	All Bank Units

## Approval Information

Date	27.12.2021
------	------------

Policy and Codes of Practice on Prevention of Laundering Crime Revenues and Financing of Terrorism

Document: POL\_AML\_03

Page: 2 of 24



I hereby certify that  
this text was translated by  
me from TR to ENG  
as true to its original  
Sworn Translator

CONTENTS

1 INTRODUCTION ..... 4

2 BASIS ..... 4

3 PURPOSE ..... 4

4 DEFINITIONS ..... 5

5 RISK MANAGEMENT ..... 8

6 OBLIGATION OF MONITORING AND CONTROL ..... 17

7 DETECTION AND REPORTING PROCEDURE OF SUSPICIOUS  
TRANSACTIONS ..... 18

8 OTHER OBLIGATIONS UNDER REGULATIONS ON PREVENTION OF  
FINANCING OF TERRORISM AND PROLIFERATION OF WEAPONS OF MASS  
DESTRUCTION ..... 20

9 COMPLIANCE OFFICER ..... 21

10 INTERNAL AUDIT ..... 22

11 TRAINING ACTIVITIES ..... 22

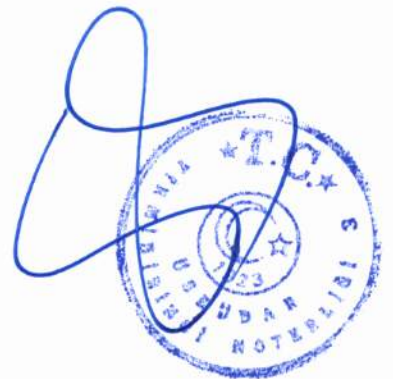
12 SUBMISSION OF INFORMATION AND DOCUMENT ..... 23

13 STORAGE OF RECORDS ..... 23

14 ENFORCEMENT AND REVIEW ..... 24

15 APPENDICES ..... 24

13 Ocak 2022



I hereby certify that  
this text was translated by  
me from TR to ENG...!  
as true to its original  
Sworn Translator

## 1 INTRODUCTION

It has become an obligation for member states to comply with the regulations and principles of the Financial Action Task Force (FATF), which was established to prevent international money laundering and financing of terrorism. As a member of FATF, harmonization of our country to international regulations, making legal regulations, and carrying out activities are duties of the Financial Crime Investigation Board (MASAK), which was established within the body of the Republic of Turkey, Ministry of Treasury, and Finance.

Having an internationally recognized and reliable position, Türkiye İhracat Kredi Bankası A.Ş. (Turkey Export Credit Bank Inc.) considers the fight against money laundering and financing of terrorism/proliferation of weapons of mass destruction as a social responsibility, in addition to compliance with legal regulations, and attaches importance to this fight. The Bank also considers this fight as an essential element of harmonization with the international system.

## 2 BASIS

The regulations that form the basis for the preparation of this policy:

- The Law No 5549 on Prevention of Laundering Crime Revenues,
- The Law No 6415 on Prevention of Financing of Terrorism,
- The Law No 7262 on Preventing the Financing of Proliferation of Weapons of Mass Destruction
- Related regulations and communiqués,
- International conventions, international recommendations, and standards.

## 3 PURPOSE

With this document, it is aimed:

- to prevent the use of the Bank for money laundering, financing of terrorism, and proliferation of weapons of mass destruction,
- raising awareness of the Bank staff on the fight against the crime revenues and informing them regarding their legal and administrative obligations,
- ensuring the compliance of the Bank's policies, procedures, and control methods with the MASAK regulations published within the scope of the laws mentioned above,

Policy and Codes of Practice on Prevention of Laundering Crime Revenues and Financing of Terrorism

Document: POL\_AML\_03

Page: 4 of 24



I hereby certify that  
this text was translated by  
me from TR to ENG  
as true to its original  
Sworn Translator

13 Ocak 2022

- reducing the risk to be exposed, ensuring the necessary harmony and cooperation in international conventions and correspondent relations, maintaining the Bank's secure banking activities, and protecting the reputation and customer quality,
- ensuring compliance with Article 66 titled "Money Laundering" and Article 67 titled "Choosing Appropriate Customers" of the "Guideline on Operational Risk Management," published by the Banking Regulation and Supervision Agency in the Official Gazette dated 17/09/2015 and numbered 6462 and updated with the Board's Decision dated 31.03.2016 and numbered 6827,
  - ensuring compliance with paragraph 3 of Article 76 of Banking Law, and
  - ensuring compliance with the "Know and Monitor Your Customer" principle.

#### 4 DEFINITIONS

**Laundering:** refers to various transactions carried out on the assets obtained from a crime for the purpose of taking them abroad or concealing their illegitimate source and creating an opinion that they were obtained legitimately,

**Bank:** refers to Türkiye İhracat Kredi Bankası Anonim Şirketi,

**Ministry:** refers to the Ministry of Treasury and Finance

**Board:** refers to the Financial Crime Investigation Board (MASAK),

**Inspection Personnel:** refers to the Tax Inspectors, Treasury, and Finance Experts employed in the Board, Customs and Trade Inspectors, Sworn Bank Auditors, Treasury Controllers, Insurance Audit Experts, and Actuaries, Banking Regulation and Supervision Agency and Capital Markets Board Experts, and Auditors and Experts of Central Bank of the Republic of Turkey,

**FATF:** Financial Action Task Force refers to the organization established within the OECD in 1989 by the G-7 countries to develop national legal systems for the prevention of money laundering and financing of terrorism, to harmonize legislation, to strengthen the role of the financial system, and to take measures to ensure continuous cooperation among member countries (Turkey became a member in 1991. The recommendations published by the organization are binding on member states.),

**Financial Institution:** refers to the banks, non-bank institutions that have the authority to issue bank 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 with insurance and reinsurance brokers,

Policy and Codes of Practice on Prevention of Laundering Crime Revenues and Financing of Terrorism

Document: POL\_AML\_03

Page: 5 of 24

I hereby certify that  
this text was translated by  
me from *TR* to *ENG*...!  
as true to its original  
Source Translator



13 Ocak 2022

leasing companies, institutions providing settlement and custody services pursuant to capital market legislation, precious metals intermediary institutions, Posta ve Telegraf Teşkilatı Anonim Şirketi (PTT) limited to banking activities,

**Fund:** refers to money or any movable or immovable, tangible or intangible goods, the value of which can be represented by money, rights, receivables, and any documents representing the same,

**Actual beneficiary:** refers to the natural person(s) who control or have the ultimate influence over the natural person, legal entity, or unincorporated entities on whose behalf transactions are performed,

**Country/Region Subject to Comprehensive Sanction:** refers to countries or regions that are subject to national or regional sanctions by the Republic of Turkey, the United Nations Security Council, the United States of America, the European Union and the United Kingdom,

**UNSC:** refers to the United Nations Security Council,

**Assets:**

refers to:

- the funds and income in possession of, or directly or indirectly under the control of a natural person or legal entity, and the benefit and value derived from the same or from their conversion to each other; and
- the funds and income in possession of a natural person or legal entity acting on behalf or on account of a natural person or legal entity, and the benefit and value derived from the same or from their conversion to each other,

**Freezing of assets:** refers to the restriction of the complete removal of the power of disposition on the assets in order to prevent the destruction, consumption, conversion, transfer, and assignment of assets and other dispositional transactions,

**Know Your Customer Principle:** refers to procedures such as having accurate and sufficient information about customers and actual beneficiaries, obtaining and confirming the documents specified in the legislation, monitoring the transactions, monitoring whether the banking activities of the customers are compatible with their income, assets, occupation information, etc.,

**Off-Shore Banking:** Off-shore banking refers to banking carried out through banks providing private banking activities, established in regions where private banking activities are based on confidentiality, where tax advantages are available, accessible transfer opportunities are provided, obtaining a license and establishing a bank is simple, and where financial confidentiality is essential,

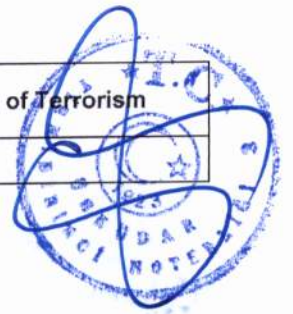
**Risk:** refers to the possibility of financial or reputational damage that the Bank or its employees may be exposed to due to the laundering of crime revenues or financing of terrorism, or the failure to comply with the legal obligations fully,

Policy and Codes of Practice on Prevention of Laundering Crime Revenues and Financing of Terrorism

Document: POL\_AML\_03

Page: 6 of 24

I hereby certify that  
this text was translated by  
me from ...TR... to ...ENG...  
as true to its original  
Sworn Translator



13 Ocak 2022

**Risky Countries:** refers to those announced by the Ministry from countries that do not have adequate regulations on the prevention of money laundering and financing of terrorism, do not cooperate in the fight against these crimes, or are considered risky by authorized international organizations,

**Insured:** refers to the customer benefiting from Bank Insurance Programs,

**Politically Exposed Persons (PEPs):** refers to the head of state or government, senior politicians, government officials, judicial or military personnel, representatives of political parties, and public institution managers who hold high-level public duties,

**Relatives and Close Associates (RCAs):** refers to relatives (spouse, child, sibling, mother, father, etc.), business contacts, and friends of politically exposed persons,

**Crime Revenue:** refers to the value of assets obtained from all kinds of crimes,

**Laundering of Crime Revenues:** refers to the transactions aimed at making the profits obtained through illegal means appear as if they were obtained through legal means, to save the said earnings in the financial system, especially in the form of cash, and to gain legitimacy by passing them through a process within the financial system and changing their identity,

**Suspicious Transaction:** refers to the presence of any information, suspicion, or any reason to suspect that the assets subject to the transaction carried out or attempted to be carried out at or through the Bank have been obtained illegally or used for illegal purposes, used for terrorist acts or by terrorist organizations, terrorists or those who finance terrorism or are related to or linked to them,

**Continuous Business Relation:** refers to the business relationship that is continuous in nature, established between the responsible party and the customer due to services such as opening an account, issuing a loan or credit card, safe deposit box, financing, factoring, financial leasing, life insurance or private pension,

**Shell Bank:** refers to a bank that does not have a physical service office in any country, does not employ full-time personnel, and is not subject to the supervision and permission of an official authority in terms of banking transactions and records,

**Financing of Terrorism:** refers to providing or collecting any money or any property, rights, receivables, income, and benefits the value of which can be represented by money, and the benefit and value resulting from their conversion, knowingly and willingly that they will be used wholly or partially in the committing of terrorist crimes,

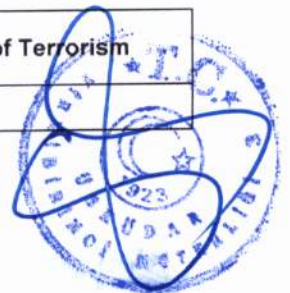
**Compliance Officer:** refers to the officer appointed by the responsible parties, vested with the necessary authority, in order to ensure compliance with the obligations imposed by the Law and the legislation enacted on the basis of the Law,

**Senior Management:** refers to the Bank's General Manager and Assistant General Managers, directors of the units within the internal systems, the directors of the units other than the consultancy units, who work in positions equivalent to or above the Assistant General Manager in terms of their powers and duties, even if they are employed with other titles,

Policy and Codes of Practice on Prevention of Laundering Crime Revenues and Financing of Terrorism

Document: POL\_AML\_03

Page: 7 of 24



13 Ocak 2022

I hereby certify that  
this text was translated by  
me from *TA* to *ENG*...  
as true to its original  
Sworn Translator



**Wolfsberg Group:** refers to the organization consisting of 13 global banks that aims to develop standards for banks on fighting against financial crimes and sanctions,

**Sanction:** refers to the regulations aimed at restricting or preventing economic activities individually or comprehensively, targeting countries, individuals, and organizations, in order to achieve economic and political goals,

**Prohibited Persons and Organizations:** refers to individuals and organizations listed in UNSC Consolidated Sanctions List, banned/sanction lists published by OFAC, EU Consolidated Financial Sanctions List, United Kingdom Consolidated List of Financial Sanctions Targets, and sanctions lists such as international and National Lists published by international authorities for the prevention of money laundering and financing of terrorism,

**Prohibited Transactions and Activities:** refers to the prohibited transactions and activities listed in UNSC Consolidated Sanctions List, banned lists published by OFAC, EU Consolidated Financial Sanctions List, United Kingdom Consolidated List of Financial Sanctions Targets, sanctions lists such as international and National Lists published by international authorities for the prevention of money laundering and financing of terrorism, and the Law No 7262 on Preventing the Financing of Proliferation of Weapons of Mass Destruction,

**Regulation (Measures Regulation):** refers to the Regulation on Measures for Prevention of Laundering Crime Revenues and Financing of Terrorism.

13 Ocak 2022

## 5 RISK MANAGEMENT

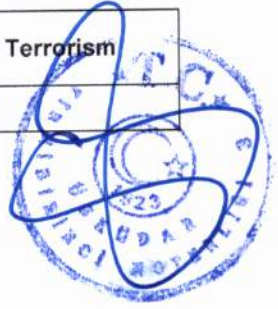
Within the framework of the "Know Your Customer" principle at our Bank, it is essential to identify customers and persons acting on behalf of customers and to reveal the actual beneficiary of the transaction, and risk management aims to define, grade, monitor, assess and reduce the risks that the Bank may be exposed to.

### 5.1 GENERAL PRINCIPLES AND RULES ON RECOGNITION OF THE CUSTOMER

#### 5.1.1 The Method of Establishing Customer Relationship and Recognition of the Customer

The principle of "Know Your Customer" is the basis of the Bank's customer acceptance policy regarding the prevention of laundering crime revenues and financing of terrorism. In this context, the Bank is responsible for identifying the customers, recognizing the actual beneficiary, taking the measures specified in the Policy for risky customers, activities, and transactions that

Policy and Codes of Practice on Prevention of Laundering Crime Revenues and Financing of Terrorism	
Document: POL_AML_03	Page: 8 of 24



I hereby certify that  
 this text was translated by  
 me from ...TR... to ...ENG...  
 as true to its original  
 Sworn Translator

require special attention, registering the declared addresses and providing additional introductory information and documents specific to the internal practices of the Bank, verifying this information, and keeping the records in physical and/or electronic environment pursuant to the legislation on the prevention of money-laundering and financing of terrorism.

The Bank fulfills its obligations through its staff, and current PayGate Inspector prohibited list scanning program.

## 5.2 BASIC PRINCIPLES IN CUSTOMER ACCEPTANCE

With regard to the transactions made or mediated by the Bank, it is obligatory to determine the identities of those who make transactions and those on whose behalf or account transactions are made before any transactions are made. In case of violation of this obligation, the sanctions specified in the relevant articles of the Law No. 5549 are applied to the Banks by the Financial Crimes Investigation Board.

Before establishing a business relationship with the Bank or making a transaction, it is obligatory for the personnel who are in direct contact with the customer to carry out identification procedures on matters specified in the Regulation.

The principle of "Know Your Customer" is the basis of the Bank's customer acceptance policy regarding the prevention of laundering crime revenues and financing of terrorism. The Bank attaches great importance to the "Know Your Customer" principle in order to protect itself from people and actions related to money-laundering and financing of terrorism. In this context, it adopts and implements a policy in line with relevant international standards and applicable legislation.

Identification: refers to obtaining information about the identity and confirming the accuracy of this information;

- a) regardless of the amount in the establishment of a continuous business relationship,
- b) when the amount of the transaction or the total amount of more than one interrelated transaction is at or above the amount specified in the legislation (seventy-five thousand TRY),
- c) when the amount of the transaction in electronic transfers or the total amount of more than one interrelated transaction is at or above the amount specified in the legislation (seven thousand five hundred TRY),
- ç) regardless of the amount, in cases requiring suspicious transaction reporting, and
- d) regardless of the amount, when there is suspicion about the adequacy and accuracy of the previously obtained customer identification information.

**Within the scope of the "Know Your Customer" principle;** necessary investigations are made before starting a continuous business relationship in matters such as:

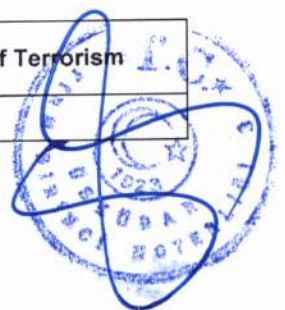
- Identification and address detection,
- Customer's business/professional information,

Policy and Codes of Practice on Prevention of Laundering Crime Revenues and Financing of Terrorism

Document: POL\_AML\_03

Page: 9 of 24

I hereby certify that  
this text was translated by  
me from TR to ENG  
as true to its original  
Sworn Translator



13 Ocak 2022

- The main business of the customers,
- Information and documents related to the insured person or asset,
- Consistency of documents and information within themselves,
- The customer's transaction profile and capacity,
- Its buyers and sellers,
- Identification of the actual beneficiary,
- workplace or place of activity,
- Providing sufficient information about the purpose and nature of the requested transaction.

**In the identification and recording of the declared address, the following points are observed:**

- Identity and address are determined and confirmed in accordance with the documents and obligations specified in the Measures Regulation. "Identification Procedures" (APPENDIX-1) are used for identification. Accuracy of information is cross-checked by using the MERNIS system, the Republic of Turkey, Ministry of Treasury and Finance Tax Identity Numbers information (information obtained electronically from the Revenue Administration), and the General Directorate of Civil Registration and Citizenship Affairs identity sharing system database, applying to the relevant trade registry office records, or by making inquiry in the database of the Union of Chambers and Commodity Exchanges of Turkey.
- At the stage of issuing the policy, it is essential to identify the insurant under the insurance policy, the buyer abroad, the direct or indirect subsidiaries of the Insured abroad, its companies, companies in which the Insured's shareholders are partners abroad (in brief, all the parties included in the insurance policy). At the stage of payment of indemnity, if they are different persons, the identification of the insured or beneficiary is made separately.
- The identity and power of the persons claiming to act on behalf of the customer are determined. Power of attorney and non-original copies of the instructions and documents must be notarized.
- Attention is paid to the consistency of documents and information within themselves.
- Records and documents regarding customer information are stored electronically and are accessible to authorized persons.
- In order to be submitted when requested by the authorities, a readable photocopy or electronic image is taken, or identity information is recorded after the submission of the originals or notarized copies of the documents that are subject to confirmation.

It is not sufficient to obtain the relevant documents once from the customers with whom a continuous business relationship is established; the information must be kept up-to-date. In particular, monitoring the business relations and transactions of high-risk customers is within the scope of the obligation.

Policy and Codes of Practice on Prevention of Laundering Crime Revenues and Financing of Terrorism

Document: POL\_AML\_03

Page: 10 of 24

I hereby certify that  
this text was translated by  
me from TR to ENG  
as true to its original  
Sworn Translator



13 Ocak 2022

Necessary measures are taken to determine whether the customer has acted on someone else's account and to determine the identity of the actual beneficiary of the transaction. If it is suspected that the person is acting on his/her own behalf and on account of someone else, despite declaring that s/he is not acting on account of someone else, reasonable research is conducted to reveal the actual beneficiary.

For the identification of the actual beneficiary in legal entities; three main issues should be taken into account:

- Ownership (shareholding) relationship,
- Final control, and
- high-level representation power.

**The points to be followed for the identification of the actual beneficiary should be as follows, respectively:**

- In establishing a continuous business relationship with legal entities registered in the trade registry; identification and confirmation of the identity of natural person partners holding shares exceeding twenty-five percent (25%) of the legal entity should be made to identify the actual beneficiary.
- If it is suspected that the natural person partner holding shares more than twenty-five percent (25%) of the legal entity is not the actual beneficiary, or there is no natural person partner holding such a share, the natural person(s) who ultimately control the legal entity should be identified, and the identification and confirmation of these persons should be made.
- In cases where the actual beneficiary cannot be identified within the scope of the above paragraphs, the natural person(s) with the highest executive power registered in the trade registry are considered as the actual beneficiaries as senior directors. Identification and confirmation of this person(s) must be made.
- In establishing a continuous business relationship with legal entities registered in the trade registry; identification and confirmation of the identity of legal entity partners holding shares exceeding twenty-five percent of the legal entity should be made. The required confirmation of the identity information of the legal entity partners residing abroad can be made through the open sources of the equivalent institutions of the Union of Chambers and Commodity Exchanges of Turkey in the relevant country or other institutions where the data is kept officially.
- At this stage, there is no need to identify the representatives of the legal entity partner holding more than twenty-five percent (25%) of the shares, and there is no need to take signatory circulars of the representatives in this context.

13 Ocak 2022

Policy and Codes of Practice on Prevention of Laundering Crime Revenues and Financing of Terrorism	
Document: POL_AML_03	Page: 11 of 24



I hereby certify that this text was translated by me from TR to ENG as true to its original  
Sworn Translator

5.3 CUSTOMER ACCEPTANCE POLICY

5.3.1 INDIVIDUALS AND ORGANIZATIONS THAT CANNOT BE ACCEPTED AS CUSTOMERS

**Our Bank:**

- 1- does not become a party to any transaction aiming to go beyond the sanctions with individuals and organizations included in the sanctions lists (OFAC List, UN Consolidated List, United Kingdom, European Union, etc.) published by authorized institutions in addition to national legislation within the scope of Prevention of Laundering Crime Revenues and Financing of Terrorism.
- 2- does not directly or indirectly mediate transactions with Shell Banks that do not exist physically, are not subject to the supervision and permission of any official authority, and do not have adequate regulations on the Prevention of Laundering Crime Revenues and Financing of Terrorism.
- 3- does not act as an intermediary in the transactions of individuals and organizations that refrain from presenting the information and documents requested during the establishment of a continuous business relationship.
- 4- does not accredit the banks located in countries where it is generally accepted that they have a bad reputation for money laundering and financing of terrorism at the international level and that the necessary controls and investigations are weak, doesn't put the high-stakes policies, checks, or letters of guarantee issued by the banks of these countries into the process. In terms of the national and international reputation of the Bank, it is essential not to enter into such a business relationship.
- 5- The necessary measures are taken and implemented with due diligence in order to prevent the establishment of business relations within the scope of prohibited transactions and activities with the prohibited persons and institutions included in the lists published by the United Nations Security Council on the prevention of financing of terrorism and proliferation of weapons of mass destruction, and become binding in our country with the Presidential Decree published in the Official Gazette, and in such other international lists, which should be taken into account by the banks of our country as well as the international financial system.
- 6- also evaluates the individuals and organizations that directly or indirectly control, act on behalf of, or on account of, or collect or provide any fund for the benefit of the individuals and organizations specified in the paragraph above within the same scope.
- 7- does not accept as customers those whose ownership structure is inexplicably complex and whose actual beneficiary cannot be identified.

13 Ocak 2022

Policy and Codes of Practice on Prevention of Laundering Crime Revenues and Financing of Terrorism	
Document: POL_AML_03	Page: 12 of 24

I hereby certify that  
 this text was translated by  
 me from TR to ENG  
 as true to its original  
 Sworn Translator



### 5.3.2 TAKING MEASURES FOR EXCEPTIONAL HIGH-RISK CUSTOMERS, ACTIVITIES, TRANSACTIONS

- a) **Country/region risk;** consists of the customers and transactions related to the countries/regions where customers are resident and affiliated, necessary regulations and measures are not taken to prevent money-laundering or financing of terrorism, do not cooperate adequately in fighting against these crimes, or are considered risky by authorized international organizations (FATF, UN, OFAC, EU, HM Treasury), located on drug production-distribution routes (grey areas), are so-called tax havens/off-shore centers, and where crimes such as smuggling, terrorism, corruption, and bribery are common, and of the customers and transactions who has a connection with the same in terms of nationality, country of birth, country of residence, place of establishment, partnership structure, authorities, transaction parties, etc.

The Bank is obliged to pay special attention to the business relations and transactions to be entered into with natural and legal persons, unincorporated entities residing in risky countries and the citizens of these countries, collect as much information as possible about the purpose and nature of transactions that do not have a reasonable legal and economic purpose, and to record the same.

The Bank takes the measures determined by the Ministry regarding risky countries, including those accepted by international organizations to which Turkey is a member.

- b) **Sensitive Sectors and Business Lines in Laundering Crime Revenues:** Special attention is paid to the provision of banking services to sectors and occupational groups with intense cash flows. In addition to customer identification and introductory documents, industry information is wholly and carefully recorded.

The Bank considers the following companies as risky and subjects them to detailed examination and monitoring:

- Companies that produce/trade dual-use and precision materials and technologies that are included in lists such as the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies and Australia Group List of Chemical Weapon Precursors, or not included such lists but suspected of being used in the development of weapons of mass destruction.

- c) **Politically Exposed Persons (PEPs) and Their Relatives and Close Associates (RCAs):** In customer management, it is determined whether there are any politically exposed persons and/or their relatives and close associates; a reasonable investigation is made to find out the source of funds and assets; and the establishment of a business relationship is decided with the approval of the Unit/Branch Manager.

- d) **Correspondent Banks:** Correspondent banking transactions are among the high-risk transactions.

Policy and Codes of Practice on Prevention of Laundering Crime Revenues and Financing of Terrorism

Document: POL\_AML\_03

Page: 13 of 24

I hereby certify that  
this text was translated by  
me from TR to ENG  
as true to its original  
sworn translator



13 Ocak 2022

Before the correspondent relationship is established:

- Reliable information is obtained by making use of publicly available sources on whether the counterparty financial institution has been investigated for money laundering or financing of terrorism, whether it has been fined or warned, the nature and subject of the work, and its reputation and audit competence,
- The system of fight against money laundering and financing of terrorism of the counterparty financial institution is evaluated, and it is ensured that the system is accurate and effective,
  - It is ensured that the relevant correspondent does not work with shell banks and does not allow accounts to be used by shell banks.

- Before establishing new correspondent relations, it is ensured that the senior manager's approval is obtained.

Accurate and satisfactory information and documents regarding the prevention of money laundering and financing of terrorism are obtained from the counterparty financial institutions with which a correspondent banking relationship will be established.

For this purpose, It is requested from financial institutions requesting to open a correspondent account by the relevant units to fill in the Wolfsberg Group questionnaire, which is not older than one year and contains information such as the business subject, the title, the measures taken to prevent money laundering, and the name of the compliance officer, and/or the "Prevention of Money Laundering Questionnaire" (APPENDIX-2).

The Regulatory **Compliance Unit** fulfills requests for information from Account Correspondents or other related financial institutions regarding the regulations on banking practices on Prevention of Laundering Crime Revenues and Financing of Terrorism.

In order to prevent any disruption in communication and any deficiencies in the records, the applications mentioned above are made with the knowledge of and through the relevant department(s) that carry out correspondent relations.

### 5.3.3 TIGHTENED MEASURES FOR HIGH-RISK GROUPS

In our Bank, the following additional measures can be applied in high-risk customers and in high-risk situations that can be determined within the framework of the risk-based approach.

- a) To obtain additional information about the customer and to update the identity of the customer and actual beneficiary more frequently,
- b) To obtain additional information about the nature of the business relationship,
- c) To obtain as much information as possible about the source of the assets subject to the transaction and the funds belonging to the customer,
- d) To obtain information about the purpose of the transaction,

Policy and Codes of Practice on Prevention of Laundering Crime Revenues and Financing of Terrorism

Document: POL\_AML\_03

Page: 14 of 24

I hereby certify that  
 this text was translated by  
 me from TR to ENG  
 as true to its original  
 Sworn Translator



13 Ocak 2022

- e) To make entering into a business relationship, maintaining the current business relationship, or making the transaction conditional on the approval of a higher-level official,
- f) To keep the business relationship under strict surveillance by increasing the number and frequency of the controls applied and identifying the types of transactions that require additional control,
- g) To require the first financial transaction to be made from another financial institution where the principles of customer identification are applied to establish a continuous business relationship.

5.3.4 SIMPLIFIED MEASURES TO IDENTIFY THE CUSTOMER

Within the scope of the Measures Regulation, the Bank may apply the simplified measures in the following transactions pursuant to the principles set forth in the FINANCIAL CRIME INVESTIGATION BOARD GENERAL COMMUNIQUÉ (SERIAL NO: 5). The procedures for which simplified measures will be applied are explained in the Identification Procedures (Appendix-1) annexed hereto.

Situations where simplified measures apply:

- Transactions where the Customer is a Financial Institution (including interbank transactions),
- In transactions where the customer is a public professional organization or public administration within the scope of general government pursuant to Law No. 5018,
- In transactions where the customer is a publicly-traded company whose shares are listed on the stock exchange,

The simplified measures cannot be applied in transactions that are considered risky in terms of money laundering and financing of terrorism. However, in cases where money laundering or financing of terrorism is suspected, the simplified measures are not applied, and these transactions are forwarded to the Regulatory Compliance unit for reporting to the Board.

5.3.5 REJECTION OF THE TRANSACTION AND TERMINATION OF THE BUSINESS RELATIONSHIP

In cases where identification cannot be made, or sufficient information cannot be obtained about the purpose of the business relationship, the business relationship is not established.

The business relationship is terminated if the identification and confirmation required due to suspicion about the adequacy and accuracy of the previously obtained customer identification information cannot be made.

In such cases, it is also evaluated whether there is any suspicious transaction.

5.3.6 SCANNING CUSTOMERS AND PAYMENTS ON SANCTION LISTS



Thereby certify that  
this text was translated by  
me from ...TR... to ...EN...  
as true to its original  
Sworn Translator

13 Ocak 2022



1866

All new customers and, where relevant, representatives, owners, and other related persons must be followed through lists provided by reputable business organizations such as Dow Jones, where the lists below are consolidated:

- European Union Financial Sanctions,
- OFAC,
- United Nations Security Council,
- United Kingdom (HM Treasury),
- Any applicable local sanction.

These scans are made systematically by the PayGate Inspector program, which is integrated into the central banking/insurance systems by the Bank.

For existing customers, the controls mentioned above are made daily and monthly, depending on updating the lists.

In the supervision of sanctions risks:

- Customers, shareholders, those acting on behalf of or on account of the customer, and final beneficiaries are scanned through the lists.
- It is examined whether the customer's transactions with or through the Bank include the Countries/Regions Subject to Comprehensive Sanctions or a person or organization subject to any Sanction.
- Until the evaluations on the scan results are completed by the authorized persons for this transaction, the customer is not accepted, and the transaction is not carried out.
- Existing customers are regularly scanned to check if they are included in such lists.

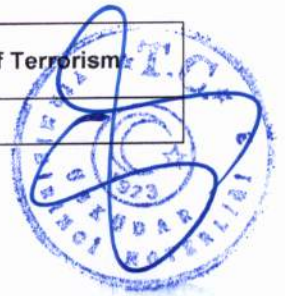
The Bank does not establish business relations with the individuals and organizations listed below; terminates the business relationship with the customers included in this scope later, without prejudice to the legal regulations; and in case of obligations under the legislation, notifications are made to the relevant authorities.

- Individuals and organizations subject to United Nations Security Council (UNSC) sanctions pursuant to the Presidential Decisions published in the Official Gazette,
- Individuals and organizations listed as Specially Designated Nationals (SDNs) by the U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC),
- Organizations in which SDN individuals and organizations directly or indirectly hold 50% or more of shares,
- Persons and organizations residing/registered in the Country/Region Subject to Comprehensive Sanctions.

Policy and Codes of Practice on Prevention of Laundering Crime Revenues and Financing of Terrorism

Document: POL\_AML\_03

Page: 16 of 24



I hereby certify that  
this text was translated by  
me from TR to ENG  
as true to its original  
Sworn Translator

13 Ocak 2022

## 6 OBLIGATION OF MONITORING AND CONTROL

The Bank carries out monitoring and control activities with a risk-based approach by considering the nature of the transactions carried out by the customers. The purpose of monitoring and control is to protect the Bank from risks and to continuously monitor and control whether its activities are carried out according to the Law and the regulations and communiqués introduced pursuant to the Law, and institution policies procedures.

In this context, the monitoring and control activities required to be carried out at the Bank within the framework of the legislation mentioned above include the following:

- a) Monitoring and control of high-risk customers and transactions,
- b) Monitoring and control of transactions with risky countries,
- c) Monitoring and control of complex and unusual transactions,
- d) Control of the information and documents about customers that must be kept electronically or in writing, and information that must be included in electronic transfer messages by sampling method, and ensuring that deficiencies are completed and that they are updated,
- e) Continuously monitoring, throughout the business relationship, whether the transactions carried out by its customers are compatible with the profession, commercial activities, business history, financial situation, risk profile, and funding sources of the customers; and keeping up-to-date information, documents, and records about its customers,
- f) Control of transactions carried out using methods or systems that enable non-face-to-face transactions,
- g) Risk-based control of services that may be exposed to abuse due to newly introduced products and technological developments, and
- h) Following the news reflected in the media regarding the laundering of crime revenues or the financing of terrorism. Checking whether the persons mentioned in the related news are customers of our Bank by contacting the relevant departments and examining the transactions if any.

Regarding the persons and institutions who are new/existing customers that are included in the international banned lists before starting the transactions or during the controls; after confirming that these persons or institutions are included in the lists mentioned above, the relevant units must inform the Regulatory Compliance Directorate via internal communication and/or e-mail.

13 Ocak 2022

Policy and Codes of Practice on Prevention of Laundering Crime Revenues and Financing of Terrorism	
Document: POL_AML_03	Page: 17 of 24

I hereby certify that  
 this text was translated by  
 me from TR to ENG  
 as true to its original  
 Sworn Translator



## 7 DETECTION AND REPORTING PROCEDURE OF SUSPICIOUS TRANSACTIONS

If there is any information, suspicion, or any reason to suspect that the money and the values that can be represented by money, which are the subject of the transactions made or attempted to be carried out at or through our Bank, are obtained illegally or used for illegal purposes; used by terrorist organizations and for the financing of terrorism or for terrorist acts, even if obtained legally; or in any way related to terrorism, the suspicious transaction is reported to MASAK about those who carry out the transaction.

Suspicious transactions should be reported regardless of monetary limits.

Suspicious Transaction Reportings are confidential. Therefore, except for the information given to the inspectors assigned with liability supervision and to the courts during the trial, the information that a suspicious transaction has been or will be reported to MASAK should not be given to anyone, including the parties to the transaction.

Individuals and organizations with suspicious transaction reports are not notified about the transaction.

Pursuant to Article 10 of Law No. 5549, the Bank and its personnel fulfilling the suspicious transaction reporting obligation cannot be held liable in any legal or penal manner due to the fact that they have reported suspicious transactions.

On the other hand, the Compliance Officer conducts the necessary investigation regarding the suspicious transaction report and notifies the Financial Crimes Investigation Board of the Ministry of Treasury and Finance pursuant to the legislation within ten business days at the latest from the date of suspicion regarding the transaction.

If new information and findings are obtained later regarding the reported transaction, the Suspicious Transaction Reporting Form must be filled out again by stating that it is an addition to the previous notification and sent to the Board without undue delay. Therefore, it is important to pay special attention to reported customers and monitor them closely. Suspicious transaction types (Appendix-3) included in the Suspicious Transaction Reporting Guide published by MASAK should not be considered as a single criterion by the related units. Suspicious transaction reporting can be made even if it does not comply with any of the types included in the Suspicious Transaction Reporting Guide.

### The following are grounds for reporting suspicious transactions:

- Whether the customer is voluntary to give his/her personal information,
- No apparent legal or economic purpose,
- Providing misleading information, documents, and contact information,
- Making loan requests for cash that has no intended use, and that is not specified where it will be used,
- Giving misleading, insufficient explanations and unconfirmed information,

Policy and Codes of Practice on Prevention of Laundering Crime Revenues and Financing of Terrorism

Document: POL\_AML\_03

Page: 18 of 24

I hereby certify that  
this text was translated by  
me from ...TR... to ...ENG...  
as true to its original  
Sworn Translator



13 Ocak 2022

№ 1866

- Making a loan/insurance request with documents such as a non-related and non-proportional contract to the customer's income and business,
- Making an insurance claim with false documents,
- The conviction that the export documents are fake,
- Complex and unusually large transactions and transactions that don't seem to have a reasonable legal and economic purpose.

In such cases, the Regulatory Compliance Manager (**Compliance Officer**) must be notified directly by preparing a Suspicious Transaction Reporting Form without undue delay. Notifications should be made by e-mail and internal communication.

Before the notification, during the investigation of the suspected transaction, attitudes and behaviors that will cause the customer to suspect that a notification will be made about him/her should be avoided.

In addition, suspicious transactions detected during the inspections carried out by the Internal Control and Inspection Board Departments are reported to the Compliance Officer in order for the same to be subject to notification regardless of the amount.

The information and documents requested by the Compliance Officer from the Liaison Offices/Branches/Regional/Head Office units must be delivered on time.

It is the Compliance Officer's authority to decide whether to report a suspicious transaction sent to the Compliance Department. In cases where the Compliance Officer finds it unnecessary to notify MASAK of the notifications received from the units, the Compliance Officer stores the justification of his/her opinion as a written decision.

The STRF, which is decided to be notified, can be faxed to the Board by the compliance officers with a cover letter. However, regardless of whether it was sent by fax, the notification is sent to the address of the "Republic of Turkey, Ministry of Treasury and Finance, Financial Crimes Investigation Board" by registered mail or by hand. Suspicious transaction reporting can also be made electronically using the MASAK.ONLINE system.

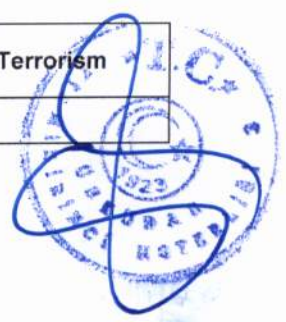
If a suspicious transaction is not reported about a transaction that should be suspected pursuant to Law No. 5549, an administrative fine is imposed on both the Bank and the personnel who perform, approve and fail to report the transaction in the amounts specified in the relevant regulations.

The Bank and its personnel fulfilling the suspicious transaction reporting obligation shall not be held liable in any legal or penal manner due to the fact that they have reported suspicious transactions.

If any information regarding suspicious transaction reporting is disclosed to third parties, those who disclosed such information shall be subject to a prison sentence and a judicial fine as specified in Law No. 5549.

13 Ocak 2022

Policy and Codes of Practice on Prevention of Laundering Crime Revenues and Financing of Terrorism	
Document: POL_AML_03	Page: 19 of 24



I hereby certify that  
 this text was translated by  
 me from ~~TR~~ to ~~ENG~~  
 as true to its original  
 Sworn Translator

Under the supervision of our Bank's General Manager, the compliance officer, and the senior manager of the relevant unit shall decide whether the existing customer relationship with the individuals or organizations that are the subject or party to the suspicious transaction reporting will be continued or not. When necessary, MASAK's opinion is taken on this matter.

### 7.1 SUSPENDING THE TRANSACTION BASED ON SUSPICIOUS TRANSACTION REPORTING

If there is **a document or serious indication that supports the suspicion** that the asset subject to the transaction attempted to be made or is currently in progress at or through the Bank is related to the crime of money laundering or financing of terrorism, the Suspicious Transaction Reporting should be sent to MASAK with the justifications with the request of the suspension of the transaction.

In case Suspicious Transaction Reporting is sent to MASAK with a request to suspend the transaction, the execution of the transaction should be refrained from until the decision about the transaction is notified to the Bank by MASAK. The suspension of the transaction is seven business days from the date of the suspicious transaction report.

13 Ocak 2013

### 8 OTHER OBLIGATIONS UNDER REGULATIONS ON PREVENTION OF FINANCING OF TERRORISM AND PROLIFERATION OF WEAPONS OF MASS DESTRUCTION

In addition to the measures to prevent money laundering in order to avoid risks and abuse in Financing of Terrorism, the Bank also acts with a risk-based approach to the prevention of Financing of Terrorism.

The Bank does not collect or provide funds for or for the benefit of or enter into any business partnerships or other business relationships in Turkey with

- individuals or organizations specified in Law No 6415 on Prevention of Financing of Terrorism, UNSC decisions and annexes thereto mentioned in the Law No 7262 on Preventing the Financing of Proliferation of Weapons of Mass Destruction, or the individuals or organizations directly or indirectly controlled by, or on behalf of, or on account of them.

The Bank does not establish business partnerships with the Banks of individuals, institutions, or organizations specified in these decisions, or the individuals or organizations directly or indirectly controlled by, or on behalf of, or on account of them; does not provide any financial services; does not establish a correspondent bank relationship, and terminates any existing one.

Policy and Codes of Practice on Prevention of Laundering Crime Revenues and Financing of Terrorism	
Document: POL_AML_03	Page: 20 of 24



I hereby certify that  
 this text was translated by  
 me from TR to ENG...  
 as true to its original  
 Sworn translator

1866

### 8.1 ASSET FREEZE / RELEASE PROCEDURES

Pursuant to the Law on Preventing the Weapons of Mass Destruction, the Law on the Prevention of the Financing of Terrorism, and the applicable legislation, the Presidential decision to freeze assets and release such decisions is published in the Official Gazette. These decisions shall be deemed to have been notified to the relevant person, institution, or organization for which the decision to freeze assets was made on the date of publication.

Decisions published in the Official Gazette are announced by e-mail. An investigation is requested from the related units with internal communication. Information regarding the absence of assets at our Bank or the absence of any record of assets shall be notified to the Presidency without delay or within seven days from the date of notification, using the notification method used in the notifications made at our Bank.

The assets of the organizations specified in UNSC decisions, or the individuals or organizations directly or indirectly controlled by, or on behalf of, or on account of them are frozen without delay by the Presidential decision published in the Official Gazette.

Notifications regarding the execution of the freezing of assets decisions and/or documents in all kinds of media regarding the transactions made after the publication of the decisions in the Official Gazette must be kept for eight years from the issuance date, and the books and records must be kept for eight years from the last registration date and submitted to the authorities if requested.

### 9 COMPLIANCE OFFICER

The compliance officer is appointed exclusively as personnel of the institution, reporting to the board of directors or to one or more members to whom the board of directors has delegated its authority.

The compliance officer at our Bank is the Regulatory Compliance Department Manager.

#### **Compliance Officer's duties, powers, and responsibilities:**

- a) To carry out the necessary studies in order to ensure the compliance of the Bank with the Law and the regulations enacted in accordance with the Law, and to ensure the necessary communication and coordination with the Board,

13 Ocak 2022

Policy and Codes of Practice on Prevention of Laundering Crime Revenues and Financing of Terrorism	
Document: POL_AML_03	Page: 21 of 24



I hereby certify that  
 this text was translated by  
 me from TR to ENG  
 as true to its original  
 Sworn Translator

1866

- b) To create policies and procedures within the scope of the applicable legislation and submit the same to the approval of the Board of Directors,
- c) To evaluate the information and findings obtained *ex-officio* or by investigating within the limits of his/her powers and possibilities regarding the suspicious transactions communicated to him/her, and notify the Board of the transactions s/he decided to be suspicious.
- d) To take the necessary measures to ensure the confidentiality of reporting and other related issues,
- e) To ensure the necessary communication and coordination with the Board and to submit the said information and documents in accordance with the format and method determined and notified to him/her by the Board, in cases where information and documents are requested,
- f) To respond to the letters sent from MASAK within the scope of the Presidential Decree regarding the freezing assets and release of decisions,
- g) To determine the training programs jointly with the Human Resources Department, and
- h) To carry out risk management, monitoring, and control procedures by considering the risks determined within the scope of the national risk assessment and to ensure the necessary communication and coordination with the Board on the subject.

13 Ocak 2022

### 10 INTERNAL AUDIT

The internal audit units yearly inspect the Bank's activities with a risk-based approach pursuant to the principles set forth in this Policy, the provisions of Law No 5549 on Prevention of Laundering Crime Revenues, Law No 6415 on Prevention of Financing of Terrorism, Law No 7262 on Preventing the Financing of Proliferation of Weapons of Mass Destruction, as well as the regulations and communiqués introduced within the scope of these laws. Findings of the internal audit are directed to the Regulatory Compliance Department, and necessary measures are taken by the relevant department to eliminate the deficiencies. The deficiencies, errors, and abuses revealed as a result of the internal audit and opinions and suggestions to prevent reoccurrence are reported to the Board of Directors by the Compliance Officer.

### 11 TRAINING ACTIVITIES

It is aimed to increase the awareness of the personnel on the subject with the training activities in order to ensure compliance with the relevant regulations and minimize the legislation risk.

Policy and Codes of Practice on Prevention of Laundering Crime Revenues and Financing of Terrorism	
Document: POL_AML_03	Page: 22 of 24



I hereby certify that  
 this text was translated by  
 me from TR to ENG.....  
 as true to its original  
 Sworn Translator

With regard to the Prevention of Laundering Crime Revenues and Financing of Terrorism; the Bank organizes training in compliance with the Bank's size, business volume, and changing conditions in order to create a corporate culture and update the employee's information by increasing the sense of responsibility on corporate policy and procedures, and risk-based approach. Training activities are carried out under the supervision and coordination of the Compliance Officer.

### 12 SUBMISSION OF INFORMATION AND DOCUMENT

Maximum effort is used to submit any information, document and related records in any media to be requested by the Board and audit staff, and to submit any information and passwords necessary to access these records available or make the same readable in an accurate and complete manner in the requested method, form and time.

Information may be requested verbally or in writing. In order to prevent any disruption in communication and any deficiencies in the records, it is essential to make the aforementioned applications with the knowledge of and through the relevant department, and for the results to be followed up by the relevant department.

It is essential to provide any information and document requested by the Financial Crimes Investigation Board and the audit staff pursuant to the Laws. In case of violation of the obligation to provide continuous information and the obligation to provide information and documents, fines and/or imprisonment determined in the applicable Laws are imposed on the person who violates the obligation.

### 13 STORAGE OF RECORDS

The information and documents are kept for periods specified in the applicable legislation in order to be submitted when necessary.

Suspicious transaction notifications are also within the scope of the storing and submission obligation.

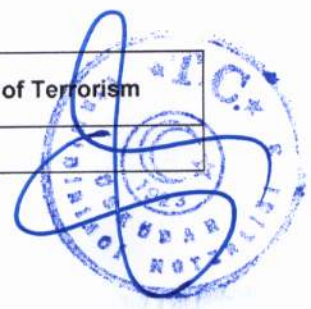
In case a notification is made by being found in the records of our Bank regarding the freezing/release of assets in the Presidential Decision and the prohibited transactions and activities within the scope of the Law No 7262 on Preventing the Financing of Proliferation of Weapons of Mass Destruction; it is obligatory to preserve and submit the documents belonging to these individuals and transactions in any media for 8 years as of the date of issue, and books and records for 8 years as of the last registration date.

With regard to the obligations and transactions imposed to our Bank by Law No. 5549; it is required for

- the documents,
- books and records,

13 Ocak 2022

Policy and Codes of Practice on Prevention of Laundering Crime Revenues and Financing of Terrorism	
Document: POL_AML_03	Page: 23 of 24



I hereby certify that  
 this text was translated by  
 me from TRK to ENG....  
 as true to its original  
 Sworn Translator



• identification documents  
to be kept for eight years from the date of issue, last registration date, and latest transaction date, respectively, and to be submitted to the authorities upon request.  
Penalties stipulated in the applicable Laws are applied to those who violate the above-mentioned rules regarding the Storage of the Records.

#### 14 ENFORCEMENT AND REVIEW

This policy and implementation principles enter into force upon approval by the Bank's Board of Directors. The policy is reviewed at least once a year in order to maintain compliance with the legislation and international standards, and, if necessary, updates are made and submitted to the approval of the Board of Directors.

General Directorate Units, Regional Directorate Units, Branches, and Liaison Offices are responsible for the implementation of the provisions of this document.

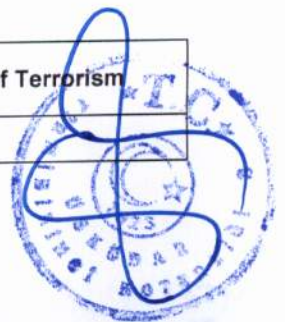
The Regulatory Compliance Department updates the document and its appendices in parallel with the amendments in legal regulations and practices.

13 Ocak 2022

#### 15 APPENDICES

- 1) Identification Procedures,
- 2) Prevention of Money Laundering Questionnaire.
- 3) Types of Suspicious Transaction and Suspicion Categories Reference Table.
- 4) Suspicious Transaction Reporting Form

Policy and Codes of Practice on Prevention of Laundering Crime Revenues and Financing of Terrorism	
Document: POL_AML_03	Page: 24 of 24



Thereby certify that  
this text was translated by  
me from ~~TR~~ to **ENG**....  
as true to its original  
Sworn Translator