

ANADOLU SİGORTA**ANTI-MONEY LAUNDERING, COUNTER-TERRORIST FINANCING AND SANCTIONS POLICY****TABLE OF CONTENTS**

1. GENERAL PROVISIONS.....	1
1.1. PURPOSE AND SCOPE.....	1
1.2. DEFINITIONS	1
1.3. AUTHORITY AND RESPONSIBILITIES	3
2. RISK MANAGEMENT.....	4
2.1. PURPOSE AND SCOPE OF RISK MANAGEMENT ACTIVITIES.....	4
2.2. KNOW YOUR CUSTOMER (KYC) PRINCIPLE AND CUSTOMER ACCEPTANCE PRINCIPLES	4
2.3. CUSTOMER IDENTIFICATION PROCEDURE AND RECORDING OF INFORMATION.....	5
2.4. IDENTIFICATION OF THE BENEFICIAL OWNER	10
2.5. OBTAINING ADEQUATE INFORMATION ON THE PURPOSE OF TRANSACTIONS	10
2.6. ONGOING MONITORING OF CUSTOMERS AND TRANSACTIONS.....	10
2.7. SANCTIONS	10
2.8. TAKING NECESSARY MEASURES FOR CUSTOMERS, ACTIVITIES, AND TRANSACTIONS REQUIRING SPECIAL ATTENTION	11
2.8.1.Reinsurers	11
2.8.2.Transactions of Customer Resident in or Connected with High-Risk Geographical Areas.....	11
2.8.3.Sectors and Lines of Business Vulnerable to Money Laundering	11
2.8.4.Insurance Transactions Related to Predicate Offenses.....	12
2.8.5.All Types of Claims Transactions.....	12
2.8.6.Cash Transactions	12
2.8.7.Transactions of Non-Profit Charitable Organizations.....	12
2.8.8.Non-Face-to-Face Transactions and New Products Offered Using Emerging Technologies ..	12
2.8.9.Enhanced Due Diligence Measures	12
2.8.10.Politically Exposed Persons (PEPs).....	13
2.8.11.Crypto Asset Service Providers (CASPs).....	13
2.9. RELIANCE ON THIRD PARTIES.....	13
2.10.SIMPLIFIED MEASURES	14
2.11.RISK MANAGEMENT ACTIVITIES	14
2.11.1.Identification and Classification of Risks	15
2.11.2.Monitoring and Assessment of Risks	15
2.11.3.Authorization Limits	15
2.11.4.Reporting	15
3. MONITORING AND CONTROL	16
3.1. PURPOSE AND SCOPE OF MONITORING AND CONTROL ACTIVITIES	16
3.2. MONITORING AND CONTROL ACTIVITIES	16
3.2.1.Key Controls Under Monitoring and Control Activities	16
3.2.2.Reporting	17
4. TRAINING.....	17
4.1. TRAINING POLICY	17
4.2. TRAINING ACTIVITIES	17
4.2.1.General Principles.....	17
4.2.2.Training Topics.....	18
4.2.3.Training Methods.....	18

4.2.4.	Selection and Development of Participating Personnel and Trainers.....	18
4.2.5.	Training Activity Program	18
5.	INTERNAL AUDIT	19
5.1.	PURPOSE AND SCOPE OF INTERNAL AUDIT ACTIVITIES	19
5.2.	INTERNAL AUDIT ACTIVITIES.....	19
5.2.1.	General Principles.....	19
6.	SUSPICIOUS TRANSACTION REPORTING, ASSET FREEZING, AND OTHER PROVISIONS	20
6.1.	DETECTION, REPORTING, AND CONFIDENTIALITY OF SUSPICIOUS TRANSACTIONS	20
6.2.	PRINCIPLES REGARDING ASSET FREEZING	20
6.3.	PRINCIPLES ON PROVIDING INFORMATION AND DOCUMENTS AND RECORD RETENTION	20
6.4.	MISCELLANEOUS PROVISIONS	21
6.5.	ENTRY INTO FORCE	21

PART I

1. GENERAL PROVISIONS

1.1. PURPOSE AND SCOPE

The Company embraces and values the fight against Money Laundering and Terrorist Financing as a corporate social responsibility beyond mere compliance with laws and regulations. Holding a reputable and trustworthy position in the international arena, our Company has placed special emphasis on alignment with the international financial system throughout its operations since its establishment.

Within this framework, the purpose of this Policy is to ensure the compliance of Anadolu Anonim Türk Sigorta Şirketi with its obligations regarding the Prevention of Laundering Proceeds of Crime, the Prevention of Financing of Terrorism, and the Prevention of Financing of the Proliferation of Weapons of Mass Destruction; to determine the strategies, internal controls and measures, operational rules, and responsibilities aimed at mitigating potential risks by evaluating its customers, transactions, and services through a risk-based approach; and to strengthen the corporate culture regarding financial crime compliance and sanctions.

This Policy also encompasses the duties and responsibilities of all units, executives, personnel, and other relevant parties of the Company.

1.2. DEFINITIONS

The terms used in this Policy document shall have the meanings set forth below:

Assets: Funds and proceeds partially or wholly owned or possessed by, or directly or indirectly controlled by, a natural person or legal entity, along with the benefits and value derived from them or resulting from their conversion into one another; as well as funds and proceeds partially or wholly owned or possessed by a natural person or legal entity acting on behalf or for the account of such person, along with the benefits and value derived from them or resulting from their conversion into one another,

Beneficial Owner (Ultimate Beneficial Owner): Natural persons conducting transactions with the Company, or the natural person or persons who ultimately control or exercise ultimate influence over the natural persons, legal entities, or unincorporated entities on whose behalf a transaction is conducted,

Compliance Officer: The personnel appointed, as stipulated in relevant legal regulations, reporting directly to the Board of Directors or to one or more Board members to whom the Board of Directors has explicitly and in writing delegated its authority, for the purpose of executing the Compliance Program for obligations regarding the Prevention of Laundering Proceeds of Crime and Financing of Terrorism,

Compliance Program: The set of measures to be established for the Prevention of Laundering Proceeds of Crime and Financing of Terrorism, the scope of which is defined in Article 5 of the Regulation on Program of Compliance,

Compliance Risk: Risks related to penalties, financial losses, and/or reputational damage to which the Company may be exposed as a result of the Company's activities or the attitudes and behaviors of Company employees not being in compliance and harmony with legislation, regulations, and standards,

Compliance Unit: The unit assigned by the Board of Directors to execute the Compliance Program, reporting directly to the Compliance Officer in order to ensure that the Compliance Officer effectively fulfills the duties and responsibilities imposed by relevant legal regulations,

Comprehensively Sanctioned Countries/Regions: Countries or regions subject to country-wide or regional sanctions imposed by the Republic of Türkiye, the United Nations Security Council, the United States of America, the European Union, and the United Kingdom,

Country Risk: The risk to which the Company may be exposed due to business relationships and transactions it enters into with citizens, companies, and financial institutions of countries announced by the Ministry among those that lack adequate regulations on preventing money laundering and terrorist financing, do not

cooperate sufficiently in combating these crimes, or are considered risky by competent international organizations,

Customer Risk: The risk of the Company being abused due to the customer's line of business enabling intensive cash use, trading of high-value goods, or easy execution of international fund transfers, or due to the customer or those acting on behalf or for the account of the customer acting for the purpose of money laundering or terrorist financing,

Delaying Transaction: Refraining from executing a transaction requested to be conducted before the Company within the framework of the principles set forth in the legislation,

Deputy Compliance Officer: Company personnel who meet the qualifications and requirements sought for a Compliance Officer for the purpose of executing the Compliance Program and who work under the Compliance Officer to fulfill the duties specified in the relevant legislation,

Financial Action Task Force (FATF): The inter-governmental body established to develop international standards and policies to combat Money Laundering and Terrorist Financing and to ensure their implementation,

Financial Group Policy: The Policy for Combating Financial Crimes and Sanctions of Türkiye İş Bankası A.Ş.,

Financial Group: A group consisting of financial institutions resident in Türkiye that are affiliated with or controlled by a parent institution headquartered in Türkiye or abroad, along with their branches, agencies, representatives, commercial proxies, and similar affiliated units,

Financing of Proliferation of Weapons of Mass Destruction (Proliferation Financing): The acts of collecting any kind of funds or providing financial services, directly or indirectly, in whole or in part, for the purpose of manufacturing, developing, acquiring (including both technologies and dual-use goods used for illegitimate purposes), stockpiling, transporting, trading, or using nuclear, radiological, chemical, or biological weapons in violation of national laws or international obligations, as well as any transactions and activities that assist in the realization of such activities,

Financing of Terrorism: The provision or collection of funds to a terrorist or terrorist organizations with the intention that they be used, or in the knowledge and willingness that they are to be used, in whole or in part, in carrying out acts regulated as offenses under the law, even without being linked to a specific act,

Freezing of Assets (Asset Freezing): The removal or restriction of the power of disposition over the asset for the purpose of preventing obliteration, consumption, conversion, transfer, assignation, conveyance and other dispositional actions of the asset,

Know Your Customer (KYC) Principle: The principle, set forth among the measures to be taken by financial and non-financial institutions and business and profession owners to prevent Money Laundering and Terrorist Financing within the framework of FATF Recommendations, of exercising due care in obtaining complete and accurate information regarding customers and adopting the implementation of all necessary measures,

Legislation: Applicable laws, regulations, and communiqués regarding the prevention of Money Laundering and Terrorist Financing, as well as decisions and instructions published by the Presidency,

MASAK / The Presidency: The Presidency of the Financial Crimes Investigation Board of Türkiye (*Mali Suçları Araştırma Kurulu Başkanlığı*),

Money Laundering: Transactions aimed at legitimizing proceeds obtained through illegal means by introducing such proceeds into the financial system—particularly to divest them of their cash form—and altering their identity and nature by passing them through a process within the financial system so as to make them appear to have been acquired through legitimate means,

Policy: The Company's Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Policy,

Politically Exposed Person (PEP): Senior natural persons entrusted with a prominent public function domestically or in a foreign country through election or appointment, as well as board members, senior executives, and other persons holding equivalent positions in international organizations,

Regulation on Measures: The Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism which was published in the Official Gazette No. 26751 on 09/01/2008,

Risk: The probability of financial or reputational loss to which the Company or Company employees may be exposed due to reasons such as the utilization of services provided by the Company for the purpose of money laundering or terrorist financing, or the Company's failure to fully comply with the obligations introduced by the laws, the regulations, and communiqués issued pursuant to the Law,

Sanctions: Regulations aimed at restricting or prohibiting economic activities, either individually or comprehensively, targeting countries, individuals, and entities in order to achieve economic and political objectives.

Senior Management: The Chief Executive Officer, Deputy Chief Executive Officers, and the heads of units within the scope of Internal Systems,

Service Risk: Risks that may be incurred within the scope of non-face-to-face transactions or new products to be offered using emerging technologies,

Suspicious Transaction: The existence of any information, suspicion, or reasonable grounds to suspect that the assets subject to transactions conducted or attempted to be conducted before or through the Company have been obtained through illegal means or used for illegal purposes, including being used for terrorist acts or by terrorist organizations, terrorists, or those who finance terrorism, or being related or linked to them,

The Company: Anadolu Anonim Türk Sigorta Şirketi (Anadolu Insurance),

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

1.3. AUTHORITY AND RESPONSIBILITIES

All authorized personnel conducting the Company's operations are presumed to know the Company's Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Policy and implementation procedures, and to have obtained all necessary intelligence regarding customer acceptance. Authorized personnel involved in all business processes are responsible for the transactions they execute within the framework of their duties in the process. Authorized personnel participating in this process are responsible for the completeness, accuracy, and reliability of all data and information provided by them that serve as the basis for decision-making.

The Compliance Officer is ultimately responsible to the Board of Directors for ensuring necessary communication and coordination with the Presidency, establishing the policy and implementation procedures regarding the prevention of laundering proceeds of crime and financing of terrorism, and conducting risk management, monitoring, control, and training activities in this regard. The Compliance Officer may explicitly and in writing delegate part or all of their duties and authorities to the Deputy Compliance Officer.

The unit assigned to execute the Compliance Program and defined as the Compliance Unit in this Policy document operates under the Compliance Officer in fulfilling the duties and responsibilities within the scope of the Compliance Program.

The operational effectiveness and adequacy of this Policy and the Compliance Program are subject to regular audit and evaluation by the Board of Auditors within the scope of internal audit.

The Board of Directors of the Company is ultimately responsible for the adequate and effective execution of the Compliance Program as a whole within the framework of this Policy. As the approving authority of this Policy, the Board of Directors is authorized and responsible within the scope of the Compliance Program to:

- Ensure the Company's compliance with obligations regarding the prevention of money laundering and terrorist financing,
- Approve the Policy, annual training programs, and any amendments thereto in line with developments,
- Appoint a Compliance Officer and one or more Deputy Compliance Officers who meet the qualifications and conditions required by the legislation,
- Approve and put into effect the Operating Regulation governing the duties, authorities, and responsibilities of the Compliance Officer, Deputy Compliance Officer, and the Compliance Unit,

- Evaluate the results of risk management, monitoring and control, and internal audit activities and ensure that necessary measures are taken, and
- Ensure that all activities are carried out in a coordinated and effective manner.

While retaining ultimate responsibility, the Board of Directors may delegate all or part of its aforementioned authorities under the Compliance Program to one or more Members of the Board of Directors.

Senior Management is responsible to the Board of Directors for ensuring that the Policies approved by the Board of Directors—or, where authority has been delegated, by the relevant delegated Board Member(s)—are implemented appropriately and effectively by all employees, that business processes and job descriptions are established in alignment with the Policy, and that necessary measures against potential risks arising in this context are taken in a timely manner.

The Company complies with the Financial Group Policy, takes all necessary measures to remain compliant with the Policy, and fulfills all requirements thereof.

PART II

2. RISK MANAGEMENT

2.1. PURPOSE AND SCOPE OF RISK MANAGEMENT ACTIVITIES

The primary purpose of risk management activities is to ensure the identification, rating, monitoring, assessment, and mitigation of risks to which the Company is exposed in connection with the potential abuse of its insurance services for the purpose of money laundering or terrorist financing. Achieving this ultimate goal is ensured by effectively monitoring and controlling customers and transactions in full compliance with legal legislation.

The general scope of risk management activities comprises centralized identification, measurement, monitoring, control, and reporting activities addressing the risks incurred due to the potential abuse of insurance services provided by the Company for the purpose of money laundering, terrorist financing, and financing of the proliferation of weapons of mass destruction, or due to the Company's failure to fully comply with the obligations introduced by Law No. 5549 on Prevention of Laundering Proceeds of Crime, Law No. 6415 on Prevention of The Financing of Terrorism, Law No. 7262 on Prevention of The Financing of the Proliferation of Weapons of Mass Destruction, and relevant regulations and communiqués.

The fundamental strategy toward this goal is to carefully plan, execute, and manage risk management activities through a risk-focused approach and within the framework of relevant legislation as well as internationally accepted principles, rules, and standards—in an independent, impartial, purposeful, efficient, and effective manner. Accordingly, it is essential to utilize the most advanced tools and methods that are feasible and appropriate.

2.2. KNOW YOUR CUSTOMER (KYC) PRINCIPLE AND CUSTOMER ACCEPTANCE PRINCIPLES

At the core of our Company's customer acceptance process in combating financial crimes lies the "Know Your Customer" (KYC) principle. As the most effective way of protecting against individuals and entities associated with financial crimes and sanctions, policies, principles, and practices compliant with legal regulations are adopted under this principle.

In order to ensure transparency in customer transactions and information, and to establish and maintain a relationship built on mutual trust, customer acceptance is realized upon performing necessary procedures and obtaining adequate knowledge regarding the following matters:

- a) Identification and verification of identity and address,
- b) Profession and primary income-generating business activity,
- c) Information and documents regarding the insured or the insured asset,

d) Internal consistency of documents and information.

If doubts arise regarding the adequacy and accuracy of previously obtained information after the establishment of the customer relationship, necessary verifications are performed immediately; where verification cannot be completed, the business relationship is terminated. Furthermore, business relationships are terminated with customers for whom a termination decision has been taken within the scope of monitoring, control, and risk management activities, as well as customers who fall under the scope of section "2.7. SANCTIONS" after their customer record has been created.

As an exception to the termination of a business relationship, all rights and receivables of individuals, entities, or organizations that become subject to asset freezing decisions under Law No. 6415 on Prevention of The Financing of Terrorism and Law No. 7262 on Prevention of The Financing of the Proliferation of Weapons of Mass Destruction after a customer record has been created shall be frozen and reported to the Presidency within the periods stipulated by law.

2.3. CUSTOMER IDENTIFICATION PROCEDURE AND RECORDING OF INFORMATION

Pursuant to the principles regarding customer due diligence, under the following conditions:

- When the transaction amount or the total amount of multiple linked transactions is equal to or exceeds the threshold triggering the customer identification obligation under the relevant legislation,
- Regardless of the amount, in cases requiring suspicious transaction reporting,
- Regardless of the amount, when there is doubt as to the adequacy and accuracy of previously obtained customer identification information,

it is a statutory requirement to identify customers and those acting on behalf or for the account of customers by obtaining their identity information within the framework of relevant legislation and verifying the accuracy of such information against official verification documents.

Customer identification must be completed prior to establishing a business relationship or executing a transaction.

The following principles are observed in the customer identification procedure and in recording declared addresses:

- a) Customer identification is carried out in accordance with the documents and obligations specified in the Regulation on Measures and the explanations issued by the Presidency on the subject.
- b) At the policy issuance stage, it is essential to identify the person taking out the insurance policy (the policyholder). At the claims payment stage, if the parties are different persons, separate identification is performed for the insured or the beneficiary.
- c) The identities and authorization of individuals claiming to act on behalf of the customer are verified.
- d) It is essential that customer information be recorded in our IT system and be accessible for centralized querying by authorized personnel.
- e) Necessary measures are taken to determine whether a person is acting for the account of another person. In this context, in order to remind individuals who act in their own name but for the account of another person of their legal responsibilities, required notices are posted in a clearly visible manner for customers at all premises where services are provided.
- f) Depending on the customer types defined within the legislation and detailed below, following the presentation of the originals or notarized copies of the verification documents during identification, legible photocopies or electronic images thereof are taken, or identity details are recorded, to be submitted to competent authorities upon request.

The implementation principles regarding the customer identification procedure and recording of information enter into force upon approval by the Member of the Board of Directors to whom the Board of Directors has

delegated its authority pursuant to the provisions of Regulation On Program Of Compliance With Obligations Of Anti-Money Laundering And Combating The Financing Of Terrorism.

Customer Identification of Natural Persons

In customer identification of natural persons, their name, surname, date of birth, nationality, type and number of the identity document, address, sample of signature, information on his/her occupation and profession and telephone number, fax number, e-mail, if any, and for Turkish citizens, as additional information, T.R. identity number, and place of birth for non-Turkish citizens shall be received.

The accuracy of the individual's first name, surname, date of birth, T.C. ID Number, and the type and number of the identity document is verified through:

- a) For Turkish nationals: Republic of Türkiye identity card, Republic of Türkiye driver's license, or passport, as well as identity documents bearing a T.C. ID Number that are explicitly stated in their special laws to have the status of an official identity document,
- b) For non-Turkish nationals: Passport, residence permit, or an identity document deemed appropriate by the Ministry.

In customer identification conducted via Republic of Türkiye driver's licenses issued prior to 1/1/2016, verification of the accuracy of the T.C. ID Number is not mandatory.

Customer Identification of Legal Persons Registered to Trade Registry

In customer identification of legal persons registered to trade registry, the title of the legal person, its trade registry number, tax identity number, field of activity, full address, telephone number, fax number and e-mail, if any, and the name, surname, date of birth, nationality, type and number of the identity document, and a sample signature of the person authorized to represent the legal person and for Turkish citizens, as additional information, T.R. identity number, and place of birth for non-Turkish citizens shall be received.

Verification of the legal entity's trade name, trade registry number, field of activity, and address is performed via trade registry registration documents; verification of the tax identification number is performed via documents issued by the relevant unit of the Revenue Administration. The accuracy of the identity information of persons authorized to represent the legal entity is verified via the identity documents specified under the heading "Customer Identification of Natural Persons", and their authority to represent is verified via registration documents.

Customer Identification of Associations and Foundations

In customer identification of associations the name of the association, its aim, log number, tax ID number, full address, telephone number, fax number and e-mail, if any, and the name, surname, date of birth, nationality, type and number of the identity documents and sample signature, and for Turkish citizens, as additional information, T.R. identity number, and place of birth for non-Turkish citizens of the person authorized to represent the association shall be received.

The association's name, aim, log number and full address of the association shall be verified through the charter of the association and documents of registry in the associations' log; tax ID number shall be verified through documents issued by the relevant unit of the Revenue Administration; the accuracy of identity information of persons authorized to represent the association is verified via the identity documents specified under "Customer Identification of Natural Persons"; and their representation authority is verified via documents evidencing their authorization to represent.

In customer identification of foundations the name of the foundation, its aim, central registration number, tax ID number, full address, telephone number, fax number and e-mail address, if any, and the name, surname, date of birth, nationality, type and number of the identity document and sample signature of the person authorized to represent the foundation and for Turkish citizens, as additional information, T.R. identity number and place of birth for non-Turkish citizens shall be received.

The foundation's name, central registration number and full address of the foundation shall be verified through foundation deed and registration documents kept by the General Directorate of Foundations; tax ID number shall be verified through documents issued by the relevant unit of the Revenue Administration; the accuracy of identity information of persons authorized to represent the foundation is verified via the identity documents specified under "Customer Identification of Natural Persons"; and their representation authority is verified via documents evidencing their authorization to represent.

Customer Identification of Trade Unions and Confederations

In customer identification of trade unions and confederations; the name of the organization, its aim, registry number, tax ID number, full address, telephone number, fax number and e-mail, if any, and the name, surname, date of birth, nationality, type and number of the identity document and sample signature of the person authorized to represent the trade unions and confederations and for Turkish citizens, as the additional information, T.R. identity number and place of birth for non-Turkish citizens shall be received.

The information gathered shall be verified through charter of these organizations and other registration documents kept by local directorates of Ministry of Family, Labor and Social Services; tax ID number shall be verified through documents issued by the relevant unit of the Revenue Administration; the identities of persons authorized to represent these organizations are verified via the identity documents specified under "Customer Identification of Natural Persons"; and their representation authority is verified via registration documents or documents evidencing their authorization to represent.

Customer Identification of Political Parties

In the customer identification of political parties, the name of the relevant unit of the political party, its full address, telephone number, fax number and e-mail address, if any, and name, last name, date of birth, nationality, type and number of the identity document and sample signature of the person authorized to represent and for Turkish citizens, as the additional information, T.R. identity number and place of birth for non-Turkish citizens shall be received.

Name and address of the relevant unit of the political party shall be verified through their charter; identity of the person authorized to represent shall be verified through the identity documents specified under "Customer Identification of Natural Persons", the authority to represent shall be verified through documents of authorization to represent.

Customer Identification of Non-resident Legal Persons and Trusts Established Abroad

Customer identification of non-resident legal persons shall be made through copies of the documents approved by the consulates of the Republic of Türkiye corresponding to the documents in related country required for legal persons residing in Türkiye or through the copies of the documents attached apostille by an authority of the country which is a party to the "Convention on Abolishing the Requirement of Legalisation for Foreign Public Documents".

Also, in the framework of risk-based approach, identity information shall be verified through notarized Turkish translations of these documents when necessary.

Where a transaction requiring customer identification is requested from obliged parties by a natural person or legal entity trustee designated under a trust agreement established abroad for the account of the assets constituting the subject of the trust agreement, prior to executing such transactions, it must be declared in writing to the obliged parties that the transaction is requested for the account of the assets established under the trust agreement.

Customer identification within the scope of trusts established abroad shall be conducted through copies of trust deed approved by consulates of the Republic of Türkiye or attached apostille by an authority of the country which is a party to the "Convention on Abolishing the Requirement of Legalisation for Foreign Public Documents". Within the framework of a risk-based approach, when necessary, identity information is verified via notarized Turkish translations of these documents. In addition, identity information obtained within the scope of identifying the trustee is verified as set forth under the sections "Customer Identification of Natural

Persons" and "Customer Identification of Legal Entities Registered with the Trade Registry". Within the scope of determining the beneficial owner, the identity information of the settlor, beneficiary or classes of beneficiaries, and, if any, persons designated as protectors/auditors under the agreement is obtained, and reasonable measures are applied to verify this information. Necessary measures are also taken to reveal the natural person or persons who ultimately exercise control over the assets in question.

Customer Identification of Unincorporated Organizations

In transactions carried out on behalf of unincorporated organizations such as building, housing estate or office block management, the name of the organization, its full address, telephone number, and fax number and e-mail address, if any, and name, last name, date of birth, nationality, type and number of the identity document and sample signature of the person authorized to represent the organization and for Turkish citizens, as additional information, T.R. identity number and place of birth for non-Turkish citizens shall be received.

The identity information of the person authorized to represent the organization shall be verified through the identity documents specified under "Customer Identification of Natural Persons", and the organization information and the authorization of the person acting on behalf of the organization shall be verified through notarized docket.

In customer identification of organizations such as unincorporated partnership; the name of the partnership, its aim, field of activity, tax identification number, its full address, telephone number, and fax number and e-mail address, if any, and name, last name, date of birth, nationality, type and number of the identity document and sample signature of the person authorized to represent the organization and for Turkish citizens, as additional information, T.R. identity number and place of birth for non-Turkish citizens shall be received.

The name, aim, activity field and the address of the partnership shall be verified through notarized partnership agreement, tax identification number shall be verified through the certificates drawn up by the relevant unit of Revenue Administration, identity of persons requesting transaction on behalf of the partnership shall be verified through identity documents specified under "Customer Identification of Natural Persons", authorization shall be verified through the documents indicating the authority to represent.

Customer Identification of Public Institutions

In transactions in which the public administrations in the scope of general administration in accordance with the Public Financial Management and Control Law No. 5018 and quasi-public professional organizations are customers, the identity of the person conducting transactions on their behalf is verified as specified under "Customer Identification of Natural Persons". Their authorization status is verified via an authorization certificate issued in accordance with the legislation.

Customer Identification of Those Acting on Behalf of Others

In the event that a transaction is requested on behalf of legal persons or unincorporated organizations by persons who are given the authority by the persons authorized to represent;

- a) Customer identification of legal persons and unincorporated organizations shall be carried out in accordance with the principles set forth above.
- b) Customer identification of persons authorized to represent legal persons or unincorporated organizations and the persons who are given the authority by persons authorized to represent shall be carried out in accordance with the procedure specified under "Customer Identification of Natural Persons". In cases where the customer identification of the person authorized to represent cannot be carried out through the identity documents specified under "Customer Identification of Natural Persons", the customer identification shall be carried out through power of attorney or circular of signature provided that they contain the information specified in identity documents and that they are notarized.

- c) c) Authorization of persons who are given the authority by the persons authorized to represent shall be verified through notarized proxy or a written instruction of persons authorized to represent. The signatures on the written instruction of persons authorized to represent shall be verified through their signatures on the notarized circular of signature.

In the event that transactions are made by another person on behalf of a customer that is natural person, customer identification of the person acting on behalf of the customer shall be carried out as specified under "Customer Identification of Natural Persons". Besides, authorization of the person acting on behalf of the customer shall be verified through the notarized power of attorney. In cases where identification of the customer on behalf of whom the act is carried out cannot be conducted as specified under "Customer Identification of Natural Persons", it shall then be conducted through the notarized power of attorney. In the event that the identification of the customer on behalf of whom the act is carried out has already been made due to previous transactions, the requested transaction can be conducted through the written instruction of the customer on behalf of whom the act is carried out provided that the customer's signature on the written instruction is verified through his/her signature which is already available to the obliged party.

In transactions carried out on behalf of minors and persons under legal disability by their legal representatives, the authority of those appointed as guardian by court decision, curators and trustees shall be verified through the original or notarized copy of the relevant court decision. In the event that fathers and mothers request a transaction on behalf of their minor child, it shall be sufficient to identify the child on behalf of whom the transaction is requested and the parent requesting the transaction as specified under "Customer Identification of Natural Persons".

Individuals and entities seeking to have a policy issued under a name different from their true identity, avoiding or showing reluctance in completing customer due diligence information and forms, or providing misleading or unverifiable information, as well as sanctioned individuals and entities listed in the lists published by the United Nations Security Council (UNSC) regarding the prevention of terrorist financing and the financing of proliferation of weapons of mass destruction that are binding on our country, and in the lists enumerated under section "2.7. SANCTIONS" of this Policy, shall not be accepted as customers. All rights and receivables of individuals, entities, or organizations that were not on the asset-freezing lists at the customer onboarding stage but are subsequently included therein shall be frozen and reported to the Presidency within the periods stipulated by law. Necessary measures in this regard are taken and meticulously implemented.

Furthermore, due care and attention shall be exercised regarding the following matters:

- a) Exercising maximum care and diligence in evaluating customer acceptance requests from individuals and entities about whom there is serious doubt, information, or documentation regarding whether their wealth and funds were acquired through lawful means,
- b) Within the scope of the requirement that customer relationships be based on mutual information exchange, trust, and transparency, refusing to accept as customers individuals and entities that avoid or are reluctant to complete customer identification information and forms, or provide misleading and unverifiable information,
- c) Investigating elements such as prior claims history of the risk to be insured and the identity of the insured or policyholder, determining the existence as well as the quantitative and qualitative characteristics of every insurable interest to be covered under the policy, and repeating the same procedures in the event of a change of the insured or assignment of the policy,
- d) Protecting against money laundering, terrorist financing, and proliferation financing transactions as a result of the adoption and implementation of the principles set forth in this Policy document by all personnel,
- e) Preserving reputation and trust carried by the brand of Anadolu Anonim Türk Sigorta Şirketi during the continuation of its insurance operations.

2.4. IDENTIFICATION OF THE BENEFICIAL OWNER

Necessary measures are taken to determine whether the customer is acting for the account of another person and to identify the beneficial owner of the transaction. Where it is suspected that a person is acting in their own name but for the account of another person despite not having declared that they are acting for another's account, reasonable inquiries and research are conducted to uncover the beneficial owner.

2.5. OBTAINING ADEQUATE INFORMATION ON THE PURPOSE OF TRANSACTIONS

It is mandatory to pay special attention to complex and unusually large transactions as well as transactions that have no apparent reasonable legal and economic purpose, to take necessary measures to obtain adequate information regarding the purpose of the requested transaction, and to retain the information, documents, and records obtained in this context.

2.6. ONGOING MONITORING OF CUSTOMERS AND TRANSACTIONS

It is mandatory to identify and continuously monitor the business relationships and transactions of high-risk customers, and to keep information, documents, and records regarding the customer up to date. An appropriate risk management system is established to determine the risk profile of customers from the perspective of money laundering and terrorist financing by taking into account their prior claims, profession, business history, financial standing, accounts, commercial activities, country of residence, and other relevant indicators, as well as suspicious transaction typologies.

2.7. SANCTIONS

Compliance is ensured with sanctions determined in line with the requirements arising from both national legislation and international operations.

In addition to national legislation, the Company ensures full compliance, at a minimum, with Sanctions related to its activities declared by:

- The United Nations Security Council (UNSC),
- The United States of America,
- The European Union,
- The United Kingdom.

In highly exceptional cases and in line with the opinions of the Compliance Unit, our Company's Senior Management may recognize Sanctions declared by other countries and international organizations in addition to those listed above. The lists to be utilized by our Company within this scope are determined by the Compliance Unit.

The Company establishes and implements a sanctions compliance program in order to identify and manage risks concerning Sanctions. It takes risks related to Sanctions into consideration during new customer onboarding, updating of customer information, and execution of customer transactions. It never knowingly becomes a party to any transaction aimed at circumventing or evading Sanctions.

Within this scope:

- Existing customers are screened at regular intervals to determine whether they appear on these lists.
- No business relationship is entered into with individuals and entities identified as appearing on these lists, and transactions requested by such individuals and entities are not executed.
- No direct or indirect intermediation is provided for transactions to which individuals identified on these lists are a party.

- Subject to applicable legal regulations, existing business relationships are terminated with customers who were not on prohibited lists at the time of establishing the business relationship but are subsequently found to have been added to such lists.
- Even if not listed on these lists, no direct or indirect intermediation is provided for transactions linked directly or indirectly to countries subject to comprehensive sanctions imposed by the United Nations Security Council (UNSC), the United States of America, the European Union, and the United Kingdom.
- No business relationship is entered into with individuals and entities subject to United Nations Security Council (UNSC) sanctions.
- No business relationship is entered into with individuals and entities listed as Specially Designated Nationals (SDN) by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), nor with entities in which such persons directly or indirectly hold an ownership interest of 50% or more.
- No business relationship is entered into with entities in which individuals and entities sanctioned pursuant to United Nations Security Council (UNSC), European Union, and United Kingdom regulations directly or indirectly hold an ownership interest of 50% or more, or hold the authority to appoint or dismiss the board of directors.
- Transactions conducted by a customer with or through the Company are examined to determine whether they directly or indirectly involve Comprehensively Sanctioned Countries/Regions or a sanctioned individual or entity.
- No direct or indirect business relationship is entered into with individuals and entities resident or registered in Comprehensively Sanctioned Countries/Regions. No intermediation is provided for transactions conducted with individuals and entities resident or registered in such countries/regions.
- In all cases, it is essential to act in accordance with the sanctions policies of Türkiye İş Bankası A.Ş. and the guidance and restrictions shared with the Company for the implementation of these policies.

2.8. TAKING NECESSARY MEASURES FOR CUSTOMERS, ACTIVITIES, AND TRANSACTIONS REQUIRING SPECIAL ATTENTION

2.8.1. Reinsurers

In selecting counterparty financial institutions with which a reinsurance relationship will be established, due care is taken to ensure that they possess the qualifications to exercise the necessary diligence regarding the prevention of money laundering and terrorist financing.

2.8.2. Transactions of Customer Resident in or Connected with High-Risk Geographical Areas

High-risk regions and areas, both domestic and foreign, are defined, and customers resident in or connected with these regions are monitored more strictly and closely. Special attention is paid to the application of these principles particularly when issuing policies to or intermediating transactions for financial institutions of countries located in high-risk geographical areas.

Offshore Centers, Free Zones, and Financial Centers: Special attention and care are given to the transactions of customers resident in offshore centers, free zones, and international financial centers where strict banking secrecy laws are enforced, as these jurisdictions constitute a center of attraction for concealing funds derived from organized crime or used in terrorist financing as a result of the banking secrecy, tax advantages, and jurisdictional immunity they provide.

2.8.3. Sectors and Lines of Business Vulnerable to Money Laundering

Special attention is paid when providing insurance services to sectors and professional groups characterized by intensive cash movements, trading of high-value goods, or easy execution of international fund transfers. In addition to customer identification and verification documents, it is ensured that sector information is carefully and completely recorded and that customer transactions are closely monitored.

2.8.4. Insurance Transactions Related to Predicate Offenses

Particularly when issuing policies to cover risks such as the transportation of goods to be exported and imported, export credit, fire, theft, and other risks of goods in warehouses and bonded warehouses, valuables including cash, marine/transit cargo, loss of profit, and fidelity guarantee, or in the event a claim occurs in relation to these insured risks, the Company exercises the necessary diligence with respect to the offenses regulated under Article 282 of the Turkish Penal Code No. 5237.

2.8.5. All Types of Claims Transactions

It is essential to examine claim files, process transactions on the basis of original documents, and verify documents to the extent possible. The Company exercises due care to select loss adjusters appropriate to the nature of the claim and to ensure that these adjusters prepare their agreed valuation reports by inspecting the risk on site.

2.8.6. Cash Transactions

Company employees and agencies are required to pay special attention to cash transactions of notable frequency or high amounts in premium payments, and necessary briefings and guidance are provided in this regard.

2.8.7. Transactions of Non-Profit Charitable Organizations

Taking into account that non-profit charitable organizations may be exploited particularly by terrorist organizations and those generating proceeds of crime, special attention is paid to the transactions they conduct.

2.8.8. Non-Face-to-Face Transactions and New Products Offered Using Emerging Technologies

It is mandatory to pay special attention to policies produced using systems that enable non-face-to-face transactions, such as transactions conducted via the internet channel; to closely monitor transactions that are inconsistent with or unrelated to the customer's financial profile and activities; and to take appropriate and effective measures, including setting limits on transaction amounts and counts.

Special attention is paid to the risk that the use of new and emerging technologies and the capabilities brought by existing and new products and new business practices—including new distribution channels—may be used for money laundering and terrorist financing purposes, and appropriate measures are taken to prevent this.

2.8.9. Enhanced Due Diligence Measures

For transactions falling within the scope of Articles 2.8.1 through 2.8.8 and in high-risk situations identified within the framework of a risk-based approach, one, several, or all of the following measures are applied:

- Obtaining additional information on the customer and updating the identification information of the customer and beneficial owner more regularly.
- Obtaining additional information on the intended nature of the business relationship.
- Obtaining information, to the extent possible, on the source of the assets subject to transaction and source of funds of the customer.
- Obtaining information on the reasons for the transaction.
- Obtaining approval of senior management to commence or continue business relationship or carry out transaction.
- Conducting enhanced monitoring of the business relationship by increasing the number and frequency of the controls applied and by selecting the patterns of transactions that needs further examination.

2.8.10. Politically Exposed Persons (PEPs)

In business relationships established and transactions conducted with Politically Exposed Persons elected or appointed by a foreign country, or their spouses, first-degree relatives, or close associates, at a minimum the following measures are applied:

- Subjecting the establishment of the business relationship, the continuation of an existing business relationship, or the execution of the transaction to senior-level approval.
- Taking reasonable measures to establish the source of assets and funds belonging to such persons or subject to the transaction.
- Keeping the business relationship under enhanced scrutiny by increasing the number and frequency of applied controls and identifying transaction types requiring additional controls.

These measures are also applied where business relationships established and transactions conducted with Politically Exposed Persons elected or appointed by Türkiye or serving in international organizations, or their spouses, first-degree relatives, or close associates, are assessed as high-risk.

The term "close associates of Politically Exposed Persons" refers to any social, cultural, or economic closeness that may be considered a unity of interest or purpose, such as kinship beyond the first degree, engagement, company partnership, or being a company employee.

Where Politically Exposed Persons leave office or lose such status, the implementation of the aforementioned measures continues for at least one year from the date they leave office or lose such status. This period may be extended if transactions or business relationships conducted with such persons continue to pose a risk.

2.8.11. Crypto Asset Service Providers (CASPs)

Where the customer is a crypto asset service provider, at a minimum the following measures are applied in establishing a business relationship and in other transactions requiring customer identification with such customers:

- Information is obtained, to the extent possible, regarding the source of the assets subject to the transaction and the funds belonging to the customer.
- Information is obtained regarding the purpose of the transaction.
- The business relationship is kept under close scrutiny by increasing the number and frequency of applied controls and identifying transaction types requiring additional control.
- The establishment of the business relationship is made subject to senior-level approval.

When establishing a business relationship with a customer that is a crypto asset service provider, special attention is paid to whether the relevant firm is included on the list ("*Faaliyette Bulunanlar Listesi*") published by the Capital Markets Board of Türkiye.

2.9. RELIANCE ON THIRD PARTIES

The Company may establish business relationships or carry out transactions by relying on measures taken related to the customer by another financial institution on identification of the customer, the person acting on behalf of customer and the beneficial owner, and on obtaining of information on the purpose of business relationship or transaction. Reliance on a third party is permissible provided that the Company is satisfied that:

- The third parties have taken other measures which will meet the requirements of customer identification, record keeping and the principles of customer due diligence, and are also subject to regulations and supervision in combating money laundering and terrorist financing, and
- The certified copies of documents relating to customer identification shall immediately be provided from the third party when requested.

Where a business relationship is established or a transaction is conducted by relying on a third party, the identity of the customer is immediately received from the third party.

Transactions conducted on behalf of a customer with another financial institution, as well as relationships with agencies and persons contracted to provide services that are an extension of or complementary to core service units, do not fall within the scope of the third-party reliance principle. Furthermore, the principle of reliance on third parties cannot be applied if the third party is resident in a high-risk country.

2.10. SIMPLIFIED MEASURES

Subject to authorization by the Ministry:

- In transactions conducted with another financial institution,
- In transactions where the customer is a public administration within the scope of general government pursuant to Law No. 5018 or a professional organization having the status of a public institution,
- In transactions where the customer is a publicly traded company whose shares are listed on a stock exchange,

and in other transactions outside these categories as determined by the Ministry by transaction type, simpler measures may be applied with respect to customer due diligence measures.

Practices within the scope of simplified measures are determined in accordance with the relevant regulations of the Ministry. In cases where a risk of money laundering or terrorist financing may arise due to the transaction, simplified measures shall not be applied, and consideration shall be given to whether the transaction may constitute a suspicious transaction.

2.11. RISK MANAGEMENT ACTIVITIES

Risk management activities regarding the implementation of the Compliance Program are designed by the Compliance Officer within the framework of relevant Legislation and the provisions of this Policy and are carried out by the Compliance Unit. In this context, matters identified within the scope of the national risk assessment are also taken into consideration. The implementation principles regarding risk management activities enter into force upon approval by the Member of the Board of Directors to whom the Board has delegated its authority pursuant to the provisions of Regulation On Program Of Compliance With Obligations Of Anti-Money Laundering And Combating The Financing Of Terrorism.

Risk management activities cover, at a minimum:

- Developing risk identification, rating, classification, and assessment methodologies based on customer risk, service risk, and country risk,
- Rating and classifying services, transactions, and customers according to risks,
- Ensuring the monitoring and control of high-risk customers, transactions, or services; taking necessary measures to mitigate risks and reporting them so as to alert relevant units; and developing appropriate operational and control rules for executing transactions with senior-level approval and auditing them when necessary,
- Retrospectively questioning the consistency and effectiveness of risk identification and assessment methodologies, as well as risk rating and classification methods, through case studies or actual executed transactions, and reassessing and updating them based on conclusions reached and evolving conditions,
- Following up on recommendations, principles, standards, and guidelines introduced by national legislation and international organizations regarding matters falling within the scope of risk, and carrying out necessary development work,
- Reporting risk monitoring and assessment results to the Board of Directors at regular intervals.

2.11.1. Identification and Classification of Risks

Risks are classified under the "Company Risk Catalogue". The Company Risk Catalogue serves as the fundamental document used in identifying and classifying all potential risks and is updated in parallel with changing conditions and realized events.

Risks incurred in this regard are monitored, assessed, and controlled separately under the categories of customer risk, service risk, and country risk, at a minimum.

2.11.2. Monitoring and Assessment of Risks

In assessing customer, service, and country risks related to money laundering and terrorist financing, parameters such as the customer's line of business, high-risk countries in which the customer operates, policy coverages provided, claims history, and policy cancellation requests are primarily taken into consideration.

Both at the inception of the business relationship and throughout its continuation, customers are assigned to appropriate risk categories with respect to the nature and scope of their activities and their relationships and transactions with the Company, within the framework of other customer-specific information and criteria, if any. When determining a customer's risk category, the customer themselves and the customer, service, and country risks associated with the insurance products and services they utilize are considered and evaluated holistically.

While customers and their transactions in medium and low risk categories are subject to the Company's standard monitoring and controls on the subject, customers and their transactions falling into the high-risk category are closely tracked through fit-for-purpose monitoring and control methods.

Special attention is paid to customers falling into the high-risk category in terms of customer, service, and country risks. In this context, centralized monitoring and control activities carried out with a risk-based approach by the Compliance Unit are primarily designed and executed to focus on customers and transactions in the high-risk category.

Customer groups as well as products and services falling into the high-risk category are determined by the Compliance Unit with a risk-based approach within the framework of the legislation and this Policy, and are subjected to effective monitoring and controls appropriate to their characteristics.

Providing risk-related data and intelligence is the duty and responsibility of executive business units. Communication channels are established to ensure that all obtained information is immediately taken into account within decision-making, monitoring, reporting, and auditing processes.

2.11.3. Authorization Limits

Where deemed necessary, in addition to underwriting authorities granted at the policy issuance stage and claims payment authorities granted at the claims settlement stage, the Board of Directors establishes new authorities and limits for the purpose of controlling the risks defined in this Policy document, such as making decisions to enter into a business relationship with a customer, maintain an existing business relationship, or pay a claim indemnity subject to the approval of a higher-level individual or committee in connection with the outputs produced by the risk rating system.

In order to ensure that practices are monitored and rapid and effective decisions are taken, the Board of Directors may authorize the Office of the Chief Executive Officer regarding the determination of special authorities, provided that the scope and duration of the authority, as well as the principles of monitoring, auditing, and reporting, are explicitly specified.

2.11.4. Reporting

Risk monitoring and assessment results are regularly reported by the Compliance Unit to the Board of Directors. The reporting system is ensured to be adequate and competent. All matters identified as a result

of risk management activities are included in risk, compliance, and other reports in a complete, accurate, regular, objective, clear, and understandable manner.

PART III

3. MONITORING AND CONTROL

3.1. PURPOSE AND SCOPE OF MONITORING AND CONTROL ACTIVITIES

The primary purpose of monitoring and control activities is to protect the Company against risks arising from the abuse of its services for the purpose of money laundering or terrorist financing and to continuously monitor and control whether its operations are conducted in compliance with the legislation and Company Policies and procedures.

Control, assessment, and reporting activities carried out separately and independently from daily operations—both centrally and across all units of the Company—to ensure that Company activities are conducted accurately, regularly, efficiently, effectively, and securely in compliance with the legislation and in accordance with the policies, rules, implementation principles, and instructions established by Company management, to develop control systems and controls related to incurred risks, and to ensure the timely prevention, detection, and remediation of errors and deficiencies, constitute the general scope of monitoring and control activities.

3.2. MONITORING AND CONTROL ACTIVITIES

Monitoring and control activities are designed and executed with a risk-based approach under the supervision and coordination of the Compliance Officer within the framework of relevant legislation and the provisions of this Policy. Within this scope, alongside standard controls to be applied to all operations of the Company, appropriate and effective control processes, systems, and methods are determined and implemented for closer tracking of customers, transactions, and activities deemed high-risk and requiring special attention. The implementation principles regarding monitoring and control activities enter into force upon approval by the Member of the Board of Directors to whom the Board has delegated its authority pursuant to the provisions of Regulation On Program Of Compliance With Obligations Of Anti-Money Laundering And Combating The Financing Of Terrorism.

3.2.1. Key Controls Under Monitoring and Control Activities

Monitoring and control activities regarding operations carried out by Company units fundamentally encompass controls of the following types and nature:

- Monitoring and controlling customers and transactions in the high-risk group,
- Monitoring and controlling transactions conducted with high-risk countries,
- Monitoring and controlling complex and unusual transactions,
- Controlling, via sampling methods, whether transactions whose single amount or total amount across multiple linked transactions exceeds the threshold specified in the Legislation are consistent with the customer profile,
- Monitoring and controlling linked transactions that, when taken together, exceed the threshold requiring customer identification,
- Controlling information and documents about customers that must be retained in electronic or written form, ensuring deficiencies are completed, and updating them,
- Monitoring whether the transaction conducted by the customer is consistent with information regarding the customer's business, risk profile, and sources of funds,
- Controlling transactions executed using systems that enable non-face-to-face transactions,

- Conducting risk-focused controls of services that may become vulnerable to abuse due to newly launched products and technological developments,
- Controlling the compliance and appropriateness of activities and transactions with relevant legislation and the policies, rules, implementation principles, and instructions determined by Company management,
- Controlling compliance with limits and restrictions established within the Company in connection with the nature, importance, and riskiness of activities, and monitoring excesses and non-compliances in this context,
- Controlling compliance of activities and transactions with approval and authorization mechanisms established within the Company and with defined functional segregation of duties,
- Controlling the accuracy of transaction details, activities, and outputs belonging to the risk rating system,
- Toward the effectiveness of communication channels, controlling how frequently Company personnel report transactions they deem suspicious to the Compliance Officer,
- Controlling the appropriateness, adequacy, and effectiveness of risk-responsive controls against established principles and standards,
- Conducting monitoring and control activities within the framework of national legislation regarding Politically Exposed Persons and Crypto Asset Service Providers.

3.2.2. Reporting

As a result of monitoring and control activities, Suspicious Transaction, Non-Compliance, and Deficiency Reports addressed to the Compliance Unit are prepared by the personnel performing this activity within the units. These reports are prepared periodically—or instantaneously where a suspicious transaction is detected—within the procedures and principles whose format and scope are determined by the Compliance Officer, containing findings, information, opinions, and evaluations regarding suspicious transactions, non-compliances, malfunctions, deficiencies, and other matters detected in relation to unit operations within the scope of monitoring and control activities, while providing an opportunity for relevant unit managers to respond.

PART IV

4. TRAINING

4.1. TRAINING POLICY

Compliance with obligations introduced by the legislation is ensured, a corporate culture is established by raising personnel awareness of their responsibilities regarding the Company's Policy and procedures on the prevention of laundering proceeds of crime and financing of terrorism as well as the risk-based approach, and the knowledge of personnel on these matters is continuously updated. The Company's training activities are carried out toward this purpose.

4.2. TRAINING ACTIVITIES

4.2.1. General Principles

Training activities are conducted in accordance with relevant legislation and the written policy and implementation procedures adopted by the Board of Directors within this framework. The training program is prepared annually by the Compliance Officer with the participation of relevant units in the headquarter and approved by the Board of Directors or the Board Member to whom the Board has delegated its authorities regarding the training program.

In carrying out training activities in this direction, the following general principles are observed:

- By utilizing regulations and informational materials as well as recommendations, standards, and academic/scientific studies issued by official and professional bodies involved in combating money laundering and terrorist financing at national and international levels, it is ensured that all employees and agencies—primarily Company executives—possess an adequate level of knowledge.
- Training activities are reviewed with the participation of relevant units based on measurement and evaluation results and are repeated at regular intervals according to need.
- Ensuring the timely completion by relevant individuals of e-learning courses assigned to employees and agencies under the Policy is the responsibility of the line managers to whom the employees report, and for agencies, the directorate responsible for agency relations.
- Training activities are executed within the training program prepared with the participation of relevant units under the supervision and coordination of the Compliance Officer, and the effective implementation of the training program is overseen by the Compliance Officer.

4.2.2. Training Topics

Trainings to be provided to personnel and Company agencies for the prevention of laundering proceeds of crime and financing of terrorism cover, at a minimum, the following topics:

- Concepts of money laundering and terrorist financing,
- Stages and methods of money laundering and case studies on this subject,
- Legislation regarding the prevention of laundering proceeds of crime and financing of terrorism,
- Risk areas,
- Company policy and procedures,
- Within the framework of legislation: principles regarding customer due diligence, principles regarding suspicious transaction reporting, obligation to retain and submit records, obligation to provide information and documents, and sanctions/penalties to be imposed in case of non-compliance with obligations,
- International regulations in the field of combating money laundering and terrorist financing.

4.2.3. Training Methods

Classroom training, e-learning, and other diverse training methods, audiovisual training materials, and communication channels such as the internet or intranet are effectively utilized so as to ensure the dissemination of training activities across Company personnel and agencies.

4.2.4. Selection and Development of Participating Personnel and Trainers

Personnel and trainers participating in training activities are determined by the Human Resources and Training Manager, taking into account the opinion of the Compliance Officer, from among employees who can successfully fulfill this duty in accordance with the competence and professional care standards required by the job in terms of their knowledge, skills, experience, and personal qualifications. Special importance is attached to selecting the trainers who will deliver the training and ensuring that they receive the necessary training for this purpose. Training activities may also be fulfilled by outsourcing services externally.

Training and development opportunities that contribute to the growth of personnel and trainers participating in training activities, the enhancement of their knowledge and skills, and the successful and high-quality fulfillment of their duties are appropriately and effectively utilized. Personnel and trainers participating in training activities are encouraged, incentivized, and supported to attend trainings that provide nationally or internationally recognized professional certifications on anti-money laundering and counter-terrorist financing and to obtain such certifications.

4.2.5. Training Activity Program

Training activities are carried out within the framework of the annual Training Program prepared with the participation of relevant units under the supervision and coordination of the Compliance Officer.

The annual training program includes training dates, regions where training will be delivered, training methods, total training hours, number of personnel to be trained and its ratio to the total headcount, distribution of personnel to be trained by unit and title, training content, and the titles and areas of expertise of the trainers. The training program is approved by the Board of Directors or the Board Member to whom the Board has delegated its authorities regarding the training program. Information and statistics regarding training activities are reported to the Presidency through the Compliance Officer by the end of March of the following year.

PART V

5. INTERNAL AUDIT

5.1. PURPOSE AND SCOPE OF INTERNAL AUDIT ACTIVITIES

The purpose of internal audit activities is to provide assurance to the Board of Directors regarding the effectiveness and adequacy of the entirety of the Compliance Program.

Evaluation and reporting activities carried out separately and independently from daily operations to determine whether the policies and rules, implementation principles, and instructions established by the Company, as well as risk management, monitoring and control, and training activities, are adequate and efficient; whether the Company's Compliance Program is adequate and effective; and whether transactions are conducted in compliance with the legislation and Company's policies and procedures, constitute the general scope of internal audit activities.

5.2. INTERNAL AUDIT ACTIVITIES

5.2.1. General Principles

Internal audit activities are carried out by the Board of Auditors in accordance with relevant legislation and the written policy and implementation procedures determined by the Board of Directors within this framework. In executing internal audit activities accordingly, the following general principles are observed:

- The effectiveness and adequacy of the entirety of the Compliance Program are audited and evaluated annually through a risk-based approach.
- Deficiencies detected during monitoring and control activities, as well as customers, services, and transactions involving risk, are included within the scope of audit.
- When determining the units and transactions to be audited, taking into account transaction volume, it is ensured that units and transactions of a quantity and nature capable of representing the entirety of transactions executed by the Company are audited.
- Findings included in reports prepared within the scope of internal audit activities are remediated on a priority basis by the responsible departments, taking Compliance Risk into account.

Deficiencies, errors, and abuses uncovered as a result of internal audit activities, together with opinions and recommendations aimed at preventing their recurrence, as well as audit findings regarding Compliance Risk, are reported to the Compliance Unit and the Board of Directors. Necessary information and statistics required under the legislation regarding executed internal audit activities are regularly maintained and reported to the Presidency by the Compliance Officer within the specified periods and principles.

PART VI

6. SUSPICIOUS TRANSACTION REPORTING, ASSET FREEZING, AND OTHER PROVISIONS

6.1. DETECTION, REPORTING, AND CONFIDENTIALITY OF SUSPICIOUS TRANSACTIONS

Suspicious transactions related to money laundering and terrorist financing are reported to the Presidency by the Compliance Officer or Deputy Compliance Officer within the framework of the legislation.

Where there is information, suspicion, or reasonable grounds to suspect that a transaction conducted or attempted to be conducted before or through the Company is related or linked to money laundering and terrorist financing, necessary investigations are also conducted to the extent possible, and any transaction concluded to be suspicious is reported to the Presidency within the timeframe and principles specified in the legislation.

Where there are documents or serious indications supporting the suspicion that the assets subject to an attempted or ongoing transaction are linked to the offense of money laundering and terrorist financing, the suspicious transaction report is submitted to the Presidency together with its justifications and a request for the suspension of the transaction, and the Company refrains from executing the transaction for the period stipulated in the legislation.

Necessary communication and cooperation are ensured within the framework of the legislation among the parties involved in the process of detecting, examining, evaluating, and reporting suspicious transactions to the Presidency. All relevant parties involved in or privy to the matter exercise the utmost care and diligence required under the legislation regarding the confidentiality and security of suspicious transaction reports and internal reports made within the Company in this context, as well as the protection of the parties to such reports.

The principles and implementation rules regarding the execution of decisions related to suspicious transaction reporting are governed by a separate internal Company implementation procedure.

6.2. PRINCIPLES REGARDING ASSET FREEZING

With respect to the implementation of asset freezing decisions under Law No. 6415 on Prevention of Financing of Terrorism dated 7/2/2013 and Law No. 7262 on Prevention of Financing of the Proliferation of Weapons of Mass Destruction dated 27/12/2020, the Company takes all measures—including efforts to identify, assess, monitor, and mitigate risks related to the breach, non-implementation, and evasion of asset freezing decisions, as well as advanced controls for the enforcement of such sanctions.

Asset freezing decisions taken pursuant to the provisions of Law No. 6415 and Law No. 7262, as well as decisions lifting such freezes, are published in the Official Gazette. Continuous monitoring of decisions is performed by also taking potential match criteria into account, and it is immediately verified whether the natural person and legal entity information contained in the decisions matches the customer/beneficiary records held by our Company. In the event of a customer or beneficiary subject to sanctions, the assets belonging to the relevant individuals, entities, and organizations are frozen, and an immediate block is placed on all requested payments.

The principles and implementation rules regarding the execution of decisions related to asset freezing are governed by a separate internal Company implementation procedure.

6.3. PRINCIPLES ON PROVIDING INFORMATION AND DOCUMENTS AND RECORD RETENTION

All information, documents, and related records in any medium requested by the Presidency or the Presidency's examiners are provided completely and accurately. Information requests regarding the Company's practices on the prevention of laundering proceeds of crime and financing of terrorism from reinsurance companies, other institutions with which a business relationship is maintained, or institutions and officials authorized to request information and documents from insurance companies other than the

Presidency are fulfilled under the control of the Compliance Officer. Whether information requests outside these will be met is evaluated by the Compliance Officer.

It is essential that all information, documents, and records required to be obtained from customers pursuant to the legislation be retained in a manner that allows easy access when needed and, at a minimum, for the periods stipulated in legal regulations.

The Company may share information regarding customer due diligence, accounts, and transactions with other institutions within the financial group to which it belongs, within the framework of the principles set forth in the Financial Group Policy. Confidentiality provisions written in special laws do not apply to intra-group information sharing. Financial institutions affiliated with the group may not share information indicating that a suspicious transaction report has been filed.

Along with the Compliance Officer of the Financial Group, the Board of Directors of the parent financial institution is also responsible for taking the necessary measures to ensure that information is shared securely within the group. Such responsibility also applies to the compliance officers and boards of directors of the financial institutions affiliated with the group.

6.4. MISCELLANEOUS PROVISIONS

Implementation principles and methods regarding the matters set forth in this Policy document, as well as the fundamental operating principles of the processes and systems established within the Company for this purpose, are set out in the internal control regulation, circulars, and operating procedures.

This Policy document is formally communicated to relevant personnel and Company agencies against their signature. Subsequent amendments to the corporate policy that was duly communicated against signature may be communicated to Company personnel and agencies via e-mail management, provided that a "Read" confirmation is obtained.

6.5. ENTRY INTO FORCE

This Policy enters into force on the date it is approved by the Board of Directors or by the Member or Members of the Board of Directors to whom the Board has delegated its authority pursuant to the provisions of Regulation On Program Of Compliance With Obligations Of Anti-Money Laundering And Combating The Financing Of Terrorism. The Policy is reviewed at least once a year in order to maintain alignment with legislation and international standards and, where necessary, updated and submitted for the approval of the Board of Directors or, if authority has been delegated, the delegated Member or Members of the Board of Directors. Subsequent amendments and updates to the Policy likewise enter into force upon the approval of the Board of Directors or the delegated Member or Members of the Board of Directors.