



**ANADOLU HAYAT
EMEKLİLİK**

**Anadolu Hayat Emeklilik A.Ş.
(Anadolu Life & Pensions)**

**POLICY FOR THE PREVENTION OF
LAUNDERING OF PROCEEDS OF CRIME
AND FINANCING OF TERRORISM**

November 2017

**ANADOLU HAYAT EMEKLİLİK A.Ş.
POLICY FOR THE PREVENTION OF LAUNDERING OF PROCEEDS OF CRIME
AND FINANCING OF TERRORISM**

İçindekiler

1. INTRODUCTION	3
2. ABBREVIATIONS AND DEFINITIONS	3
3. PURPOSE	5
4. SCOPE	5
5. AUTHORITY AND RESPONSIBILITIES	5
6. RISK MANAGEMENT	7
6.1. Customer Due Diligence	7
6.2. Identifying the Beneficial Owners.....	7
6.3. Customer Acceptance Guidelines	8
6.4. Customer Identification and Recording the Information	9
6.5. Individuals and Entities that cannot be Accepted as Customers	10
6.6. Additional Measures for Enhanced Customer Acceptance	10
6.7. Simplified measures	11
7. MONITORING AND CONTROL	12
8. INTERNAL AUDIT AND REPORTING	13
9. TRAINING.....	13
10. PROCEDURES OF SUSPICIOUS TRANSACTION REPORTING	14
11. CUSTOMERS UNDER THE SCOPE OF THE SUSPICIOUS TRANSACTION REPORTING	15
12. INFORMATION REQUESTS OF OTHER INSTITUTIONS.....	15
13. MAINTENANCE AND CONFIDENTIALITY OF RECORDS.....	15
14. OBLIGATION TO PROVIDE INFORMATION AND DOCUMENTS.....	15
15. OTHER CONSIDERATIONS	15
16. ENTRANCE INTO FORCE	15

1. INTRODUCTION

Due to the sensitivity of the international community regarding the prevention of Laundering of Proceeds of Crime and Financing of Terrorism, many countries are making legal arrangements and strengthening their existing practices. Legal arrangements regarding the subject are also being realized in our country and the public in our country shares the same sensitivity.

Anadolu Hayat Emeklilik A.Ş. (“the Company”), attaching great importance to the issue and taking into account the damage caused by it in the social life; considers the prevention of Laundering of Proceeds of Crime and Financing of Terrorism as a social responsibility beyond a mere matter of complying with laws and regulations. The Company also sees this combat as an important component of integration and compliance with the international system.

The Company's policy for the prevention of laundering of proceeds of crime and financing of terrorism; is based on the international initiatives, conventions and regulations to which our country is a party, internationally accepted approaches, methods and practices, the legislation in force and on the belief and commitment of the Company to maintain the reputation and trust it holds.

2. Abbreviations and Definitions

Ministry: T.C. Ministry of Treasury and Finance

FATF: Financial Action Task Force is an autonomous intergovernmental international body responsible for developing and promoting policies for combating money laundering, terrorist financing and the financing of weapons of mass destruction.

Beneficial owner: Natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.

Service Risk: Risk that the Company may be exposed in relation to new products that may be offered by using developing technologies or services not carried out on a face to face basis.

Postponement of transaction: To suspend or not to allow the execution of the transaction.

Assets: Money, any kind of movable or immovable, tangible or intangible goods or rights which have monetary value, and any kind of legal documents or instruments certifying rights on them.

MASAK: Financial Crimes Investigation Board.

Legislation: The applicable law, regulations and communiqués as well as the decisions and orders by MASAK to prevent Laundering of Proceeds of Crime and Financing of Terrorism.

Customer Risk: Risk whereby the Company may be abused on the grounds that the customer's scope of business requires the use of large amounts of cash; allow the trading of high-value assets or international fund transfers; or the customer or any person who acts on behalf of him acts for the purpose of laundering of proceeds of crime and financing of terrorism.

Customer Due Diligence: According to the recommendations of the FATF; among the measures to be taken by financial and non-financial institutions and business and professional

owners to prevent money laundering and financing of terrorism; adopting the principle of taking full and accurate information about customers and adopting all necessary measures.

Policy: The Company's Policy for the Prevention of Laundering of Proceeds of Crime and Financing of Terrorism.

Risk: The possibility of financial or reputational harm to the Company or the employees of the Company, due to reasons such as the use of services provided by the Company for the purpose of laundering proceeds of crime or financing of terrorism, or failure to fully comply with the obligations imposed by the Legislation.

Politically Exposed Person: State or government president having top level public responsibilities, top level politicians, government officials, judicial or military personnel, representatives of political parties attaining an important status, people who are managers of public institutions, and family members and close associates.

Laundering of Proceeds of Crime (Laundering): Transactions whereby those earnings raised from unlawful means are injected into the financial system so as to convert them into non-cash form in particular to create the impression that they are derived from legal means, and to make them pass through a process in the financial system so as to conceal the illegal origins of the funds.

The Company: Anadolu Hayat Emeklilik A.Ş.

Suspicious Transaction: The case where there is any information, suspicion or reasonable grounds to suspect that the asset, which is subject to the transactions carried out or attempted to be carried out within or through the obliged parties, has been acquired through illegal ways or used for unlawful purposes such as financing of terrorism.

Permanent Business Relationship: A business relationship that is established between obliged parties and their customers through services such as opening an account, lending loan, issuing credit cards, safe-deposit boxes, financing, factoring or financial leasing, life insurance and individual pension, and that is permanent due to its characteristics.

Financing of Terrorism: Providing or collecting funds for a terrorist or for terrorist organizations with the intention that they are used or knowing and willing that they are to be used, even without being linked to a specific act, in full or in part, in perpetration of the acts that are set forth as crime by the law.

Compliance Unit: The unit assigned by the Board of Directors to carry out the compliance program, directly supervised by the Compliance Officer; in order to ensure that the Compliance Officer is able to fulfill its duties and responsibilities effectively.

Compliance Officer: The officer assigned by obliged parties who is vested the required authority for ensuring compliance with obligations introduced by law and legislation effected based on the law.

Compliance Program: The integral package of the measures built in the Company on the basis of the applicable Legislation and the Company Policy to prevent laundering of proceeds of crime and financing of terrorism.

Country Risk: The risk which is possible to be exposed by obliged parties due to business relationships and transactions with citizens, companies and financial institutions of the

countries; those are identified under the legislation out of those lacking appropriate money laundering and financing of terrorism laws and regulations, being non-cooperative in the fight against these offences or being identified by competent international organizations as risky.

Compliance Risk: Risk that the Bank may suffer sanctions, financial losses and/ or loss of reputation in the event that the Bank's operations and the attitudes and acts of the Bank's staff members are not appropriate and in compliance with the applicable legislation, regulations and standards.

Senior Management: Chief Executive Officer and Deputy Chief Executive Officers of the Company and managers who work in positions equal to or higher levels.

3. Purpose

The Company attaches importance to the effectiveness of its internal regulations and practices for the prevention of money laundering and financing of terrorism and as a policy aims;

- Protecting the reputation and trust merits of the Company brand,
- Ensuring compliance of the risk management, internal audit, execution, reporting, monitoring and control methods with the legislation and implementation of the Compliance Program,
- Preventing the use of the Company for money laundering and financing of terrorism,
- Determining the strategies, internal controls and measures, rules of operation and responsibilities for reducing the risk that may be exposed; by evaluating the customers, transactions and services provided with a risk-based approach,
- Raising the awareness of employees about legal obligations and principles related to the subject.

4. Scope

This Policy covers the executives, employees and agents, representatives and similar affiliates of the Company at all levels; in terms of their duties, authorities and responsibilities related to the prevention of laundering proceeds of crime and financing of terrorism.

This policy consists of the following policies related to the prevention of laundering proceeds of crime and the financing of terrorism;

- Risk management,
- Monitoring and control,
- Training and
- Internal auditing.

5. Authority and Responsibilities

The Company's Board of Directors is ultimately responsible for ensuring that the Compliance Program as a whole carried out adequately and effectively in the framework of this Policy. Within the scope of Compliance Program, Board of Directors is authorized and responsible from;

- Ensuring compliance of the Company with the provisions regarding the prevention of laundering of proceeds of crime and financing of terrorism,
- Approving the policy and annual training programs,
- Assigning the Compliance Officer,
- To determine the duties, authorities and responsibilities of the Compliance Officer and the Compliance Unit.
- Evaluating the results of risk management, monitoring, control, and internal audit activities and enabling for the required measures to be taken,
- Ensuring that all activities are carried out in a coordinated and effective way.

The Board of Directors may transfer all or part of the abovementioned authority within the scope of the Compliance Program to one or more members of the Board of Directors.

Senior Management of the Company is responsible to Board of Directors for;

- Establishing the workflows and assignment regulations within the frame of principles of corporate management, as to comply with the Policy,
- The right and effective fulfillment of the works and transactions by all employees, requiring the implementation of this policy,
- Taking the required measures on a timely manner to ensure that the Company is not faced with the risks relating with laundering of proceeds of crime and financing of terrorism.

The Compliance Officer; who reports to the Board of Directors or one or more members of the Board of Directors to which authority is transferred, is assigned, authorized and responsible from;

- Ensuring compliance of the Company with obligations related to the prevention of laundering proceeds of crime and financing of terrorism and pursue the necessary communication and coordination with MASAK,
- Establishing the Policy and submitting it to the approval of Board of Directors,
- Carrying out risk management, monitoring and control activities for the implementation of Compliance Program within the scope of the Policy,
- Submitting the works relating with training program for the prevention of money laundering and the financing of terrorism for the approval of the Board of Directors and enabling the effective implementation of the approved training program,
- Evaluating the information and findings obtained as relating with Suspicious Transactions and reporting the transactions that are deemed to be suspicious to MASAK,
- Reporting of information and statistics related to internal audit and training activities to MASAK within the set deadlines.

The compliance unit operates under the Compliance Officer to fulfill its duties and responsibilities in the scope of Compliance Program.

The executives and employees of the Company at all levels, agents, representatives and similar affiliates should fulfill all duties and responsibilities in the proper and effective implementation of this Policy for the aim to avoid the Company from being faced with risks relating with laundering of proceeds of crime and financing of terrorism.

Effectiveness and efficiency in implementing the Policy and Compliance Program will be regularly subject to inspection and evaluation within the scope of internal audit. The responsible divisions primarily handle the findings that are stated on the reports being issued. Findings of audit as relating with Compliance Risk are submitted to Compliance Unit and to the Board of Directors.

6. Risk Management

The risk identified within the framework of this policy is the possibility of financial or reputational harm to the Company or its employees that may be incurred, due to reasons such as the use of services provided by the Company for the purpose of money laundering or financing of terrorism or the failure to fully comply with the obligations imposed by the Legislation. Risk management policy aims to identify, rate, assess and mitigate the risks that may be incurred.

Appropriate processes and methods are established and implemented effectively for the purpose of risk identification, rating, assessment and mitigation based on customer, service and country risks. Services, transactions and customers are rated and categorized according to risks. With a risk based approach; reporting is made to alert the relevant units, the transactions are performed with the approval of a higher authority when necessary, and the appropriate operation and control rules for auditing are developed.

Risk identification, rating and assessment methods are updated according to developing conditions. National Legislation on the issues covered by the risk and the recommendations, principles, standards and guidelines issued by international organizations are followed and necessary developments are carried out.

Customers and transactions in the medium and low risk categories are subject to the Company's standard monitoring and control, while customers and transactions in the high-risk category are closely monitored with appropriate monitoring and control methods. For the customers in the high-risk category within the scope of customer, service and country risks; a risk-based approach is designed and implemented in accordance with their qualifications and effective, monitoring and control activities within the Compliance Unit.

The risk management policy covers the rules and procedures for implementing the Company's customer acceptance principles.

6.1. Customer Due Diligence

The "Customer Due Diligence" principle lies at the basis of customer acceptance process of the Company regarding the prevention of laundering of proceeds of crime and financing of terrorism. Within the scope of this principal; implementation that complies with the international standards, recommendations and applicable legislation is carried out.

6.2. Identifying the Beneficial Owners

Necessary measures are taken and implemented with due diligence, in order to identify the beneficiary owners in the permanent business relationship establishment and in the realization of the requested transactions.

6.3. Customer Acceptance Guidelines

Customer acceptance, is carried out after completing the necessary actions and taking the information stated below.

- Identification and verification of customer information and address,
- Identifying the Beneficial Owners,
- Information on job and profession,
- Place of business or operations
- Consistency of documents and information,
- Taking necessary measures for customers, operations and transactions that require special attention.

In addition, the following issues are taken into consideration:

- Internal Policy, risk management, legislation, regulations regarding contract transactions, provision of customer identification information, reporting, training, monitoring and auditing activities are reviewed regularly.
- Insurance and private pension contract transactions can be carried out by the customer himself, his surrogate, his legal representative, the policyholder, the participant and the person making the payment for and on behalf of the participant.
- Necessary documents are requested for the transactions carried out on behalf of minors.
- It is required that the notifications must be approved by the Notary; in particular, when the customer is not sufficiently recognized verification by the Notary who organizes the document is necessary.
- Adequate information is provided on the purpose and nature of the transactions. It is obligatory to take special precautions for complex and extraordinary transactions and transactions that do not have reasonable legal and economic purpose, to take necessary measures to obtain sufficient information about the purpose of the requested transaction and to keep the information, documents and records obtained in this context.
- Control activities are carried out in accordance with the legislation of the country regarding the Politically Exposed Persons.

The principles are determined for; the identification of the customers, registering the declared addresses, providing the necessary information and documents, making the necessary confirmation and verifying them in case of suspicion, record keeping in physical and/or electronic environment.

Additional measures are taken for customer groups identified as high risk. These measures include; developing applications for continuous monitoring of transactions and customers, performing the transactions for high-risk customer groups with the approval of a higher authority, obtaining information as much as possible about purpose of the transaction and the source of Assets subject to the transaction, providing additional information and documents within the scope of the customer's recognition, taking additional measures in respect to confirmation of the information provided.

6.4. Customer Identification and Recording the Information

- Customer identification shall be completed before the business relationship is established or the transaction is conducted.
- Customer identification is carried out by procurement of information, confirmation, control and verification of the identity of the customer, in accordance with the current legislation and the Company's Policy and processes.
- The name or title of the customer, legal entity and structure, address and documents received from the customer; if possible, shall be confirmed by the information and documents obtained from the public records.
- Persons claiming to act on behalf of the customer are identified and their authorization shall be verified.
- It is essential that customer information is recorded in the Company's data processing system and is open to querying by authorized persons.

Identification is realized,

- Irrespective of any amount where a Permanent Business Relationship is established,
- Irrespective of any amount whenever there is a suspicion as to the sufficiency and correctness of any customer identity obtained before,
- Irrespective of any amount in circumstances where a Suspicious Transaction should be reported,
- Whenever the transaction amount, or the aggregate amount of more than one transaction linked to each other exceed the threshold defined in the legislation

by obtaining identity information of customers and those acting on behalf of the customers and by verifying this information.

The Company can 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 third parties is possible only if it is ensured 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 financing of terrorism in accordance with international standards if the third parties are resident abroad,
- The certified copies of documents relating to customer identification shall immediately be provided from the third party when requested.

In case of the establishment of business relationship by relying on a third party, the identity data of the customer shall immediately be received from the third party. In such a circumstance, the ultimate responsibility shall remain with the Company.

The transactions which the financial institutions conduct between themselves on behalf of customers and relationships between financial institution and its agents, similar units or outsourcing entities are not within the scope of the principle of reliance on third parties. The

principle of reliance on third parties may not be applied to the cases where the third party is resident in a risky country.

6.5. Individuals and Entities that cannot be Accepted as Customers

- Individuals and entities who wish to trade under a different name than their real identity, avoid giving the customer identification information and filling in the relevant forms and who are reluctant or misleading cannot be accepted as a customer. In cases where customer identification and its verification which are required to be conducted due to suspicion on the adequacy and accuracy of the previously obtained customer identification information cannot be carried out, the business relationship shall be terminated.

- If there is any suspicion, information or document that the assets and funds of individuals and entities are not legally earned, they are not accepted as customers.

- The individuals and entities determined to be included in the lists published by official institutions in the scope of combating proceeds from crime are not accepted as customers. After the customer relationship, the individuals and entities whose deficiencies have been identified in this regard, are canceled and the Company does not mediate the related life insurance / private pension transactions.

- The individuals and entities listed in accordance with United Nations Security Council (UNSC) resolutions or MASAK legislation are not accepted as customers.

6.6. Additional Measures for Enhanced Customer Acceptance

Customer Transactions in Relation to High Risk Geographic Areas

The definition of high risk regions and areas within and outside the country is made in the following categories, and the resident or related customers in these regions are followed up more frequently and closely.

Additional measures are applied to the countries; specifically in high-risk geographic areas, announced in the list of countries by the Ministry as "Risky Countries" or in the "Non-Cooperative Jurisdictions" list published by FATF, in which Turkey is also a member.

Non-Cooperative Countries and Territories

Enhanced measures are applied to the business relations and services of the citizens, companies and financial institutions of the countries included in the Non-Cooperative Countries and Territories list published by FATF.

Cross-Border Centers, Free Zones and Finance Centers

Enhanced measures are applied to the transactions of customers established in; cross-border centers (Offshore) that form a center of attraction for the need to save funds earned from organized crime or used for financing terrorism, by providing banking secret, tax advantage and judicial immunity, free zones and finance centers where strict banking privacy laws are applied.

High-risk Sector and Business Lines in Laundering Proceeds of Crime

Activities including intensive use or transfer of cash/foreign currency, activities dealing in high-value items etc. or international fund transfers and sector and occupational groups as being accepted to be risky and unfavorable

Services to sectors and occupational groups which use/transfer cash intensively, high-value goods or international fund transfers, and offering risky products/services required to be monitored closely with special attention. Customer identification and identifier documents, as well as a careful and complete record of business information and close monitoring of customer transactions is required.

High-risk Insurance and Pension Transactions

Close monitoring with special attention is required to customer funds and transactions arising from unrecognized activities and which cannot be directly related to their business, particularly arising from lump sum payments (cash value) and electronic fund transfers.

Special attention is required to the transactions that non-profit charitable organizations which will be able to exploited, in particular by terrorist organizations and those who receive proceeds of crime.

Company employees and intermediaries are informed to pay special attention to the contracts with a noticeable frequency and/or high value transactions.

Customer requests using the internet and call center that allow transactions without face-to-face contact with the company employees are evaluated with special attention by the unit authorities accepting the customer.

Special attention is paid to operate systems that allow centralized control of the operations carried out through these channels.

6.7. Simplified measures

Simplified measures can be taken in terms of customer due diligence, under the conditions allowed by the Ministry.

- In transactions carried out between financial institutions on behalf of themselves,
- In transactions where the customer is a public administration or quasi public professional organization in the scope of general administration in accordance with the Public Financial Management and Control Law No. 5018,
- In transactions related to pension schemes that provide retirement benefits to employees by way of deduction from their salaries and of pension agreements,
- In transactions where the customer is a public company and its shares are listed on the stock exchange.

simplified measures may be applied.

Simplified measures may not be applied in cases where money laundering or terrorist financing risks might occur due to the transaction and shall take into account that the transaction is possibly a suspicious transaction.

7. Monitoring and Control

Operations are constantly monitored and controlled to protect the Company against risks and to ensure that its operations are in accordance with the legislation. Monitoring and control activities are designed and conducted on a risk-based approach under the supervision and coordination of Compliance Officer. In this respect, in addition to standard controls applicable to all operations of the Company, certain appropriate and effective control processes, systems and methods are identified and implemented in order to monitor more closely those customers, transactions and operations that are deemed to be of high risk and require special diligence and attention.

Within the scope of continuous monitoring of customers and transactions; risk profiles of customers in terms of money laundering and terrorist financing are taken into consideration by taking into account the profession, job history, activities, financial situation, accounts and transactions of the customers and the country in which it is established/operates and the current information. Customers, business relations and transactions with high risk are identified and followed up with risk management, monitoring and control processes and systems.

The provision of data and intelligence related to risk is the duty and responsibility of the executive units. Communication channels shall be established to ensure that any information obtained is taken into account immediately in the process of decision making, monitoring, reporting and auditing.

Monitoring and control activities basically cover the following activities:

- Monitoring and control of high-risk customers and transactions,
- Monitoring and control of transactions executed with risky countries,
- Monitoring and control of complex and unusual transactions
- Controlling those transactions above a specific amount threshold through sampling in order to check its compliance with the customer profile,
- Monitoring and control of transactions that are linked to each other and exceed the amount which requires the identity verification,
- Controlling the veracity, timeliness and adequacy of customer data and documents,
- Continuous monitoring of the compliance of a customer transaction with his scope of business, risk profile and fund resources throughout the transaction,
- Controlling the transactions carried out through systems that allow the execution of transactions without a face-to-face interaction,
- Risk based control of services that may become prone to misuse due to newly introduced products and technological developments.

Central monitoring and control activities are carried out by the Compliance Unit. To effectively implement the Compliance Program in accordance with the applicable legislation and the policy and procedures and the on-the-spot audit and control of the compliance of the transactions, are provided through internal audit and internal control activities. Results of the central monitoring and control activities as well as the data and information reported as a result of the internal audit and internal control activities are monitored and evaluated as a whole at the Compliance Unit under the supervision of the Compliance Officer.

Reports in the scope of monitoring and control activities are submitted periodically or in a momentary manner in case of determining a suspicious transaction.

8. Internal Audit and Reporting

Special attention is paid to; compliance with obligations related to prevention of laundering proceeds of crime and to establish internal audit, reporting and communication systems to identify and prevent suspicious transactions in advance or to detect suspicious transactions.

Purpose of internal audit is to provide assurance to the Board of Directors regarding the effectiveness and sufficiency of integrity of Compliance Program of the Company. Within this scope; efficiency and effectiveness of the Company's Policy, processes, risk management, monitoring, control and training activities and compliance of transactions with the legislation, policy and procedures are audited and evaluated with a risk-based approach on an annual basis.

While determining the scope of internal audit, failures identified during the monitoring and control works and risky customers, services, and transactions are included within the scope of audit. While the divisions and operations that will be audited are determined, organization structure, business and transaction volume of the Company are also considered. Within this scope, it is ensured that the divisions and transactions, that can represent all of the transactions that are realized within the Company, are audited.

The deficiencies, mistakes, and abuses that are determined are reported to the Board of Directors together with the opinions and proposals aiming to avoid them to reoccur.

Regarding internal audit activities, necessary information and statistics are kept regularly within the framework of the legislation and reported to MASAK by the Compliance Officer within the determined time and principles.

The application and reporting principles and methods related to internal audit activities within the scope of the Compliance Program are regulated and implemented by the Board of Internal Audit within the framework of this Policy.

9. Training

Training activities are carried out within the framework of the provisions of the relevant legislation and this Policy including all relevant employees, in order to know the legal and administrative obligations within the prevention of laundering proceeds of crime and financing of terrorism. Training program is prepared by the Compliance Officer with the participation of the relevant Training Department of the Company. The effective implementation of the training program is monitored by the Compliance Officer.

Purpose of the training policy is; ensuring compliance with the obligations set forth in the legislation, to improve corporate culture and awareness regarding the legal obligations, policies and implementations of the Company within this scope and to provide current information to the employees.

In order to ensure that the training activities are applied throughout the Company, class training, e-training, other various training methods, visual and aural training materials, communication channels such as internet or intranet are used in an effective way.

Necessary information and statistics are kept on a regular basis within the framework of the legislation in relation to the training activities carried out and reported to MASAK by the Compliance Officer within the determined time and principles.

The trainings to be given shall at least cover the following subjects;

- The concepts of laundering proceeds of crime and terrorist financing,
- The stages, methods of laundering proceeds of crime and case studies on this subject,
- Legislation regarding prevention of laundering proceeds of crime and terrorist financing,
- Risk areas,
- Company Policy and procedures,
- In the framework of Law and related legislation; principles relating to customer identification, principles relating to suspicious transaction reporting, obligation of retaining and submitting, obligation of providing information and documents, sanctions to be implemented in violation of obligations,
- The international regulations on combating laundering and terrorist financing.

10. Procedures of Suspicious Transaction Reporting

Suspicious transactions related to money laundering and financing of terrorism are reported to MASAK within the framework of the legislation.

In case there are information or matters creating suspicion that a transaction that is realized or attempted to be realized within the Company or with the mediation of the Company, is related or connected with the laundering of proceeds of crime and financing of terrorism, by conducting necessary researches within reasonable limits, reporting of transaction being deemed as suspicious is made to MASAK within the frame of specified periods and principles.

If there are documents supporting the suspicion that a transaction being attempted or continued is related with a crime of laundering or financing of terrorism or if there are serious indications in that regard, Suspicious Transaction Reporting is made to MASAK by submitting the justifications and requesting for the transaction to be suspended and during the period determined as per the legislation, it is avoided for the transaction to be realized.

Necessary communication and cooperation required under the applicable legislation are established between those parties involved in the process of the identification, examination and consideration and reporting of the Suspicious Transaction to MASAK.

For ensuring the confidentiality and safety of Suspicious Transaction Reports and internal reports being realized within the Company in this regard, and for protecting the parties being involved in these reports, the utmost care required within the frame of legislation is shown by those who are involved with the subject.

Company employees, in performing their duties pay special attention to transactions below:

- Transactions not related to the business or proportional to income of the customer,
- Refraining from providing documents and information within the scope of legal obligations;
- Perceiving the purpose of avoiding reporting and recording procedures,
- Providing misleading and non verifiable information,
- Large-scale and unusual (transfers) with banks located in risky geographical regions and countries

In the event of such transactions, the information and documents of the transaction are provided to assist the Board of Inspectors, inspectors and law enforcement units and are reported to the Compliance Officer in accordance with the Suspicious Transaction Reporting Form. Suspicious transactions related to laundering proceeds of crime and the financing of

terrorism are reported to MASAK by the Compliance Officer within the time and principles specified in the legislation.

11. Customers Under the Scope of the Suspicious Transaction Reporting

The Compliance Officer shall decide whether the existing customer relationship will be maintained or not with customers who are subject to or side to Suspicious Transaction Reporting and is notified in writing to the related unit.

12. Information Requests of Other Institutions

Information requests of other institutions involved in business relationship, about the Company's implementation of prevention of laundering proceeds of crime or financing of terrorism or the activity of reviewing and declaring conformity forms shall be carried out by the Compliance Officer.

13. Maintenance and Confidentiality Of Records

All the information, documents, and records that are required to be obtained and preserved relating with the customers and transactions in accordance with the regulations, are kept within the frame of periods and principles that are specified in the applicable legislation of our country, in a way to be available whenever they may be required. Necessary measures within the scope of legislation are implemented for the confidentiality of the relevant data, documents and records of customers and transactions.

14. Obligation to Provide Information and Documents

The reporting activities to be carried out within the scope of continuous information providing and the requests coming from the institutions and officials authorized to request information and documents, are fulfilled with utmost care and in accordance with the provisions of the legislation.

15. Other Considerations

The principles and procedures regarding the subjects in this Policy document and the basic operation principles of the processes and systems established within the Company for this purpose are regulated by the internal legislation of the Company.

Corporate Policy is notified in accordance with the signature requirement and changes in the Policy shall be notified by publishing on-line by the Company's internal legislation.

16. Entrance into force

This Policy and the amendments to this policy shall enter into force on the date of approval by the Board of Directors. Arrangements and implementations in the company's legislation according to this Policy are made by the General Management.