MİLLÎ REASÜRANS

POLICY FOR COMBATING FINANCIAL CRIMES AND SANCTION

Istanbul, 2026

TABLE OF CONTENTS

MİLLİ REASÜRANS T.A.Ş.

POLICY FOR COMBATING FINANCIAL CRIMES AND SANCTIONS

SECTION 1

GENERAL PRINCIPLES

I. INTRODUCTION

Milli Reasürans T.A.Ş., with its long-standing history and a distinguished reputation in international insurance and reinsurance sector, regards compliance with all applicable legislation, standards, and regulations across its operations not merely as a legal obligation, but as an integral component of its social responsibility and accordingly considers the combating of Financial Crimes within this framework.

II. PURPOSE AND SCOPE

This Policy aims to establish a general risk-based framework for controls and measures to be implemented across all Company activities and to clearly define responsibilities within the scope of combating the laundering of proceeds of crime, the financing of terrorism, and the financing of proliferation of weapons of mass destruction, as well as ensuring compliance with domestic and international sanctions.

The Policy covers all business units, managers, employees, and relevant third parties involved in the Company's business processes. It is essential for all employees to act in accordance with this Policy, and to maintain and strengthen a sustainable culture of preventing Financial Crimes and complying with sanctions obligations throughout the Company.

As a financial subsidiary within the Türkiye İş Bankası A.Ş. Financial Group, the Company complies with the Financial Group Policy. All foreign branches and subsidiaries of the Company are expected to take all necessary measures and fulfil their obligations to ensure compliance with the Financial Group Policy and/or this Policy. The provisions set out in this Policy constitute the minimum measures to be complied with. Where the regulations of the countries in which the Company's foreign branches and subsidiaries operate require the implementation of more stringent measures, such measures shall be applied. In the event that the legislation of the relevant country does not permit the application of the measures set out within this Policy, the matter is reported to the FCIB and additional measures are taken.

III. DEFINITIONS

Asset: Funds, proceeds, and benefits and values derived from them or inter-conversion of them, owned or possessed or directly or indirectly controlled by a natural or legal person, funds, proceeds, and benefits and values derived from them or inter-conversion of them, owned or possessed by a natural or legal person who act on behalf or for the benefit of this natural or legal person.

Audit Committee: The committee consisting of at least two non-executive board members, established to ensure that the Board of Directors soundly fulfils its duties and responsibilities regarding internal systems and to provide assurance for the execution of the Board's audit and supervision activities.

Bank: Türkiye İş Bankası A.Ş.

(Ultimate) Beneficial Owner: Natural person(s) who ultimately control(s) or has ultimate influence over the legal person(s) or unincorporated organizations conducting transactions within the Company.

Board of Directors: The Board of Directors of Milli Reasürans T.A.Ş.

Chief Executive Officer (CEO): Chief Executive Officer of Milli Reasürans T.A.Ş.

Compliance Officer: The Company employee exclusively assigned and authorized by the Company who is responsible for ensuring the Company's compliance with the obligations arising from the Legislation.

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

Countries/Regions Subject to Comprehensive Sanctions: Countries or regions which are subject to country/region-wide sanctions by The Republic of Türkiye, United Nations Security Council, United States of America, European Union or United Kingdom.

Country Risk: Risk that the Company may be exposed to due to the reinsurance activities, or any transaction on the basis of those activities, that may be engaged with the individuals, corporations or financial institutors of a country, which is announced by the Ministry of Treasury and Finance, or lacks satisfactory regulations to combat Financial Crimes, or fails to display a satisfactory performance of collaboration in order to prevent such crimes or is considered by the international institutions to be risky.

Customer Risk: Risk whereby the Company may be exploited on the grounds that the customer's business field requires the use of large amounts of cash or allows international fund transfers; or the customer or those acting on their behalf acting for the purpose of Laundering of Proceeds of Crime and Financing of Terrorism.

FATF: Financial Action Task Force.

FCIB: Financial Crimes Investigation Board

Financial Crime: Activities involving the Laundering of Proceeds of Crime and the Financing of Terrorism.

Financial Group: The group consisting of branches, agencies, representatives, commercial agents and similar affiliated units of financial institutions that are resident in Türkiye and are affiliated to or controlled by a parent institution whose head office is in Türkiye or abroad.

Financial Group Policy: Türkiye İş Bankası A.Ş. Financial Group Policy for Combating Financial Crimes.

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.

Freezing of Asset: 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.

Institution / Company: Milli Reasürans Türk A.Ş.

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.

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

Misconduct: Misconduct is defined as defective work practice or behaviors that disrupt the proper functioning of work processes or cause harm to expected outcomes, as well as the failure to carry out duties prescribed by the Personnel Regulation, non-compliance with its mandatory provisions, or the undertaking of prohibited actions by it.

Ongoing Business Relationship: A business relationship that is established between the Company and its customers, and that is ongoing due to its characteristics,

Policy: Milli Reasürans T.A.Ş. Policy for Combating Financial Crimes and Sanctions.

Politically Exposed Person: High-level real persons who are entrusted with a prominent public function by election or appointment domestically or in a foreign country and members of the board of directors, senior executives and other persons who have equivalent duty of international organizations.

Postponement of Transactions: Refraining from the execution of a transaction intended to be conducted within the Company in accordance with the principles set forth in the legislation.

Risk: The financial losses or loss of reputation that the Company or the Company employees may suffer due to the fact that Company's reinsurance activities are used for the purpose of Laundering of Proceeds of Crime and Financing of Terrorism, or due to the failure to completely comply with the obligations imposed by the Code on the Prevention of Laundering of Criminal Proceeds, or any other regulations or communiqué enacted on the basis of that Code.

Sanctions: Regulations aimed at comprehensively or non-comprehensively restricting or blocking the economic activities of the countries, individuals or entities to achieve economic and political goals.

Senior Management: Chief Executive Officer and Deputy Chief Executive Officers of the Company.

Service Risk: The risk that the Company may be exposed in the context of non-face-to-face transactions or new products to be offered by using emerging technologies.

Simplified Measures: Regulations set forth by the FCIB Communiqué No: 5, which allow the customer due diligence measures to be applied in a more simplified manner conducting a risk-based approach in cases where the risk of money laundering and terrorist financing may be considered low.

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 Company, has been acquired through illegal ways or used for illegal purposes and is used, in this scope, for terrorist activities or by terrorist organizations, terrorists or those who finance terrorism.

IV. MISSIONS, DUTIES AND RESPONSIBILITIES

The Company's Board of Directors is the ultimate body responsible for the implementation of the Policy in an adequate and effective way.

Board of Directors is authorized and responsible for;

- Assigning the Compliance Officer,
- Ensuring the Company's compliance with provisions regarding combating Financial Crimes,
- Approving the Policy, and any amendments to be made as per developments,
- Evaluating the results of risk management, monitoring, control, and internal audit activities set out in the Policy, and ensuring that the necessary measures have been taken,
- Ensuring that all activities are carried out in a coordinated and effective way.

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

- Establishing the workflows and assignment regulations within the frame of principles of corporate management and in compliance with the Policy,
- Implementation of the processes by all employees in line with the Policy and in an effective way,
- Taking the required measures in a timely manner to ensure that the Company mitigates the risks relating with Financial Crimes and Sanctions.

Compliance Officer is assigned, authorized and responsible for;

- To carry out the necessary work to ensure the implementation of the Policy and to ensure the necessary communication and coordination with FCIB,
- Establishing the Policy and submitting it to the Board of Directors for approval,
- Developing, updating, publishing and monitoring the Company procedures in relation to the implementation of the Policy, and to monitor and coordinate how those procedures are implemented in practice,
- Carrying out risk management, monitoring and control activities,
- Submitting findings and deficiencies identified through monitoring and control activities to the Board of Directors,
- Evaluating the information and findings obtained about Suspicious Transactions and reporting the transactions that were deemed to be suspicious to FCIB,
- Review the records of information and statistics related to the activities of internal audit and training and reporting them to FCIB when requested.

All employees of the Company and its subsidiaries are obliged to fulfill their duties and responsibilities correctly and diligently in order to ensure the appropriate and effective implementation of the Policy and its related processes, as well as to avoid exposure risks related to Financial Crimes and Sanctions. Failure to comply with the Policy shall constitute

Misconduct, and disciplinary action may be taken in accordance with the nature and severity of Misconduct.

Effectiveness and efficiency in implementing the Policy will be regularly subject to inspection and evaluation within the scope of internal audit. The findings that are stated on the reports being issued are primarily handled by the responsible departments by considering Compliance Risk. Findings of audit relating to Compliance Risk are submitted to the Board of Directors.

SECTION 2

KNOW YOUR CUSTOMER

I. KNOW YOUR CUSTOMER PRINCIPLE AND RULES FOR ACCEPTANCE OF CUSTOMERS

The “Know Your Customer” principle is the foundation of customer acceptance process of the Company regarding combating Financial Crimes.

The Company attaches great importance on the “Know Your Customer” principle in order to be protected from persons and actions relating to Financial Crimes and Sanctions and carries out an implementation that complies with the international standards, recommendations, and applicable regulations.

Within the scope of “Know Your Customer” principle, the Company performs the following:

- Identifying the customer,
- Identifying the Beneficial Owners,
- Obtaining sufficient information about the purpose and nature of requested process,
- Performing risk assessment of customer during customer acceptance process and updating the risk assessment during the business relationship,
- Evaluating the customers and transactions in terms of the principals in Section 3 – Sanctions,
- Monitoring the status and the transactions of the customer throughout the business relationship,
- Taking the necessary measures relating with customers, activities and transactions requiring special attention.

The said measures are taken within the framework of Legislation and Policy, and the processes are established by the responsible departments under the responsibility of Senior Management.

Under the Law on the Prevention of the Financing of Terrorism and the Law on the Prevention of the Financing of Proliferation of Weapons of Mass Destruction, in terms of the risks of the violation, non-implementation and avoidance of Freezing of Asset decisions, the Company defines, assesses, monitors and mitigates the risk and applies advanced controls for the implementations of the aforementioned sanctions. In this regard, in case it has been identified that the persons, institutions and organizations, whose Assets are frozen, have Assets held by the Company, any kinds of accounts, rights and claims of those customers are frozen and reported to FCIB within the timeframes specified by the law. Also, the Company takes the necessary measures to avoid business relationships to be established with sanctioned persons, institutions and organizations for whom there is a Freezing of Asset decision.

The Company takes necessary measures to determine whether a customer or Beneficial Owner is Politically Exposed Person or not.

In the customer acceptance process, in line with the risk parameters defined by the Company, risk scores of customers are determined, and the appropriate customer acceptance processes are implemented. During Ongoing Business Relationship, customer risk ratings are reviewed periodically or, where necessary, prior to the completion of the periodic interval.

In cases where identification cannot be done or sufficient information about the purpose of business relationship cannot be obtained, the Company does not establish a business relationship or carry out the transactions of the related parties until the suspicion and deficiencies are overcome.

II. IDENTIFICATION

The company verifies the customer's identity in a timely, complete, and accurate manner, in accordance with applicable legislation, policies, and business processes, before establishing an Ongoing Business Relationship and conducting any transaction.

Identification is performed;

- irrespective of the amount where an Ongoing Business Relationship is established,
- irrespective of the amount whenever there is a suspicion as to the sufficiency and correctness of the 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 exceeds the threshold defined in the applicable Legislation

by obtaining identity information of customers and those acting on behalf of or for the account of customers as specified in the Legislation, and by verifying the accuracy of such information in cases required by the Legislation.

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 or for the account of customer and the Beneficial Owner, and on obtaining 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 by the third party when requested,
- the identity verification of the customer, whose information is shared, is not carried out under Simplified Measures by the third party.

In case of the establishment of business relationship by relying on a third party, the customer’s identification information shall be immediately received from the third party. In such instances, the ultimate responsibility shall remain with the Company. The principle of “reliance on third parties” may not be applied to the cases where the third party is resident in a risky country.

In accordance with the internal regulation established in line with the Policy, for the purpose of establishing an Ongoing Business Relationship and undertaking the requested transactions, necessary measures are duly adopted and diligently applied to identify and know the Beneficial Owner.

Special attention is paid to complex and large-amount transactions and to those which do not have a reasonable legal or economic purpose, and the necessary measures are taken to obtain sufficient information about the purpose and nature of transaction that is requested.

SECTION 3

I. SANCTIONS

In addition to national Legislation, as a minimum, the Company shall ensure full compliance with the sanctions as announced by,

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

and which are applicable to its activities. The company may, where necessary, accept sanctions imposed by other countries and international organizations in addition to those listed above. In that case, the sanctions lists to be considered are to be determined by the Compliance Officer.

The Company does not get involved intentionally in any transaction designed to circumvent the sanctions. The Company oversees Compliance Risks arising from the Sanctions at the customer onboarding, customer information update and execution of customer transactions. In this regard,

- Customers and their shareholders, power of attorney holders and beneficial owners are screened against sanctions lists.
- The Company examines whether the transactions the customer conducts with the Company directly or indirectly involve Comprehensive Sanctions-Specific Countries/Regions or individuals or entities subject to Sanctions.
- Until the review of the screening results is completed by the authorized personnel, customer onboarding and/or transactions are not concluded.
- Existing Customers are periodically screened against the aforementioned sanction lists.

The Company does not execute transactions involving the individuals and entities falling within the scope listed below, does not accept such individuals and entities as customers, and without prejudice to legal regulations terminates its business relationship with customers who are subsequently included in this scope;

- The Persons or entities subject to United Nations Security Council sanctions,
- The Persons or entities designated as Specially Designated Nationals (SDN) by the U.S. Treasury Department the Office of Foreign Assets Control,
- The entities owned directly or indirectly 50% or more by the individuals or entities designated as SDN,

- The Persons or entities domiciled / registered in Comprehensive Sanctions Target Countries/Regions.

The transactions of these individuals and entities within the scope of licenses and similar documents issued by the competent authorities can be performed exceptionally and with the approval of the Compliance Officer.

Excluding the scope listed above, in case the relevant sanction program permits to maintain the customer relationship or to execute the transaction, the final decision rests with Senior Management, by obtaining the opinions of the Compliance Officer and if deemed necessary by the Compliance Officer, by obtaining the opinions of the Corporate Compliance Division of the Bank.

The extent of the relationship with the customers who pose risk in terms of sanctions for the Company shall be determined by Senior Management with a risk-based approach taking into account the opinion of the Compliance Officer. In this regard, customer relationships may be terminated categorically or on an individual basis.

It is essential that the Company should act in line with the guidance and limitations shared by the Bank regarding the implementation of the provisions related to Sanctions.

SECTION 4

RISK MANAGEMENT

I. PURPOSE AND SCOPE OF RISK MANAGEMENT

The main purpose is to define, grade, assess, and minimize the risks related to Financial Crimes and Sanctions which the Company may be exposed to.

For this purpose, the Company grades the customers, services, products, and countries within the frame of customer, service, and country risks that could be exposed to. The Company manages these risks by establishing the processes that define, rate and assess those starting with the customer acceptance process. In this regard, the results of national risk evaluation are also taken into account.

II. RISK MANAGEMENT ACTIVITIES

Risk management activities related to prevention of Financial Crimes and Sanctions are designed and carried out by the Compliance Officer within the frame of relevant regulation and Policy provisions.

The activities related to risk management covers;

- Developing risk defining, rating, classifying and assessing methods based on Customer Risk, Service Risk and Country Risk,
- Rating and classifying countries, services or transactions and customers depending on risks,
- Developing proper operational and control rules for ensuring monitoring and controlling risky customers, transactions or services; taking necessary measures to mitigate the risks; reporting in a way that warns related units; carrying out the transactions with the approval of Senior Management and controlling those, when necessary,
- Questioning retrospectively the coherency and effectiveness of risk defining and assessing methods and risk rating and classifying methods depending upon sample events or previous transactions, reassessing and updating them according to achieved results and new conditions,
- Carrying out required development work through pursuing principles, standards and guidelines established by national Legislation and international organizations related to issues under the scope of risk,
- Reporting risk monitoring and assessing results to Senior Management and the Board of Directors.

Countries and customer groups that are within the high-risk category are specified by the Compliance Officer utilizing a risk-based approach within the frame of Legislation and Policy, and those are subject to effective monitoring and controls in accordance with their qualities.

In assessing the Customer Risk related to Financial Crimes and Sanctions, basically the criteria below are considered:

- Occupation and field of activity of customer,
- Establishment type of customers which are legal entities,
- The suitability and adequacy of the regulations and supervisory practices aimed at combating Financial Crimes in the country, region, and/or business activity of which the client is a national and/or resident and/or operates,
- Duration of the business relationship between the customer and the Company,
- The activity period of customers which are legal entities,
- Negative news about the customer that can be associated with Financial Crimes and Sanctions.

At the beginning of business relationship and during the continuation of relationship, the customers are placed in appropriate risk categories with respect to their activities and the nature and scope of their transactions and relations with the Company, taking into account above stated fundamental criteria and other specific information and criteria about the customer.

Information and documents that are obtained from the customers within the scope of the “Know Your Customer” principle are updated once a year for customers within high-risk category, once in two years for customers in medium risk category, and once in four years for customers in low-risk category.

Customers in high-risk category and their transactions are monitored closely with monitoring and control methods that are appropriate for the purpose. Enhanced due diligence is implemented for the customers who are in high-risk category with regards to customer, service, and country risks. Within this frame, the central monitoring and control activities that are designed and carried out with a risk-based approach by Compliance Officer are mainly focused on customers and transactions within high-risk category.

In order to reduce the risks undertaken relating to the groups which are specified as being high risk as a result of risk assessment, one, more than one or all the additional measures stated below, are taken:

- Developing procedures for ongoing monitoring of transactions and customers,
- Requiring approval of the next level personnel for establishing business relationship, sustaining current business relationship or carrying out transactions,
- Gathering as much information as possible on the intended nature of the business relationship, purpose of the transaction and source of assets that are subject to transaction,
- Obtaining additional information and documents under the scope of customer due diligence, and taking additional measures for verifying and certifying the information submitted, updating more frequently the identification data of customer and Beneficial Owner,
- 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 need further examination,
- Developing processes for specifying the type of customers with whom business relationships will not be established.

The risk categories of the customers are determined according to the identification information, and the other customer information compliant with the current Legislation and international standards.

In this regard, the individuals and companies that are;

- Specified as to be applied special attention as per FATF recommendations,
- Engaged in high-risk activities in terms of Laundering of Proceeds of Crime and Financing of Terrorism according to international standards,
- Required to be monitored closely due to being resident of or associated with risky countries or regions,

- Required to be monitored closely with special attention as being accepted to be risky and unfavorable by the authorized legal bodies due to the connection with Laundering of Proceeds of Crime and Financing of Terrorism and other Financial Crimes

are monitored within the high-risk category.

In the business relations established and transactions conducted with customers whose ultimate beneficial owners include Politically Exposed Persons elected or appointed by a foreign country, or their spouses, first-degree relatives, or close associates, the following measures shall be taken as a minimum:

- Requiring approval of the Senior Management for establishing business relationship, sustaining current business relationships or carrying out transactions,
- Taking reasonable measures to determine the source of assets and funds belonging to these persons or subject to transaction,
- Conduct enhanced monitoring of the business relationship by increasing the number and frequency of the controls applied and by selecting the patterns of transactions that need further examination.

These measures are applied to Politically Exposed Persons who are elected or appointed by Türkiye or who are working for international organizations or their spouses, first-degree relatives, and close associates in case the business relations and transactions with them are deemed high-risk.

Close associates of Politically Exposed Persons mean people who have all kinds of social, cultural or economic affinity, which can be considered as a unity of interests or purposes, such as kinship other than first degree, being engaged, company partnership or being a company employee.

In the event that Politically Exposed Persons resign from office or lose their qualifications, the implementation of the measures specified above shall continue for at least one year from the date of their resignation or loss of these qualifications. This period may be extended if the transactions or business relations with these persons pose a risk.

In terms of Service Risk;

- Products and services based on new and advancing technologies,
- Businesses and transactions, the ultimate beneficiaries of which are not clearly and completely defined,
- Other products, services and types of transactions that are required to be given special attention in the concept of the risk management, monitoring and control activities related to the combat against Financial Crimes and Sanctions to be carried out in accordance with international standards, Legislation in effect and this Policy,

are monitored within high-risk category.

Within the scope of Country Risk, the countries that are designated as being high risk in accordance with the criteria specified below are closely monitored:

- Evaluations of whether they have got sufficient regulations and implementations with regards to combating Financial Crimes, being realized within the scope of recommendations issued by FATF,
- The report being prepared by United Nations Narcotic Drugs and Crime Office and reflecting the situation of countries with regards to narcotic drugs,
- The report being prepared by United Nations Narcotic Drugs and Crime Office and reflecting the situation of countries with regards to human trafficking,
- Corruption perception index being issued by international institution named "Transparency International" and reflecting the indices of countries relating with corruption,
- International Narcotic Control Strategy Report (INSCR),
- Countries being specified on the list of "Risky Countries" announced by the Ministry of Treasury and Finance,
- Countries to which sanctions are implemented at an international level within the frame of decisions of United Nations Security Council due to the policy and implementations relating with Laundering of Proceeds of Crime or Financing of Terrorism,
- Countries being announced by European Union or OFAC and being specified as bearing high risks in terms of the Laundering of the Proceeds of Crime,
- Offshore centers, free zones, and finance centers,
- Tax havens.

SECTION 5

MONITORING AND CONTROL

I. PURPOSE AND SCOPE OF MONITORING AND CONTROL

The main purpose of the monitoring and control procedures is to protect the Company against the risks and to ensure that its operations are constantly monitored and controlled subject to the applicable Legislation and the Policy and related procedures.

Monitoring and control activities are established and applied on a risk-based approach. In this respect, certain monitoring and control methods that suit the nature and level of risks associated with the Company customers and transactions shall be developed and effectively implemented.

II. MONITORING AND CONTROL ACTIVITIES

Monitoring and control activities are designed and conducted using a risk-based approach under the coordination and supervision of the Compliance Officer subject to the applicable Legislation and Policy. 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.

Monitoring and control activities basically cover the following:

- Monitoring and control of high-risk customers and transactions,
- Monitoring and controlling transactions executed with risky countries,
- Monitoring and controlling complex and unusual transactions and transactions that don't have any reasonable legal and economic purpose,
- Controlling those transactions above a specific amount threshold through sampling in order to check its consistency 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, up-to-datedness and adequacy of customer data and documents, and ensuring that missing ones are remediated,
- Continuous monitoring of the compliance of a customer transaction with the information compiled about his scope of business, risk profile and sources of funds throughout the transaction,
- Controlling the transactions carried out through systems that allow the execution of transactions without a face-to-face relation,
- Risk-focused control of those services that may remain exposed to abuse and risks in respect of Financial Crimes and Sanctions on the grounds of new products, transactions, services, activities and technological developments and
- other monitoring and controls that may be necessary in this respect.

Central monitoring and control activities are carried out by the Compliance Officer through the system. The effectiveness of practices and the appropriateness of processes carried out in the Head Office's business units and branches are ensured through on-site inspection and control within the scope of 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 by the Compliance Officer as a whole.

Measures are taken to continuously monitor customers and transactions, taking into account Freezing of Asset decisions. If there is any increase in the frozen Assets, these increases are

also subject to the Freezing of Asset provisions and reported to FCIB within the timeframes specified by the law.

SECTION 6

TRAINING

I. PURPOSE AND SCOPE OF TRAINING

Training activities are conducted within the Company to improve corporate culture and awareness as well as providing up-to-date information to employees regarding the risks related to Financial Crimes and Sanctions, and related legal obligations, Policy, procedures, and practices of the Company

Training activities are conducted in accordance with legislation and policy provisions and cover all relevant employees.

II. TRAINING ACTIVITIES

Training activities of the Company are designed and carried out under the supervision of the Compliance Officer. In order to ensure that the training activities are applied throughout the Company, in-class training, e-training, other training methods, visual and audial training materials, communication channels such as internet or intranet are utilized in an effective way. All new hires undergo training at the start of their employment. It is ensured that each related employee receives training within this scope at least once a year. Within the frame of amendments in the Legislation, certain updates will be made in the content of trainings. In coordination with the Organizational Development and Talent Management Department, employees' training status is monitored. The timely completion of the e-training assigned to employees is the responsibility of the related department manager.

Special importance is given to selecting the lecturers who will give the training and in providing them with the necessary training for this purpose. It is followed up and evaluated closely to ensure that the training courses are suitable and sufficient for meeting the requirements. Training activities are reviewed as per the measurement and evaluation results.

The necessary information and statistics regarding the training activities are kept regularly and reported by the Compliance Officer to FCIB upon request.

III. TRAINING SUBJECTS

The training courses shall at least cover the following subjects;

- Laundering of Proceeds of Crime and Financing of Terrorism terms,

- The stages, methods of Laundering of Proceeds of Crime and case studies on this subject,
- Legislation regarding prevention of Laundering of Proceeds of Crime and Financing of Terrorism,
- Risk areas,
- Company Policy and procedures,
- Within the framework of Law and related Legislation;
    - Principles relating to customer identification,
    - Principles relating to Suspicious Transaction reporting,
    - Obligation to keep and presentation of documents,
    - Obligation of providing information and documents,
    - Sanctions to be implemented in case of violation of obligations,
- The international regulations on combating Laundering and Financing of Terrorism.

SECTION 7

INTERNAL AUDIT

I. PURPOSE AND SCOPE OF INTERNAL AUDIT

Purpose of internal audit is to provide assurance to the Board of Directors in regard to the effectiveness and sufficiency of integrity of this Policy and the Company's activities relating to combat against Laundering of Proceeds of Crime and Financing of Terrorism.

Within the scope of internal audit,

- Establishment and execution of business processes of the Company in accordance with the Policy,
- risk management, monitoring, control activities as well as the efficiency and effectiveness of training activities which aim to provide up-to-date information to employees, and to enhance the corporate culture and awareness related to the Policy and its applications, and the Company’s compliance with the applicable legislation, regulations, Policy, and procedures

are investigated and evaluated by Internal Audit with a risk-based approach within the frame of regulations. Deficiencies, mistakes, and frauds that are determined are reported to the Board of Directors together with the opinions and proposals aiming to prevent them from recurring.

The scope and methodology of internal audit are determined to provide reasonable assurance in a manner that the whole is represented, while considering the deficiencies identified in monitoring and control activities, as well as risky customers and transaction risk and volumes.

The information and statistics required within the frame of regulations in relation with the internal audit activities are kept on a regular basis and they are reported by the Compliance Officer to FCIB upon request.

SECTION 8

OTHER PROVISIONS

I. SUSPICIOUS TRANSACTION REPORTS

In case there are information or matters creating suspicion that a transaction carried out or intended to be carried out by or through the Company is related or connected with the Laundering of Proceeds of Crime and Financing of Terrorism, the necessary investigations will be conducted to the extent possible, and the transaction deemed suspicious will be reported to FCIB within the timeframes and principles specified in the legislation.

If there are documents supporting the suspicion that a transaction being attempted or continued is related with Financial Crimes or if there are serious indications in that regard, Suspicious Transaction reporting is made to FCIB by submitting the justifications and requesting for the transaction to be delayed and during the period determined by the Legislation, it is avoided for the transaction to be realized.

Necessary communication and cooperation required by the applicable Legislation are established between the parties involved in the process of identification, examination and consideration and reporting of the Suspicious Transaction to the FCIB.

For ensuring the confidentiality and privacy of Suspicious Transaction Reports and internal reports being produced by the Company in this regard, and for protecting the parties involved in these reports, the maximum care required within the frame of Legislation is exhibited by those who are involved in this matter.

II. MAINTENANCE AND CONFIDENTIALITY OF INFORMATION, DOCUMENTS, AND RECORDS

All information, documents, and records that are required to be obtained and preserved in relations to the customers and transactions in accordance with the regulations, are kept within the frame of periods and principles specified by Legislation, in a way to be available whenever they may be required.

Necessary measures are taken and implemented within the framework of the relevant Legislation to ensure the confidentiality of information, documents and records related to customers and transactions. Reporting activities for the purposes of continuous information disclosure as well as requests from those authorities authorized to seek information and

documents under the applicable Legislation are fulfilled with utmost diligence, subject to the applicable Legislation.

The Company may share the information about knowing the customer, their accounts and transactions with the institutions in the Financial Group on the basis specified in the Financial Group Policy. The confidentiality provisions stipulated under specific legislation do not apply information sharing within the Financial Group. However, institutions within the Financial Group are prohibited from disclosing or sharing information regarding the filling of a Suspicious Transaction Report.

III. EFFECTIVENESS AND REVIEW

The Policy is reviewed at least once a year with the aim of ensuring compliance with the regulations and international standards and updates, whenever required, are submitted for the approval of Board of Directors. Any amendments or updates that may be reflected in relation to the Policy later on are also enforced with the approval of the Board of Directors.