İŞ YATIRIM ANTİ-FINANCIAL CRIME AND SANCTIONS POLICY

1. OBJECTIVE

The main objective of the policy is to ensure the fulfilment of our Corporation's obligations regarding the combat against Financial Crimes, the implementation of the Compliance Program prepared with a risk-based approach to ensure compliance of the Corporation with the obligations introduced by the Legislation, taking into account the international recommendations, standards and good practices published by FATF, and our Corporation's compliance with local and international sanctions, to assess the customers, transactions and services with a risk-based approach, to determine the strategies, controls and measures, operating rules and responsibilities for mitigating the risks that may be posed to our Corporation, including reputation risk, and keeping the risks under control, and to strengthen the culture of our Corporation regarding the combat against Financial Crimes.

2. SCOPE

This Policy covers our Corporation's Board of Directors, Senior Management, Head Office units and all branches in terms of duties, authorities and responsibilities related to the combat against Financial Crimes.

Financial subsidiaries of Türkiye İş Bankası A.Ş. included in the Financial Group shall comply with the Financial Group Policy. In this context, our corporation is directly included in this scope as it is a financial subsidiary of TÜRKİYE İŞ BANKASI A.Ş.

It is expected that our Corporation's Head Office units, domestic branches and domestic and foreign subsidiaries take all necessary measures to comply with the policy and take necessary measures to the extent that they are related to their fields of activity. The provisions in the policy include the minimum measures to be implemented; and in case the foreign financial subsidiaries of our corporation are required to implement more stringent measures under the legislation of those countries than the provisions in the policy, the relevant strict measures shall be applied.
This Policy comprises Risk Management, Monitoring and Control, Training, Internal Audit, Obligations and Sanctions Policies, in relation with the Corporation's combat against Financial Crimes;.

This Policy shall be revised once a year, taking into account the measures within the scope of the Compliance Program determined in the Regulation on the Program on Compliance with the Obligations Regarding the Prevention of Laundering of Criminal Revenues and Terror Finance, and the Financial Group's Compliance Program, and necessary updates shall be made.

3. BASIS

This Policy has been prepared on the basis of the "Law on Prevention of Laundering Criminal Revenues" No. 5549, the "Regulation on Measures Regarding Prevention of Laundering Criminal Revenues and Terror Finance" published on the Official Gazette No. 09.01.2008/26751, the "Regulation on the Program of Compliance with Obligations Regarding the Prevention of Laundering of Criminal Revenues and Terror Finance" published on the Official Gazette No. 16.09.2008/26999, the "Law on the Prevention of the Terror Finance" No. 6415, the "Regulation on Procedures and Principles related to Implementation of the Law on the Prevention of the Terror Finance" published on the Official Gazette No. 31.05.2013/28663, the Financial Crimes Investigation Board's "General Communiqué" (Serial No: 5) published on the Official Gazette no. 09.04.2008/26842, and the Financial Crimes Investigation Board's "General Communiqué" published on the Official Gazette no. 30.04.2021/31470 (Serial No: 19), the Laws, regulations and communiqués and MASAK resolutions and instructions on the "Prevention of Financing the Proliferation of Weapons of Mass Destruction" published on the Official Gazette number 27.12.2020/ 7262.

"General Communique for Financial Crimes Investigation Committee" no. 21 as published in the Official Gazette issued on 17/11/2022 under no. 32016, the Implementation Guideline for Publicly Exposed Person

4. DEFINITIONS

Term	Definition and Description
Bank	Türkiye İş Bankası A.Ş.
Information Abuse	Issuing a purchase or sale order for the relevant capital market instruments or modifying or cancelling the order given, based on information that has not yet been disclosed to the public about the capital market instruments or the issuers, which may affect the prices, values, or the decisions of the investors, and thereby obtaining benefits, directly or indirectly
FATF	Financial Action Task Force
Financial Crime	Activities involving Laundering of Criminal Revenues, Terror Finance, Information Abuse or Market Fraud
Real Beneficiary	Real persons performing transactions with the Corporation, the real person or persons who ultimately control or have ultimate influence over the real or legal persons or unincorporated entities on whose behalf the transactions are performed.
Service Risk	Risks arising from instruments traded by investors
Related Unit(s)	The units that are responsible together, separately or all together, according to their job descriptions, within the scope of the laws, regulations and communiqués in force on Combating Financial Crimes, Preventing the Laundering of Criminal Revenues and Terror Finance.
Financial Group	The Financial Group of TÜRKİYE İŞ BANKASI A.Ş., including our Corporation, comprising financial domiciled in Turkey and their branches, agencies, representatives, commercial agents and similar subsidiary units affiliated to or under the control of a parent corporation headquartered in Turkey or abroad,
Financial Group Policy	Türkiye İş Bankası A.Ş. Financial Group's Anti-Financial-Crimes and Sanctions Policy
Publicly Exposed Person (*)	Top level natural persons to whom a significant public duty is assigned by means of elections or appointment in Turkey or abroad, or board members of international institutions, top level executives and other persons holding equivalent positions;
Spouses, Next of Kin and Relatives of Publicly Exposed Person	Spouses or next of kin of Publicly Exposed Person, or individuals with whom all kinds of social, cultural or economic relations are

	established based on kinship (other than next of kin relation), engagement, company partnership or company employee which may be considered as an alliance of interest or goal;
Country/Territory Subject to Comprehensive Sanctions	Countries or territories subject to national or regional sanctions by the Republic of Turkey, the United Nations Security Council, the United States of America, the European Union and the United Kingdom
Corporation	İş Yatırım Menkul Değerler A.Ş.
Unlicensed Bank	A bank that does not have a physical service office in any country, does not employ full-time personnel, and is not subject to the supervision and permission of an official authority in terms of banking transactions and records.
(Presidency of) MASAK	Presidency of the Financial Crimes Investigation Board
Legislation	Applicable laws, regulations and communiques, and MASAK resolutions and instructions on the Prevention of Laundering Criminal Revenues and Terror Finance
Customer Risk	The risk of abuse of obligations, based on factors such as the customers line of business allowing for heavy use of cash, trading of high-value goods or international fund transfers; the customer or those acting for on account of the customer acting with the intention of Laundering Criminal Revenues or Terror Finance
Transactions Requiring Special Attention	Paying special attention to complex and unusually large transactions and transactions that do not seem to have a reasonable legal and economic purpose, taking necessary measures to obtain sufficient information about the purpose of the requested transaction, and keeping the information, documents and records obtained in this context in order to present them to the authorities when requested.
Market Fraud	Making purchases or sales, placing orders, cancelling orders, modifying orders or performing account movements, in order to create a false or misleading impression regarding the prices, price changes, supply and demand of capital market instruments
Policy	Corporation's Anti-Financial-Crime and Sanctions Policy
Risk	The possibility of financial or reputational loss that our Corporation or Corporation's employees may be exposed to, due to reasons such as utilizing services provided by the Corporation, for the purpose of Laundering Criminal Revenues or Terror Finance, or failure to fully comply with the obligations imposed by the Law on Prevention of Laundering Criminal Revenues and

	the regulations and communiqués issued under that Law.
Risk Database	The database on which it is checked, before opening an account, whether the person, the entity and the Real Beneficiaries of the entity (the controlling shareholders with 25% or more share capital) are included in the national and international lists published within the scope of Prevention of Laundering Criminal Revenues and Terror Finance.
Politically Exposed Person (PEP)(*)	Head of state or government, top politicians, government officials, judicial or military personnel, representatives of important political parties and public administration officials in top public offices, and their family members and relatives
Laundering Criminal Revenues (Laundering)	Transactions aimed at depicting the profits earned through illegal means as though they were earned through legal means, to convert cash revenues into non-cash form by introducing them into the financial system, and render them legitimate through a process within the financial system and changing their nature.
Continuous Business Relationship	A continuous business relationship established between our corporation and the customer as a result of opening of an account and the services provided.
Suspicious Transaction	The existence of any information, suspicion or any reason to suspect that the assets involved in the transaction performed or attempted with or through our corporation has been earned illegally or used for illegal purposes, and in this context, for terrorist acts or by terrorist organizations, terrorists or those who finance terrorism
Terror Finance	Providing funds to or collecting funds for terrorists or terrorist organizations, even without being associated with a certain act, for the purpose of using, or knowingly and willingly that it will be used, in the realization of the acts stipulated as a crime under the law.
Compliance Officer	Our corporation's staff who is commissioned by the Board of Directors to ensure compliance with the Law on the Prevention of Laundering of Criminal Revenues and the obligations introduced by the Legislation enacted under the law, who can decide independently, request all information and documents related to their field of duty from all units, and have the authority to access them in a timely manner.
Assistant Compliance Officer	Our corporation's staff who reports to the Compliance Officer, who meets the requirements and qualifications of the Compliance Officer in order to conduct the Compliance Program in order to fulfil the duties specified in the relevant

	Legislation. Where necessary, the Compliance Officer delegates all or part of his duties and authorities, expressly in writing, to the Assistant Compliance Officer.
Compliance Program	A set of measures to combat Financial Crimes, within the framework of the relevant Legislation and Corporate Policy within the Corporation.
Compliance Risk	Risks related to sanctions, financial losses and/or loss of reputation that the Corporation may be exposed to as a result of the Corporation's activities or the acts and conduct of its employees in breach of the Legislation, regulations and standards.
Country Risk	Risks that the Corporation may be exposed to as a result of business relationships to be entered into with, and the acts of, citizens, companies or financial institutions of countries that do not have adequate regulations on the Prevention of Laundering Criminal Revenues and Terror Finance, do not cooperate adequately in the combat against such crimes, or are considered risky by authorized international organizations and countries, as announced by the Ministry of Treasury and Finance
Senior Management	General Manager and Deputy General Managers
Sanction	Regulations aimed at restricting or preventing economic activities, individually or comprehensively, targeting countries, individuals and organizations, in order to achieve economic and political goals

(*) The most important standard about measures that need to be taken against the publicly exposed persons is the FATF Recommendation No. 12. These persons who are called "politically exposed persons (PEPs)" in the said recommendation are referred to as "Publicly Exposed Persons" in the Communiqué no. 21 as well as the "Implementation Guideline for Publicly Exposed Persons" by taking into account the points emphasized in the FATF definition.

5. RESPONSIBILITIES

- The Bank's Board of Directors is ultimately responsible for the adequate and effective execution of the Policy and Compliance Program as a whole.
- Senior management is responsible towards the Board of Directors for establishing business processes and job regulations within the framework of corporate governance principles in accordance with the Policy, for effective implementation as intended, of the processes by all employees, for timely taking the necessary measures to ensure that our Corporation is not exposed to risks related to Financial Crimes and Sanctions.
- The Compliance Officer, who reports to the Board of Directors, shall perform his powers and responsibilities with the contribution of the relevant units, as specified in the internal regulations of the Corporation.
- Assistant Compliance Officer is responsible for fulfilling the duties and powers delegated to him expressly in writing by the Compliance Officer where necessary.
- All employees of the Corporation at all levels are obliged to fulfil all their duties and responsibilities accurately and carefully, ensuring that the policy, related processes and the Compliance Program are implemented at our Corporation's Head Office and branches effectively as intended, and that the Corporation is not exposed to risks related to Financial Crimes and Sanctions. Failure to comply with the Policy or any violation of the Policy may result in disciplinary penalties.

- The effectiveness and adequacy of the Policy and Compliance Program in practice are regularly audited and evaluated within the scope of internal audit. The determinations included in audit reports are primarily resolved by the responsible departments, by considering the Compliance Risk. Audit findings on Compliance Risk are presented to the Board of Directors by the Board of Inspectors through the Audit Committee.

6. RISK MANAGEMENT AND KNOW-YOUR-CUSTOMER

6.1. Risk Management

6.1.1. Objective

- The objective of the risk management policy is to define, rank, monitor, evaluate and reduce the risks that our Corporation may be exposed to.

6.1.2. Know Your Customer Policy and Customer Acceptance Principles

- The principle of “Know Your Customer” is the basis of our corporation's customer acceptance process in the combat against Financial Crimes. Our corporation attaches great importance to the "Know Your Customer" principle in order to be protected from people and actions related to Financial Crimes; and in this context, acts in line with international standards, recommendations and the applicable Legislation.
- Within the scope of “Know Your Customer” principle; processes are established under the responsibility of Senior Management, by taking necessary measures within the framework of the Legislation and Policy, in identifying the Real Beneficiary, recognizing the Real Beneficiary, providing sufficient information about the purpose and nature of the requested transaction, conducting risk assessment of the customer during the customer acceptance process, and updating the risk assessment dynamically during the business relationship, evaluating the customer and his transactions within the framework of the principles under the topic "Sanctions", monitoring the transactions and processes during the business relationship, taking necessary measures for the transactions that require special attention, implementing tightened measures in continuous business relationship established through remote identification.
- Corporations included in the Financial Group take necessary measures to avoid entering into business relations with persons, corporations or organizations listed in the United Nations Security Council resolutions, within the scope of the Law on Prevention of Terror Finance and the Law on Prevention of Financing the Proliferation of Weapons of Mass Destruction. All accounts, rights and receivables of persons, corporations or organizations that are not included in the aforementioned lists during the establishment of a Continuous Business Relationship, but are subsequently included in such lists shall be frozen and reported to MASAK within the periods specified in the law.
- Monitoring and control activities are conducted within the framework of the country's Legislation regarding Politically Exposed Persons and Publicly Exposed Persons and Spouses, Next of Kin and Relatives of . Publicly Exposed Persons;
- In the customer acceptance processes during account opening through digital remote identification method, the risk scores of customers shall also be determined systematically in line with the risk parameters set by the Corporation, and appropriate customer acceptance processes are applied. In addition, all customers are assessed under the risk rating system during the Continuous Business Relationship.
- Under the legislation, in cases where the customer cannot be identified or sufficient information cannot be obtained about the purpose of the business relationship, no business relationship shall be established and the transactions requested by the relevant parties shall not be conducted, unless and until such suspicions and deficiencies are eliminated.
- Continuous Business Relationship shall not be established with anonymous or fake names, gambling/illegal bettors, unlicensed banks and natural and legal persons subject to restrictions under the "Sanctions".
- Business relationships shall be terminated by closing the accounts of customers who are found to have committed fraud or gambling/illegal betting transactions, customers who fail to provide

requested information and documents about themselves and their transactions, and whose business relationship is decided to be terminated within the scope of monitoring and control and risk management activities, and who become subject to "Sanctions" after creation of the customer entry.

- As an exception to this article, after creation of customer entry, the accounts of persons, corporations and organizations subject to resolutions of the United Nations Security Council, within the scope of the Law on Prevention of Terror Finance and the Law on Prevention of Financing of Weapons of Mass Destruction, but all their accounts, rights and receivables shall be suspended and reported to MASAK within the period stated under the law.
- Within the scope of know-your-customer principles specified in the Regulation, the issues related to identification of customers who open an account with our Corporation and are in a Continuous Business Relationship, the documents to be obtained during identification, identification in the subsequent transactions, identification of those acting on behalf of others, identification of the Real Beneficiary, special attention to legal persons, checking the authenticity of the documents requiring confirmation, rejection of transaction and termination of the business relationship are set forth in the “Investor Account Transactions Implementation Principles”; and the cases where simplified measures can be applied within the scope of third party trust principle are specified in the "Implementation Principles on Prevention of Laundering Criminal Revenues and Terror Finance".
- Our corporation may share information regarding the identification of customer, the accounts and the transactions, with other affiliated institutions within the Financial Group, in accordance with the principles set forth in the Financial Group Policy. ın The processes within this scope are regulated in our domestic legislation, under the “Implementation Principles on Prevention of Laundering Criminal Revenues and Terror Finance”.

6.2. Objective and Scope of Risk Management

- The main purpose of Risk Management is to identify, rank, assess and mitigate the risks associated with Financial Crimes that the posed to our Corporation.
- For this purpose, our Corporation takes customer, service and country risks into account, and manages these risks by creating processes that define, rank and assess the risks, starting from the customer acceptance process.
- Definition and potential risk examples regarding financial risks that may be posed to our Corporation (credit risk, market risk, structural interest rate risk, liquidity risk) and non-financial risks (operational risk, legal and ethical risk, technology, information systems and interruption risk, human resources risk, model risk, reputation and perception risk, strategy and perception risk) are given in İş Yatırım Menkul Değerler A.Ş. Risk Catalogue. The Risk Catalogue is updated by the Risk Management Department.
- The rules to be followed during cash and asset transfers from the customer's account are included in the "Cash and Securities Transfers Application Principles" of our Corporation.

6.3. Risk Management Activities

- Risk management activities are designed by the Compliance Officer within the framework of the relevant Legislation and Policy provisions, and conducted by the Risk Management Department.
- Activities related to risk management include development of methods for identification, rating, classification and assessment of risks based on Customer Risk, Service Risk and Country Risk, considering the issues determined within the scope of national risk assessment, risk-rating of Services, transactions and customers, taking necessary measures to mitigate risks, monitoring, controlling and reporting risky customers, transactions or services to alert the relevant units; developing appropriate operation and control rules to conduct the processes upon approval of a higher authority and to audit them when necessary, retrospectively querying the consistency and effectiveness of risk identification, assessment, rating and classification methods over case studies or transactions performed, and reconsidering the results and developing conditions, conducting necessary development studies by following the risk-related principles, standards

and guides introduced by the national legislation and international organizations.

- Risk monitoring and evaluation results are reported by the Compliance Officer to the Board of Directors.
- The criteria used in assessment of Customer Risk during the business relationship, in relation with prevention of Laundering Criminal Revenues and Terror Finance, are specified in the "Application Principles on the Prevention of Laundering Criminal Revenues and Terror Finance".
- Countries and customer groups, products and services in high risk category are determined by the relevant units with a risk-based approach within the framework of the Legislation and the Policy, and are subject to effective monitoring and controls according to their nature. Relevant processes are included in the "Application Principles on the Prevention of Laundering Criminal Revenues and Terror Finance".
- During the Continuous Business Relationship, the customers are included in the appropriate risk categories by the Corporation in terms of the nature and scope of their activities, transactions, and relationships with the Corporation, within the framework of the fundamental criteria above, and other customer-specific information and criteria if any.
- Information of "high" risk customers, obtained through Investor Information Form, should be updated whenever necessary. Sales Units are responsible for obtaining up-to-date information about the customer and sharing remarkable changes with the Compliance Officer.
- For the groups determined as high risk as a result of the risk rating, the minimum measures to be taken in order to mitigate the assumed risk are specified in the "Application Principles on the Prevention of Laundering Criminal Revenues and Terror Finance".
- The risk categories of the customers are determined in accordance with the current legislation and international norms, in the light of their identity details, field of activity, and other available customer information.
- Accordingly; persons or organizations requir0ing special attention according to FATF recommendations, deemed necessary to be followed closely due to being located in or associated with risky countries or regions, operating in high-risk areas in terms of Laundering Criminal Revenues and Terror Finance according to international norms, or who are considered by competent legal authorities as high risk and thus Require Special Attention in terms of Laundering Criminal Revenues and Terror Finance and other financial crimes, or who predominantly use products and services in high-risk category, and other customers who are considered risky and Requiring Special Attention as to their current nature, fields of activity, or nature of their transactions, within the scope of risk management, monitoring and control activities under the Compliance Program to conducted in accordance with international norms, applicable Legislation and the Policy provisions, shall be monitored within the high-risk category.
- Within the scope of Service Risk; Risk classification is made according to the type of product offered to the customer.
- Following measures shall be implemented as a minimum in business relations and transactions executed with a Publicly Exposed Person who has been elected or appointed by a foreign jurisdiction or his spouses, next of kin, relatives or close people:

  - To subject the engagement of business relation, the maintenance of existing business relation or the execution of the transaction to the approval of the top level officer
  - To take reasonable measures to identify the origin of the assets and funds owned by these persons or subject to the transaction
  -To keep the business relation under tight monitoring and supervision by increasing the number and frequency of the applied controls and identifying the transaction types that require additional controlThese measures shall also be applied if the business relation established or transaction executed with the Publicly Exposed Person appointed or selected in Turkey or holding a position in international institutions or their spouses, next of kin., relatives or close persons are considered highly risky ones.

- Relatives of a Publicly Exposed Person mean spouses or next of kin of Publicly Exposed Person, or individuals with whom all kinds of social, cultural or economic relations are established

based on kinship (other than next of kin relation), engagement, company partnership or company employee which may be considered as an alliance of interest or goal;

- ●In the event that a Publicly Exposed Person quits his position or is deprived of his such qualifications, the measures described above in the third paragraph shall remain applicable and in force for at least one year from the date of their quittance or disqualification. This term may be extended in the event that transactions executed or business relations maintained with these individuals pose a riskWithin the scope of Service Risk; Risk classification is made according to the type of product offered to the customer.

- Within the scope of Country Risk, controls are conducted over the Risk Database.

6.4. Identification

- Since accounts are opened by our Corporation with customers only within the scope of Continuous Business Relationship; before entering into any transaction with any customer, identification is performed by obtaining information regarding identity within the framework of the relevant Legislation and confirming the accuracy of such information.
- Identification is performed under the Legislation, by obtaining and confirming the accuracy of the identity details of customers and those acting for or on account of the customers, regardless of the amount during establishment of Continuous Business Relationship, and regardless of the amount when there is suspicion about the adequacy and accuracy of the customer identification details previously obtained, and regardless of the amount in cases that require Suspicious Transaction notification, and when the transaction amount or the total amount of interconnected transactions exceed the amount stated in the Legislation.
- Our Corporation may establish a business relationship or enter into a transaction, in reliance of measures taken by a third party financial corporation about identification of the customer or the person for or on account of the customer and of the Real Beneficiary, and obtaining information about the business relationship or the purpose of the transaction.
- Trust in a third party requires ensuring that the third party takes other measures to meet the requirements of the identification, record keeping and know-your-customer rule, and if it is domiciled abroad, that it is also subject to regulations and inspections in accordance with international standards in the field of Anti-Money Laundering and Terror Finance, and that the certified copies of documents regarding identification can be obtained promptly from the third parties when requested.
- In such case, our Corporation shall remain ultimately responsible. In case of establishing a business relationship in reliance of a third party, the customer's identity details shall be obtained immediately from the third party. The third-party trust principle does not apply if the third-party is located in risky countries.
- We do not maintain a separate correspondent relationship as our accounts with T. İş Bankası A.Ş. are used with international money transfers.

7. SANCTIONS

- In addition to the national legislation, our corporation considers full compliance with, as a minimum, the Sanctions announced by the United Nations Security Council (UNSC), the European Union, the United States of America, the United Kingdom in relation with its activities. In very exceptional cases and upon approval of the relevant units, our Corporation may also recognize the Sanctions announced by other countries and international organizations in addition to those listed above. The lists to be used by the Corporation in this context are determined by the relevant units.
- Our Corporation establishes and implements a Sanctions Compliance Program to identify and manage the Sanction risks. The Corporation does not knowingly become party to any transaction aimed at circumventing the Sanctions, and takes into account the risks of Sanctions in accepting new customers, updating customer information and performing customer transactions.

- During the establishment of a Continuous Business Relationship, the customers, the shareholders, and those acting for or on account of the customer, and real beneficiaries are scanned through the risk database containing the relevant lists. Existing customers are scanned on the risk database at regular intervals to see if they are included in the sanction lists. No customer is accepted and no transaction is carried out before completion of assessments on the scanning results. Our Corporation does not establish business relationship with persons and corporations included in the sanctions lists, and terminates the business relationship with its customers who are subsequently included in such list, without prejudice to legal regulations. Where the sanctions programs allow to continue with a business relationship or perform a transaction, the ultimate decision on the matter shall be given by Senior Management. In this context, with a risk-based approach, relationships with some customers may be terminated individually or categorically, and the scope of the service to be provided to some customers may be narrowed.

8. MONITORING AND CONTROL

8.1. Objective

- The goal of the monitoring and control policy is to protect our Corporation from risks and to constantly monitor and control whether our activities are conducted in accordance with the laws, and regulations and communiqués issued under the law, and the Corporation's Policies and Procedures.
- Monitoring and controls are established and implemented with a risk-based approach. In this framework, monitoring and control methods appropriate to the nature and level of risks associated with the Corporation's customers, transactions and services are developed and implemented effectively.

8.2. Monitoring and Control Activities

- Monitoring and control activities are designed and conducted with a risk-based approach under the coordination of relevant units, within the framework of relevant Legislation and Policy provisions. In this context, in addition to the standard controls to be applied to all activities of the Corporation, appropriate and effective control processes, systems and methods are determined and implemented for the closer follow-up of customers, transactions and activities which are seen as high risk and requiring special attention.
- Monitoring and control activities primarily cover the following issues: Monitoring and control of customers and transactions in high-risk group, Monitoring and control of transactions with risky countries, Control of transactions in excess of the specified amounts consistent with the customer profile, Continuous monitoring of consistency with the information regarding the customer’s business, risk profile and sources of funds, throughout the business relationship, identifying, through the Surveillance System, transactions that are suspected to be for artificial price and artificial market formation, taking the necessary customer-specific actions if such transactions become continuous, obtaining necessary information and documents within the scope of know-your-customer rule, checking through sampling method the customer instructions and recorded telephone calls, checking the compliance, adequacy and currency of existing information and documents of the customers and completing the deficiencies, checking by sampling method the documents that should be kept electronically or in writing about the customers and completing the deficiencies, checking whether the Corporation's activities are conducted in accordance with the law and the regulations and communiqués issued under the law, and the Corporation's Policies and Procedures, checking the transactions performed through remote communication systems, Risk-based checking of services that may be exposed to risk and abuse in terms of Financial Crimes and Sanctions in connection with new products and technological developments, and performing other monitoring and controls that may be included in this context.
- On-site inspection and control of the effectiveness of the implementation of Compliance

Program at the Head Office Units and Branches within the framework of the applicable Legislation, the Policies and processes, and of compliance of the transactions are conducted within the scope of internal audit activities. The data and information reported as a result of internal audit activities are subject to follow-up and evaluation as a whole by the Board of Supervisors.

9. TRAINING POLICY

9.1. Objective

- The goal of the training policy, which covers all relevant employees of our Corporation, is to develop the corporate culture and awareness about the risks related to Financial Crimes and Sanctions, and the legal obligations, policy, procedures and practices of our Corporation in this context, and to equip the employees with up-to-date information.

9.2. Training Activities

- Training activities are designed and conducted under the supervision of the Compliance Officer and under the coordination of the Human Resources Department, within the framework of the provisions of the relevant Legislation the Policy, and covers all relevant employees. The training program is prepared annually by the Compliance Officer, with the participation of relevant Head Office Units of the Corporation, and approved by the Board of Directors.
- Newly recruited personnel who may directly or indirectly encounter the risk of Prevention of Laundering Criminal Revenues and Terror Finance must participate in the training activities. The personnel who have received training before and are successful in the exam do not take the training again, and are obliged to learn and apply the changes and updates in our legal and Corporate practices notified to them. It is the responsibility of the managers and the Human Resources Department to ensure that the e-trainings assigned to the employees within the scope of the policy are completed on time by the relevant personnel. Within the framework of changes in the relevant Legislation and other developments, the content and timing of the trainings are updated. The relevance and adequacy of the trainings are closely monitored and evaluated.

- To what extent training courses are fit for needs and are adequate is closely monitored and assessed. Training activities are reviewed with participation from the relevant departments and are based on measurement and assessment results. They are regularly repeated depending on needs.
- Necessary information and statistics regarding the training activities conducted within the framework of the Legislation are kept regularly and reported to MASAK by the Compliance Officer within the period and principles determined in the Legislation.

9.3. Training Subjects

- The trainings cover, at minimum; “the concepts of Laundering Criminal Revenues and Terror Finance, the stages and methods of Laundering of Criminal Revenues and case studies on this subject, the Legislation on prevention of Laundering of Criminal Revenues and Terror Finance, Risk Areas, Measures to be Implemented, Corporate Policies and Procedures, and the principles regarding identification of the customer, principles regarding Suspicious Transaction reporting, the obligation to preserve and present, the obligation to provide information and documents within the framework of the Law and relevant Legislation, and the Sanctions to be applied in case of non-compliance with the obligations and international regulations on combating money laundering and the Terror Finance”, and the principles regarding the implementation of MASAK resolutions on freezing of assets.

10. INTERNAL AUDIT

10.1. Objective

- The goal of internal audit is to provide assurance to the Board of Directors regarding the

effectiveness and adequacy of this Policy and the Compliance Program as a whole.

- Within the scope of internal audit; Establishment and execution of the business processes of the Corporation in line with the Policy, The efficiency and effectiveness of the policies and processes, risk management, monitoring and control and training activities, and compliance of the Corporation's activities with the current Legislation, Policies and procedures are reviewed and audited annually within the framework of the legislation, with a risk-based approach, and the deficiencies, errors and abuses detected, as well as opinions and suggestions to prevent their reoccurrence, are reported to the Board of Directors.

10.2. Internal Audit Activities

- The principles and methods of implementation and reporting regarding internal audit activities are regulated and implemented by the Board of Supervisors within the framework of the Policy.
- In determining the scope of internal audit, the deficiencies identified in the monitoring and control studies and the risky customers, services and transactions are included in the scope of the audit.
- In determining the unit/branch and transactions to be audited, the organizational structure, and business and transaction volume of the Corporation are taken into consideration. In this context, it is ensured to audit sufficient number and quality of units/branches and transactions that represents all the transactions conducted within the Corporation.
- The necessary information and statistics regarding the internal audit activities conducted within the framework of the Legislation are kept regularly and reported to MASAK by the Compliance Officer within the specified time and according to the specified principles.

11. OBLIGATIONS

11.1. Suspicious Transaction Notifications

- If there is any information or suspicion that a transaction performed or intended to be performed with or through the Corporation is related to or connected with the Laundering of Criminal Revenues and Terror Finance, the transaction deemed suspicious shall be reported to MASAK, after necessary investigations to the extent possible. within the framework of the period and principles set forth in the legislation.
- In the event that there is a document or serious indication supporting the suspicion that the asset involved in an attempted or ongoing transaction is related to Financial Crimes, then a Suspicious Transaction notification is sent to MASAK with justifications, for postponing the transaction, and the transaction is avoided during the period specified in the Legislation.
- Necessary communication and cooperation is ensured within the framework of the Legislation between the parties involved in the process of detecting, examining and evaluating Suspicious Transactions and reporting them to MASAK.
- All relevant parties or individuals who are aware of the issue must pay utmost attention within the framework of the Legislation regarding the confidentiality and security of Suspicious Transaction notifications and the relevant internal reports within the Corporation, and the protection of the parties involved in the notifications.

11.2. Retention and Confidentiality of Information, Documents and Records - Sharing with the Financial Group Information

- All information, documents and records required to be obtained and kept regarding customers and transactions in accordance with the legislation must kept within the framework of the period and principles specified in the Legislation and in a way that can be accessed when necessary.
- Necessary measures are taken and implemented within the framework of the relevant Legislation regarding the confidentiality of information, documents and records related to customers and transactions. Reporting activities within the scope of continuous information disclosure and requests from institutions and officials legally authorized to request information and documents are fulfilled with utmost care, within the framework of the Legislation.
- The Corporation may share the information regarding identification of the customer, and

accounts and transactions, with other institutions within the Financial Group, according to the principles set forth in the Financial Group Policy.

11.3. Effectiveness and Review

- The Policy enters into force on the date of approval by the Board of Directors. The Policy is reviewed at least once a year in order to maintain compliance with the Legislation and international standards, and if necessary, updates are made and submitted to the Board of Directors for approval. Modification and updates on the Policy shall also enter into effect upon approval of the Board of Directors.

This Policy has been adopted by the Board of Directors.