İŞ YATIRIM POLICY ON COMBATING FINANCIAL CRIMES AND SANCTIONS

1. OBJECTIVE

The main purpose of this Policy is to ensure performance of our Institution's obligations on combating Financial Crimes, implementation of Compliance Program based on risk-based approach, for the Institution's compliance with obligations enforced under Legislation considering international standards, best practices and recommendations published by FATF, our Institution's compliance with local and international sanctions, and determination of strategies, controls and measures, operational rules and responsibilities for assessment of the Clients, transactions and provided services with a risk-based approach and keeping under control and mitigation of risks including reputation-related risk exposure of our Institution, and strengthening our Institution's employees' Institutional culture on combat against Financial Crimes.

2. SCOPE

This Policy covers our Institution's Board of Directors, Top Management, Headquarters units and all branches with regard to our Institution's duties, authorizations and responsibilities in relation to combat against Financial Crimes.

Financial affiliates included in Türkiye İş Bankası A.Ş. Financial Group are to comply with the Financial Group Policy. Our Institution is directly included in this context, as it is a financial affiliate of Türkiye İş Bankası A.Ş.

Our Institution's Headquarters units, domestic branches and domestic and foreign affiliates are expected to take all measures and due action for compliance with the policy, to the extent of their areas of activity. Policy provisions contain the minimum measures required to be implemented; and if our Institution's foreign financial affiliates are required to apply stricter measures than the policy provisions in accordance with the legislation of the relevant countries, then such stricter measures are to be applied.

This Policy comprises Risk Management, Monitoring and Control, Training, Internal Audit, Obligations and Sanctions Policies in respect to Institution's combat against Financial Crimes.

This Policy is to be reviewed once a year considering the Compliance Program of the Financial Group comprising the measures under the Compliance Program established by the Regulation on the Compliance Program Regarding the Obligations on Suppression of the Laundering of the Proceeds from Crime and Financing of Terrorism and necessary amendments are to be made.

3. LEGAL BASIS

This Policy has been drafted on the basis of the provisions of the "Law on Suppression of Laundering of the Proceeds from Crime" numbered 5549, "Regulation on the Measures for Suppression of the Proceeds from Crime and Financing of Terrorism" published on the Official Gazette dated 09.01.2008 and numbered 26751, Regulation on Compliance Program Regarding the Obligations on Suppression of the Laundering of the Proceeds from Crime and Financing of Terrorism published on the Official Gazette dated 16.09.2008 and numbered 26999, the "Law on Prevention of Financing of Terrorism" numbered 6415, the "Regulation on the Rules and Procedures on Implementation of the Law on Prevention of Financing of Terrorism" published on the Official Gazette dated 31.05.2013 and

numbered 28663, and the "Communiqué Regarding the Financial Crimes Investigation Board" (Serial No:5) published on the Official Gazette dated 09.04.2008 and numbered 26842.

4. DEFINITIONS

Term	Definition and Description
BİAŞ	Borsa İstanbul A.Ş.
Information Abuse	Placing purchase or sales orders or changing or cancelling such orders for capital market instruments based on information directly or indirectly related to capital market instruments or issuers not yet publicly available, that may affect the prices or values of capital market instruments or the decisions of investors, thus deriving benefits
FATF	Financial Action Task Force
Financial Crime	Laundering of the Proceeds from Crime, Financing of Terrorism, Abuse of Information or Marketing Fraud activities
Real Beneficiary	Real persons carrying out transactions with the Institution, real person the transaction is carried out on behalf of or real person or persons who ultimately control or have ultimate influence on a legal entity or unincorporated association
Service Risk	Risks arising from the instruments utilised by Investors
Related Unit(s)	Units that are individually or collectively responsible, with respect to their job descriptions, under the relevant laws, regulations and communiqués regarding Combating Financial Crimes and Suppression of Laundering of the Proceeds from Crime and Financing of Terrorism .
Financial Group	Türkiye İş Bankası A.Ş. Financial Group including our Institution, comprising financial institutions based in Turkey, affiliated with or under control of a parent company based in Turkey or abroad, and branches, agencies, representatives and commercial agents and other affiliated units of such financial institutions
Financial Group Policy	Türkiye İş Bankası A.Ş. Financial Group Policy on Combating Financial Crimes and Sanctions
Countries/Territories subject to Comprehensive Sanction	Countries or territories subject to sanctions implemented country-wide or regionally by the Republic of Turkey, United Nations Security Council, United States of America, European Union and United Kingdom
Institution	İş Yatırım Menkul Değerler A.Ş
MASAK (Presidency)	Chair of the Financial Crimes Investigation Board

Legislation	Applicable laws, regulations and communiqués, and decisions and instructions MASAK in relation to Suppression of the Laundering of Proceeds from Crime and Financing of Terrorism
Client Risk	Risk of abuse of liable persons due to the Client's business activities allowing frequent use of cash, or trade of high-value assets, or facilitation of international fund transfers; or the client or persons acting in the name or on account of the client for the purposes of Laundering of the Proceeds from Crime and Financing of Terrorism
Transactions Requiring Special Attention	Showing due care on complex and extraordinarily large transactions and transactions without an apparent reasonable legal and economic purpose, taking necessary measures to obtain adequate information on the purpose of requested transaction and to retain such information, documents and records for submission to authorities upon request
Marketing Fraud	Effecting sales or purchases, placing order, cancelling order, modifying order or making account movements to create an incorrect or misleading impression on capital market instrument prices, price changes, supply and demand
Policy	Institution Policy on Combating Financial Crimes and Sanctions
Risk	Risk of financial or reputation loss that our Institution or our Institution's employees may be exposed to, due to utilization of services offered by the Institution for the purposes of Laundering of Proceeds from Crime and Financing of Terrorism, or failure to fully comply with the obligations under the Law on Suppression of Laundering the Proceeds from Crime and the regulation and communiqués introduced thereunder
Risk Database	The database checked for whether or not the person, institution or the Real Beneficiaries (controlling shareholders having 25% or more share capital) of such institution with which a Continuous Business Relationship is to be established, thereof are listed on the national and international lists published regarding Suppression of Laundering the Proceeds from Crime and Financing of Terrorism , before opening of an Account
Politically Influenial Person	President of the state or government, senior politicians, government officers, judicial or military personnel, prominent political party representatives and public institution managers having a senior public mission, and family members and relatives of such persons
Laundering of Proceeds from Crime (Laundering)	Transactions aiming at presenting illegally earned income as though earned through legal means, by injecting such revenues to the financial

	system to render them legitimate, converting into non-cash, and changing its nature by having them pass through a process in the financial system
Continuous Business Relationship	Continuous business relationship between our Institution and the client in connection with opening an account and the services received
Suspicious Transaction	Presence of any information, doubt or any doubtful matter that the asset in a transaction performed or attempted with or through our Institution has been earned through illegal means or used for illegal purposes, or used for terrorist acts or by, or related to or connected with terrorist organizations, terrorists or financiers of terror
Shell Bank	A bank without a physical service office in any country that does not employ full time personnel, and is not subject to supervision or licence by an official authority as to its banking transactions and records
Financing of Terror	Provision or raising of funds to or for terrorists or terrorist organizations, with the intent of or knowingly and intentionally for such funds to be fully or partially used in acts constituting crime under law unconditional of associating with a particular act
Compliance Officer	Our Institution's personnel authorized by the Board of Directors, who can make independent decisions, and request all information and documents from all units in their areas of duty and have timely access to such information and documents, to ensure compliance with the obligations under the Law on Suppression of Laundering of the Proceeds from Crime and the Legislation introduced thereunder
Assistant Compliance Officer	Institution employee reporting to the Compliance Officer and meeting the conditions and qualifications required of a Compliance Officer, assigned to fulfil the duties stated in the Legislation to carry out the Compliance Program
Compliance Program	Entirety of measures taken by the Institution within the scope of relevant Legislation and the Institution Policy on combating Financial Crimes
Compliance Risk	Risks regarding the Institution's exposure to sanctions, financial losses and/or reputation loss arising from noncompliance and nonconformity of the Institution's activities or the behaviours and attitudes of the Institution's employees with the Legislation, regulations and standards
Country Risk	Exposure to risk due to business relationships, and the transaction under such business relationships, to be entered into with citizens, companies or financial institutions of countries which do not have adequate regulations on Suppression of Laundering of the Proceeds from Crime and Financing of Terror, or do not adequately cooperate in combating such crimes, or which are considered risky by authorized

	international institutions, or which are announced by the Ministry of Treasury and Finance
Top Management	General Manager and Associate General Managers
Sanctions	Regulations to restrict or prevent economic activities individually or comprehensively, targeting countries, persons and institutions, in order to achieve economic and political goals

5. RESPONSIBILITIES

- Board of Directors have the ultimate responsibility for adequate and effective enforcement of the Policy and the Compliance Program as a whole.

- Top Management shall be responsible towards the Board of Directors, for establishing Business processes and task guidelines in compliance with the Policy within the framework of corporate governance principles, and performance of Transactions by all employees effectively and according to the intended purposes, taking measures timely to ensure that our Institution is not exposed to risks related to Financial Crimes and Sanctions.

- Compliance Officer and Assistant Compliance Officer, who report to the Board of Directors, shall fulfil their authorizations and responsibilities with the contribution of relevant units as described in our Institution's internal regulations.

- All employees of our Institution at all levels are obliged to accurately and carefully fulfil all their duties and responsibilities on ensuring that Institution is not exposed to risks related to Financial Crimes and Sanctions, by effectively implementing the policy, the relevant processes and the Compliance Program at our Institution's Headquarters and branches according to the intended purposes. Disciplinary penalties may be imposed upon failure to comply with the Policy or violation of the policy in any manner.

- Practical effectiveness and adequacy of the Policy and the Compliance Program shall be regularly audited and assessed within the scope of internal audit. Findings mentioned in the reports shall be primarily remedied by the responsible departments considering the Compliance Risk. Audit findings on Compliance Risk shall be submitted by the Compliance Officer and/or Assistant Compliance Officer to the Chairperson of the Supervisory Board, and by the Chairperson of the Supervisory Board to the Board of Directors through the Audit Committee.

6.RISK MANAGEMENT AND KNOW-YOUR-CLIENT

6.1. Risk Management

6.1.1. Objective

- Risk management policy aims at ensuring that the risks that our Institution may be exposed to are defined, rated, monitored, assessed and mitigated.

6.1.2. Know-Your-Client Principle and Client On-Boarding Principles

- Our Institution's client on-boarding process regarding combating Financial Crimes is based on "Know-Your-Client" principle. Our Institution emphasizes "Know-Your-Client" principle in order to protect against persons and acts associated with Financial Crimes; and conducts its

activities in compliance with international standards, recommendations and applicable Legislation.

- Within the scope of the "Know-Your-Client" principle; identification, identifying Real Beneficiary, obtaining adequate information on the purpose and nature of requested transaction, performing risk assessment of client during Client on-boarding process and dynamically updating the risk assessments during the business relationship, assessing the Client and its transactions according to the principles under the "Sanctions" title, monitoring the Client's status and its transactions during the business relationship, and taking necessary measures on Transactions Requiring Special Attention are conducted under the top Management's responsibility by taking necessary measures by responsible units according to the Legislation and the Policy.

- Institutions in the Financial Group are to take necessary measures to prevent entering into a business relationship with persons, entities or organizations listed in the United Nations Security Council's resolutions in connection with the Law on Prevention of Financing of Terrorism and the Law on Preventing the Proliferation of Financing Weapons of Mass Destruction. All accounts, claims and receivables of persons, entities or organizations that are not included in such lists during the stage of establishing Continuous Business Relationship but are included afterwards, shall be suspended, and reported to MASAK within the time period stipulated in the law.

- Monitoring and control activities are to be performed regarding Politically Influential Persons according to the Legislation of the country.

- In digital account openings, risk scores of clients are to be determined based on a system during the client on-boarding process according to the risk parameters set by our Institution, and client on-boarding processes are implemented accordingly. In addition, all clients are dynamically subjected to risk scoring during the Continuous Business Relationship.

- In cases where the client cannot be identified or adequate information cannot be obtained on the business relationship in accordance with the Legislation, no business relationship shall be established and the transactions requested by such persons shall not be performed unless and until such doubts and deficiencies are remedied.

- No Continuous Business Relationship shall be established with unnamed or imaginary names, gambling/illegal betting organizers, unlicensed banks and real and legal persons under restriction under the "Sanctions" topic.

- Accounts are to be closed and business relationships shall be terminated with clients who are found to be engaged in fraud or gambling/illegal betting, clients whose information and documents regarding themselves and their transactions are not provided, and clients who are subject of decisions regarding termination of business relationships in relation to the monitoring and control and risk management activities, and clients who are in the scope of Sanctions after their registry.

- As an exception to this article, accounts of persons, entities organizations who have become subject of resolutions of the United Nations Security Council, within the scope of the Law on Prevention of Terrorism of Finance and the Law on Preventing the Proliferation of Financing Weapons of Mass Destruction, after client registry, shall not be closed, but all accounts, claims and receivables shall be suspended and reported to MASAK within the period of time specified under law.

- Within the scope of know-your-client principles under the Regulation, matters related to identification of clients who open accounts and have Continuous Business Relationship with our Institution, and documents to be taken for identification, and identification in subsequent transactions, and identification of persons acting on behalf of others, and identification of Real Beneficiary, and showing due care on legal entities, and checking the authenticity of confirmation documents, and refusal of transaction and termination of the business relationship are set forth in the "Application Principles of Investor Account Transactions"; and practices in relation to the principle of trust in a third party, and applicability of simplified measures are set forth in the "Application Principles of Suppression of the Laundering of Proceeds from Crime and Financing of Terror".

- Information on client identification, accounts and transactions may be shared with other institutions included in the Financial Group of our Institution, according to the principles set forth in the Financial Group Policy. Such processes are regulated under the "Application Principles of Suppression of the Laundering of Proceeds from Crime and Financing of Terror" in our internal legislation.

6.2. Purpose and Scope of Risk Management

- Primary goal of Risk Management is to define, rate, assess and mitigate our Institution's exposure to risks related to Financial Crimes.

- For this purpose, our Institution considers Client, Service and Country Risks, and establishes and manages processes to define, rate and assess these risks, starting from the client on-boarding process.

- Details of risks that our Institution may be exposed to, within the scope of Client Risk, Service Risk and Country Risk; transactions requiring Special Attention, monitoring of client status and transactions, measures taken against technological risks, and relationships with risky countries, and definitions and applications regarding electronic transfers are set forth in the "Application Principles of Suppression of the Laundering of Proceeds from Crime and Financing of Terror".

- Definitions and examples of potential risks in relation to financial risks (credit risk, market risk, structural interest rate risk, liquidity risk) and non-financial risks (operational risk, legal and ethical risk, technology, information systems and operational disruption risk, human resources risk, model risk, reputation and perception risk, strategy and perceiving risk) that our Institution may be exposed to are given in İş Yatırım Menkul Değerler A.Ş. Risk Catalogue. Risk Catalogue is being updated by Risk Management Department.

- Rules to be observed in cash and asset transfers from Client account are described in our Institution's "Cash and Asset Transfers Application Principles".

6.3. Risk Management Activities

- Risk management activities are designed by the Compliance Officer and Assistant Compliance Officer within the framework of relevant Legislation and the Policy provisions, and conducted within Risk Management Department.

- Risk management activities covers development of risk definition, rating, classification and assessment methods based on Client Risk, Service Risk and Country Risk, considering the issues specified within the scope of the National risk assessment, risk-based rating of Services, transactions and clients, taking necessary risk-mitigation measures, monitoring and checking Risky clients, transactions or services, and reporting to inform the relevant units; development

of appropriate operational and controlling rules for performing transactions with the approval of immediate higher management and supervision of such transaction when necessary, inquiring retrospectively the consistency and effectiveness of Risk definition, assessment, rating and classification methods based on sample cases or actual realized transactions, and re-assessing and updating them based on conclusions reached and the emerging conditions, monitoring the principles, standards and guidelines introduced by national Legislation and international institutions on the Risk matters, and making necessary development studies.

- Risk monitoring and assessment results are to be reported by the Compliance Officer and/or Assistant Compliance Officer to the Board of Directors.

- The criteria used in assessment of Client Risk in relation with the Suppression of Laundering of Proceeds from Crime and Financing of Terror during the business relationship are described in the "Application Principles of Suppression of the Laundering of Proceeds from Crime and Financing of Terror".

- Countries, client groups, products and services in high risk category are specified by relevant departments with a risk-based approach based on the relevant Legislation and the Policy, and are subjected to effective monitoring and controls according to their nature. Relevant processes are described in the "Application Principles of Suppression of the Laundering of Proceeds from Crime and Financing of Terror".

- Clients are allocated to appropriate risk categories by our Institution, based on the primary criteria above in relation to the nature and scope of their activities and relationships and transactions with our Institution, and other idiosyncratic information and criteria, during the Continuous Business Relationship.

- Information obtained in the Investor Information Form from clients which are found to be in "high" Risk level must be updated quarterly. Relevant units shall be responsible for obtaining current information from the client in quarterly periods and disclosing notable changes to the Compliance Officer and Assistant Compliance Officer.

- Minimum measures to be taken to reduce the risks to be assumed in relation with groups found to have a high risk rating are described in the "Application Principles of Suppression of the Laundering of Proceeds from Crime and Financing of Terror".

- Risk categories of clients are determined according to the applicable Legislation and international norms, in light of identity information, areas of activity and other client information available.

- Accordingly; persons or institutions that require Special Attention according to FATF recommendations, which are required to be closely monitored due to being based in or associated with Risky countries or regions, engaged in activities which are considered high-risk pursuant to Laundering of Proceeds from Crime and Financing of Terror according to International norms, or considered risky and undesirable by competent legal authorities due to relation with Laundering of proceeds from crime, financing of terror and other financial crimes and required to be closely monitored with Special Attention, and heavily use products and services in high-risk category, and other clients which are considered risky and require Special Attention due to their nature, areas of activity or nature of transactions, within the scope of risk management, monitoring and control activities under the Compliance Program to be conducted according to international norms, applicable Legislation and the Policy provisions are also tracked in high risk category.

- Within the scope of Service Risk; risk classification is made according to the type of product served to the Client.

- Within the scope of Country Risk, controls are performed via the Risk Database.

6.4. Identification

- As our Institution opens account for clients only within Continuous Business Relationship, clients are identified before performing transactions under the relevant Legislation, by obtaining ID information and confirming the accuracy of such information.

- Identification is done under the relevant Legislation, by obtaining ID information of the clients and persons acting in the name of or on account of the clients, and confirming the accuracy of such information, without regard to amount during establishment of Continuous Business Relationship, and without regard to amount in case of doubt as to adequacy and accuracy of client ID information obtained previously, and without regard to amount in cases requiring reporting of Suspected Transaction, and when the Transaction amount or total amount of several interrelated transaction exceeds the amount stated in the Legislation.

- Our Institution may establish business relationship or perform transaction, in reliance of measures taken by a third party financial institution in relation with the client, on obtaining information regarding the identity of the client, the person acting in the name of the client, and the Real Beneficiary and the purpose of business relationship or transaction.

- Reliance on a third party is possible, provided that it is made sure that the Third party has taken other measures to fulfil the requirements of the identification, record retention and know-your-client rule, and if it is foreign-based, that it is subject to regulations and supervision according to international standards in combating against Laundering and Financing of Terror, and that the certified copies of ID documents are to be promptly provided by the third party upon request.

- In such case, ultimate responsibility rests with our Institution. In case of establishing business relationship based on reliance to a Third party, client's ID details are to be obtained promptly from the third party. The principle of reliance in a third party is not applicable in cases where the third party is based in risky countries.

- In international money transfers, we do not have any correspondence relationship as our accounts with T. İş Bankası A.Ş. are used.

7. SANCTIONS

- Our Institution considers full compliance with national Legislation, as well as Sanctions related to its activities, imposed by the United Nations Security Council (UNSC), European Union, United States of America, United Kingdom, at the least. Our Institution may adopt Sanctions imposed by other countries and international institutions in addition to those listed above, in extremely exceptional cases, upon approval of relevant units. The lists to be used by our Institution in this context are specified by the relevant units.

- Our Institution establishes and maintains a Sanctions Compliance Program to identify and manage the Sanction risks. Our Institution does not intentionally become a party to any transaction aiming at overriding the Sanctions, and considers Sanctions risks in new client on-boarding, updating client information, and performing client transactions.

- In establishment of Continuous Business Relationship, clients, shareholders, persons acting in the name or on account of the client, and ultimate beneficiaries are scanned on the lists. Sanctions lists in regular intervals for whether existing clients are listed under. No client on-

boarding shall take place, no transaction shall be performed without completing assessments on the scanning results, and our Institution does not establish any business relationship with persons or entities which appear on sanctions lists, and the business relationship with clients that subsequently enter such lists shall be terminated, without prejudice to legal requirements. In cases where the Sanction programs allow the continuity of business relationship or performing the transaction, ultimate decision on the matter shall be given by Top Management. In this context, relationships with some clients may be terminated either individually or based on categories, or the scope of service to be provided to the clients may be restricted, with a risk-based approach.

8. MONITORING AND CONTROL

8.1. Purpose

- The purpose of monitoring and control policy is to protect our Institution against risks, and continuously monitor and check the compliance of activities with the law and regulations and communiqués introduced thereunder, and our Institution's Policies and Procedures.

- Monitoring and controls are established and performed with a risk-based approach. Within this framework, monitoring and control methods are developed and effectively implemented according to the nature and levels of risks associated with our Institution's clients, transactions and services.

8.2. Monitoring and Control Activities

- Monitoring and control activities are designed and conducted with a risk-based approach, in coordination with relevant units, under the relevant Legislation and the Policy provisions. Within this framework, in addition to standard controls applicable to all activities of our Institution, appropriate and effective control processes, systems and methods are to be specified and implemented for closer monitoring of clients, transactions and activities considered high-risk and requiring Special Attention.

- Monitoring and control activities basically cover the following: monitoring and control of clients and transactions in high-risk group, monitoring and control of transactions with Risky countries, control of the consistency of transactions above specified amounts with the client profile, continuous monitoring of consistency of the Client transactions with the information on client's business, risk profile and funding sources during the business relationship, and identifying client transactions suspected to aim at creating artificial price and artificial market through Oversight System, and monitoring such transactions and taking necessary client-based action if they become continuous, checking during audits and reviews the information and documents required under know-your-client rule as well as client instructions and recorded phone conversations selected with sampling method, checking the compliance, adequacy and recency of present Client information and documents and having incomplete ones completed, checking the Client documents through sampling method kept in electronic means or in print , and having incomplete ones completed, checking whether our Institution's activities are conducted in compliance with the law and the regulations and communiqués introduced thereunder and the Institution's Policies and Procedures, checking transactions through systems allowing non-face-to-face transactions, risk-driven audit of services which may become vulnerable to Financial Crimes and Sanctions risk and abuse due to new products and technological advancements, and other monitoring and controls in this context.

- On-site audit and control of effectiveness of implementations and suitability of transactions in relation to the enforcement of the Compliance Program by the Headquarters Units and Branches in connection with applicable Legislation and the Policies and processes shall be conducted

within internal audit activities. Data and information reported as a result of internal audit activities are tracked and assessed as a whole by the Supervisory Board.

9. TRAINING POLICY

9.1. Purpose

- The training policy, that covers all relevant employees of our Institution, aims at developing corporate culture and consciousness on the risks associated with Financial Crimes and Sanctions and our Institution's legal obligations, policies, procedures and practices in this context, and providing up-to-date information to our employees.

9.2. Training Activities

- Training activities are designed and conducted, under supervision of the Compliance Officer and/or Assistant Compliance Officer and in coordination with Human Resource Department, in accordance with the relevant Legislation and the Policy provisions, covering all relevant employees. Training program is prepared annually by the Compliance Officer and/or Assistant Compliance Officer with participation of relevant Headquarters Units of the Institution, and approved by the Board of Directors.

- Our Institution's personnel who may directly and indirectly face risks associated with Suppression of the Laundering of Proceeds from Crime and Financing of Terror shall attend the training activities. In this context, employees must attend e-training assigned to them, at least once a year. Under the Policy, relevant managers and Human Resources Department are responsible for ensuring that employees complete the assigned e-training on time. Content and timing of training shall be updated according to amendments in the Legislation and other relevant developments. Training shall be closely tracked and assessed in relation to adequacy and fitness for the intended purpose.

- Necessary information and statistics regarding the training activities, as required under the Legislation, are retained on a regular basis, and reported by the Compliance Officer and/or Assistant Compliance Officer to MASAK at specified times and according to the principles set by the Legislation.

9.3. Training Subjects

- Training shall at the least cover the following subjects; "the concepts of Suppression of the Laundering of Proceeds from Crime and Financing of Terror, stages and methods of the Laundering of Proceeds from Crime and case studies, Legislation on the prevention of the Suppression of the Laundering of Proceeds from Crime and Financing of Terror, Risk areas, and Know-Your-Client principles, suspected transaction reporting principles, retention and submission obligation, obligation to provide information and document, under Institution's Policies and Procedures, the Law and relevant Legislation, and sanctions applicable upon non-compliance with the Obligations, and international regulations on combat against Laundering and Financing of Terror".

10. INTERNAL AUDIT

10.1. Purpose

- The purpose of internal audit is to provide the Board of Directors with assurance regarding theeffectiveness and adequacy of this Policy and Compliance Program as a whole.

- Within the scope of the internal audit; establishment and effecting of Institution's business processes according to the Policy, efficiency and effectiveness of the Policy and processes and risk management, monitoring and control and training activities and compliance of Institution's activities with the applicable Legislation and Policy and procedures are reviewed and audited annually with a risk-based approach according to the Legislation, and any deficiency, error and abuse noted, and views and recommendations for prevention of their reoccurrence are reported to the Board of Directors.

10.2. Internal Audit Activities

- Application and reporting principles and methods related to internal audit activities are regulated and executed by the Chair of the Supervisory Board, under the relevant Policy.

- In determining the scope of internal audit, the setbacks found during the monitoring and control works, and risky clients, services and transactions are included in the scope of audit.

- In determining the units/branches and transactions to be audited, Institution's organization structure, business and transaction volume are taken into consideration. In this context, it is ensured that units/branches and transaction in quantity and quality to represent the entire transactions performed by the Institution are audited.

- Regarding the internal audit activities, information and statistics required under the Legislation are retained on a regular basis and reported by the Compliance Officer and/or Assistant Compliance Officer to MASAK in specified times and according to the principles.

11. OBLIGATIONS

11.1. Suspected Transaction Reporting

- If there is an information or suspicion that a transaction performed or intended to be performed with or through our Institution is associated or connected with Laundering of Proceeds from Crime and Financing of Terror, investigation must be performed to the extent possible, and the transaction found to be suspected must be reported to MASAK within the time period and according to the principles set by the Legislation.

- If there is a document or material indication supporting the suspicion that the assets in an attempted or continuing transaction is associated with Financial Crimes, Suspicious Transaction notification must be sent to MASAK together with justifications, along with request to defer the transaction, and such transaction must be avoided during the period of time specified under the Legislation.

- Necessary communications and collaboration under the Legislation must be ensured among the parties to the process of identifying, reviewing and assessment of Suspicious Transactions and reporting to MASAK.

- All related persons who are party to or have a grasp of the matter must show utmost care, according to the Legislation, regarding the confidentiality and security of Suspicious Transaction notifications and the internal notifications within the Institution, and on protection of persons who are party to the notifications.

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

- All information, document and records in relation with clients and transactions, required to be obtained and kept under the Legislation, must be retained during the specific time period and according to the principles set by the Legislation, and must be available whenever necessary.

- Necessary measures must be taken and implemented, regarding confidentiality of information, document and records related to clients and transactions, according to the relevant Legislation. Reporting activities regarding procurement of continuous information, and fulfilment of requests from authorities and officials legally authorized to request information and document, must be fulfilled with utmost care, according to the Legislation.

- Institution may share information on client identification, and account and transactions, with other institutions in its Financial Group, according to the principles set forth in the Financial Group Policy.

11.3. Effectiveness and Review

- This Policy enters into force on the date of approval by the Board of Directors. The Policy shall be reviewed at least once a year, to ensure compliance with the Legislation and international standards, and updated where necessary, and submitted to approval of the Board of Directors. Any subsequent amendment or update on the Policy shall also enter into force upon approval of the Board of Directors.

This Policy has been adopted by the Board of Directors.