TURKIYE IS BANKASI A.S.

POLICY FOR THE PREVENTION OF LAUNDERING OF CRIMINAL PROCEEDS AND TERRORISM FINANCING

CHAPTER ONE

GENERAL PRINCIPLES AND TERMS

1- FUNDAMENTAL BASIS OF THE POLICY

Due to the ever-increasing sensitivity shown by the international public in order to prevent laundering of criminal proceeds and terrorism financing, international attempts and regulations to pursue the fight against laundering of criminal proceeds and terrorism financing on a global basis have recently accelerated. Like many countries that feel the same urgency, our country introduces various legal regulations in this respect and places much importance on strengthening the applicable practices.

Maintaining a reputable and reliable position in the international arena due to its operations and performance since its foundation, Turkiye Is Bankası A.S. (the "**Bank**") adopts and places importance on the prevention of laundering of criminal proceeds and financing of terrorism as a social responsibility beyond a mere compliance with the laws and regulations. The Bank also considers the said prevention as an important factor in compliance and integration with the international system.

This Policy is built on:

- International initiatives, contracts and regulations to which our country is a party;
- Such international standards and recommendations as well as generally accepted approaches, methods and practices in order to prevent laundering of criminal proceeds and terrorism financing;
- The Code on the Prevention of Laundering of Criminal Proceeds and other applicable legislation based on this Code;
- The Code on the Prevention of the Financing of Terrorism and other applicable legislation based on this Code.

2- DEFINITIONS

Bank: means Turkiye Is Bankası A.S;

Service Risk: means the risk that the Bank may be exposed in relation to new products that may be offered by using ever developing technologies or to certain services such as transactions not carried out on a vis-à-vis basis, private banking or correspondent banking;

FCIB means Turkish Republic Financial Crimes Investigation Board;

Legislation means the applicable Code, Regulations and Communiqués as well as the decisions and orders by the FCIB in order to prevent laundering of criminal proceeds and terrorism financing;

Customer risk means such risk whereby the Bank may be abused on the grounds that the

customer's scope of business requires the use of large amounts of cash; allow the trading of high-value assets or international fund transfers; or the customer or any person who acts on behalf of him acts for the purpose of laundering criminal proceeds or terrorism financing;

Policy means the Bank Policy on the Prevention of Laundering of Criminal Proceeds and Terrorism Financing;

Risk means the financial losses or loss of reputation that the Bank or the Bank employees may suffer due to the fact that the services offered by the Bank are used to launder criminal proceeds or terrorism financing, 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;

Laundering of Criminal Proceeds (Laundering) mean those 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;

Terrorism Financing means 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 in the Code.

Compliance Officer means such Division Manager who shall be authorized and assigned by the Bank to make sure that the Bank shall act in compliance with its obligations arising from the applicable legislation pursuant to the Code on the Prevention of Laundering of Criminal Proceeds as well as the legislation put into force on the basis of that Code;

Compliance Program means the integral package of the measures built in the Bank on the basis of the applicable legislation and the Bank Policy in order to prevent laundering of criminal proceeds or terrorism financing;

Country Risk means such risk that the Bank may be exposed to due to the banking relations, or any transaction on the basis of those relations, that may be engaged with the individuals, corporations or financial institutors of a country, which lacks satisfactory regulations to prevent laundering of criminal proceeds or terrorism-financing, 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.

3- OBJECTIVE OF THE POLICY

The Policy basically intends to make sure that:

- the Bank shall act in compliance with its obligations to prevent laundering of criminal proceeds and terrorism financing, and shall implement the Compliance Program;

- customers, transactions and services offered shall be evaluated on the basis of a risk-based approach and those strategies, controls and measures to mitigate and control those risks that the Bank may be exposed to shall be identified next to the rules of functioning and the responsibilities;

- the Bank employees shall be trained and their awareness shall be raised about the criminal proceeds and terrorism financing and the fight against them.

4- SCOPE OF THE POLICY

Being a complementary piece of the Bank's Compliance and Compliance Risk Management Policy, this Policy covers the Bank's Board of Directors, the Senior Management, the units in the Head office and the domestic branches and all executives and employees, as well as the foreign branches and departments to the extent permitted by the legislation and competent authorities in the jurisdiction where they are located with reference to the tasks, powers and responsibilities to prevent laundering of criminal proceeds and terrorism financing.

The Bank shall further observe that those policies on the prevention of laundering of criminal proceeds and terrorism financing that may be set up and imposed by its affiliates in accordance with the applicable law shall be effectively implemented and adequate.

This Policy shall comprise of the following policies for the prevention on laundering of criminal proceeds and terrorism financing:

- Risk Management;
- Monitoring and Controlling;
- Training and
- Internal Audit.

This Policy also forms the general frame of the Bank's Compliance Program built on a risk-based approach in order to oversee that the Bank shall comply with the obligations imposed by the applicable legislation on the prevention of laundering of criminal proceeds and terrorism financing.

5- DUTIES AND RESPONSIBILITIES

The Bank's Board of Directors shall be ultimately the responsible body to conduct the Compliance Program as a whole in an adequate and effective way subject to this Policy. The Board of Directors shall be authorized and under the Compliance Program responsibility:

- to ensure that the Bank shall act in compliance with the obligations to prevent laundering of criminal proceeds and terrorism financing;
- to approve the policy and annual training courses;
- to appoint a Compliance Officer;
- to approve the Corporate Compliance Division Task Regulation that governs the tasks, powers and responsibilities of the Compliance Officer and the Corporate Compliance Division;
- to evaluate the outcome of the risk management, monitoring and control activities as well as the internal audit activities and to make sure that necessary measures are adopted; and
- to procure that all activities are run in a coordinated and effective manner.

The Board of Directors may delegate all or any of its tasks above under the Compliance Program to one or several members, provided that the ultimate responsibility therefore shall remain with the Board.

The Bank's Senior Management shall be responsible to make sure that this Policy, and the relevant procedures and the Compliance Program shall be effectively implemented by the entire personnel at the Bank's Head Office and its branches in line with the intended purpose; and those measures that would prevent the Bank from being exposed to the risks associated with laundering of criminal proceeds and terrorism financing shall be duly adopted.

The Compliance Officer who shall be accountable for towards the Board of Directors or such member(s) to whom the Board may have delegated all or any of its powers under the Compliance Program shall be responsible:

- to undertake those efforts and pursue the necessary communication and coordination with the FCIB in order to make sure that the Bank shall observe its obligations to prevent laundering of criminal proceeds and terrorism financing, and to apply the Compliance Program;

- to set up a Bank Policy and submit it for the approval of the Board of Directors;

- to set up, update, publish and monitor the Bank procedures in relation to the implementation of the Compliance Program within the Bank and subject to the Bank Policy, and to monitor and coordinate how those procedures are implemented in practice;

- to undertake the monitoring and control activities for the purposes of risk management under the Compliance Program;

- to submit his studies related to the training program in order to prevent laundering of criminal proceeds and terrorism financing for the approval of the Board of Directors, and to make sure that an approved training program shall be effectively implemented;

- to consider and interpret such data and findings he may come across through his investigations about the suspicious transactions to the extent his powers and means permit him, and to notify to the FCIB those transactions which he duly decides are suspicious ones;

- to take necessary measures to maintain the confidentiality of the notices and other related matters;

- to regularly keep the information and statistical data in relation to internal audit and training activities, and to report them to the FCIB on a timely basis.

The Corporate Compliance Division shall be accountable for towards the Compliance Officer in relation to the performance of their tasks and responsibilities under the Compliance Program.

Each staff member of the Bank at every level shall diligently undertake and carry out all his respective tasks and responsibilities to make sure that the present Policy, and the relevant procedures and the Compliance Program shall be effectively implemented at the Bank's head office and the branches in accordance with its intended purpose so as to help the Bank avoid

any kind of risks associated with laundering of criminal proceeds and terrorism financing.

The effectiveness and adequacy of this Policy and the Compliance Program in practice shall undergo regular audits and evaluations under the internal audit policies. The policy is reviewed at least once in a year to ensure compliance with the legal legislation in force and international standards.

CHAPTER II
RISK MANAGEMENT

6- OBJECTIVES AND SCOPE OF THE RISK MANAGEMENT

The fundamental objective of the risk management policy is to define, rate, evaluate and mitigate the risks associated with laundering of criminal proceeds and terrorism financing that the Bank may be exposed.

The risk management policy shall cover and extend to those measures and functioning rules to implement the Bank's customer acceptance policy.

Those processes and systems shall be established in order to define, rate, evaluate and mitigate the customer, service and country risks that the Bank may be exposed to, and it shall be ensured that they shall effectively function.

7- RULES GOVERNING THE BANK'S ACCEPTANCE OF CUSTOMERS

The Bank's customer portfolio shall be composed of those customers who shall:

- undertake the Bank-customer relation on the basis of mutual trust and in accordance with the rules of righteousness and honesty;
- comply with the applicable legislation and ethical rules in their relations with the Bank and their activities;
- have no relation to laundering of criminal proceeds or terrorism financing;
- not avoid the duly delivery of such information and documents that may be asked by the Bank subject to the applicable legislation on a timely basis;
- are efficient, high-quality and fit for the Bank's targets and objectives.

In circumstances where identity verification may not be undertaken in accordance with the applicable legislation or the Bank fails to come up with sufficient information about the purpose of the business relation, no business relation shall be established and the transactions asked by the applicants shall not be executed unless doubts and incomplete procedures in this respect are duly addressed. No account shall be opened for anonymous or fictitious names in this respect. A business relation shall be terminated in circumstances where the identity verification as well as confirmation may not be carried out in the event that a suspicion arises in relation to the veracity of the customer's identity details obtained and checked before.

In order not to establish business relationship with individuals and companies included in the lists published by the United Nations Security Council associated with combating finance of terrorism which are binding for our country and the similar other international lists that shall be taken into consideration by the international financial system and also banks of our country, necessary mesaures are taken and applied with reasonable care and diligence.

In case of correspondent banking relations, necessary measures shall be adopted subject to the applicable legislation in order to accurately define and evaluate the contents and levels of the risks that the correspondent financial institutions carry in relation to laundering of criminal proceeds and terrorism financing. In this respect, correspondent bank relations with shell banks are prohibited.

8- "KNOW-YOUR-CUSTOMER" PRINCIPLE

The "Know-Your-Customer" principle shall form the basis of the Bank's customer acceptance policy on the prevention of laundering of criminal proceeds and terrorism financing.

The Bank places much importance on the "Know-Your-Customer" principle in order to protect itself against the persons and acts in association with laundering of criminal proceeds and terrorism financing, and shall accordingly adopt a policy in line with the international standards and the applicable legislation in this respect.

Under the "Know-Your-Customer" principle, necessary measures shall be adopted subject to the applicable legislation, and the Bank Policy and Procedures in order to:

- verify the customer identity;
- confirm the beneficial owner;
- obtain satisfactory information about the purpose and nature of the requested transaction;
- monitor the position and transactions of a customer throughout the relations with him; and
- adopt those measures for those customers, activities and transactions that need special attention.

9- IDENTITY VERIFICATION

The basic preliminary condition for the Bank to establish a continuous business relation with and execute transactions for a customer is to verify the identity of that customer on a timely and accurate basis in accordance with the applicable legislation, and the Bank policy and procedures.

The identity verification shall be carried out by undertaking necessary efforts subject to the applicable legislation and the Bank Policy and procedures to identify, check and confirm the identity details of the customer.

The identity of a customer shall be verified in order to check the identity details of that customer, or of any person acting on behalf of him, and confirm the veracity of such details subject to the applicable legislation:

- irrespective of any amount where a continuous business relation is established;

- irrespective of any amount whenever there is a suspicion as to the veracity of any customer identity verified before;

- irrespective of any amount in circumstances where a suspicious transaction should be reported;

- whenever the transaction amount, or the aggregate amount of more than one transaction linked to each other exceed the threshold defined in the applicable legislation.

10- IDENTIFYING THE BENEFICIAL OWNER

Necessary measures shall be duly adopted and diligently applied subject to the applicable legislation in order to identify and know the beneficial owner for the purpose of establishing a continuous business relation and undertaking the requested transactions.

11- OBTAINING SATISFACTORY INFORMATION ABOUT THE PURPOSE AND NATURE OF THE TRANSACTIONS

A special attention should be given to those transactions which may appear too complex and too large or lack any reasonable legal or economic purpose, and necessary measures shall be adopted to obtain satisfactory information about the purpose and nature of the transaction under watch.

12- ONGOING MONITORING OF CUSTOMERS AND TRANSACTIONS

For the monitoring and control purposes, a risk profile of the customer shall be shaped up with reference to laundering of criminal proceeds and terrorism financing, taking into consideration his job, professional background, business operations, financial position, accounts and transactions, the country where he is domiciled/ is engaged in business and similar relevant current information and indicators. Customers, and business relations and transactions that come up with high risk shall be identified, and they shall be monitored through monitoring and control processes and systems on the basis of the risk management set up in this respect.

13- MEASURES NECESSARY TO ADDRESS CUSTOMERS, ACTIVITIES AND TRANSACTIONS THAT REQUIRE SPECIAL ATTENTION

Necessary measures shall be adopted in respect of the following issues that require special attention subject to the applicable legislation, and the Bank policy and procedures:

- State-of-the-art and developing technologies;
- Systems that may execute transactions without any vis-à-vis relation
- Relations with correspondent banks and risky countries
- Electronic transfers
- Business relations where there is inadequate information about their objectives

- Other customers, businesses and transactions recommended by FATF to apply special attention in terms of money laundering and terrorism financing
- Other customers, businesses and transactions that require special attention

14- RISK MANAGEMENT ACTIVITIES

Risk management activities to implement the Bank's Compliance Program shall be devised up by the Compliance Officer subject to the applicable legislation and the Policy, and shall be conducted by the Corporate Compliance Division.

Activities related to risk management shall cover at least:

- Developing risk defining, rating, classifying and assessing methods based on customer risk, service risk and country risk,
- Rating and classifying services, transactions and customers depending on risks,
- Developing proper operational and control rules for ensuring monitoring and controlling risky customers, transactions or services; reporting in a way that warns related units; carrying out the transactions with the approval of senior management and controlling it 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 works through pursuing recommendations, 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 regularly to the Board of Directors.

Risks associated with laundering of criminal proceeds and terrorism financing that the Bank may be exposed to on the grounds of its customers, and transactions and operations may be categorized into three main groups:

- Customer risk
- Service risk and
- Country risk

For the purposes of evaluating customer, service and country risks in relation to laundering and terrorism financing, the following criteria shall be basically taken into consideration:

- The level and nature of the information on the customer's position in the market and its business operations;
- Value of the assets maintained by the customer with the Bank and/ or the volume of transactions requested by him;
- Purpose and nature of the banking relations between the customer and the Bank;
- The level of adequacy and appropriateness of the regulations and monitoring policies governing the country or region in which the customer is engaged in business operations, and/ or his scope of business as to laundering of criminal proceeds or terrorism financing;
- Duration and course of the existing banking relations between the customer and the Bank;

- Nature and type of the banking products and services used by the customer.

Both at the beginning of the banking relations and throughout the term of those relations, a customer shall be categorized into the appropriate risk group on the basis of the basic criteria above and other customer-specific information and criteria with reference to that customer's scope of business as well as the nature and scope of its relations and transactions with the Bank. In order to identify the risk category of the customer, customer, service and country risks associated with the customer himself, the banking transactions undertaken by him and the banking products and services used by him shall be taken and evaluated as a whole.

Customers included in the medium and low risk categories and their transactions shall be subject to the standard monitoring and controls of the Bank applicable in that regard whereas high-risk clients and their transactions shall be closely monitored on the basis of the monitoring and control methods fit for the purpose. Customers included in the high-risk category in terms of customer, service and country risks shall undergo the enhanced" know-your-customer" principle. In this frame, central monitoring and control activities conducted at the Corporate Compliance Division on the basis of a risk-based approach shall be essentially designed and conducted in such a manner to focus on the high-risk customers and transactions.

Customer groups, and products and services that fall within the high risk category shall undergo effective monitoring and control procedures that suit the nature of those customers, products and services and are defined by the Corporate Compliance Division on the basis of a risk based approach subject to the applicable legislation and the present Policy.

At least the following measures are taken for mitigating the risk to be undertaken related to groups determined as risky as a result of risk rating activities:

- Developing procedures for ongoing monitoring of transactions and customers,
- Requiring approval of one level higher officer for establishing business relationship, sustaining current business relationships or carrying out transactions,
- Gathering as much information as possible on the purpose of the transaction and source of the asset 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.

The risk categories of the customers are determined according to the identification information, business activities 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 through FATF recommendations,
- Required to be monitored closely since they are resident in or associated with risky countries or regions,
- Operating on high risk activities in terms of money laundering and terrorism financing due to the international standards (activities including intensive use or transfer of cash/foreign currency, activities dealing in high-value items etc.),

- 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 money laundering, terrorism financing and other financial crimes,
- Frequently using banking products and services in high risk category

and similar other customers that are required to be monitored closely since their current profiles, activities or banking relationship and transactions are accepted as risky in the concept of the risk management, monitoring and control activities included in the compliance program that is being carried out compliant with the international standards, domestic legislation and this policy.

In terms of service risk;

- Electronical transfers,
- Private banking products and services,
- Systems enabling non-face to face transactions,
- Products and services related to new and developing technologies,
- Business and transactions of which the beneficiary owners can not be determined fully and precisely,
- Similar 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 included in the compliance program that is being carried out compliant with the international standards, domestic legislation and this policy.

are monitored in high risk category.

The following countries and regions and those customers associated with or residing in these countries and regions shall be closely monitored in the high risk category in terms of country risk:

- Those countries included in the "Jurisdictions subject to a FATF call on its members and other jurisdictions to apply counter-measures to protect the international financial system from the on-going and substantial money laundering and terrorist financing (ML/FT) risks emanating from the jurisdictions" as published by FATF
- Those countries named in the "Risky Countries" as published by the applicable Ministry
- Those countries sanctioned internationally due to the United Nations Security Council resolutions because of the policy and procedures associated with money laundering and terrorism financing
- Those countries published by OFAC or European Union and said to have high risks in respect of laundering of criminal proceeds
- Overseas centers, free zones and financial centers
- Tax havens
- Those countries lacking adequate regulations in order to prevent laundering of criminal proceeds and terrorism financing

CHAPTER III

MONITORING AND CONTROL

15- PURPOSE AND SCOPE OF THE MONITORING AND CONTROL ACTIVITIES

The basic purpose of the monitoring and control procedures is to protect the Bank against the risks and to ensure that its operations are constantly monitored and controlled subject to the applicable legislation and the Bank policies and procedures.

Monitoring and control activities shall be 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 Bank customers, transactions and services shall be developed and effectively implemented.

16- MONITORING AND CONTROL ACTIVITIES

Monitoring and control activities shall be designed and conducted on a risk-based approach under the coordination and supervision of the Compliance Officer subject to the applicable legislation and the present Policy. In this respect, in addition to standard controls applicable to all operations of the Banks, certain appropriate and effective control processes, systems and methods shall be 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 control of transactions executed with risky countries
- Monitoring and control of complex and unusual transactions
- Controlling those transactions above a specific amount threshold through sampling in order to check its compliance with the customer profile
- Monitoring and control of transactions that are linked to each other and exceed the amount which requires the identity verification;
- Controlling the veracity, up-to-dateness and adequacy of customer data and documents, and ensuring that missing ones are made up;
- Continuous monitoring of the compliance of a customer transaction with the information compiled about his scope of business, risk profile and fund resources throughout the transaction;
- Controlling the transactions carried out through systems that allow the execution of transactions without a vis-a-vis relation;

- Risk-focused control of those services that may remain exposed to abuse and risks in respect of laundering of criminal proceeds and terrorism financing on the grounds of new products and technological developments and
- Other monitoring and controls that may be necessary in this respect

Central monitoring and control activities shall be carried out by the Corporate Compliance Division. To effectively implement the compliance program in accordance with the applicable legislation and the Bank Policy and procedures at the Bank's Head Office and its branches, and the on-the-spot audit and control of the compliance of the transactions, shall be provided through internal audit and internal controlling 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 shall be monitored and evaluated as a whole at the Corporate Compliance Division under the supervision of the Compliance Officer.

CHAPTER IV
TRAINING

17- PURPOSE AND SCOPE OF THE TRAINING POLICY

The purpose of the training policy of the Bank which extends to the entire personnel is to raise the corporate awareness and culture about the risks associated with laundering and terrorism financing, and about the legal liabilities and policy and procedures and practices of the Bank in this respect, and to equip the personnel with updated data.

18- TRAINING ACTIVITIES

The Bank's training activities oriented at preventing laundering of criminal proceeds and terrorism financing shall be designed and conducted under the supervision and coordination of the Compliance Officer subject to the applicable legislation and the present Policy, and shall extend to the entire personnel related thereto. Training program shall be prepared by the Compliance Officer in participation of the relevant Head Office divisions at the Bank. It is the Compliance Officer who shall supervise the effective implementation of the training program.

The Bank shall effectively and reasonably use the in-class training, e-training and other various training methods as well as visual and audile training materials, and communication channels such as Internet or Intranet so that training activities shall be applied throughout the entire Bank.

Special attention shall be paid to selecting the trainers and to the fact that they should be given appropriate training in this respect.

The contents of the training may be differentiated on the basis of the office term of the addressed staff members in the Bank, their positions and offices and without any deviation from the underlying purpose so that each employee shall regularly receive the trainings fit for him. Such content may be updated from time to time subject to the changes to the applicable legislation and other developments. It is essential that the training to be provided to the personnel shall address those matters defined in the applicable legislation as a minimum.

Whether or not the training courses offered to the personnel are fit for the needs and

satisfactory shall be closely monitored and evaluated.

Necessary information and statistical data in relation to the training courses in progress shall be regularly kept subject to the applicable legislation, and shall be reported by the Compliance Officer to FCIB at such times and in such manner to be defined.

CHAPTER V

INTERNAL AUDIT

19- PURPOSE AND SCOPE OF THE INTERNAL AUDIT

The purpose of the internal audit is to give assurance to the Board of Directors as to the effectiveness and adequacy of the entire Compliance Program of the Bank.

Through the internal audit, whether or not the Bank's policy and procedures as well as the risk management, monitoring and control and training activities, and whether the Bank's operations are in compliance with the applicable legislation and the Policy and procedures shall be reviewed and audited annually and on the basis of a risk-based approach and the deficiencies, mistakes and abuses determined as the result of internal audit and the opinions and proposals for prevention of reappearance of them shall be reported to the Board of Directors.

20- INTERNAL AUDIT ACTIVITIES

The implementation and reporting rules and methods in relation to the internal audit activities under the Compliance Program shall be designed and implemented by the Board of Inspectors subject to this Policy.

While determining the scope of internal audit, the faults detected during the monitoring and controlling workings and the customers, services and transactions containing risk shall be included within the scope of audit.

While determining the units and transactions to be audited, the business size and business volumes of the Bank shall be taken into consideration. In this scope, unit and transaction in the quantity and characteristics of which can represent the whole transactions carried out by the Bank shall be ensured to be audited.

Such information and statistical data required under the applicable legislation in relation to the internal audit activities in progress shall be regularly kept and reported by the Compliance Officer to FCIB at such time and in such manner to be defined.

CHAPTER VI

MISCELLANEOUS

21- REPORTING SUSPICIOUS TRANSACTIONS

Any suspicious transactions that may be associated with laundering of criminal proceeds and terrorism financing shall be reported to the FCIB.

Where there is information or matters that would arise suspicions, indicating that a transaction which was or is to be executed by or through the Bank upon an application is associated or related with laundering of criminal proceeds or terrorism financing, necessary investigation to the extent permitted by the applicable means shall be carried out and any transaction concluded to be suspicious shall be reported to the FCIB within such term and subject to such conditions defined in the applicable legislation.

Necessary communication and cooperation required under the applicable legislation shall be established between those parties involved in the process of the identification, examination and consideration and reporting of the suspicious transaction to the FCIB.

Maximum care and diligence shall be paid by all concerned parties that are either involved in or aware of the process subject to the applicable law that suspicious transaction reporting as well as the internal reporting within the Bank shall be kept confidential and safe, and the parties involved in the process shall be duly protected.

22- RETAINING AND CONFIDENTIALITY OF INFORMATION, DOCUMENTS AND RECORDS

Pursuant to the Code on the Prevention of Laundering of Criminal Proceeds and the related applicable legislation, all documents, data and records that should be received and retained in relation to the customers and transactions shall be diligently retained and kept for such term and subject to such conditions defined in the applicable legislation with easy access when and if required.

Necessary measures shall be adopted and diligently applied in line with the applicable legislation in order to maintain the confidentiality of the relevant data, documents and records. 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 shall be considered and fulfilled with utmost diligence and care subject to the applicable legislation.

23- EFFECTIVENESS

This Policy shall be effective upon its approval by the Board of Directors. On the date when this Policy comes into effect, the “Our Bank’s Policy on Prevention of Laundering of Criminal Proceeds and Terrorism Financing” currently in force on the basis of the resolution adopted by the Board of Directors on 29.11.2005 under no 31929 shall be abolished. Any subsequent amendments and updates to this policy shall be effective after their approval by the Board of Directors.