POLICY OF ANTI-MONEY LAUNDRING& KNOW YOUR CUSTOMER

INTERNAL CONTROL DEPARTMENT
(November/2019)

CONTENTS

1. INTRODUCTION

This document defines the domestic policies and rules of the Bankwhich are established within the scope of the measures included in the adjustment program to be established with a risk-based approach in order to ensure compliance with the regulations and communiqués issued for the implementation of the Law No. 5549 on Prevention of Laundering Proceeds of Crime.

1.1 DEFINITIONS

In this Procedure, the these terms shall have the following meanings;

Law:	Law No. 5549 on Prevention of Laundering Proceeds of Crime dated 11/10/2006
Regulation on Measures:	Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism published in the Official Gazette No. 26751 dated 09/01/2008,
Regulation on Compliance:	Regulation on the Compliance Program Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism published in the Official Gazette No. 26999 dated 16/09/2008,
Proceeds of Crime:	Means proceeds derived from crime,
Money Laundering Offense:	Means the crime of processing the asset values resulting from commission of a criminal offense for which the lower limit is imposed for imprisonment of six months or more, with an attempt to export or to hide its illegitimate source and to convince that it is obtained in a legitimate way,
The Ministry:	Republic of Turkey Ministry of Finance
MASAK:	Republic of Turkey Ministry of Finance the Financial Crimes Investigation Board
Examiner:	Finance Inspector, Account Specialist, Customs Inspector, Revenues Controller, Bank Examiner, Treasury Controller, Banking Regulation and Supervision Specialist and Capital Markets Board Specialist,
Bank:	GSD Investment Bank A.S.,
Personnel:	GSD Investment Bank A.S. Personnel working in the headquarters, domestic branches, agencies, representatives and commercial agents and affiliated units,

Continuous business relationship:	Means the business relationship with continuity between our bank and the customer, as a result of services such as opening an account, granting a loan, financing, factoring, leasing,
Beneficial Owner:	Real persons who perform transactions with the Bank, real person/persons who control or are the final beneficiary of the accounts or transactions of real persons, legal entities or institutions which are not legal entities, who are acted on behalf of,
Financial Institution:	Means banks, other organizations authorized to issue bank cards or credit cards, competent institutions, money lenders under the scope of legislation on money lending business, financing and factoring companies, capital market intermediary institutions, futures intermediary firms and portfolio management companies, trustees, investment trusts, insurance, re-insurance and pension companies, insurance and re-insurance brokers, leasing companies, organizations providing settlement and custody services within the framework of capital market legislation and Postal and Telegraph Organization A.S. as limited to the banking activities,
Risk:	Means the possibility of loss of reputation or financial damage to which our Bank or its personnel may be exposed for reasons such as the use of the services provided by our Bank for the purpose of laundering proceeds of crime or financing of terrorism or our Bank's failure to comply with the obligations in accordance with the Law and regulations and communiqués issued pursuant to Law,
Customer Risk:	The risk of abuse of the Bank as a result of enabling intensive use of cash, the purchase or sale of high value goods or the easy transfer of international funds for the business line in which the client operates; and actions of the client or those acting on behalf or account of the client for the purpose of laundering proceeds of crime or financing of terrorism,
Service Risk:	The risk that the Bank may be exposed to due to non-face-to-face transactions, private banking, correspondent banking services or new products to be presented using emerging technologies,
Country Risk:	The risks that may be incurred by business associations and transactions with citizens, companies and financial institutions of the countries announced by the Ministry and which do not have adequate regulation on the prevention of laundering and financing of terrorism, do not cooperate in fight against these crimes, are considered risky by the competent international authorities,
Risky Countries:	Refers to the countries announced by the Ministry and which do not have adequate regulation on the prevention of laundering and financing of terrorism, do not cooperate in fight against these

crimes, are considered risky by the competent international authorities,

Shell Bank: Means 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,

Wire Transfer: Means the transaction carried out to transfer a certain amount of money and securities from a financial institution on behalf of the originator to the beneficiary persons in another financial institution by using electronic means,

Compliance: Means the adjustment with the legislation and the policies and rules of the Bank and the banking practices regarding the prevention of the laundering of proceeds of crime and financing of terrorism,

Compliance Program: Means the body of measures consisting of the establishment of institutional policies and procedures, risk management, monitoring and control, training and internal audit activities, appointment of compliance officer and establishment of a compliance unit; in order to prevent the laundering proceeds of crime or financing of terrorism, as stated in Article 5 of the Regulation on Compliance;

Institutional Policy: Means the policies which shall be established by taking the size, business volume of the Bank and nature of the transactions carried out into consideration, within the context of the compliance program regarding customer acceptance, identification and recognition, risk management, monitoring and control, training and internal audit,

Compliance Officer: Means the personnel who is assigned and authorized to ensure compliance of the bank with the liabilities imposed by the Law and the legislation enacted on the basis of Law,

1.2. OBJECTIVE

These policies intend to ensure compliance of the Bank with its obligations to prevent the laundering proceeds of crime and financing of terrorism and define the strategies, internal controls and measures, rules of operation and responsibilities to mitigate the risks that Bank customers are exposed to by evaluating the Bank's customers, transactions and services with a risk-based approach and ensure employee awareness of these issues.

1.3. SCOPE

The institutional policy covers the activities of all departments, units and branches of the Bank as well as, agencies, representative offices and similar affiliated units.

1.4. GENERAL PRINCIPLES

1. This policy has been established through a risk-based approach to ensure compliance with the obligations related to the prevention of laundering proceeds of crime and financing of terrorism, and of our customers, transactions and services.

2. It is expected that our banking activities will be carried out in accordance with the principles stated in the policies mentioned below, the application instructions and work flows should be determined in accordance with these principles and the relevant personnel should be informed in timely, including the amendments made, and all personnel should pay utmost care and attention in accordance with their responsibilities. No level of Bank personnel has the authority to take initiative in transactions that do not comply with legal obligations.

3. In the application instructions and work flows to be prepared in accordance with this policy, departments, units and persons responsible for the approval, realization, reporting and monitoring of transactions in accordance with risk limits and those responsible for operational rules are determined.

4. Any amendments in the legislation regarding prevention of proceeds of crime and financing of terrorism shall be reflected to the bank's internal regulations without delay and personnel shall be informed.

5. Necessary precautions shall be taken for the retainment for the minimum period of eight years and submission to the authorities if requested, from the date of issuance of the documents relating to liabilities and operations in every environment, the date of the last registration of the books and records; from the date of the last transaction of documents and records relating to identification. The date on which the account is closed is taken into consideration as the start date of the documents related to the ID clarification related to accounts.

6. Measures shall be taken in order to inform the related institutions in a timely and complete manner, within the scope of the obligation to provide information continuously.

7. All personnel shall exercise due diligence to provide appropriate working environment and necessary facilitation during the audit of MASAK and auditors in accordance with the relevant regulations, to provide all kinds of information and documents requested without introducing any written provisions in special law, to keep books and documents ready and available on time, to ensure access to all records including data processing system.

8. This policy come into force with the approval of the Board of Directors and can only be amended by the approval of the Board of Directors.

9. These policies for prevention of laundering proceeds of crime and financing of terrorism are informed to the relevant personnel.

10. It is essential that our Bank comply with the AML policies and procedures of the majority shareholder of our Bank within the scope of our country's legislation. The AML policies and procedures of the majority shareholder of our Bank are evaluated by the Compliance Unit and the rules that are not contrary to the legislation of our country are reflected in our Bank's procedures.

    All departments, units, branches, institutions subject to consolidation and all personnel must comply with the AML policies, procedures and instructions of our Bank's majority shareholder and our Bank in all work and transactions.

    It is the primary responsibility of every employee to protect the majority shareholder of our Bank and our Bank from the AML risk. All personnel must exercise due diligence to avoid the AML risk, to avoid conflict with legal regulations, bank policies and procedures and the regulations of our bank's majority shareholder and to take all necessary precautions to ensure that the bank is not exposed to AML risk.

1.4.1. Customer Acceptance, ID Clarification and Recognition

The Bank establishes an effective customer acceptance, ID clarification and customer recognition system in accordance with the general principles of the client recognition and having the following characteristics in order to comply with the obligations of prevention of laundering of proceeds of crime and financing of terrorism.

1. In terms of establishing a continuous business relationship based on openness and trust in the Bank with the customers, sufficient information shall be gathered on the real identity and address, the consistency of the documents and information within themselves, the nature and intention of the business relationship, the reasons for choosing the bank, business, business activities, business history, financial situation and funding sources, necessary precautions shall be taken to ensure that all customers are recognized, unrecognized and unidentified customers' transactions are not accepted, it shall be ensured that the personnel pay maximum attention to these rules in their customer transactions.

2. Regardless of the amount in the continuous business relationship, when the total amount of transaction or the amount of multiple transactions connected with each other is twenty thousand TL or more, when the amount of transactions in domestic or foreign electronic transfers or the total amount of multiple transactions connected with each other is two thousand TL or more,regardless of the amount in situations that require the reporting of suspicious transactions, regardless of the amount when there is doubt about the adequacy and accuracy of previously obtained customer credentials, information about the identity shall be collected and this information shall be confirmed and the identity of the persons acting on behalf or account of the customers and the customers shall be determined.

3. ID Clarification shall be completed before establishing a business relationship or performing a transaction requiring identification.

4. Compliance with the new regulations of the information within the scope of identity determination of the customers who have been established before the obligations set forth in the legislation on terrorism financing and whose identity has been determined according to the legislation in force before that date shall be completed within the deadlines determined by the relevant legislation The transactions requested by the customers which can not be completed within the specified times shall not be carried out without proper ID clarification. In addition, if there are no transactions requested by the customer up to the time specified in the legislation, the information within the scope of the identification of these customers shall be complied with at the date of the first transaction request of the customer including transactions not carried out face to face and before the transaction is carried out.

5. For all new and existing customers, a minimum level of information about the customer's status, needs, and business relationship objectives shall be obtained, recorded, and retained before opening any accounts or performing transactions.

6. In case of any suspicion about the authenticity of the documents used for the purpose of confirming the information for identification purposes (fake, stolen, etc.), the authenticity of the document shall be verified by reference to the person, institution or other competent authorities who regulate the document of doubt as to the extent possible.

7. In the subsequent transactions of the customers who have been previously duly identified within the continuous business relationship scope, the information on the identity shall be compared with the information by our bank. In the event that the received information is suspected to be inaccurate, the accuracy of this information shall be verified by comparing the information in these documents with the information in the Bank after the presentation of the principal identity documents or their notarized certified copies.

8. Necessary precautions shall be taken to determine if the person requesting the transaction is acting on his/her behalf but on the account of another person, and the identity of the beneficial owner (person who is acted on the account of) . The identification and authorization status of the persons who declare that they are acting on behalf of another person and the identification of the beneficial owner of the transaction shall be performed.

9. When a continuous business relationship is established with legal entities registered with the trade registry, the identity of real and legal person partners who have a share of

more than 25% shall be determined, measures shall be taken to ensure that they have the right information about those who manage, control and hold the entity.

10. If anyone who claims that he or she does not act on someone else's behalf is suspected to have acted on his/her behalf but for someone else's account, a reasonable level of investigation shall be done by the personnel in order to reveal the real beneficiary.

11. Special attention shall be paid if the requested transaction is complicated, extraordinarily large, with no apparent reasonable legal and economic purpose, necessary precautions shall be taken to obtain sufficient information about the purpose of the process, the information, documents and records obtained in this way shall be retained for presentation to the supervisory staff or authorities when requested.

12. In the matters of determining the identity of the client, the person acting on the client's behalf and the real beneficiary and obtaining information about the business relationship or the purpose of the transaction, our group companies can establish or operate a business relationship by relying on a financial institution (third party) in their area to take precautions in relation to the customer. In this case, our bank shall immediately receive the customer's credentials from the third party. In such cases, the ultimate responsibility under the legislation belongs to our bank. This does not apply to transactions between financial institutions and our Bank on behalf of the customer, agents and similar units, and relationships with the persons who have the services of extension or complementary services of the main service units. The third party trust principle shall not be applied in transactions with financial institutions other than our group companies.

13. Employees; can not establish a business relationship and can not perform the transaction requested from them in cases where they are unable to clarify an identification or obtain sufficient information about the purpose of the business relationship.

14. In case the identification and confirmation that has to be done due to the suspects about the adequacy and authenticity of previously obtained customer credentials can not be done, the business relationship shall be terminated and it shall also be assessed whether or not they are of a nature that could be subject to a suspicious transaction notification. There is no need to terminate the business relationship if there is no doubt about the adequacy of the customer's identity.

15. In foreign correspondent relationships; it shall be investigated for whether the financial institution has been under investigation for laundering and financing terrorism, whether it has been punished or not, its business subject, its reputation and whether it has been subject to adequate testing, it shall be assessed to ensure that the system of fight against laundering and terrorism of financing of this financial institution is effective and

appropriate, the approval of the General Manager or the relevant Assistant General Manager shall be obtained before establishing a new correspondent relationship, signed questionnaires shall be provided, including policies on the prevention of proceeds of crime and terrorism financing, necessary measures shall be taken to ensure that the counterpart financial institution has taken adequate measures within the framework of the existing legislation and that it can provide the identity information of the concerned customers when requested in cases where the correspondent relationship includes the use of transacted correspondent accounts.

16. No correspondence relationship shall be established with shell banks and financial institutions that can not be sure that their accounts do not use shell banks.

17. If there is any suspicion, information or document that the assets and funds of persons and institutions have not been obtained from legal means, these persons and institutions shall not be accepted as customers, and also guarantees and sureties shall not accepted even if they are not direct customers.

18. In the event that the transactional assets made or attempted to be made via the bank or bank; is obtained from illegal means or used for illegal purposes, in this context, for terrorist acts or for use by terrorist organizations, terrorists or terrorist financiers, or any information, suspicion or doubt is existent that it is related to these, suspicious transactions shall be immediately reported to the Compliance Officer in accordance with the principles and procedures set forth in the "Suspicious Transaction Notification Application Instruction" to be prepared and announced to the entire Bank. No amount shall be taken into account in the notification of the suspicious transactions mentioned, whether there is a reasonable cause to require a suspicion or doubt shall be assessed by considering multiple transactions together when necessary.

19. No information can be given to anyone, whether or not the suspicious transaction notification has been made or will be made, other than the information given to the inspectors assigned to the obligation audit and to the courts during the trials, including those involved in the transaction. The confidentiality obligation shall also include all personnel who reports internally to the Compliance Officer and are aware of any suspicious transaction notifications in any way.

1.4.2. Risk Management:

This policy, Risk management which takes the size of the bank, the business volume and the nature of the transactions carried out into consideration, aims to identify, rate, monitor, evaluate and mitigate the risks that can be incurred in the issues of laundering of proceeds of crime and financing of terrorism. For this purpose, an effective risk management system in accordance with the following principles shall be established within the Bank.

1. The risk-based approach shall continuously monitor that transactions carried out by customers are in accordance with information regarding customers' business, business activities, business history, financial situation, risk profile and funding sources.

2. Information, documents and records about customers shall be kept up to date. Careful attention must be given to the fact that the documents to be submitted or deposited to the Bank during application contain adequate information and that the information provided is coherent.

3. The correctness of the information received for the identification of customers, such as the telephone and fax number and e-mail address, shall be verified by contacting them using these tools when necessary within the framework of the risk-based approach.

4. Transactions that are carried out outside of the continuous business relationship shall also be closely monitored by the risk-based approach.

5. The bank shall pay special attention to the risk of using facilities introduced by new and developing technologies for money laundering and terrorist financing and to take appropriate measures for its prevention.

6. Special attention shall be paid to transactions such as cash electronic transfers,

7. The transactions which are not related to the customer's financial profile and not suitable for their activities shall be closely monitored; it shall be observed whether there is a reasonable ratio between the customers' job/profession, financial situation and operations; appropriate and effective measures shall be taken, including setting the maximum amount and the number of transactions.

8. Special attention shall be paid to the business relationships and transactions with real persons and legal entities, non-legal entities located in risky countries and citizens of this country; information is gathered and recorded as far as possible regarding the nature and purpose of transactions which are not reasonably for legal and economic purposes.

9. Risk management activities are carried out within the Bank within the scope of the legislation related to the laundering of proceeds of crime and financing of terrorism.

1.4.3. Monitoring and Control:

In order to protect the bank against the risks arising from the legislation on prevention of laundering proceeds of crime and financing of terrorism and to monitor and control continuously whether the activities are carried out in accordance with the the Law and the regulations and communiqués issued in accordance with the Law and and the institutional

policies and procedures, monitoring and control activities shall be carried out within the Bank under the scope of the following principles, considering the size of the bank, the volume of business and the nature of the transactions carried out.

1. Monitoring and controlling activities shall at least include the following activities;

   - Monitoring and controlling the customers and transactions in the high-risk group,
   - Monitoring and controlling transactions conducted with risky countries,
   - Monitoring and controlling complex and unusual transactions,
   - Obliged party's control, through sampling method, of whether the transactions exceeding the amount which the obliged party will determine according to the risk policy are consistent with the customer profile,
   - Monitoring and controlling linked transactions which, when handled together, exceed the amount requiring customer identification,
   - Control of customer related information and documents which are required to be kept in electronic environment or in written form and the information required to be placed in wire transfer messages, completing the missing information and documents and updating them,
   - During the business relationship, ongoing monitoring whether the transaction conducted by the customer is consistent with information regarding business, risk profile and fund resources of the customer,
   - Control of the transactions carried out through using systems enabling the performance of non face-to-face transactions,
   - Risk based control of services that may become prone to misuse due to newly introduced products and technological developments

2. Monitoring and control activities are carried out by the Compliance Officer within the scope of the principles specified in MASAK legislation. The Compliance Officer has the authority to request all kinds of information and documents related to the duties of all units within the Bank and to have access to them in a timely manner.

3. The deficiencies determined by the Internal Control Department regarding the compliance with the obligations imposed pursuant to the law shall be reported to the relevant units and the results shall be followed in order to take necessary measures.

1.4.4. Training:

In order to ensure compliance with the obligations imposed by the Law and regulations and communiques issued in accordance with the Law, to create a corporate culture by increasing the sense of responsibility of personnel regarding the institutional policy and procedures and risk-based approach and to update personnel knowledge, training activities shall be carried out within the bank, in line with the business volume, size and changing conditions.

1.4.5. Internal Audit:

Internal audit activities shall be carried out within the bank in order to provide assurance to the Board of Directors on the effectiveness and adequacy of the whole compliance activities.