1. Introduction

Q Yatırım Bank A.Ş. maintains strict adherence to all applicable national and international laws and regulations pertaining to the prevention of money laundering, the financing of terrorism and the proliferation of weapons of mass destruction, bribery and corruption, and sanctions programs. The company acknowledges the significant societal harm engendered by these issues and, as part of its social responsibility, accords a high priority to this initiative.

2. Definitions

OFAC-The Office of Foreign Assets Control: An office under the US Department of the Treasury that imposes economic and trade sanctions based on US foreign policy and national security objectives against countries, regimes, terrorism-linked groups, international drug traffickers, individuals, organizations and entities engaged in the proliferation of weapons of mass destruction, and individuals and groups linked to other high-threat activities.

Money Laundering Offences: In accordance with Article 282 of the Turkish Penal Code No. 5237, dated 26/09/2004, it refers to the act of subjecting assets derived from an offense, punishable by a minimum term of six months' imprisonment or more, to various transactions with the intent to transfer such assets abroad, conceal or disguise their illicit origin, or create the false appearance that they were lawfully acquired.

Payable-Through Accounts: A type of account opened by a foreign financial institution at a financial institution domiciled in Türkiye within the scope of a correspondent banking relationship, which allows the foreign institution's clients to conduct transactions directly through the account.

Simplified Measures: Regulations introduced under Communiqué No. 5 by MASAK (Financial Crimes Investigation Board), which allow for the simplified implementation of the requirements related to the principle of customer identification in cases where, based on a risk- based approach, the risk of money laundering and financing of terrorism can be considered low in terms of transaction types.

HM Treasury: The Ministry responsible for controlling public expenditures and for developing and implementing the UK Government’s public finance and economic policies. The Office of Financial Sanctions Implementation (OFSI), which operates under HM Treasury, is responsible for providing authoritative guidance to the public to ensure the proper understanding, compliance, and enforcement of financial sanctions implemented within the United Kingdom.

Auditor: Tax Inspectors, Treasury and Finance Specialists employed at the Presidency, Customs and Trade Inspectors, Sworn Bank Auditors, Treasury Controllers, Insurance Supervisory Specialists and Actuaries, experts from the Banking Regulation and Supervision Agency and the Capital Markets Board, as well as auditors and specialists from the Central Bank of the Republic of Turkey, who conduct audits and inspections within the scope of the legislation on the Prevention of Laundering Proceeds of Crime.

Electronic Transfer: A transaction conducted for the purpose of sending a specified amount of money and securities from a financial institution on behalf of the sender to a recipient at another financial institution through electronic means.

Financial Institution: Banks; entities authorized to issue bank cards or credit cards other than banks; authorized institutions specified in foreign exchange legislation; finance and factoring companies; capital market intermediary institutions and portfolio management companies; payment institutions and electronic money institutions; investment partnerships; insurance, reinsurance, and pension companies; insurance and reinsurance brokers; financial leasing companies; institutions providing clearing and custody services within the scope of capital markets legislation; and the Posta ve Telgraf Teşkilatı Anonim Şirketi (Turkish Post and Telegraph Organization) limited to banking activities.

Fund: Any property, whether movable or immovable, tangible or intangible, rights, receivables, or any documents representing such assets, the value of which can be expressed in monetary terms.

Ultimate Beneficial Owner: Natural persons who ultimately control the natural persons conducting transactions before the obliged party, or the natural or legal persons, or unincorporated entities on whose behalf the transaction is conducted, or who have ultimate authority over the relevant account or transaction.

PEPs-Politically Exposed Persons: Individuals who are entrusted with prominent public functions, whether domestically or in a foreign country, through election or appointment, as well as members of the governing bodies and senior executives of international organizations, and other individuals holding equivalent positions.

Financing of Proliferation: Activities related to the financing of the transfer and export of nuclear, chemical, and biological weapons, which, compared to conventional weapons, cause mass fatalities, significant property damage, and long-lasting environmental and health issues.

FATF-Financial Action Task Force: An organization established in 1989 under the OECD by the G-7 countries aims to develop national legal systems to prevent money laundering and the financing of terrorism, harmonize regulations, strengthen the role of the financial system, and ensure continuous cooperation among member countries through the implementation of effective measures.

Financial Crimes Investigation Board (MASAK): The Presidency operating within the Ministry of Finance, responsible for preventing and detecting money laundering offenses, is tasked with policy development, regulation, information gathering and analysis, research and investigation, and transmitting the collected information and findings to the relevant authorities.

Assets:

- The funds and income owned or possessed by a natural or legal person, or directly or indirectly controlled by them, along with the benefits and value derived from these or resulting from the conversion of these assets into one another,

- Additionally, the funds and income owned or possessed by a natural or legal person acting on behalf or account of another, along with the benefits and value derived from these or resulting from the conversion of these assets into one another.

Asset Freezing: The removal, consumption, conversion, transfer, assignment, or any other disposal of assets is prevented by the removal or restriction of the authority to dispose of the assets, in order to prevent their elimination or unauthorized handling.

Customer Profile: A profile consisting of information about the customer conducting transactions within the group, including their profession, business activities, employment history, financial status, sources of funds, and preferred products and services.

Risk: The potential for financial or reputational loss to our group or its employees due to the misuse of the services we provide for money laundering or terrorist financing purposes, or due to non-compliance with the obligations set forth in the regulations and communiques issued under the relevant laws.

High-Risk Countries: Countries that lack adequate regulations for the prevention of money laundering and the financing of terrorism, do not cooperate in combating these offenses, or are identified as high-risk by competent international authorities.

Bribery: The offering, promising, giving, requesting, or accepting of an advantage to encourage an illegal, unethical, or trust-violating action.

Proceeds of Crime (Money Laundering): Money or assets that have not been obtained through lawful means and/or have not been subject to taxation. (This includes assets derived from crimes under national legislation that carry a minimum sentence of six months or more in prison.)

Money Laundering (ML): Any transaction aimed at removing assets derived from illegal activities from the country, concealing their illicit origin, or creating the impression that they have been obtained through lawful means.

- The first stage refers to the physical disposal of cash proceeds derived from illegal activity by integrating the funds into the financial system – Placement

- The second stage is the process of the separation of illicit proceeds from their source as much as possible by using different techniques to create complex layers of financial transactions – Layering

- In the third stage laundered funds are introduced into the legitimate economy, appearing to have originated from a legitimate source – Integration

Permanent Business Relationship: A business relationship that is established between obliged parties and their customers through services such as opening an account, lending loan or issuing credit cards, safe deposit boxes, financing, factoring or financial leasing, life insurance and individual pension, and that is permanent due to its characteristics.

Suspicious Transaction Report: The report submitted to the Compliance Department regarding customers and transactions deemed suspicious by Branches and Head Office Units.

Shell Bank: A bank that does not exist physically in any country, does not employ full-time employees, and is not subject to the supervision and permission of an official authority in terms of banking operations and records.

Terrorist Financing (TF): The act of providing or collecting funds for a terrorist or terrorist organizations, either fully or partially intended for the commission of terrorist offenses, with or without direct association with a specific act, knowingly and willingly.

International Sanctions: Financial sanctions including decisions and regulations issued by international authorities (such as the UN, USA, EU, UK) regarding countries, individuals, institutions, or vessels due to reasons such as money laundering, terrorist activities, or anti- democratic practices.

Compliance Unit: A department consisting of employees responsible for implementing the compliance program, working under the supervision of a compliance officer. (This function is performed by the Compliance Department at Q Yatırım Bankası A.Ş.)

Compliance Officer: The officer who is employed for the purpose of ensuring the compliance with obligations established through the Law No. 5549 on Prevention of Laundering Proceeds of Crime or the legislation issued on the basis of the Law and who is entrusted with the required authority.

Deputy Compliance Officer: An employee appointed exclusively as institutional staff, who meets the requirements and qualifications required for the compliance officer, and who is assigned by the Board of Directors or its designated members to act under the compliance officer. This person may be delegated some or all of the compliance officer's duties and powers in writing and explicitly.

Compliance Program: All of the measures which is to be established for the prevention of ML/TF.

Executive Management: The General Manager and Deputy General Managers of the Bank, the Managers of units working under Internal Systems, as well as managers of units other than consultancy units carrying out duties in a position that is equivalent to, or higher than deputy general manager position in terms of authorities and duties, even if they are employed for different positions.

Senior Management: The Board of Directors of the bank and the senior executive management.

Sanction: Regulations aimed at restricting or preventing economic activities, either individually or comprehensively, targeting countries, individuals, and organizations, in order to achieve economic and political objectives.

Countries/Regions Subject to Comprehensive Sanctions: Countries or regions subject to sanctions imposed at a national or regional level by the Republic of Türkiye, the United Nations Security Council, the United States, the European Union, and the United Kingdom.

Corruption: The direct or indirect solicitation, offering, giving, or acceptance of an illicit commission, or other unjust benefit, or the promise of such benefit, which influences or alters the necessary conduct of an individual in the ordinary performance of their duties, or in the case of benefiting from an unfair commission or undeserved advantage.

'Nested Account' Activities: In a financial institution providing correspondent banking services, the use of vostro accounts opened by one financial institution, where the institution that opened the account allows a third bank to provide services to or facilitate transactions for other financial institutions.

3. Abbreviations

EU: European Union,

USA: The United States of America,

UN: United Nations,

FATF: Financial Action Task Force

Group Compliance Policy: T. Yyyy Yyyysı A.Ş. Anti-Money Laundering and Countering the Financing of Terrorism Policy (AML/CFT Policy)

MASAK: Financial Crimes Investigation Board

OFAC: Office of Foreign Assets Control

OFSI: Office of Financial Sanctions Implementation

ML/TF: Money laundering and terrorist financing (crimes such as financing the proliferation of weapons of mass destruction and bribery/corruption are also falling under this abbreviation).

Regulation on Measures: Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism

UK: United Kingdom of Great Britain and Northern Ireland

Regulation on Compliance: Regulation on Program of Compliance with Obligations of Anti- Money Laundering and Combating the Financing of Terrorism

4. Objective and Scope

The Compliance Policy aims to achieve the following objectives:

- Ensuring Q Yatırım Bankası A.Ş.'s compliance with legal obligations related to the prevention of money laundering, the financing of terrorism/weapon proliferation, and the prevention of bribery and corruption, while maintaining its national and international reputation,

- Evaluating customers, transactions, and services using a risk-based approach, and developing strategies to mitigate potential risks,

- Establishing internal controls, operational procedures, and responsibilities within the bank, and raising awareness among bank employees on these matters.

The standards outlined in this policy encompass the minimum requirements stipulated by relevant legislation, with the aim of safeguarding the interests of the Bank, its employees, and its customers against any potential exploitation in relation to ML/TF.

5. Roles and Responsibilities

Under Law No. 5549 on the Prevention of Money Laundering, the **Board of Directors** is ultimately responsible for ensuring the fulfillment of the group's obligations regarding "AML/CFT".

The Board of Directors is authorized and responsible for the following under the Compliance Program:

- Ensuring the Bank's compliance with obligations related to the fight against Financial Crimes,

- Approving the policy, annual training programs, and any changes thereto based on developments,

- Appointing a Compliance Officer and Deputy Compliance Officer,
- Approving the Corporate Compliance Department's Task Regulation, which outlines the duties, authority, and responsibilities of the Compliance Officer and the Corporate Compliance Department.
- Evaluating the results of risk management, monitoring, control, and internal audit activities, and ensuring that necessary measures are implemented,
- Ensuring that all activities are carried out in a coordinated and effective manner.

The responsibility of the Bank's Executive Management is to report to the Board of Directors on the following matters:

- The establishment of business processes and task regulations in compliance with the Policy, within the framework of banking corporate governance principles,
- Ensuring that processes are implemented in a fit-for-purpose and effective manner by all employees,
- Taking timely measures to ensure that the bank is not exposed to financial crimes and sanctions-related risks.

The Compliance Officer, working under the Board of Directors, is responsible, authorized, and accountable for the following matters;

- Carrying out the necessary activities to ensure the implementation of the Policy and Compliance Program, and establishing the required communication and coordination with the Financial Crimes Investigation Board (MASAK),
- Drafting the Policy and submitting it for approval to the Board of Directors,
- Establishing, updating, publishing, and coordinating the implementation of the Bank’s procedures related to the application of the Policy and Compliance Program within the Bank, and monitoring the operational process,
- Conducting risk management, monitoring, and auditing activities,
- Submitting the work related to the training program for approval to the Board of Directors and ensuring the effective implementation of the approved training program,
- Evaluating the information and findings obtained regarding suspicious transactions, and reporting transactions deemed suspicious to Financial Crimes Investigation Board (MASAK),
- Maintaining regular records of information and statistics related to internal audit and training activities, and reporting them to Financial Crimes Investigation Board (MASAK) within the specified timeframe.

The Compliance Officer may delegate some or all of his/her duties and authorities to the Deputy Compliance Officer in writing.

Within the scope of the compliance program, risk management and audit operations are carried out by observing

the three-tier line of defense and ensuring coordination between tasks/responsibilities.

All employees at every level of the bank are responsible for diligently and accurately fulfilling their duties and responsibilities to ensure that the Policy, related processes, and the Compliance Program are implemented effectively and purposefully at the bank's headquarters and branches, in order to prevent the bank from being exposed to financial crimes and sanctions-related risks. Non-compliance with the Policy or any violation of the Policy may result in disciplinary actions.

The effectiveness and adequacy of the implementation of the Policy and Compliance Program are subject to regular audits and evaluations as part of the internal audit process. The findings presented in the reports are to be addressed as a priority by the responsible departments, with compliance risk in mind. Audit findings related to compliance risk are reported to the Corporate Compliance Department and, through the Audit Committee, to the Board of Directors.

6. Legal Framework

The legal basis for the group's policy on the prevention of ML/TF (Money Laundering/Terrorist Financing) is established by **Law No. 5549 on the Prevention of Money Laundering, Law No. 6415 on the Prevention of the Financing of Terrorism, and Law No. 7262 on the Prevention of the Financing of the Proliferation of Weapons of Mass Destruction**, along with the regulations and communiqués issued in relation to these laws. Our group also takes into account, in addition to the national regulations on the prevention of ML/TF issued by Financial Crimes Investigation Board (MASAK), the recommendations, principles, standards, and regulations set by international regulatory bodies such as FATF, provided they do not conflict with national regulations.

7. Compliance Program

In order to comply with national regulations and international standards and to carry out audit activities within this scope, the Compliance Policy Q Yatırım Bankası A.Ş., related to the prevention of ML/TF includes the following measures:

- Appointment of a Compliance Officer and/or Deputy Compliance Officer, and the establishment of a Compliance Unit,
- Development of policies and procedures for the prevention of ML/TF, and the preparation of subordinate administrative documents for this purpose,
- Providing necessary information to the employees in order to raise awareness on the Bank's policies,
- Identification, assessment, monitoring, evaluation, and mitigation of risks the bank may be exposed to within the scope of ML/TF prevention, along with the execution of risk management activities,
- Execution of risk-based monitoring and audit activities, depending on the size, business volume, and scope of services provided,
- Providing training to employees within the framework of ML/TF prevention legislation,

- Conducting internal audit activities to ensure the implementation of the policies and procedures related to ML/TF prevention established within the scope of the Compliance Program,

The Compliance Policy is reviewed at least annually by the Compliance Department in the context of regulatory changes or from a risk-based perspective, revised if necessary, and submitted for approval to the Board of Directors.

8. Risk Management

The purpose of risk management is to identify, assess, and evaluate the risks associated with money laundering and the financing of terrorism that the bank may be exposed to, and to ensure that the necessary measures are taken to mitigate such risks.

The bank reassesses and updates its risk management policy, taking into account emerging conditions, as well as the recommendations, principles, standards, and guidelines set by national regulations and international organizations. Activities carried out within this scope are reported at regular intervals to the Board of Directors and/or the Audit Committee and/or the relevant Board Member(s) to whom the Board of Directors has delegated authority.

Risk management also includes internal measures and operational rules related to customer identification; a customer acceptance policy is established to comply with the "**Know Your Customer**" principle as outlined in national and international regulations regarding the prevention of ML/TF.

Risk Areas: Within the framework of a risk-based approach, four risk areas have been identified: customer risk, product/service risk, sector risk, and country/region risk.

Customer risk refers to the potential for the bank to be exploited by the customer due to actions taken by the customer or by individuals acting on behalf of the customer, with the intention of money laundering or financing terrorism.

Transactions not conducted face-to-face with bank customers, cash-based transactions that are difficult to track, and new products to be offered using emerging technologies pose a risk of ML/TF, and therefore, entail **product and service risks**.

Certain sectors and industries pose a high ML/TF risk due to factors such as high cash usage, the ease with which the source of funds can be concealed and difficult to trace, and the ability to easily hide the true purpose of activities. Customers operating in such high-risk industries constitute **sector risk**.

Countries that do not fully implement or inadequately apply FATF recommendations and are therefore included in FATF's high-risk and increased monitoring lists, as well as countries subject to comprehensive sanctions/embargoes by the UN, OFAC, EU, OFSI, and national authorities, countries and regions located along drug production and distribution routes, where crimes such as smuggling, terrorism, corruption, and bribery are widespread, and tax havens/cross-border centers (offshore) constitute **country/region risk**.

Risk Rating: The bank assesses customers, products/services, sectors, and countries/regions within its scope of operations based on its risk perception in the identified risk areas, and categorizes them into three distinct levels:

- Prohibited / Not Worked With

- High Risk
- Standard Risk

Entities categorized under the **Prohibited / Not Worked With** risk level are not accepted as customers, and no transactions are facilitated on their behalf. Transactions of existing customers whose risk rating changes to Prohibited / Not Worked With are rejected, and the process of terminating the customer relationship is initiated. Products/services at this risk level are not offered by the bank, and no business relationships are established with countries/regions at this risk level.

Enhanced measures are applied for countries, customer groups, products, and services classified under the **high-risk** level.

Standard procedures are followed for customers and transactions classified under the **standard risk** level.

At the onset of the banking relationship and throughout its duration, customers are classified into appropriate risk categories based on the above fundamental criteria, as well as any customer-specific information and criteria related to the nature and scope of their activities, relationship with the bank, and transactions.

Under the “Know Your Customer” principle, the information and documents obtained from the customer are updated annually for high-risk customers, every two years (2) for medium-risk customers, and every four years (4) for low-risk customers.

Customers and transactions in the high-risk level are closely monitored and controlled using appropriate monitoring and control methods.

9. Know Your Customer

At the core of the bank’s customer acceptance process for combating financial crimes lies the "Know Your Customer" principle.

The bank places great emphasis on the “Know Your Customer” principle to protect itself from individuals and actions related to financial crimes and sanctions. In this regard, it implements practices in compliance with international standards, recommendations, and applicable regulations.

The bank takes all necessary measures to know its individual and legal entity customers in terms of social, financial, and personal information. For this purpose, it obtains all relevant documents, particularly those related to identity information, and verifies their accuracy. It is not sufficient to obtain the relevant documents from customers with whom a continuous business relationship is established only once. Customers are monitored based on their risk levels, their transactions are controlled, and any changes that occur are tracked.

Under the “Know Your Customer” principle, processes are established under the responsibility of executive management, with necessary measures taken by the responsible units in accordance with regulations and the policy framework, as follows:

- Identity verification,
- Identification of the Ultimate Beneficial Owner,

- Obtaining sufficient information about the purpose and nature of the requested transaction,
- Risk assessment of the customer during the acceptance process and dynamic updating of the risk assessment throughout the business relationship,
- Evaluation of the customer and transactions in accordance with the principles of "Sanctions”,
- Monitoring the customer's status and transactions throughout the business relationship,
- Taking necessary measures for customers, activities, and transactions requiring special attention.

Customer accounts must be opened in the customer's real name, surname, or title. Customers cannot be accepted using another name, an anonymous name or a pseudonym.

- In cases where identification cannot be determined or sufficient information cannot be obtained regarding the purpose of the business relationship; customer acceptance cannot be performed and the requested transaction cannot be realized.
- Those whose ownership structure is inexplicably complex and whose ultimate beneficiary owner cannot be identified are not accepted as customers.
- Within the scope of the requirement that customer relations should be based on mutual exchange of information, trust and openness, persons and organizations that refrain from filling out the introductory information forms or provide misleading, unverifiable information are not accepted as customers.
- Customers' names and surnames/titles are queried from globally recognized lists of public figures. In case a match is detected, necessary measures are taken against public figures.
- Account opening requests of third parties on behalf of one or more persons (except for accounts to be opened on behalf of persons under custody and guardianship or minors) shall not be carried out unless it is clearly documented that it is legally authorized by the Customer and the purpose and necessity of opening an account is clearly disclosed.
- In case there is a doubt, information or document in the assessment made regarding the fact that the material assets of the persons and organizations with whom a business relationship or customer relationship will be entered into are not acquired through legal means; business relations shall not be entered into with such persons and organizations, and their guarantees and sureties shall not be accepted.
- In case of any doubt regarding the adequacy and accuracy of the previously obtained data on customer ID and in the event that the necessary identification and confirmation is not possible, the customer relationship shall be terminated.

The Bank performs the identification of the customer in a timely, complete and accurate manner within the framework of the applicable legislation, policies and processes in the establishment of a Permanent Business Relationship and before the transaction is executed.

Identification is performed as follows;

- It is performed regardless of the amount in the establishment of a Permanent Business Relationship,

- In cases of doubt regarding the adequacy and accuracy of previously obtained customer ID data, it is carried out regardless of the amount,

- In cases where Suspicious Transaction report is required, it is executed regardless of the amount,

- When the transaction amount or the total amount of multiple related transactions exceeds the amount specified in the Legislation, it is carried out by obtaining the identity data of the customers and those acting on behalf or account of the customers within the framework of the relevant Legislation and confirming the accuracy of this information.

Identification of the Ultimate Beneficial Owner: The ultimate beneficiary is defined as the natural person who performs transactions at the Bank, the natural person on whose behalf the transaction is carried out, the natural person, legal entity or unincorporated entities that ultimately control or have ultimate control over the account or transaction owned by them. Accordingly, the Bank shall take the necessary measures to determine whether someone else is acting on behalf of someone else and to reveal the ultimate beneficial owner of the transaction.

In establishing customer relationships with legal entities, the bank identifies the natural persons who are ultimate beneficial owners holding a share of twenty-five percent or more in the legal entity.

If there is suspicion that a natural person shareholder holding twenty-five percent or more of the legal entity is not the beneficial owner, or if no such natural person shareholder exists, necessary measures shall be taken to identify the natural person or persons who ultimately control the legal entity. The identified natural person or persons shall be deemed the ultimate beneficial owner(s); if the ultimate beneficial owner cannot be identified, the natural person or persons registered in the commercial registry with the highest level of executive authority shall be considered the ultimate beneficial owner(s) by virtue of their position as an executive manager.

Necessary measures shall be taken to identify the natural person or persons who ultimately control entities without legal personality. If the ultimate beneficial owner cannot be identified, the natural person or persons with the highest level of executive authority shall be deemed the beneficial owner(s) by virtue of their position as an executive manager.

Transactions Requiring Special Attention: The Bank pays special attention to complex and unusually large transactions and transactions that do not have a reasonable legal and economic purpose, and takes the necessary measures to obtain sufficient information about the purpose of the requested transaction and to preserve the information, documents and records obtained.

Monitoring of Customer Status and Transactions: Within the scope of an ongoing business relationship, transactions conducted by customers must be continuously monitored to ensure consistency with information regarding the customers' profession, commercial activities, business background, financial status, and sources of funds. Additionally, the information, documents, and records related to customers should be updated periodically. If transactions inconsistent with the stated purpose of establishing the business relationship and/or the customer profile are detected during customer acceptance, the customer relationship shall be reassessed.

Accounts opened are continuously monitored to verify whether they are being actively used by the person in whose name they were opened.

Taking Measures Against Technological Risks: The Bank pays special attention to the risk of new and emerging technologies being exploited for money laundering and terrorist financing, and takes appropriate measures to prevent such misuse. Special attention is given to transactions conducted using systems that enable non-face-to-face operations. Transactions that are inconsistent with the customer's financial profile or activities,

or unrelated to their business, are closely monitored. Appropriate and effective measures, including setting limits on amounts and number of transactions, are implemented.

Correspondent Banking: Enhanced due diligence measures are applied in establishing and maintaining relationships with correspondent banks. No business relationships may be established with shell banks or with other banks that provide services to shell banks. Furthermore, no correspondent accounts or nested account services shall be provided.

Electronic Transfers: Necessary measures shall be taken to minimize risks in electronic transfers facilitating the domestic or international transfer of funds considered high-risk for money laundering and terrorist financing (ML/TF).

Domestic and international electronic transfer messages shall include at least the mandatory minimum information about the **sender** and the recipient.

For international transfers involving high-risk countries and customers, information and documents that leave no doubt about the nature of the transaction shall be obtained from the relevant parties.

Simplified Measures: Simplified measures may be applied in relation to the obligation of customer identification in accordance with the provisions set forth in Financial Crimes Investigation Board (MASAK) General Communiqué No. 5.

Enhanced Measures: For customers and transactions classified as high risk, one or more of the measures specified in the Financial Crimes Investigation Board (MASAK) Regulation on Measures, under the section on Enhanced Measures, shall be applied to mitigate the risk.

10. Monitoring and Control

It is essential that the bank continuously monitors whether its activities are conducted in compliance with the relevant law, regulations, and communiqués issued pursuant to the law, as well as the institution's policies and procedures, to protect against money laundering and terrorist financing (ML/TF) risks. Monitoring and control activities are conducted based on a risk-based approach, taking into account the size and transaction volume of group entities.

The Compliance Unit is responsible for conducting monitoring for this purpose and ensuring that the risk assessment remains up to date. The Compliance Unit establishes a centralized monitoring and control system to detect money laundering and terrorist financing risks as well as suspicious transactions. This system enables the monitoring of the activities of group entities, primarily high-risk customers and transactions, based on predetermined criteria and scenarios.

Monitoring and control activities shall, at a minimum, include the following:

- Monitoring and control of customers and transactions in the high-risk category,
- Monitoring and control of transactions conducted with high-risk countries,
- Monitoring and control of complex and unusual transactions,

- Sampling-based verification of whether transactions exceeding a predetermined amount are consistent with the customer profile,

- Monitoring and control of linked transactions that, when aggregated, exceed the threshold requiring customer identification,

- Verification, completion, and updating of information and documents related to customers that must be retained electronically or in writing, as well as mandatory information included in electronic transfer messages,

- Continuous monitoring throughout the business relationship to ensure that transactions conducted by the customer are consistent with the customer's business, risk profile, and sources of funds,

- Monitoring of transactions conducted through systems that enable non-face-to-face operations,

- Risk-based control of services that may become vulnerable to abuse due to newly introduced products and technological developments,

- Screening of customers and transactions against sanction and watch lists.

During the evaluation process, the Compliance Unit may request any information and documents related to the respective responsibilities from all departments of the bank. In this context, the departments from which information and documents are requested are obliged to provide the requested information, documents, and access rights, and to facilitate the Compliance Officer/Compliance Directorate as necessary.

11. Suspicious Transaction Report

In case there is any information, suspicion, or circumstance warranting suspicion that funds or assets involved in transactions conducted at or through the bank are derived from illegal sources or used for illegal purposes; or even if legally obtained, are used by terrorist organizations, those financing terrorism, terrorist acts, or are otherwise connected to terrorism; a **suspicious transaction report** shall be submitted to Financial Crimes Investigation Board (MASAK) regarding the parties involved in the transaction.

No information regarding the submitted suspicious transaction report shall be disclosed to anyone, including the parties involved in the transaction, except for the audit personnel assigned to compliance oversight and the courts during legal proceedings.

Pursuant to Article 10 of Law No. 5549, the bank as a legal entity and its personnel who fulfill the suspicious transaction reporting obligation shall not be held legally or criminally liable in any way for having made such a report.

12. Internal Audit

The purpose of internal audit is to provide assurance to the Board of Directors regarding the overall effectiveness and adequacy of the Compliance Program. The bank ensures that its institutional policies and procedures, risk management, monitoring and control activities, and training programs are reviewed and audited annually using a risk-based approach to assess their adequacy and effectiveness. This includes evaluating the sufficiency and

effectiveness of the risk policy and verifying that transactions are conducted in accordance with the Law, related regulations issued pursuant to the Law, and the bank's policies and procedures.

Within the scope of internal audit operations;

- Deficiencies, errors, and abuses identified as a result of internal audit, along with recommendations and opinions aimed at preventing their recurrence, shall be reported to the Board of Directors.

- When determining the scope of the audit, deficiencies identified in monitoring and control activities, as well as customers, services, and transactions that involve risks, shall be included within the audit scope.

- When selecting units and transactions to be audited, it is ensured that the units and transactions chosen represent a sufficient quantity and quality to cover the entirety of the bank's operations.

Activities within this scope are carried out by the Bank's Inspection Board. Information and statistics related to internal audits are reported annually to Financial Crimes Investigation Board (MASAK) by each group entity in accordance with their obligations.

13. Training

The purpose of the bank's training policy on the prevention of money laundering and terrorist financing is to ensure compliance with the obligations imposed by the Law and other regulations issued pursuant to the Law; to foster a sense of responsibility among personnel regarding the bank's policies, procedures, and risk-based approach; to cultivate an institutional culture; and to keep employees' knowledge up to date.
Training activities related to the prevention of money laundering and terrorist financing are conducted in accordance with the bank's size, business volume, and changing conditions.

The bank's training policy encompasses matters such as the organization and execution of training activities, the responsibilities for conducting these activities, the selection and development of personnel and trainers participating in the training, and the training methods. The bank's training activities are carried out within the framework of an annual training plan approved by the Board of Directors.

Training programs aimed at preventing money laundering and terrorist financing (ML/TF) are prepared by the Compliance Officer in collaboration with the units responsible for training, if any. The effective implementation of the prepared programs is carried out under the supervision and coordination of the Compliance Officers.

All newly hired personnel shall receive training on the prevention of money laundering and terrorist financing (ML/TF) within six months from their start date. This training is planned and delivered by the bank's specialized compliance staff, with the Compliance Unit's expert trainers responsible for conducting the sessions. Training activities shall be conducted in a manner consistent with the institution's size, business volume, and evolving conditions, incorporating regulatory changes, and shall be repeated periodically based on training assessment and evaluation results. In conducting training activities, various methods such as seminars, panel discussions, and remote learning programs are utilized. Training activities are documented and recorded.

Compliance Units and units responsible for training appoint a sufficient number of trainers and ensure they acquire the necessary knowledge and competencies. Priority is given to those who have attended training sessions organized by Financial Crimes Investigation Board (MASAK) during the selection of trainers.

To ensure the specialization of Compliance Officers, Compliance Unit personnel, and training staff in their respective fields, participation in domestic and international training programs and seminars is facilitated.

Information and statistics related to training activities are reported annually to Financial Crimes Investigation Board (MASAK) in accordance with regulatory obligations.

The training provided by the bank to personnel within the target group shall, at a minimum, cover the following topics:

- Concepts of money laundering and terrorist financing,
- Stages and methods of money laundering, including case studies,
- Legislation related to the prevention of money laundering and terrorist financing,
- Risk areas,
- Institutional policies and procedures,
- International regulations in the field of anti-money laundering and combating the financing of terrorism (AML/CFT),
- Principles of customer identification (Know Your Customer - KYC),
- Procedures for reporting suspicious transactions,
- Obligations for retention and presentation of records,
- Obligations to provide information and documents,
- Sanctions applicable in case of non-compliance with obligations.

14. Ongoing (Continuous) Reporting

Pursuant to Article 6 of the Law on the Prevention of Money Laundering, the bank is obliged to report to Financial Crimes Investigation Board (MASAK) any transactions it is involved in or facilitates that exceed the prescribed threshold amount.

The types of transactions subject to ongoing reporting, the manner and timing of information submission, and other procedures and principles related to the implementation shall be determined by the Ministry of Treasury and Finance. The Ministry may issue guidelines for the electronic submission of reports, and notifications shall be made in accordance with these guidelines.

The bank is responsible for establishing and operating the necessary mechanisms to ensure timely and accurate reporting as requested by Financial Crimes Investigation Board (MASAK).

15. Provision of Information and Documents

All types of information, documents, and records in any format, including microfilm, magnetic tape, diskette, CD, and similar media, requested by Financial Crimes Investigation Board (MASAK) or audit personnel must be

provided in full and accurate form, without delay, in the required manner, format, and timeframe. Additionally, all necessary information and passwords to access or render these records readable must be supplied, and all required facilitation must be ensured.

Without prejudice to the provisions regarding the right to defense, information and documents cannot be withheld by invoking provisions set forth in special laws.

16. Obligations for Retention and Presentation of Records

All documents within the scope of the legislation on the Prevention of Laundering Proceeds of Crime must be retained for ten years as follows and must be submitted to the relevant authorities upon request by the competent authorities:

- Documents: from their date of issuance,
- Books and records: from the date of the last entry,
- Customer identification documents: from the date of the last transaction.

Documents and records related to internal reports made to the Compliance Officer, suspicious transaction reports filed, and their attachments, as well as written justifications for suspicious transactions for which the Compliance Officer has decided not to file a report, are also subject to retention and presentation obligations.

17. Financial Sanctions

To the extent that it does not conflict with the laws of the country to which it is subject, the bank operates in compliance with the sanction and embargo measures (international financial sanctions) imposed by UN, USA, EU, and UK.

The bank considers sanction risks during new customer onboarding, updating customer information, and the execution of customer transactions. Within this scope:

- Customers, shareholders, persons acting on behalf of or in the account of the customer, and ultimate beneficial owners are screened against relevant sanction lists.
- Transactions conducted by the customer with or through the bank are examined to determine whether they directly or indirectly involve countries/regions subject to comprehensive sanctions or individuals/entities subject to sanctions.
- Customer acceptance and transaction execution shall not proceed until the evaluation of screening results is completed by authorized personnel responsible for this task.
- Regular screenings are conducted at periodic intervals to verify whether existing customers appear on these lists.

Within this scope, individuals, entities, and organizations listed by the authorities specified below, whose engagement or facilitation of transactions is completely prohibited, as well as those owned, controlled by, or

acting on behalf of these persons and entities, shall not be accepted as customers. In cases where existing customers fall within this scope, the customer relationship shall be terminated immediately, without prejudice to national legal regulations.

- United Nations Security Council Consolidated Sanctions List
- European Union Consolidated Financial Sanctions List
- United States OFAC SDNs (Specially Designated Nationals) List
- United Kingdom OFSI (Office of Financial Sanctions Implementation) Consolidated List

18. Compliance Process and Responsibilities

The bank performs the following actions:

- Establishes policies and procedures encompassing the requirements of national and international regulations related to the prevention of money laundering and terrorist financing (ML/TF).
- Carries out all business and transactions in accordance with the legislation.
- Carries out its internal policies and procedures in accordance with international obligations, applicable legislation and the provisions of the Bank's Compliance Policy.

Establishes ethics and anti-corruption procedures and appropriate channels for employees to report violations. Furthermore, measures are implemented to ensure the protection of employees who report misconduct and the confidentiality of their reports (whistleblowing).

Reports on the issues within the scope of the Bank's Compliance Policy are submitted quarterly by the Compliance Units of the organizations to the member of the Board of Directors to whom they report and at least annually to the Board of Directors.

19. Effective Date and Review

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

20. Document History

Date	Version	Resolution No.	Description
09.01.2023	PLT-GNL-002-v1	YK-2023-07	Initial Release
28.12.2024	PLT-GNL-002-v2	YK-2024-169	Update
30.07.2025	PLT-GNL-002-v3	YK-2025-253	Update