POLICY ON ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

CONTENT

Policy Summary Profile 3
1. INTRODUCTION 4
2. OBJECTIVE 4
3. SCOPE 4
4. REFERENCES 5
5. RESPONSIBILITY 6
6. EFFECTIVE DATE AND AMENDMENTS 6
7. DEFINITIONS AND ABBREVATIONS 6
8. AUTHORITIES and RESPONSIBILITIES 14
8.1. General Responsibilities 14
8.2. Responsibilities of the Board of Directors 14
8.3. Management and Executive Vice Presidents 15
8.4. Responsibilities of Division Managers 15
8.5. Assigning the Compliance Officer/Assistant Compliance Officer and Establishing the Compliance Unit 15
9. THREE LINES of DEFENSE IN COMPLIANCE FUNCTION 16
10. QNB FINANCIAL GROUP 17
10.1. INFORMATION SHARING WITHIN THE FINANCIAL GROUP 17
11. COMPLIANCE PROGRAM FRAMEWORK 18
12. ESTABLISHING INSTITUTIONAL POLICIES and INSTRUCTIONS 19
13. RISK MANAGEMENT ACTIVITIES 20
13.1. Risk-based Approach and Customer Risk Classification Methodology 21
13.2. Customer Risk Classification 22
13.3. Updating KYC Information 22
14. CUSTOMER ACCEPTANCE 22
14.1. KYC Principles 22
14.2. Customer Acceptance and CDD 22
14.3. Situations Requiring CDD 24
14.4. Simplified Due Diligence 24
14.5. Enhanced Due Diligence (EDD) 25
14.6. Additional Measures for High-Risk Customer Groups 25
14.7. Know Your Product/Service 26

Accountable	Approval	Validity Approval	Confidentiality
Internal Control and Compliance Department	Board of Directors	Eda Kocaer	Inhouse

POLICY ON ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

14.8. Identification of UBO 26
14.9. Transactions Requiring Special Attention 27
14.10. Monitoring the Customer Profile and the Transactions 27
14.11. Taking Measures Against Technological Risks 27
14.12. Relationships with Risky Countries 27
14.13. Politically Exposed Persons (PEPs) 28
14.14. Non-Profit Organizations (NPOs) 28
14.15. Correspondent Banking Relationship 28
15. MONITORING and CONTROL ACTIVITIES 28
16. SYSTEM and CONTROLS 29
17. OBLIGATION to REPORT SUSPICIOUS TRANSACTIONS 30
18. TRAINING 30
19. INTERNAL AUDIT 31
20. SANCTIONS 32
21. PERIODICALLY REPORTING 32
22. PROVIDING INFORMATION AND DOCUMENTS 32
23. RECORD KEEPING and SUBMITTING 33
24. DEVIATIONS and EXCEPTIONS 33

POLICY ON ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

Policy Summary Profile

Policy Name	Policy on Anti-Money Laundering and Counter Financing of Terrorism
Function/Division	Enpara Bank A.Ş Financial Crimes Compliance Unit
Date Created	20/09/2024
Next Review Date	12/01/2026
Last Updated Date	10/09/2026
Last Review Date	10/09/2026
Version	3.0

POLICY ON ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

1. INTRODUCTION

Enpara Bank A.Ş. (Enpara Bank) considers and values taking and implementing effective measures is an ethical principle to ensure fully compliance with national and international laws and regulations and sanctions in the fight against money laundering (ML), financing of terrorism (FT), financing the proliferation of weapons of mass destruction (FPWMD) and the fight against other financial crimes.

Enpara Bank is a subsidiary of QNB National Bank Q.P.S.C. (QNB Group) and establishes its institutional policies in line with those of QNB Group and Group Compliance Policy on Anti-Money Laundering and Combating Financing of Terrorism to the extent allowed by national legislation.

Enpara Bank consider this Policy when preparing their additional policies and instructions based on this Policy.

Enpara Bank maintains zero tolerance for knowingly facilitating money laundering, terrorist financing, proliferation financing, sanctions evasion, fraud, or other financial crimes.

2. OBJECTIVE

This Policy aims to establish training, internal audit, monitoring and control and risk management systems with a risk-based approach regarding prevention of ML/FT/FPWMD, ensure compliance with the obligations imposed by the Laws in force in this context, take the necessary measures, including the appointment of Compliance Officers and Assistant Compliance Officers, determine the obliged parties and the procedures and principles for implementation, and establish a common compliance program. It also aims to:

- Prevent the Bank's from being used for money laundering, financing of terrorism and proliferation financing of weapons of mass destruction and other illegal transactions,
- Ensure compliance with applicable laws and regulations, avoid legal sanctions that may be imposed on the Bank and ensure, enhance and protect the credibility, integrity and reputation of the Bank,
- Adopt a risk-based approach and ensure that appropriate strategies are prepared to minimize the risks that may be encountered by the Bank,
- Provide guidance to the senior management as well as the managers and employees of the Bank,
- Ensure that the Bank employees are aware of the rules regulating the fight against Money Laundering, Financing of Terrorism and Financing of the Proliferation of Weapons of Mass Destruction (ML/FT/FPWMD), determine the controls, measures, operational rules and responsibilities within the Bank and ensure that such employees gain awareness and take responsibility for compliance with these rules.

3. SCOPE

This policy covers all business units enters into force upon approval by the Board of Directors (BoD) of Enpara Bank.

This policy applies to all employees, contractors, outsourced service providers, temporary staff, consultants, and third parties acting on behalf of Enpara Bank.

Accountable	Approval	Validity Approval	Confidentiality
Internal Control and Compliance Department	Board of Directors	Eda Kocaer	Inhouse

POLICY ON ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

Institutional Policy establishes a common standard for Enpara Bank with a risk-based approach to ensure compliance with the Laws and related legislation aimed at prevention of ML/FT/FPWMD.

This Policy includes risk management, monitoring and control, training and internal audit policies, including Politically Exposed Persons (PEPs) and Know Your Customer (KYC) principles, Sanctions Policy, along with the policies on information sharing within QNB Financial Group.

This Policy was prepared in accordance with local and international legislation, Financial Group Compliance Policy and QNB Group policies on the prevention of ML/FT/FPWMD. In case of any non-compliance, enhanced measures as allowed by the local legislation should be applied.

Enpara Bank's risk appetite is set out in the Risk Appetite Statement as an annex to this Policy. It sets out the Enpara Bank's willingness to assume certain risks and avoid or mitigate other risks to achieve its strategic objectives and business plan. The Risk Appetite Statement includes the ML/FT/FPWMD and Sanctions risk appetite and is an integral and fundamental part of how Enpara Bank manages risk.

Working Principles and Procedures of the Anti-Money Laundering and Financing of Terrorism (AML/CFT) Committee was prepared in order to increase the effectiveness of the implementation of this Policy and to ensure that decisions are taken when necessary, regarding ML/FT/FPWMD risks.

4. REFERENCES

Obligations regarding prevention of ML/FT/FPWMD, risks and penalties in case of violation of such obligations and prevention strategies are set out in the laws in effects and related regulations, communiqués and guidelines. Principle legislation is listed below:

Presidential Decrees:

- Presidential Decree no.1 on Presidency Organization (relevant articles: 231, 232)

Laws:

- Law no. 5549 on Prevention of Laundering Proceeds of Crime
- Law no. 6415 on the Prevention of the Financing of Terrorism
- Law no. 7262 on the Prevention of the Financing of Proliferation of Weapons of Mass Destruction
- Article 282 of the Turkish Criminal Law No.5237

Regulations:

- Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism
- Regulation on Program of Compliance with Obligations of Anti-Money Laundering and Combating the Financing of Terrorism
- Regulation on Postponement of Transactions Within the Scope of Prevention of Laundering Proceeds of Crime and Financing of Terrorism

POLICY ON ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

- Regulation on the Procedures and Principles Regarding the Implementation of Law on the Prevention of the Financing of Terrorism
- Regulation on the Procedures and Principles Regarding the Implementation of the Law on the Prevention of the Proliferation Financing of Proliferation of Weapons of Mass Destruction

Communiques:

- MASAK General Communique No.5
- MASAK General Communique No.7
- MASAK General Communique No.8
- MASAK General Communique No.12
- MASAK General Communique No.13
- MASAK General Communique No.19
- MASAK General Communique No.21
- General Communique STR regarding Financing of Terrorism

In addition to the local legislation, the Bank adopts recommendations, guidelines and standards published by international regulatory authorities and institutions listed below:

- FATF Recommendations and Implementation Methodologies,
- Basel Principles (Know Your Customer Principles for Banks),
- EU Directives,
- UNSC Resolutions,
- Wolfsberg Principles,
- EGMONT Group.

5. RESPONSIBILITY

The Internal Control and Compliance Department is responsible for the development, implementation, and, where necessary, periodic review and update of this Policy.

6. EFFECTIVE DATE AND AMENDMENTS

This Policy and any amendments thereto shall enter into force upon approval by the Board of Directors, following the review and recommendation of the Audit Committee.

7. DEFINITIONS AND ABBREVATIONS

MASAK: MASAK (Financial Crimes Investigation Board) is the main service unit within the Ministry of Treasury and Finance and reports directly to the Minister of Treasury and Finance.

FATF (Financial Action Task Force): FATF is an intergovernmental organization established by the G7 member countries in Paris in 1989. Türkiye is a member of FATF. FATF aims to determine the international standards and promote the effective implementation of legal, regulatory and operational measures related to the fight against ML/FT/FPWMD and against other threats to the integrity of the international financial system.

Obliged party: The obliged party is defined in subparagraph d of paragraph 1 of article 2 of the Law No. 5549 on Prevention of Laundering Proceeds of Crime and in paragraph 1 of article

POLICY ON ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

4 of the Regulation on Measures regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism.

KYC Principles: KYC principles are given under the articles between articles 5 and 26 of section 3 of the Regulation on Measures regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism.

Compliance Program: It refers to the measures to be taken for AML/CFT purposes as determined within the scope of the Regulation on Program of Compliance with Obligations of Anti-Money Laundering and Combating the Financing of Terrorism.

Financial Institution: It refers to banks, institutions other than banks who have the authority to issue bank cards or credit cards, authorized exchange offices given in legislation on foreign exchange, financing and factoring companies, Capital Markets Brokerage Houses and portfolio management companies, payment service providers and electronic money institutions, insurance, reinsurance and pension companies, and insurance and reinsurance brokers, financial leasing companies, furnishing settlement and custody services within the framework of capital markets legislation, precious metals intermediary institutions, crypto asset service providers and T.C. Post and Telegraph Organization (PTT) limited to banking activities.

Financial Group: It means a group consisting of financial institutions located in Turkey and their branches, agencies, representatives and commercial agents and similar affiliated units which are affiliated to or controlled by a parent company whose head office is in Türkiye or abroad.

Compliance Officer: The compliance officer is employed and authorized as required to ensure compliance with the obligations stated in the Law No. 5549 on Prevention of Laundering Proceeds of Crime and in the legislation implemented as per the Law.

Assistant Compliance Officer: The assistant compliance officer has the conditions and qualifications of a compliance officer, is assigned as the company personnel exclusively and reports to the Compliance Officer to carry out the compliance program.

Compliance Unit: This unit reports to the Compliance Officer and consists of the personnel assigned to carry out the compliance program. **(Financial Crime Compliance Division)**

Board of Directors: It is the decision-making body with the highest level of executive authority within the institution (BoD).

Senior Executive: According to the Regulation on Corporate Governance Principles of Banks, it refers to the bank's general manager, executive vice presidents (EVPs), managers of units within the scope of internal systems, and—even if employed under different titles—managers of units other than advisory units, who hold positions equivalent to or higher than an executive vice president (EVP) in terms of their authorities and duties.

Senior Management: According to the Regulation on Corporate Governance Principles of Banks, it refers to the Board of Directors and senior executives of the bank.

POLICY ON ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

Audit Committee: According to Article 24 of the Banking Law No. 5411, refers to the committee consisting of at least two non-executive members of the board of directors, established to assist the board of directors in its audit and supervision activities.

Parent Financial Institution: QNB Bank A.Ş.

Institutions in the Financial Group: They are the financial institutions resident in Türkiye within QNB Financial Group.

QNB Financial Group: QNB Financial Group is comprised of QNB Bank, which is the parent financial institution, along with its subsidiaries and affiliates and the financial institutions located in Türkiye that are affiliated to or controlled by QNB Group, based on the financial group definition.

Financial Group Compliance Officer: QNB Bank Compliance Officer (They are assigned as the parent financial institution's compliance officer to carry out the compliance program at Financial Group level.)

Financial Group Assistant Compliance Officer: QNB Bank Assistant Compliance Officer (They are assigned as the parent financial institution's assistant compliance officer to carry out the compliance program at Financial Group level.)

Financial Group Compliance Unit: It refers to QNB Bank Financial Crime Compliance Division.

Financial Group Compliance Policy: Within the scope of the compliance program, this policy is prepared by taking into account the size, business volume and nature of the transactions of the enterprises and by considering the issues determined for the national risk assessment. At a minimum, it includes risk management, monitoring and control, training and internal audit policies and policies on information sharing for the Group.

Revenue of Crime: It refers to the asset value obtained through criminal activity.

Laundering Crime: Laundering crime is regulated under article 282 of the Turkish Criminal Law no.5237 dated September 26, 2004. This crime is generally defined as all kinds of transactions aimed at hiding the illegal sources of revenues obtained through predicate crimes and to make such revenues appear as if they were obtained from legal sources.

Article 282 of our Turkish Criminal Code No: 5237 (Laundering of assets arising from crime);

- The opinion that the assets values originating from a crime that requires a prison sentence of six months or more are taken abroad or concealing their illegitimate source or that they have been obtained through a legitimate way. The person who subjected him to various procedures in order to arouse him is punished with imprisonment from three to seven years and a judicial fine of up to twenty thousand days.
- The person who purchases, accepts, holds or uses the value of the property that is the subject of this crime, without participating in the commission of the crime in the first paragraph, will be sentenced to imprisonment from two years to five years. punished with a penalty.

POLICY ON ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

- If this offense is committed by a public official or by a person of a certain profession during the execution of this profession, the penalty shall be increased by half.
- In the event that this offense is committed within the scope of the activity of an organization established to commit a crime, the penalty shall be increased one-fold.
- Due to the processing of this crime, legal measures specific to these persons are determined.

Before the start of prosecution for this offense, the offense shall not be imposed on the person who provides the seizure of the assets of the offense or facilitates his / her capture by informing the competent authorities of the crime.

Suspicious Transaction: It refers to cases where there is any information, suspicion or reasonable grounds to suspect that the asset, which is subject to the transactions carried out or attempted to be carried out within or through the obliged parties, was acquired through illegal ways or used for illegal purposes and is used, in this scope, for terrorist activities or by terrorist organizations, terrorists or those who finance terrorism.

Suspicious Transaction Reporting (STR): Suspicious transactions are reported to MASAK by the obliged parties regardless of the transaction amount. Compliance Officer is responsible for this reporting.

Terrorism Financing Crime: It refers to providing or collecting funds for a terrorist or terrorist organizations for the purpose of being used wholly or partially to perform the acts regulated as a crime as per article 3 of the Law no. 6415 on the Prevention of the Financing of Terrorism, or to do so knowingly and willingly, even without being linked to a specific act.

Financing the Proliferation of WMD: It is the violation of Law No. 7262 on the Suppression of the Financing of the Proliferation of Weapons of Mass Destruction and United Nations Security Council (UNSC) sanction decisions aimed at prevention of financing the proliferation of WMD.

Money Laundering/ Financing of Terrorism/ Financing of Proliferation of Weapons of Mass Destruction: ML/FT/FPWMD

Fund: It refers to bank loans, bank and traveler's cheque, remittance, securities, stocks, collateral, bonds, bills, policies, letters of credit and similar securities, the value of which can be represented by money or money itself in any kind of form and all kinds of goods, rights, receivables movable or immovable, tangible or non-tangible and all kinds of documents, including electronic or digital, that confirm and represent property rights or interest on such goods, rights, receivables.

Asset: Asset is defined as funds and income partially or fully owned or possessed by, or directly or indirectly controlled by, a real or legal entity, and the benefits and value derived from them or their conversion, funds and income partially or fully owned or possessed by a real or legal entity acting on behalf or account of them, and the benefits and value derived from them or their conversion to each other.

Asset freeze: Asset freeze refers to removal or restriction of the power of disposition on the assets in order to prevent the destruction, consumption, conversion, transfer, relocation and assignment of assets and other saving transactions (within the framework of exceptions).

POLICY ON ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

Risky countries: These are the countries which do not have an adequate level of AML/CFT regulations, do not cooperate enough to fight such crimes or are deemed risky by authorized international organizations (as announced by the Ministry).

Risk: It refers to the possibility of financial loss or reputation loss that the obliged or their personnel may incur in case the services provided by the obliged are used for money laundering or terrorism financing or in case the obliged fail to fully comply with the Law or with the obligations set out by the regulations and communiques issued as per the Law.

Service risk: It refers to the risk that the obliged parties may encounter within the scope of services such as non-face to face transactions, private banking, correspondent banking, etc. or new products to be presented via developing technologies.

Customer risk: It refers to exploitation of obliged parties due to the fact that the customer's business line allows high amount of cash usage, trading of goods of high value or international fund transfer or the customer or anyone else acting on behalf or account for the customer is involved in money laundering or terrorism financing activities.

Country risk: It refers to the risk that the obliged parties may encounter due to business relations and transactions with citizens, companies or financial institutions in countries which do not have an adequate level of AML/CFT regulations, do not cooperate enough to fight such crimes or are deemed risky by authorized international organizations (as announced by the Ministry).

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

Ultimate Beneficial Owner (UBO): UBO is defined legally as real person or persons who has ultimate control over or who has ultimate influence over real persons, legal entities or unincorporated organizations on whose behalf a transaction is being conducted within and obliged party,

It may be the real person who ultimately owns or controls any customer, whether a real person or a legal entity, or it may be the real person on whose account transactions or activities are carried out. The UBO is in any case a real person or persons.

In other words, UBO refers to:

- For an account, the individual(s) who ultimately owns or has effective control over the account,
- For a transaction, the individual(s) for whom or on whose behalf the transaction is or will ultimately be performed (whether by proxy, trusteeship or mandate, or by any other form of representation),
- For a legal entity or legal arrangement, the person/persons who ultimately owns or has effective control over the legal entity or the legal arrangement.

UBO of an account includes any person whose instructions any of the following are accustomed to act:

POLICY ON ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

- Signature authority/authorities of the account,
- Any person who directly or indirectly gives instructions to the signature authorities (or one of them).

In terms of determining the UBO for legal entities, three main situations are considered ownership (shareholding) relationship, ultimate control and senior managing official. In this context, the definition of UBO for a legal entity includes;

- For high-risk customers, real person(s) who, directly or indirectly, owns or controls at least 10% of the shares or voting rights of the legal entity,
- For low and medium risk customers, real person(s) who, directly or indirectly, owns or controls at least 20% the shares or voting rights of the legal entity,
- Real person(s) who, directly or indirectly, otherwise exercises control over the legal entity's management,
- Real person(s) holding the position of senior managing official, whose authorization to represent the legal entity is/are registered to Trade Registry.

Within the scope of permanent business relationship with other legal entities and unincorporated organizations, necessary measures are taken in order to detect the real person(s) who is/are ultimately controlling the legal entity. In case where the beneficial owner is not detected, the real person(s) holding the position of senior managing official within them are considered as beneficial owner.

Shell bank: It means a bank which does not have any physical office in any country, does not employ full time staff and is not subject to control and authorization of an official authority in terms of banking transactions and registrations.

PEPs: Politically/Publicly Exposed Persons (PEPs) are defined as high-level real persons to whom an important public duty has been entrusted to them by election or appointment in the past or now within the country or in a foreign country; and members of the board of directors of international organizations, senior executives and other persons who have served equivalently to them. PEPs are addressed under three categories:

- Foreign PEPs; high-level real persons to whom an important public duty has been entrusted by election or appointment in a foreign country,
- Domestic PEPs; high-level real persons to whom an important public duty has been entrusted by election or appointment within the country,
- International Organization PEPs; members of the board of directors of international organizations, senior executives and other persons who have served equivalently to them.

PEPs also include the persons who serve important public duties such as:

- Heads of state or government, ministers, deputy ministers (senior officials),
- Members of the parliament,
- Judges who serve at court of accounts, supreme court, constitutional court or higher level of judicial bodies and whose decrees cannot be appealed unless exemption,
- Members of Board of Directors of Central Banks,
- Ambassadors, Deputy Chief of Mission,
- Senior judicial, administrative or military officials,

POLICY ON ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

- Senior persons serving in administration, management or audit bodies of governmental agencies,
- Government business enterprises,
- Senior politicians,
- Senior officials of political parties.

Family members of PEPs include the persons related to the PEP up to second degree via bloodline or marriage. These are:

- Mother and father,
- Spouse and spouse's family,
- Children, step children, siblings and spouses of these persons, grandchildren.

Close associations/partners of PEPs include the person/persons who have a partnership or business relationship with the PEP in a legal or judicial arrangement or who is/are the UBO of a legal entity or legal arrangement owned or effectively controlled by the PEP.

PEP Entity refers to any company, business or other legal entity that has been formed by, or for the benefit of a PEP, has a key controller who is a PEP and has a PEP that is an UBO.

Risk-Based Approach: This approach is defined as measures and practices to identify, assess, understand and mitigate ML/FT/FPWMD risks in terms of the Risk Assessment Methodology for ML/FT/FPWMD.

Know Your Customer (KYC): Obliged parties have to determine the identities of the persons making transactions or persons on whose behalf and account transactions are made and take other necessary measures before performing transactions made or mediated by them within the scope of KYC principles. This principle aims to protect the obliged parties from persons and acts related to ML/FT/FPWMD, to provide them with adequate information about customers and their activities in terms of effective management of risks, to apply the required measures to obtain such information and to use this information effectively by taking additional measures considered as "advanced measures" if necessary. KYC serves as the basis for all other processes related to the prevention of relevant crimes.

Customer Due Diligence (CDD): It refers to fulfilling the liabilities regarding identity authentication and verification and taking the measures for this purpose (confirming the authentication as required, determining whether the customer is acting on his/her own behalf or on behalf of another person, identifying the UBO, collecting information about the purpose and nature of the business relationship, etc.).

On-going Monitoring: In relation to a customer, this refers scrutinizing transactions under the business relationship, customer's business and risk profile, sources of income and wealth, and when required, a review of the records by the obliged parties to keep the records up-to-date and relevant.

KYC Review: It refers to regularly updating the customer information as per ML/FT/FPWMD risk classification to ensure that such information is valid, accurate and up-to-date.

Source of Wealth (SoW): It refers to the source of wealth (total assets) of the customer or

POLICY ON ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

UBO. When identifying the SoW, financial institutions should determine why the customer owns the relevant assets and how he/she collected such assets.

Source of Funds (SoF): It refers to the source of money or financial assets of the customer. When identifying the SoF, financial institutions should try to understand the activity that enabled the collection of such funds (for ex: selling a house, inheritance, etc.).

High Net Worth Individuals (Private banking): Banking services that banks offer exclusively to customers with a certain profile are referred to as private banking. Within private banking, these are customers whose assets such as deposits, investments, etc. have a very high value. (The determined lower limit can be updated in line with the evaluations of the relevant business unit.)

Non-Resident Customer: According to the local legislation, place of residence refers to a location where one intends to stay permanently. Persons whose official place of residence is in Türkiye and who reside in Türkiye continuously for more than six months in a calendar year are considered to be residents of Türkiye. Below stated foreigners are not considered to be residents even if they stay in Türkiye for more than six months:

- Business persons, scientists, experts, civil servants, members of press, persons in similar conditions and persons who came to Türkiye for education, treatment, vacation or travel,
- Persons who are detained or who stayed in Türkiye due to force majeure such as imprisonment, conviction or sickness.

Accordingly, non-resident customers include but are not limited to:

- Persons who do not have a residence permit in Türkiye,
- Companies and organizations established outside Türkiye,
- Foreign embassies and consulates, representatives of international and regional organizations and their foreign employees,
- Foreigners who have visitor visa within the non-resident period,
- Students who study in national schools and universities and who came to Türkiye primarily to study,
- Foreigners who came to Türkiye to receive treatment in national or touristic hospitals,
- Foreign workers who work seasonally in Türkiye within the non-resident period,
- Foreign companies which are licensed by a foreign institution outside Türkiye, which fully or partially belong to the companies or organizations in Türkiye, which do not conduct any activity in Türkiye or have not conducted any activity in Türkiye for less than a year,
- Foreign companies who have carried out activities within the scope of special agreements with the government or other residents in Türkiye for less than a year.

Virtual Assets/Virtual Asset Service Providers: Virtual assets are any valuables that replace currency, can be exchanged or transferred digitally, can be used for payment or investment purposes, are not linked to banknotes or other monetary tools. Virtual asset service providers are real persons or legal entities involved in one or more virtual asset services on behalf or in favor of a business, another real person or another legal entity.

POLICY ON ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

8. AUTHORITIES and RESPONSIBILITIES

8.1. General Responsibilities

All employees are responsible for prevention of ML/FT/FPWMD and other financial crimes.

It is imperative that all employees and members of management within Enpara Bank are aware of and appropriately implement the policies and procedures in place to protect the group against ML/FT/FPWMD activities.

All executives and employees of the Enpara Bank must be informed about the policies and instructions as part of their organizational responsibilities and they must comply with such policies and instructions.

All employees within Enpara Bank have a responsibility to assist in identifying ML/FT/FPWMD activities. Actions and transactions that are considered as or that facilitate ML/FT/FPWMD and other financial crimes should not be performed. Therefore, all employees should be aware that a failure in implementing the institutional policies and instructions may result in gross misconduct and disciplinary proceedings.

8.2. Responsibilities of the Board of Directors

Enpara Bank prepare a separate compliance program considering the standards and policies set out by this Policy. BoD is ultimately responsible for carrying out the whole compliance program adequately and efficiently for the scope of nature of activities of the Enpara Bank.

BoD is authorized to and responsible for assigning compliance officer and assistant compliance officer, explicitly determining in written form the authorities and responsibilities of the compliance officer and the compliance unit, ratifying institutional policies, annual training programs and amendments to be made in accordance with developments, assessing the results of risk management, monitoring and control and internal audit activities carried out under the scope of the compliance program, taking required measures for timely elimination of the detected errors and deficiencies, and ensuring an efficient and coordinated performance of all the activities carried out under the scope of the compliance program.

Risk management and monitoring and control activities related to ML/FT/FPWMD are carried out by the Compliance Officer under the supervision, audit and responsibility of the BoD.

BoD assign a Compliance Officer and at least one Assistant Compliance Officer to manage compliance program and the potential risks related to ML/FT/FPWMD with a robust risk-based framework.

BoD also ensures that the Compliance Officer has the authority to make decisions with an independent will, to request all kinds of information and documents related to his/her field of duty from all units of the Bank and to access them in a timely manner.

BoD may transfer some or all of its authorities within the scope of this Policy two to one or more of its members residing in Türkiye (explicitly and in written form). This kind of an authority transfer cannot remove the authority of the BoD in this field.

POLICY ON ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

In order to ensure that the Compliance Officer can effectively fulfill his/her duties and responsibilities, the BoD ensure that a Compliance Unit/Department directly reporting to the Compliance Officer and tasked with the execution of the implementation of the compliance program is formed and sufficient personnel and resources are allocated to Compliance Unit/Departments by considering issues such as business size, transaction volume, the number of branches and employees or criticality of possible risks.

8.3. Management and Executive Vice Presidents

Senior Executives of the Enpara Bank report to the BoD and their duties and responsibilities within the scope of this Policy as approved by the BoD are:

- Ensuring that the business processes carried out by the business units reporting to him/her and the codes of conduct comply with this Policy,
- Ensuring that the engagements and transactions required to implement this Policy are carried out by the employees accurately and in line with the regulations,
- Ensuring that the measures to mitigate and manage the potential risks for the institutions are implemented timely and effectively.
- Granting prior approval for initiating or continuing a business relationship with Correspondent Banks, Non-Profit Organizations, or PEPs that are classified as high-risk.

8.4. Responsibilities of Division Managers

Division Managers across Enpara Bank bear the responsibility of proper application of the institutional policies within their departments. They shall ensure that their all employees and their respective business department/units implement all necessary KYC processes and procedures correctly and in accordance with their institutional policies.

8.5. Assigning the Compliance Officer/Assistant Compliance Officer and Establishing the Compliance Unit

Compliance Officers are responsible for conducting ML/FT/FPWMD risk assessments, implementing compliance program, reporting suspicious transactions, implementing relevant policies and instructions in line with relevant local laws, QNB Group Policies, Financial Group Compliance Policy and regulations and recommendations of the FATF and the Basel Committee.

The Compliance Officer and Assistant Compliance Officer of Enpara Bank have been appointed to carry out the Compliance Program.

Compliance Officer’s duties and responsibilities are:

- Carrying out the necessary engagements to ensure compliance with the Law and relevant regulations on ML/FT/FPWMD and ensuring communication and coordination with MASAK,
- Preparing institution policies and instructions and submitting the policies of the institution to the board of directors for approval,

- Preparing risk management policy and performing risk management activities,
- Preparing monitoring and control policies and carrying out relevant activities,
- Conducting inquiries, within the scope of his/her authority and available resources, into transactions that are either reported to him/her or identified ex officio as potentially suspicious; assessing the information and findings obtained; and reporting to the Presidency any transactions determined to be suspicious,
- Taking the necessary measures to ensure the confidentiality of notifications and other relevant matters,
- Maintaining regular records of information and statistics related to internal audit and training activities, and submitting them to the Presidency within the timeframes specified in the applicable laws and related regulations,
- Presenting to the Board of Directors the training program initiatives aimed at preventing ML/FT/FPWMD, and ensuring the effective implementation of the approved training program.

Compliance Officer reports via Audit Committee to the Enpara Bank's BoD and/or BoD member/s residing in Türkiye as authorized by the BoD.

Compliance Officers and Assistant Compliance Officers shall have sufficient seniority, knowledge and authorization to fulfill their responsibilities independently.

Enpara Bank Financial Crimes Compliance Department, which reports directly to the Enpara Bank Compliance Officer, operates as the Compliance Unit.

9. THREE LINES of DEFENSE IN COMPLIANCE FUNCTION

With this Policy, Enpara Bank establishes an effective risk management with a strong governance structure, taking into account the size, business volume, nature and characteristics of the transactions carried out. "Three Lines of Defense" approach is implemented, which enables the determination of duties and responsibilities in the functioning of the established structures and processes. It is essential that all three lines act in coordination and communication.

- **First Line of Defense:**

  First line of defense includes related Business Units and their employees who carry out transactions related to products and services offered to customers, including the customer acquisition process (including factors such as direct communication with customers, product ownership, customer information ownership).

- **Second Line of Defense:**

  Second line of defense covers compliance units and internal control functions to ensure that necessary measures are taken to monitor and control risks and to mitigate risks, especially the determination of policies and strategies to identify, rate, classify and develop assessment methods for the risks that organizations may face within the scope of prevention of ML/FT/FPWMD.

It covers making the necessary controls and warnings regarding the engagements and transactions carried out by the First Line of Defense, providing training and information to raise awareness, performing analyses based on risk management control results and assessments based on control results and developing conditions, reporting risk monitoring and assessment results to the BoD via the Audit Committee regularly.

It also involves determining the risk appetite within the scope of prevention of ML/FT/FPWMD.

- **Third Line of Defense:**

Third line of defense refers to the internal audit units of institutions. They provide recommendations regarding the adequacy and effectiveness of management of ML/FT/FPWMD risks and give assurance to the BoD in this context.

10. QNB FINANCIAL GROUP

The fact that a parent company holds the power to appoint or discharge the majority of the executive board members constituting the basis for decision making, through directly or indirectly holding the majority of the capital, without seeking the condition to hold at least fifty one per cent of the capital, or through holding the privileged shares without having the majority of the capital, or through possessing the majority of the right to vote depending on agreements made with other shareholders, or through any kind of way demonstrates that a financial institution is affiliated to or controlled by the parent company.

Financial Group consists of financial institutions resident in Türkiye and their branches, agencies, representatives and commercial agents and similar affiliated units which are affiliated to or controlled by a parent company whose head office is in Türkiye or abroad. If the parent company is a financial institution, it is deemed as the parent financial institution; otherwise, one of the financial institutions affiliated to or controlled by the parent company is determined as the parent financial institution.

QNB Bank reports the titles, the shareholding and controlling information and contact information of the parent company of the financial group, the parent financial institution and headquarters of other financial institutions to MASAK. MASAK may determine another financial institution as the parent financial institution instead of the parent financial institution determined and reported to MASAK.

10.1. INFORMATION SHARING WITHIN THE FINANCIAL GROUP

QNB Financial Group share information relating to Customer Due Diligence, accounts and transactions in order to ensure that the measures in the scope of this Policy are taken at the group level.

This Policy covers securely sharing information and documents obtained within the scope of customer identification regarding prevention of ML/FT/FPWMD as well as issues deemed risky as a result of risk management, monitoring and control activities among the Financial Group and taking necessary measures for confidentiality.

POLICY ON ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

Information sharing is carried out under the supervision and responsibility of Compliance Officers and/or Assistant Compliance Officers. Enpara Bank is also informed about the information sharing between the Financial Group.

It may also share information on the following issues;

- Obtaining additional information and performing evaluations in case of a conclusion that the transactions performed or attempted during or after the establishment of a business relationship may create risks for the Financial Group,
- Conducting risk assessments regarding the customers with whom it is decided not to establish a permanent business relationship in terms of ML/FT/FPWMD risks,
- Taking measures when required against violation of international sanctions.

Employees working in the institutions within the Financial Group cannot disclose the information they have learned and cannot use this information for the benefit of themselves or third parties. In this context, sanctions in the relevant laws shall be applied to those who disclose the information that should be kept confidential.

Confidentiality provisions written in special laws shall not be applied to information sharing within the Group. Information shared within the Financial Group cannot be transferred on to the parties other than legally authorized bodies.

Financial institutions within the Financial Group cannot share information on the fact that suspicious transaction report has been submitted.

The financial group compliance officer and the executive board of the parent financial institution is also be responsible for taking the necessary measures to securely share information within the group. This responsibility is also applied for compliance officers and BoD the institutions within the Financial Group.

11. COMPLIANCE PROGRAM FRAMEWORK

This Policy sets out the common standards within the framework of the compliance program established with a risk-based approach to ensure Enpara Bank's compliance with the regulations related to the prevention of ML/FT/FPWMD. Enpara Bank are responsible for taking and implementing the following minimum measures to comply with this Policy, considering the legal obligations in their field of activity:

- Assigning the Compliance Officer and Assistant Compliance Officer and establishing the Compliance Unit,
- Preparing the policies and instructions for prevention of ML/FT/FPWMD,
- Carrying out risk management activities,
- Carrying out monitoring and control activities,
- Carrying out training activities,
- Carrying out internal audit activities,
- Taking the measures for preparation of policies and instructions on information sharing about KYC, accounts and transactions within the group in a secure manner.

POLICY ON ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

12. ESTABLISHING INSTITUTIONAL POLICIES and INSTRUCTIONS

This policy is established in writing in line with the Law and the regulations and communiqués issued as per the Law, under the supervision and coordination of the Compliance Officers.

Enpara Bank informs its personnel about institutional policies.

Enpara Bank prepare policies and instructions based on this policy by considering issues such as business size, transaction volume, the number of branches and employees or criticality of possible risks in a way that complies with the QNB Group and Financial Group Compliance Policy. At minimum, this policy include; risk management, monitoring and control, training and internal audit activities, principles for intra-group information sharing.

This Policy, cover risk identification, assessment, monitoring and mitigation activities for the risks of violation, failure to implement and avoidance of asset freezing decisions within the scope of Law No 6415 on the Prevention of Financing of Terrorism and Law No 7262 on the Prevention of Financing the Proliferation of Weapons of Mass Destruction, and advanced controls for the implementation of such sanctions. In the monitoring and control activities within the scope of the institutional policy, measures are taken to continuously monitor customers and transactions, taking into account asset freezing decisions and potential matching criteria. In this context, the sender and recipient information in electronic transfer messages are also taken into consideration.

Issues stipulated within the scope of local risk assessment are taken into account while preparing this policy.

With institutional policies, it is ensured that company employees are informed and aware of below issues;

- Compliance with the liabilities regarding prevention of ML/FT/FPWMD,
- Implementing the asset freeze decisions effectively and carrying out the required monitoring and control activities,
- Assessing the customers, transactions and services with a risk-based approach,
- Determining the strategies, internal controls and measures, operation rules, and responsibilities to mitigate potential risks.

Issues such as who is responsible for the measures and operational rules and who or which unit is responsible for approving, performing, reporting and monitoring the transactions based on certain risk limits are clearly defined in the institutional policies and procedures as per the institution policy. Duties and authorizations are assigned to ensure that the employee who will be responsible for monitoring, controlling and auditing the transactions and work flows of the Bank according to risks is not the same employee who performs these transactions.

Recommendations, principles, standards, and guidelines introduced by other local and international organizations are also used while preparing the Policy and instructions provided that they do not violate local regulations.

POLICY ON ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

13. RISK MANAGEMENT ACTIVITIES

The aim of risk management is to identify, assess, monitor, assess and reduce the risks associated with ML/FT/FPWMD that financial institutions may be exposed to.

The risk management policy covers, at a minimum, the internal procedures and operational rules related to KYC measures. To this end and within the scope of prevention of ML/FT/FPWMD, QNB Group establishes its Customer Acceptance Policy within the boundaries of this Policy to enforce the KYC principle as mandated by local and international regulations.

Risk management activities include, at a minimum, the activities listed below:

- 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; taking necessary measures for mitigating risks; reporting in a way that warns related units; carrying out the transaction with ratification of senior authorities and controlling it, when necessary,
- Questioning retrospectively the coherency and efficiency 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 BoD.

Enpara Bank evaluates alarms regarding risky transactions generated by scenarios to be defined in software products by using them to identify risky transactions. Enpara Bank ensure that relevant units are informed to take necessary measures to mitigate the risks identified as a result of such engagements.

Risk management activities are monitored continuously according to changing and developing conditions. Necessary improvement engagements are performed by following up recommendations, principles, standards, and guidelines introduced by local regulations and international organizations.

The Bank conducts and documents an Enterprise-Wide Money Laundering and Terrorist Financing (ML/TF) Risk Assessment at least annually and whenever significant changes occur in products, services, delivery channels, customer segments, jurisdictions or applicable regulatory requirements.

The assessment shall consider:

- Customer risk;
- Product and service risk;
- Geographic and jurisdictional risk;

- Delivery channel risk;
- Emerging threats and typologies;
- Regulatory findings and enforcement actions;
- Internal audit findings;
- MASAK National Risk Assessment Report and other competent authority guidance.

The outcomes of the assessment shall be reviewed by Senior Management and reported to the Board and relevant Committees. Appropriate controls should be implemented to mitigate identified ML/TF risks.

13.1. Risk-based Approach and Customer Risk Classification Methodology

Enpara Bank implements a proactive risk-based approach to manage and mitigate ML/FT/FPWMD risks to ensure that the measures taken are proportionate to the risks identified and are implemented in the most effective manner according to priorities, with maximum attention paid to the highest risks that may be encountered. This process involves acknowledging the existence of risks, assessing risks and developing strategies to manage and mitigate identified risks.

Assessment of ML/FT/FPWMD risks includes the application of appropriate assessment methods when establishing a permanent business relationship and the ongoing assessment and monitoring of transactions throughout the business relationship.

Enpara Bank implements an appropriate policy to mitigate ML/FT/FPWMD risks considering business size and volume, business profile, risk profile and nature of transactions in accordance with QNB Group's Risk Assessment Methodology and the requirements of national regulations.

Enpara Bank classifies its customers according to the risk profiles which are assessed based on the following factors with a risk-based approach:

- Customer Risk: Determining the source of income or type of activity,
- Geographic/Regional Risk: Involvement of customers with regions associated with ML/FT/FPWMD or other illegal activities,
- Product Risk: Specific products and service types,
- Delivery Channel Risk: How the service is offered

Customer Due Diligence is carried out within the scope of above-mentioned risk factors as per the risk classification of customers.

Enhanced Due Diligence is applied for customers that are classified as high risk. It is also applied for the other customers who are assessed as high risk independently from the risk classification and these customers are subject to ongoing monitoring.

Within the framework of the risk-based approach, separate processes are applied for certain high risk customer categories such as PEPs and Non-Profit Organizations (NPOs).

POLICY ON ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

13.2. Customer Risk Classification

The information obtained during the process of establishing a permanent business relationship with new customers or the information of existing customers that is changed/updated according to Risk Assessment Methodology criteria and certain weight calculations constitute the risk profiles of customers.

Enpara Bank classifies its customers as high, medium and low risk.

Enpara Bank should identify, assess, monitor and update the ML/FT/FPWMD risks yearly and regularly as per the National Risk Assessment.

13.3. Updating KYC Information

The information and documents of existing customers obtained within the scope of KYC should be regularly reviewed and updated. The update period should be applied as follows according to the risk levels of the customers within the scope of ML/FT/FPWMD;

- Between 12-18 months for high risk customers,
- Between 24-30 months for medium risk customers,
- Between 36-42 months for low risk customers.

14. CUSTOMER ACCEPTANCE

14.1. KYC Principles

In general, KYC principle refers to paying attention to obtaining complete and accurate information about customers and adopting all necessary measures to comply with local and international regulations.

Collecting adequate information and using this information effectively in terms of KYC constitutes the basis for all processes regarding the prevention of ML/FT/FPWMD. It also ensures that the relevant institution identifies suspicious actions and offers protection against fraud attempts. It protects the institution from financial and reputation risks.

Applying the KYC principle and performing an adequate CDD are the basis for protecting against ML/FT/FPWMD and other financial crimes and effectively managing possible risks.

14.2. Customer Acceptance and CDD

Within the scope of the Law no.5549 and related regulations, based on KYC Principles, documents for identity authentication, transaction types that require authentication, their monetary limits and other principles and procedures about KYC and other issues are determined.

CDD refers to the measures taken to define the customer, person/s that act on behalf of the customer, UBO/s before establishing business relations with the customer and to identify and confirm the identity of such persons.

During customer acceptance;

POLICY ON ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

- Enpara Bank is obliged to determine the identities of those who perform transactions and those on whose behalf or accounts transactions are performed, to provide the necessary controls and take other necessary measures to identify UBO/s, and to obtain information about the purpose and nature of the relationship before the transaction is performed when it comes to the transactions performed or brokered.
- Customer risk profiles are created upon risk assessments.
- Information and documents to be collected within the scope of risk assessment, KYC and CDD should be kept up-to-date.
- Information should be obtained regarding the financial profile, activities, income/asset sources of customers along with requested products and services, etc. In high-risk cases, necessary additional information and documents should be taken from customers including those regarding the source of the transaction or assets.
- Enpara Bank regularly checks whether its customers are included in any sanctions lists issued by the United Nations, the European Union, the United Kingdom, The Office of Foreign Assets Control of the US Department of the Treasury (OFAC) and other regulators.
- Enpara Bank's customers should be eager to continue the business relationship in line with relevant rules and should have reasonable information and awareness about banking activities, products and tariffs. BoDs may establish other specific rules about these criteria as it may vary in time.
- Enpara Bank should open accounts for the customers who are real persons, legal entities or other types of customers that align with its goals and objectives.
- It will not accept the establishment of a business relationship with customers who do not comply with this Policy and/or the local and international regulations they are obliged to comply with.
- It will conduct enhanced CDD for all high-risk customers including but not limited to PEPs and NPOs.
- It is forbidden to open anonymous accounts, deal with anonymous customers and shell banks or open accounts in fictitious names.
- Business relations are not established and the transactions demanded are not executed where sufficient information on purpose of business relation cannot be obtained and identification cannot be completed.
- Business relations are terminated when identification and ID verification that should be carried out due to suspicions regarding sufficiency and accuracy of previously obtained customer ID information cannot be performed.
- All new and existing customers will be screened against local and international sanctions lists and PEP lists before establishing business relations and continuously as long as they are customers, and necessary measures will be taken.

Enpara Bank is prohibited from carrying out any transactions for the services related to virtual assets or virtual currencies.

After originals or notarized copies of documents which are subject to verification are submitted, their legible photocopy or electronic image is received or information regarding the identity is recorded in order for submittal upon request of authorities. In case of suspicion regarding the authenticity of the documents used to confirm the information received within this scope, the authenticity of the document should be verified, to the possible extent, by contacting the person or institution that issued the document or other competent authorities.

POLICY ON ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

Business units and their personnel which establish business relations with customers are responsible as the first line of defense.

14.3. Situations Requiring CDD

CDD should be carried out as a general rule when establishing business relations with a new customer. Under the following circumstances (including but not limited to those below), the customer information obtained initially should be reviewed and updated, the customer should be re-visited or re-assessed:

- Change of UBO or authorized signatory of the existing business relationship and/or accounts,
- Transactions with values larger than the threshold values specified in the customer acceptance process,
- Realization of an important (unusual) transaction,
- Significant changes in implementation of the business relationship or the operation of the customer account,
- Significant changes in customer documents,
- Suspicious about the accuracy or adequacy of the information and documents previously obtained within the scope of KYC,
- Electronic transfers above the specified threshold values,
- Suspicion of ML/FT/FPWMD regardless of transaction amount,
- Procurement of a new product or service by a customer.

14.4. Simplified Due Diligence

Simplified Due Diligence may be carried out in cases where the probability of encountering ML/FT/FPWMD risks is very low or where customer risk category is low.

This allows a simplified manner of implementing the KYC principle when ML/FT/FPWMD risks are assessed as low.

The main situations which allow adopting simplified measures in terms of KYC are as follows:

- Transactions carried out by financial institutions among themselves,
- Transactions where the customer is a professional organization such as a public administration/institution within the scope of general management as per the Law no.5018,
- Establishment of a business relationship via mass customer acceptance within the scope of salary payment agreements,
- Transactions related to pension plans/contracts that grant pension rights by discounting from the salary of employees,
- Transactions where the customer is a public company with shares quoted to stock exchange.

Enpara Bank cannot apply simplified measures in cases where ML/FT/FPWMD risks may arise due to the transaction and considers that the transaction may be a suspicious transaction.

14.5. Enhanced Due Diligence (EDD)

EDD and ongoing monitoring is also applied when the customer risk category is high and transactions involve countries classified as high risk, when there is a suspicion that a customer may be associated with or involved in ML/FT/FPWMD or when a person or entity is subject to sanctions or other initiatives related to these matters.

In general, EDD and ongoing monitoring should be implemented for the following categories of customers and products/services:

- Transactions that are not performed face-to-face and new technologies,
- Politically Exposed Persons (PEPs),
- Correspondent banking relationships and financial institutions operating in high-risk regions,
- Bearer's stocks and bearer's share warrants,
- Non-Profit Organizations, Charities, Communities, Clubs (such as associations, foundations, etc.)
- Regional risks (from impaired international cooperation, non-cooperative and sanctioned jurisdictions and jurisdictions with high propensity for corruption and known for criminal activities such as drug trafficking),
- Interface or distribution channel risk,
- Third party trust for CDD,
- Customers who do not reside in Turkey,
- Complex legal entities/institutions, regulations and structures,
- High net-worth individuals that receive private banking services,
- Dealers in precious metals and stones,
- Real estate agents,
- Special purpose vehicles (SPVs),
- Lawyers, notaries and other independent legal professionals and accountants,
- Trust and company service providers,
- Other high-risk customers as per customer risk assessment methodology.

14.6. Additional Measures for High-Risk Customer Groups

Enpara Bank apply, in proportion to the identified risk, one or more or all of the following enhanced measures for the groups defined to be high risk as a result of risk rating in order to ensure mitigating the risk to be undertaken;

a) Obtaining additional information on the customer and updating more regularly the identification data of customer and beneficial owner,
b) Obtaining additional information on the intended nature of the business relationship,
c) Obtaining information, to the extent possible, on the source of the asset subject to transaction and source of funds of the customer,
d) Obtaining information on the reasons for the transaction,
e) Obtaining approval of senior manager to commence or permanent business relationship or carry out transaction,
f) Conducting enhanced monitoring of the business relationship by increasing the number and frequency of the controls applied and by selecting the patterns of transactions that needs further examination,

g) Requiring that in the establishment of permanent relationship the first financial transaction is carried out through another financial institution subject to customer due diligence principles.

As a minimum, the measures listed in subparagraphs (a) to (g) above shall be applied in the payment service (terminal service) performed through the terminal provided within the scope of the payment instrument acceptance service under subparagraphs (a) and (b) and subparagraph (c) of the first paragraph of Article 12 of the Law No.6493 on Payment and Security Settlement Systems, Payment Services and Electronic Money, the establishment of a business relationship with the customer (merchant) and other transactions requiring identification. The measure specified in the subparagraph (g) might not be applied. It is regularly checked that the terminals in question are used in accordance with the purpose of the business relationship or that they are not made available to other persons except for the cases permitted by the relevant legislation; in case of detection of any violation in this context, necessary measures shall be taken, including termination of the business relationship.

14.7. Know Your Product/Service

Product and service recognition helps to identify the risks associated with ML/FT/FPWMD and other illegal activities posed by different types of products and services provided to customers.

All new products and services are subject to ML/FT/FPWMD risk assessment followed by compliance review and approval, as well as approval by other relevant departments. The risk methodology will be commensurate with the complexity of the risks associated with the products offered to customers and processes are designed to identify and control product/service risk, including during the product development stages.

14.8. Identification of UBO

Enpara Bank is required within the scope of the principles regarding KYC to identify the persons who carry out transactions with or through them and the persons on whose behalf of or for the whose benefit transactions are carried out before the transaction is carried out and to take other necessary measures.

Necessary measures are taken to determine whether the customer is acting on behalf of someone else and the identity of the beneficiary owner of the transaction. In cases where there is a suspicion that the person is acting in his/her own name but for the benefit of someone else although he/she has declared that he/she is not acting for the benefit of someone else, measures for the identification of the UBO should be applied.

UBO is determined with a risk-based approach. Enpara Bank takes the necessary measures to reveal the UBO of the transaction.

In terms of determining the UBO for legal entities, three main situations are considered ownership (shareholding) relationship, ultimate control and senior managing official.

Within the scope of permanent business relations, required measures are taken in order to reveal real person/s who control other legal entities and unincorporated organizations as ultimate decision makers.

UBO information should be kept up-to-date as part of CDD.

14.9. Transactions Requiring Special Attention

Enpara Bank is required to pay special attention to complex and unusual large transactions and the ones which have no apparent reasonable legitimate and economic purpose, to take necessary measures in order to obtain adequate information on the purpose of the requested transaction, and to keep the information, documents and records obtained in this scope in order for submittal upon request of authorities.

14.10. Monitoring the Customer Profile and the Transactions

Enpara Bank is required to follow up permanently the transactions conducted by their customers whether they are in compliance with the information regarding the customer's profession, commercial activities, business history, financial status, risk profile and sources of funds within the scope of permanent business relationships and keep up-to-date information, documents and records regarding the customer. Furthermore, the accuracy of information regarding the telephone and fax number and e-mail address of customers received for customer identification is verified, if necessary, within the scope of risk-based approach using these means by contacting with the relevant person. Financial Group also take the necessary measures in order to follow up the transactions conducted out of permanent business relationship in risk-based approach. Financial Group establish, with this purpose, appropriate risk-management systems.

14.11. Taking Measures Against Technological Risks

QNB Financial Group is required to pay special attention to the risk of using facilities introduced by new and developing technologies, existing and new products including new delivery channels, and new business applications for ML/FT/FPWMD and to take appropriate measures for its prevention.

Financial Group is required to take appropriate and effective measures including paying special attention to operations such as establishment of permanent business relationship, depositing, withdrawing and wire transfers which are carried out by using methods and systems enabling the institutions to conduct non face-to-face transactions, closely monitoring the transactions that are not consistent with financial profile or activities of the customer or do not have connection with his/her activities, and establishing a limit to amounts and number of transactions.

14.12. Relationships with Risky Countries

Enpara Bank is required to pay special attention to business relationships and transactions with the real persons and legal entities, unincorporated organizations and the citizens located in risky countries and to obtain information about the purpose and the nature of the transactions, as far as possible, which have no apparent reasonable legitimate and economic purpose and to record them.

14.13. Politically Exposed Persons (PEPs)

Enpara Bank should implement appropriate risk management systems and undertake enhanced CDD measures to determine whether a customer or UBO is a PEP, a family member or a close relationship/partner.

PEPs are assessed as high risk. Risk levels of domestic PEPs can be reduced, provided that they are not low risk, depending on the assessment to be performed on the basis of information obtained about them.

PEPs are assessed with a risk-based approach for at least a year from the date they resign or lose their qualifications. This period may be extended if the transactions or business relations with such persons pose a risk.

Prior to opening accounts for PEPs, the approval of the Senior Management shall be obtained by the Bank through the Financial Crime Compliance Unit.

Prior to establishing a business relationship with PEPs, the approval shall be obtained from both the Financial Crime Compliance Unit/Division and the Senior Executive of the relevant business unit.

Business relationships shall not be continued with PEPs or persons who have a connection with them, unless the approval of the Senior Management is obtained.

14.14. Non-Profit Organizations (NPOs)

Enpara Bank shall not enter into a relationship nor offer any financial services to non-profit organizations such as charities, humanitarian, associations and foundations, unless prior approval of Financial Crime Compliance Unit and the Senior Executive of the relevant business unit.

All approved NPOs customers shall be classified as high-risk customers and subjected to enhanced due diligence and continuous monitoring.

14.15. Correspondent Banking Relationship

Enpara Bank shall apply a risk-based approach in the management of correspondent banking relationships to mitigate the risks of MF/TF/FPWMD, suitable to the size, business profile and risk profile of its businesses and activities.

In this regard, the prior approval of the Financial Crime Compliance Unit and the Senior Executive of the relevant business unit is required to establish any correspondent banking relationship.

15. MONITORING and CONTROL ACTIVITIES

Enpara Bank carry out monitoring and control activities within the scope of institutional policy considering their business size and volume and the nature of transactions they perform. The purpose of these activities is to protect the institutions from ML/FT/FPWMD risks and to ongoing monitor and control whether their activities are carried out in line with the Law, related

regulations, this Policy and its instructions. Monitoring and control activities include the following at a minimum:

- Monitoring and controlling the customers and transactions in high-risk group,
- Monitoring and controlling transactions conducted with risky countries,
- Monitoring and controlling complex and unusual transactions,
- Institutions within the Enpara Bank's control, through sampling method of whether the transactions exceeding the amount which the institutions 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, getting the absent information and documents completed 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 in terms of ML/FT/FPWMD risks.

Enpara Bank implements effective processes through certain systems to identify the risks of new and existing customers and to ongoing monitor and control their accounts and transactions.

Financial Crimes Compliance Unit is granted access to internal information resources and systems within the scope of monitoring and control activities.

Any deficiencies detected upon such controls are reported to relevant business units so that necessary measures are taken and results are followed up.

16. SYSTEM and CONTROLS

Enpara Bank uses appropriate methods or systems to screen new and existing customers according to their business size and business volume against international sanctions lists and internal lists, to identify suspicious customers and transactions and to perform risk classification.

It installs necessary systems and carries out effective processes for ongoing monitoring of accounts and transactions with the aim of detecting, monitoring and assessing high risk customers and transactions.

All regulations related to the prevention of ML/FT/FPWMD including the scenarios, parameters and thresholds in the system used for detecting suspicious transactions and effectiveness and efficiency of other systems/methods are updated yearly or when necessary, according to current technologies and developments.

POLICY ON ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

17. OBLIGATION to REPORT SUSPICIOUS TRANSACTIONS

Through training and briefings, Enpara Bank employees are made aware that they are obliged to report suspicious transactions and the information they obtain within the scope of prevention of ML/FT/FPWMD and that failure to fulfill this obligation will result in criminal sanctions.

Enpara Bank employees report the suspicious transactions to the Compliance Officer/Assistant Compliance Officer and specific employees of the Compliance Division/Unit via the hotline established for this purpose and in accordance with the principles of confidentiality in the intranet system of the relevant institutions and/or in writing via e-mail. Such reporting is examined and are reported as suspicious transactions to MASAK via Compliance Officer/Assistant Compliance Officer if required.

Except for audit employees that are in charge of obligation audit and courts during trials, no information is disclosed to anyone, including the parties to the transaction that was or will be reported as suspicious to MASAK.

No information is disclosed about suspicious transaction notifications at Financial Group level as well.

All employees are prohibited from disclosing confidential information within the scope of this Policy, relevant Law and regulations. Legal penalties and disciplinary measures will be applied to those who violate such regulations.

18. TRAINING

Enpara Bank is required to carry out training activities in compliance with business size, business volume and changing conditions for prevention of ML/FT/FPWMD.

Enpara Bank organizes training programs for its employees to ensure compliance with the relevant Law and regulations within the scope of prevention of ML/FT/FPWMD, to inform and update information on local and international regulations, to increase the awareness of responsibility in line with institutional policies and instructions and risk-based approach principles and to create an effective compliance culture in this area.

Within the scope of this policy, Enpara Bank establishes a training policy that includes issues such as the functioning of training activities, who will be responsible for carrying out such functions, determining and training of employees and trainers who will participate in training activities along with the training methods.

Training activities are conducted under the supervision and coordination of the Compliance Officer. The training program is prepared by the Compliance Officer with the participation of relevant units. Compliance Officer supervises the effective implementation of the training program. Training activities are reviewed by relevant business units based on assessment and measurement results and they are repeated regularly and upon requirement.

Compliance Officers submit the annual training program engagements to the approval of the BoD member residing in Türkiye. It is ensured that the approved training program is conducted effectively.

POLICY ON ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

Enpara Bank carries out the training activities via seminars, conferences, classroom trainings or online trainings. Trainings are prepared and given by managers in Compliance Units or by experts outsourced from external companies. Training activities are conducted in coordination with the training units of the institutions.

Except for support staff such as drivers, executive assistants, technical personnel, security guards, all employees who need to know and apply the legislation within the scope of prevention of ML/FT/FPWMD are included in the training program.

Training subjects at least cover the following issues;

- The concepts of ML/FT/FPWMD,
- Money laundering stages, methods and case studies,
- Legislation on prevention of ML/FT/FPWMD ,
- Risk areas,
- Institutional policies and procedures,
- Know Your Customer principles,
- Principles related to suspicious transaction reporting,
- Obligation of keeping and submitting,
- Obligation of providing documents and information,
- Penal sanctions to be imposed in case of failure to fulfill obligations,
- International regulations regarding prevention of ML/FT/FPWMD .

Enpara Bank includes issues related to local and international sanctions into the training programs as well.

Enpara Bank reports the information and statistics regarding the training activities to MASAK in the period determined by MASAK through the Compliance Officer using the forms specified by MASAK.

19. INTERNAL AUDIT

Within Enpara Bank, internal audit activities are conducted by the Internal Audit Department to provide assurance to the BoD on the effectiveness and adequacy of the overall compliance program.

Thus, it is ensured that the issues of whether the policies and procedures of institutions, risk management, monitoring and control activities and training activities are adequate and efficient, whether the risk policies of institutions are adequate and efficient, whether the transactions are carried out in line with the relevant Law, related regulations, the policies and procedures of the institution are examined and audited annually and with a risk-based approach.

Any deficiency, error and misconduct which come to light as a result of internal audit activities are reported to the Audit Committee and the Board of Directors along with opinions on suggestions for prevention.

POLICY ON ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

While determining the scope of audit, the faults determined during the monitoring and controlling workings and the customers, services and transactions containing risk should be included within the scope of control.

While determining the units and transactions to be audited, the business size and business volumes of Enpara Bank should 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 obliged party shall be ensured to be audited.

Enpara Bank's internal audit is carried out by Enpara Bank IAD. In order to ensure the independence of the employees to be authorized to perform internal audit activities, they should not have been on duty or authorized for taking the other measures within the scope of the Compliance Program.

Enpara Bank reports the information and statistics regarding the internal audit activities to MASAK in the period determined by MASAK through the Compliance Officer using the forms specified by MASAK.

20. SANCTIONS

Complying with the sanction decisions of the United Nations (UN), the European Union (EU), United Kingdom (UK) and the Office of Foreign Assets Control (OFAC) of the US Department of the Treasury applicable for any business or transaction under all conditions and operating in accordance with best practice guidelines issued by regulatory institutions are a separate policy of the Bank. Enpara Bank establishes the necessary procedures, guidelines and mechanisms to ensure compliance with these regulations and to prevent the risk of non-compliance with sanctions.

21. PERIODICALLY REPORTING

Enpara Bank is required to report the transactions, to which they are parties or intermediaries, exceeding the amount determined by the Ministry to MASAK.

The transaction types subject to periodically reporting, reporting procedure and periods, other implementation principles and procedures should be determined by the Ministry.

Regarding the implementation of Law No 5549, periodically reporting may be requested from the public institutions and organizations, and institutions and organizations in the nature of public bodies other than the obliged parties.

22. PROVIDING INFORMATION AND DOCUMENTS

When requested by MASAK or examiners, public institutions and organizations, natural and legal persons, and unincorporated organizations should fully and accurately provide all kinds of information, documents and related records in every type of environment, any kind of information and passwords necessary for accessing to or making these records decipherable, and render necessary convenience.

Without prejudice to the provisions on the right of defense, information and documents may not be withheld on the grounds of provisions written in special laws.

POLICY ON ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

23. RECORD KEEPING and SUBMITTING

Enpara Bank is obliged to keep for eight years the documents related to the customer accounts and transactions regarding the obligations in the relevant Laws and transactions from the date of issuance; books and records from the last registration date; and ID authentication documents from the last transaction date and to present it to the authorities if requested.

As the bank is subject to the provisions of the Banking Law, it is required to retain records related to customer accounts and transactions for a minimum period of ten years.

24. DEVIATIONS and EXCEPTIONS

Any deviation or non-compliance with the requirements of this Policy should be reported to QNB Group who will assess the risks and advise on alternative controls to mitigate inherent risks.

Deviations from this Policy will be considered on a case basis with documented justification and only in limited, exceptional circumstances. Exceptions should not apply where there are laws or regulations to be complied with.