

"APPROVED"  
Meeting of the Supervisory Board  
PIRAEUS BANK ICD JSC  
protocol № 22\_20 from 21.08.2020.

**POLICY OF PIRAEUS BANK ICB JSC  
ON PREVENTION AND COUNTERACTING TO LEGALIZATION  
(LAUNDERING) OF PROCEEDS FROM CRIME, FINANCING OF  
TERRORISM AND FINANCING OF PROLIFERATION OF WEAPONS OF  
MASS DESTRUCTION  
(*EXTRACT*)**



**Policy of JSC "PIRAEUS BANK ICB" on prevention and counteracting to legalization (laundering) of proceeds from crime, financing of terrorism and financing of proliferation of weapons of mass destruction**

---

**Content**

<b>1. GENERAL PROVISIONS</b> .....	<b>3</b>
<b>2. PURPOSE, TASKS, AND PRINCIPLES OF AML/CFT</b> .....	<b>6</b>
<b>3. THE INTERNAL ORGANIZATIONAL BANK STRUCTURE OF THE AML/CFT SYSTEM</b> .....	<b>8</b>
<b>4. DETERMINATION OF RISK-APPETITE OF THE BANK IN THE FIELD OF AML/CFT</b> .....	<b>10</b>
<b>5. RESPONSIBILITY</b> .....	<b>14</b>
<b>6. FINAL PROVISIONS</b> .....	<b>14</b>

Financial Monitoring Department	Version code	Version date	Pages
	438FCD-PLC-21082020-1.0	21/08/2020	<b>2 з 15</b>

## **1. GENERAL PROVISIONS**

The Policy of JSC "PIRAEUS BANK ICB" on prevention and counteracting to legalization (laundering) of proceeds from crime, financing of terrorism and financing of proliferation of weapons of mass destruction (from now on - AML/CFT Policy/Policy) regulates the general requirements for the proper organization of the internal banking system of counteraction of money laundering of proceeds from crime, financing of terrorism and/or financing of proliferation of weapons of mass destruction (from now on - the intrabank system of AML/CFT) to prevent the use of JSC "PIRAEUS BANK ICB" (from now on - the Bank) to legalize (launder) of proceeds from criminal, terrorist financing and financing the proliferation of weapons of mass destruction (from now on - ML/FT).

In particular, this Policy sets out the purpose, objectives and fundamental principles that the Bank is guided by when complying with the requirements of the legislation of Ukraine on the prevention and counteraction of ML/FT (from now on - AML/CFT).

The requirements of this Policy apply to all entities of the internal banking system of AML/CFT, which are defined by this Policy and are mandatory for their implementation.

The Bank Supervisory Board (from now - the Supervisory Board) communicate the Policy to the Bank Management Board and the Bank Responsible Officer (AML Officer) for conducting financial monitoring to form a clear understanding of the Supervisory Board's expectations regarding:

- 1) creation of the proper organization and functioning of the internal banking system of AML/CFT and conducting of primary financial monitoring, the operation of an appropriate system of risk management of ML/FT;
- 2) risk-appetite of the Bank in the field of AML/CFT<sup>1</sup> (including, if available, established prohibitions/restrictions on specific activities and/or attracting certain types of customers for service);
- 3) the scope required for the development and approval of the Bank's internal documents on AML/CFT;
- 4) requirements for the construction of three lines of protection in the field of AML/CFT and the distribution of duties and responsibilities among the Bank employees;
- 5) functioning of internal control over AML/CFT issues;
- 6) ensuring training activities on AML/CFT issues.

---

<sup>1</sup> is a component of the Bank's risk appetite for Compliance Risks, namely 13.1 Money-laundering / Terrorism Financing (ML / TF) Risk. At present, the Bank has zero-tolerance for such risks - see the current version of Annex II: Quantified Risk Appetite Statements, Risk Bearing Capacity, Monitoring Indicators (EWS) to PIRAEUS Bank's Risk and Capital Management Strategy.

Financial Monitoring Department	Version code	Version date	Pages
	438FCD-PLC-21082020-1.0	21/08/2020	<b>3 з 15</b>

## 1.2 Terms and reductions.

The following abbreviations are used in this AML/CFT Policy:

**Law on AML/CFT** – Law of Ukraine “On Prevention and Counteraction to Legalization (Laundering) of Proceeds from Crime, Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction;

**UBO** – Ultimate Beneficiary Owner;

**Client** - any person who:

- applies for the provision of services to the subject of primary financial monitoring;
- uses the services of the subject of primary financial monitoring;
- is a party to the agreement (for the subjects of primary financial monitoring, in respect of which the National Commission on Securities and Stock Market by Article 18 of the Law on AML/CFT performs the functions of state regulation and supervision);

**Supervisory Board of the Bank** - Supervisory Board of PIRAEUS BANK ICB, JSC;

**NBU** – National Bank of Ukraine;

**DD** – due diligence;

**AML/CFT** – prevention and counteraction to legalization (laundering) of proceeds from crime, financing of terrorism and financing of proliferation of weapons of mass destruction;

**list of persons** - a list of terrorists connected with terrorist activities or subject to international sanctions, formed under the procedure established by the Cabinet of Ministers of Ukraine and published on the official website of the specially authorized body (FIU of Ukraine);

**FIU** – Financial Intelligence Unit (The State Financial Monitoring Service of Ukraine);

**SPFM** – subject of the primary financial monitoring;

**FATF** - Group to develop financial measures to combat money laundering;

**PEP** (PEPs in plural) – a natural person who is politically exposed, a member of his family or a person related to a politically exposed person or another person whose ultimate beneficial owner is a politically exposed person, a member of his family or a person related to a politically exposed person;

In this AML/CFT Policy, terms and concepts are used in the following meanings:

**Bank** - PIRAEUS BANK ICB JOINT STOCK COMPANY;

**responsible executor** - an employee of the Bank who, by his official duties and/or instructions of the Bank's management, has the authority to perform certain operations and is responsible for their proper execution;

Financial Monitoring Department	Version code	Version date	Pages
	438FCD-PLC-21082020-1.0	21/08/2020	4 з 15

**Responsible employee/AML Officer** - the responsible employee of the Bank for conducting financial monitoring;

**internal documents of the Bank on the issues of AML/CFT** - policies, rules, programs, methods, other documents developed and approved by the Bank to properly perform the functions of SPFM;

**de-risk** - a phenomenon in which SPFM refuses to establish (maintain) business relationships with customers to avoid risks, rather than managing them;

**shell company** - a legal entity, trust or other similar legal entity, in respect of which (which) the Bank has reasonable suspicions that its (his) activities may be fictitious;

**due diligence(DD)** - measures including:

- identification and verification of the client (his/her representative);
- identification of the ultimate beneficial owner of the client or its absence, including obtaining the ownership structure to understand it, and data that allow establishing the ultimate beneficial owner, and taking measures to verify his identity (if any);
- establishing (understanding) the purpose and nature of future business relationships or conducting a financial transaction;
- conducting regular monitoring of business relations and financial transactions of the client, carried out in the process of such relations, on the compliance of such financial transactions with the subject of primary financial monitoring information about the client, its activities and risks (including, if necessary, about the source of funds related to financial transactions);
- ensuring the relevance of received and existing documents, data and information about the client;

**acceptable level of ML/FT risks** - a risk that is managed, controlled by the Bank, can not cause an increase in legal risk and reputational risk, as well as deterioration of the financial results of the Bank or harm its creditors and customers;

**risk-appetite** (propensity to risk) of the Bank in the field of AML/CFT - the amount of risk of ML/FT, determined in advance and within an acceptable level of risk of ML/FT, for which the Bank has decided on the feasibility/need to maintain it to achieve its strategic goals and implementation of the business plan;

**reputation risk** - the real or potential risk to income and capital that arises from an adverse perception of the Bank's image by customers, counterparties, potential investors, or supervisors that affects the Bank's ability to establish new relationships with counterparties, provide new services or maintain existing relationships. lead the Bank (or its managers) to financial losses or reduction of the customer base, bringing to administrative, civil or criminal liability;

Financial Monitoring Department	Version code	Version date	Pages
	438FCD-PLC-21082020-1.0	21/08/2020	5 з 15

**legal risk** - existing or potential risk to the Bank's income or capital, which arises due to violation or non-compliance by the Bank with the laws of Ukraine, regulations and may lead to financial losses, abuse, the involvement of the Bank and/or its managers in administrative, civil or criminal liability;

### 1.3. Regulatory framework

The Policy is developed following the requirements of current legislation and internal documents of the Bank, in particular:

- Law of Ukraine "On Banks and Banking Activity" of December 7, 2000, № 2121-III [as amended (from now on - the Law on Banks)]
- Law of Ukraine "On Preventing and Counteracting to Legalization (Laundering) of the Proceeds from Crime, Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction" of December 6, 2019, № 361-IX [as amended (from now on - the Law on AML/CFT) ];
- "Regulations on financial monitoring by banks," approved by the Resolution of the Board of the National Bank of Ukraine of May 19, 2020 №65 (from now on - the Resolution № 65);
- "Regulations on licensing of banks," approved by the Resolution of the Board of the National Bank of Ukraine of December 22, 2018 N 149 (as amended).
- "Regulations on the organization of the risk management system in banks of Ukraine and banking groups," approved by the Resolution of the Board of the National Bank of Ukraine of June 11, 2018, N 64 (as amended). (hereinafter - Resolution № 64)

## 2. PURPOSE, TASKS, AND PRINCIPLES OF AML/CFT

### 2.1. The purpose of the AML/CFT Policy

The purpose of implementing the AML/CFT Policy is to ensure compliance of the Bank's activities with the requirements of the current legislation of Ukraine, regulations of the specially authorized executive body for financial monitoring (from now on - FIU), the National Bank of Ukraine (from now on - NBU), the Ministry of Finance of Ukraine, recommendations The Financial Action Task Force (FATF) and the Basel Committee on Banking Supervision and other official documents governing the prevention and counteraction to legalization (laundering) of the proceeds from crime, financing of terrorism and financing of proliferation of weapons of mass destruction, and also internal normative documents of the Bank, which are obligatory for the Bank's employees (depending on their job responsibilities), taking into account the norms of the legislation of Ukraine.

### 2.2. Tasks of the AML/CFT Policy

The task of implementing the AML/CFT Policy is:

- ✓ establishment of proper organization and functioning of the intrabank system of AML/CFT and conducting of primary financial monitoring;

Financial Monitoring Department	Version code	Version date	Pages
	438FCD-PLC-21082020-1.0	21/08/2020	6 з 15

- ✓ ensuring the operation of an appropriate ML/FT risk management system;
- ✓ determination of the Bank's risk appetite in the field of AML/CFT (including, if available, established prohibitions/restrictions on specific activities and/or attracting certain types of customers for service);
- ✓ determining the amount required for the development and approval of the Bank's internal documents on AML/CFT issues;
- ✓ setting requirements for the construction of three lines of protection in the field of AML/CFT and the distribution of duties and responsibilities among the Bank's employees;
- ✓ ensuring the functioning of internal control over AML/CFT issues;
- ✓ conducting training events on AML/CFT issues

### **2.3. Principles of the AML/CFT Policy**

**AML/CFT policies are based on the basic principles of prevention and counteraction:**

- ✓ priority protection of legitimate interests of citizens, society and the state from damage caused by legalization (laundering) of proceeds from crime, terrorist financing and financing the proliferation of weapons of mass destruction;
- ✓ giving priority to measures to prevent legalization (laundering) of proceeds from crime, terrorist financing and financing the proliferation of weapons of mass destruction over measures to combat them;
- ✓ application of a risk-oriented approach during financial monitoring;
- ✓ coordination of interaction of participants of the interbank system of prevention and counteraction;
- ✓ the inevitability of measures to freeze assets related to terrorism and its financing, a proliferation of weapons of mass destruction and their funding;
- ✓ the inevitability of punishment and the persuasiveness and proportionality of measures of influence for violations of legislation in the field of prevention and counteraction;
- ✓ protection of the Bank's Employees from threats and other harmful or discriminatory actions related to compliance with the requirements of the Law on AML/CFT;
- ✓ release from liability for damage caused in connection with the performance of obligations to conduct financial monitoring within limits and in the manner prescribed by the Law on AML/CFT;
- ✓ preservation, protection of information and completeness, relevance and timeliness of information exchange;
- ✓ availability to the participants of the interbank system of information necessary for financial monitoring;
- ✓ release from liability for providing data with limited access by the requirements of the Law on AML/CFT;

Financial Monitoring Department	Version code	Version date	Pages
	438FCD-PLC-21082020-1.0	21/08/2020	7 3 15

- ✓ cooperation and interaction in the field of prevention and counteraction with the competent authorities, whose activities are aimed at ensuring participation in this area by Ukraine's legislation.

The AML/CFT policy sets out the Bank's general principles for complying with Ukrainian legislation on preventing and counteracting money laundering, terrorist financing, and the proliferation of weapons of mass destruction and is not a restricted document.

### **3. THE INTERNAL ORGANIZATIONAL BANK STRUCTURE OF THE AML/CFT SYSTEM**

#### **3.1. Proper organization of the intrabank AML/CFT system**

The Bank is a subject of primary financial monitoring of the national financial monitoring system and takes appropriate measures in the field of prevention and counteraction to legalization (laundering) of proceeds from crime, terrorist financing, and financing of proliferation of weapons of mass destruction.

The purpose of creating, proper organization of the internal banking system of AML/CFT and conducting the initial financial monitoring of the Bank is:

- compliance with the requirements of the legislation of Ukraine in the field of AML/CFT;
- the ability to accurately identify and report threshold and suspicious financial transactions (activities);
- prevention of the use of the Bank's services and products for conducting financial transactions by clients for ML/FT.

The subjects of the intrabank system of AML/CFT are:

- 1) the Supervisory Board of the Bank;
- 2) the Management Board of the Bank;
- 3) Internal Audit Department;
- 4) Financial Monitoring Division (AML Division);
- 5) Subdivisions of the Bank that conduct / ensure the handling of operations or provision of services

#### **3.2. Construction of three lines of protection in the field of AML/CFT and distribution of duties and responsibilities among the Bank's employees<sup>2</sup>**

---

<sup>2</sup> Each line of protection of the Bank is aimed to accurately organize the internal banking system of AML/CFT and conduct primary financial monitoring, by the defined powers, acts appropriately.

This division of responsibilities and responsibilities relates exclusively to the construction of protection in the field of AML/CFT to meet the requirements of NBU Resolution №65, development of a standard banking risk management system, according to NBU Resolution №64 and the requirements of Piraeus SA Group, based on the distribution defined in internal Bank documents on risk management.

Financial Monitoring Department	Version code	Version date	Pages
	438FCD-PLC-21082020-1.0	21/08/2020	8 з 15



The Bank has created an intrabank AML/CFT system based on the distribution of responsibilities between the system's subjects using the model of three lines of protection:

1) the first line of protection - at the level of the Bank's divisions that conduct and/or provide operations or provide services to the Bank's Clients. Employees of the Bank's divisions (from now on - the responsible executors) are liable for non-performance of duties and/or inaction in the field of AML/CFT by their official duties and/or instructions of the Bank's management.

2) the second line of protection - at the level of the Financial Monitoring Division, the Bank's Responsible Officer (AML Officer), ensures the organization of the internal banking system of the AML/CFT and the Bank's primary financial monitoring, following the requirements of the AML/CFT legislation and internal documents of the Bank on financial monitoring.

3) the third line of protection - at the level of the Internal Audit Department of the Bank, provides verification and evaluation of the effectiveness of the internal banking system of AML/CFT and verification and evaluation of the Bank's initial financial monitoring.

Each line of protection of the Bank shall take appropriate measures to organize the internal banking system of AML/CFT accurately and conduct initial financial monitoring by the defined powers.

### **3.3. Ensuring the effectiveness of the internal banking system of financial monitoring and responsibility for its improper organization.**

To achieve the efficiency of the internal banking system of financial monitoring, the Bank ensures the following main measures:

- ✓ takes measures following the legislation to ensure that the Responsible Employee (AML Officer) undergoes training in the field of AML/CFT within three months from the date of his / her appointment, as well as in-service training of the Responsible Employee by undergoing training at least once every three years in educational institution of FIU and in other educational institutions as agreed by FIU;
- ✓ fulfills the requirements of the National Bank for following (elimination of violations) of the requirements of the legislation in the field of prevention and counteraction made based on, within the powers and in the manner provided by the Law;
- ✓ establishes for employees the Procedure of notifying the Chairman of the Management Board and/or the Responsible Officer about violations of the requirements of the legislation in the field of AML/CFT, including without indication of authorship (anonymously), with the provision of appropriate means;
- ✓ protects employees in connection with the notification of the Chairman of the Management Board and/or the Responsible Employee, the National Bank about the violation of the requirements of the legislation in the field of AML / CFT;

Financial Monitoring Department	Version code	Version date	Pages
	438FCD-PLC-21082020-1.0	21/08/2020	<b>9 3 15</b>

- ✓ does not allow to the management, membership in the Supervisory Board, Management Board of the Bank or control by the Bank persons who have not expunged or not removed in the prescribed manner criminal record for mercenary criminal offenses or terrorism, as well as their accomplices in such criminal attacks;
- ✓ does not allow the formation of the authorized capital of the Bank at the expense of funds, the sources of origin of which cannot be confirmed;
- ✓ takes other defined measures in the field of AML/CFT.

The Chairman of the Management Board of the Bank, as well as the Responsible Employee, are responsible for the improper organization and conduct of the primary financial monitoring.

The responsible employee shall inform the Chairman of the Management Board of the Bank/Acting Chairman of the Management Board about the AML/CFT measures following the Procedure established by internal regulations.

The Bank's responsible employee (AML Officer) subordinates directly to the Supervisory Board of the Bank and reports to it.

Chairman of the Management Board of the Bank, Responsible Employee of the Bank / Acting Responsible employee of the Bank, as well as other employees involved in the primary financial monitoring, in case of violation of the legislation on prevention and counteraction, shall be liable by the law.

#### **4. DETERMINATION OF RISK-APPETITE OF THE BANK IN THE FIELD OF AML/CFT**

##### **4.1. Proper risk management system**

The Bank applies a risk-oriented approach in its activities, which is proportional to the nature and scale of the Bank's operations.

The risk-oriented approach is applied by the Bank continuously and provides identification, assessment of all real and potential risks of ML/FT, inherent in the Bank's activities (risk profile of the Bank) and its Clients, and provides timely development of ML/FT risk management measures. their minimization.

The risk-oriented approach is based on a two-stage risk assessment and includes:

1) evaluation of the Bank's risk profile:

- ✓ identification and assessment of ML/FT risks inherent in the Bank's activities;
- ✓ analysis of existing ML/FT risk management measures to reduce (minimize) them;
- ✓ determination of the Bank's risk appetite in the field of AML/CFT(acceptable for the Bank level of ML/FT risk);

Financial Monitoring Department	Version code	Version date	Pages
	438FCD-PLC-21082020-1.0	21/08/2020	<b>10 з 15</b>

2) assessment of the Client's risk profile:

- ✓ identification and evaluation of the primary risk of the business relationship (financial transaction without establishing a business relationship) with the client;
- ✓ analysis of existing ML/FT risk management measures to reduce (minimize) them to the level of ML/FT risk acceptable to the Bank (within the risk of the Bank's appetite in the field of AML/CFT);
- ✓ assessment of the business relationship (financial transaction without establishing a business relationship) with the client.

Based on the assessment of ML/FT risks inherent in its activities, the Bank determines its risk appetite (acceptable level of risk) in the field of AML / CFT, taking into account:

- 1) risks that the Bank is ready to accept;
- 2) risks that the Bank may accept, but only after taking measures to manage such risks (their minimization);
- 3) risks that are unacceptable to the Bank.

#### **4.2. Requirements for the Bank's ML/FT risk management system**

The Bank's ML/FT risk management system is considered inadequate if at least one of the signs and facts of repeated financial transactions involving suspicion of using the Bank for ML/FT or committing another crime resulting from non-compliance with the measures, established by AML/CFT.

##### **Signs of an inadequate risk management system:**

- 1) improper implementation of a comprehensive assessment/reassessment of the Bank's ML/FT risks, including those inherent in its activities (risk profile of the Bank), documenting their results, monitoring, risk control and maintaining the Bank's risk profile to minimize the use of the Bank's services for ML/FT;
- 2) non-implementation of the DD, improper assessment/reassessment of the risk of business relations (financial transactions without establishing business relations) with Clients (risk profiles of Clients), documenting their results, monitoring measures, risk control and maintaining risk profiles of the Bank's Clients to minimize the use of the Bank's services for ML/FT;
- 3) improper application of a risk-oriented approach, which is the Bank's misunderstanding of the risks of ML/FT, which exposes its Client, failure to take adequate measures to minimize the identified risks (Simplified DD for low-risk clients and Enhanced DD for high-risk clients), lack of differentiated (multilevel) risk-oriented Procedure for agreeing on business relations with clients;
- 4) failure to take timely and adequate measures to minimize the identified risks of ML/FT to an acceptable level of risks of ML/FT;

Financial Monitoring Department	Version code	Version date	Pages
	438FCD-PLC-21082020-1.0	21/08/2020	11 з 15

- 5) lack of useful tools to prevent multiple, large amounts of financial transactions (activities) by Clients, in which there are suspicions of using the Bank for ML/FT or committing other crimes, including monitoring of business relations with Clients and financial transactions of Clients carried out in the process of such business relations;
- 6) lack of effective internal control over financial monitoring, untimely detection by the internal audit of problems and shortcomings in the internal banking system of AML/CFT and signs of inadequate risk management system of ML/FT;
- 7) lack of an effective system of escalation of suspicions and problematic issues in the field of AML/CFT, which made it impossible to timely and adequately consider them, including reporting information/facts concerning violations or possible violations of Ukrainian legislation in the field of AML/CFT;
- 8) the lack of a proper system for detecting PEPs, which has led to the Bank's failure to take appropriate measures against them, as defined by the legislation of Ukraine in the field of AML/CFT;
- 9) lack of a proper Client UBO detection system;
- 10) failure of the Bank to properly document the Bank's employees' actions and to record events related to the Bank's performance of SPFM functions.
- 11) inadequate provision of secrecy of financial monitoring and confidentiality of information on information exchange with the FIU, including the fact of transfer of data on the financial transaction to FIU.

#### **4.3. Basic prohibitions and restrictions**

In determining its risk appetite, the Bank imposes the following prohibitions/restrictions on its activities, taking into account their unacceptable risk for the Bank:

- 4.3.1. does not open or maintain anonymous (numbered) accounts;
- 4.3.2. does not establish correspondent relations with shell banks, as well as with non-resident banks and other financial institutions, in respect of which it is known that they maintain correspondent relations with shell banks;
- 4.3.3. does not establish business relations, and does not conduct financial transactions, does not provide services directly or indirectly with Clients (customer representatives), who are:
  - casinos and bookmakers operating without a license or supervision, in particular, companies engaged in online gambling;
  - who provide financial or insurance services without an appropriate permit or control by the executive bodies;
  - persons who trade cryptocurrencies (for example Bitcoins);

Financial Monitoring Department	Version code	Version date	Pages
	438FCD-PLC-21082020-1.0	21/08/2020	12 з 15

4.3.4. does not establish business relations (except as provided by UN Security Council resolutions) and does not conduct expenditure financial transactions, does not provide services directly or indirectly to Clients who are:

- persons and / or organizations that are included in the list of persons or in respect of which international sanctions or sanctions of authorized state bodies of Ukraine have been applied;
- persons and / or organizations acting on behalf of and on behalf of persons and / or organizations included in the list of persons or in respect of whom international sanctions or sanctions of authorized state bodies of Ukraine have been applied;
- persons and / or organizations directly or indirectly owned or ultimately beneficially owned by persons and / or organizations included in the list of persons or subject to international sanctions or sanctions of authorized state bodies of Ukraine;
- the counterparty of the financial transaction or the financial institution that provides the business transaction is a person belonging to the persons specified in paragraph 4.3.4, and the Bank becomes aware of this during the provision of services/transactions;

4.3.5. does not open accounts in US dollars to persons and does not carry out financial transactions in US dollars if at least one of the parties to the financial transaction has a registration, residence, or location in the Islamic Republic of Iran and the Republic of Cuba, Northern Cyprus.

4.3.6. refuses to establish (maintain) business relations / refuse the client to open an account (service), including by terminating business relations and closing the account / refusing to conduct a financial transaction in the case of:

- if the identification and/or verification of the client, as well as the establishment of data that allows identifying the ultimate beneficial owners, is impossible or if the Bank has doubts that the person acts on its own behalf;
- setting an unacceptably high risk for the client or failure of the client to provide the documents or information necessary for the proper DD and/or verification of the client;
- submission by the client or his/her representative of inaccurate data or presentation of information to mislead the Bank;
- detection that the bank or other financial institution with which the correspondent relationship has been established is a shell bank and / or maintains a correspondent relationship with the shell bank;
- if it is impossible to identify the person on whose behalf or in whose interests the financial transaction is conducted and to establish its ultimate beneficial owner or beneficiary (beneficiary) in the financial transaction;

Financial Monitoring Department	Version code	Version date	Pages
	438FCD-PLC-21082020-1.0	21/08/2020	13 з 15

- clients in respect of whom the Bank, based on the results of studying the client's activities, has reasonable suspicions that they have performed ML/FT operations and other crimes;

4.3.7. The Bank also does not establish/maintain business relations with the Clients and does not carry out financial transactions to the persons specified in the **Client's Eligibility Policy**, a component of the **Compliance Policy** (Policy of compliance with legal norms and standards) of PIRAEUS BANK ICB JSC.

4.3.8. The Bank shall also terminate any relationship with an existing Client if, due to the due diligence, Bank finds that the client falls into one of the categories specified in this section (for example, as a result of the revocation of a securities license, provision of inaccurate information to the Bank or submission of information to mislead the Bank, etc.).

4.3.9. The Bank does not transfer funds in the absence of mandatory information that must accompany the financial transaction for the transfer of funds.

4.3.10. The Bank, the Bank's managers, the AML Officer, other employees of the Bank involved in the initial financial monitoring, the ultimate beneficial owners of the Bank do not use their powers and related opportunities or refrain from using them to legalize (launder) income, obtained by illegal means, financing terrorism and financing the proliferation of weapons of mass destruction or assisting others in committing such acts.

4.3.11. Based on the analysis results, the Bank determines (if necessary) in its internal documents on AML/CFT additional prohibitions/restrictions in its activities (for specific events and/or attracting certain types of customers for service).

4.3.12. All other risks may be accepted by the Bank, including after taking risk management measures (their minimization). In taking appropriate risks, the Bank takes into account the availability of sufficient means to manage them, particularly the availability of the necessary resources.

4.3.13. By applying a risk-oriented approach, the Bank refrains from the unreasonable application of de-risking, which contradicts the risk-oriented approach and does not promote financial inclusion.

## **5. RESPONSIBILITY**

The defined Procedure of internal control in the Bank and the determination of the Bank's employees who make decisions at different stages (types) of control under their functional responsibilities, ensure the principle of "higher position - greater authority and responsibility."

## **6. FINAL PROVISIONS**

The AML/CFT Policy is not a restricted document. The AML/CFT Policy is indefinite, enters into force after its approval by the Bank's Supervisory Board from the date following the date of the Bank's Supervisory Board

Financial Monitoring Department	Version code	Version date	Pages
	438FCD-PLC-21082020-1.0	21/08/2020	<b>14 з 15</b>



**Policy of JSC "PIRAEUS BANK ICB" on prevention and counteracting to legalization (laundering) of proceeds from crime, financing of terrorism and financing of proliferation of weapons of mass destruction**

---

decision, and is valid until its revocation or approval by the Bank's Supervisory Board of the new AML/CFT Policy, which the previous one loses force.

AML/CFT Policy are reviewed as necessary. Changes and/or additions to this AML/CFT Policy shall be made by approving them by the Supervisory Board of the Bank under the established Procedure.

Employees of the Bank (depending on their job responsibilities) get acquainted with this AML/CFT Policy under the signature in the case of:

- approval, amendments to the AML/CFT Policy - within the deadlines set by the regulations of the National Bank of Ukraine.
- Employment in the Bank - before the beginning of official duties.

For improper compliance by employees with the requirements of this AML/CFT Policy, the Bank may take measures of influence within Ukraine's current legislation.

In case of non-compliance of any part of this Policy with AML/CFT with the current legislation of Ukraine, including in connection with the adoption of new acts of legislation of Ukraine or regulations of the National Bank of Ukraine, this Policy is valid in the part that does not contradict the legislation.

Financial Monitoring Department	Version code	Version date	Pages
	438FCD-PLC-21082020-1.0	21/08/2020	15 з 15