APPROVED
by Supervisory Board
JSC «BANK 3/4»
Protocol No. 10
of 28 June 2024

POLICY
on issues of Prevention and Counteraction to Legalization (Laundering) of Criminal Proceeds, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction of JSC “BANK 3/4”

(new edition)

Kyiv 2024

CONTENT

1. GENERAL PROVISIONS

1. The Policy on issues of Prevention and Counteraction to Legalization (Laundering) of Criminal Proceeds, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction of JSC “BANK 3/4” (hereinafter - the Policy) has been developed with purpose to prevent the use of the services of JSC “BANK 3/4” (hereinafter - the Bank) for legalization (laundering) of criminal proceeds, financing of terrorism and financing of proliferation of weapons of mass destruction (hereinafter - ML/TF) and counteracting any other activity preceding or promoting the ML/TF.

In particular, this Policy defines the purpose, objectives and basic principles that the Bank is guided when fulfilling the requirements of Ukrainian legislation on the prevention and counteraction of ML/TF.

2. The Policy has been developed in accordance with requirements of the current legislation of Ukraine, international standards and recommendations on financial monitoring issues, in particular:

- the Law of Ukraine 'On Banks and Banking’ (hereinafter - the Law on Banks);
- the Law of Ukraine ‘On Prevention and Counteraction to Legalization (Laundering) of Criminal Proceeds, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction (hereinafter - the Law);

the Law of Ukraine "On Sanctions" (hereinafter - the Law on Sanctions);

- Regulation on implementation of financial monitoring by banks, approved by the Resolution of the Board of the National Bank of Ukraine as of 19.05.2020 No. 65 (as amended) (hereinafter - the Regulation 65);
- Regulation on the implementation of special economic and other restrictive measures (sanctions), approved by the Resolution of the Board of the National Bank of Ukraine as of 11.05.2023 No. 65 (as amended) (hereinafter - the Regulation on Sanctions);
- Regulations on the organization of the internal control system in Ukrainian banks and banking groups, approved by the Resolution of the Board of the National Bank of Ukraine as of 02.07.2019 No. 88;
- Regulations on the organization of the risk management system in Ukrainian banks and banking groups, approved by the Resolution of the Board of the National Bank of Ukraine as of 11.06.2018 No. 64 (as amended);
- International standards (FATF Recommendations, Directives of the European Parliament and the Council of Europe, the Basel Committee on Banking Supervision, the OFAC sanctions programs, etc.);
- recommendations of the State Financial Monitoring Service of Ukraine, in particular, the National Risk Assessment and Typological Research, which are posted on the official page of this institution;
- other legislative and regulatory acts of Ukraine regulating AML/CTF issues;
- the Bank's Charter, the Bank’s Code of Corporate Governance, the Bank’s Corporate Ethics Code, the Bank's internal regulatory documents (hereinafter – IRD).

3. The requirements of this Policy are applied to all subjects of the intra-bank AML/CTF system, which are defined by this Policy and are mandatory for their implementation.

4. The Policy is submitted by the Supervisory Board of the Bank (hereinafter - the Bank’s Board) to the Bank’s Management Board and the Bank's Compliance Officer responsible for AML in order to form a clear understanding of the expectations of the Bank’s Board regarding:

- proper organization and functioning of the intra-bank AML/CTF system and conducting primary financial monitoring, functioning of the proper ML/TF risk management system;
- the Bank’s risk appetite in the field of AML/CTF (including, if any, established prohibitions/restrictions on the implementation of certain types of activities and/or attracting the certain types of clients for service);

- the scope of the Bank's IRD on AML/CTF issues required for the development and approval;
- requirements for the construction of three lines of defence on AML/CTF field and the allocation of duties and responsibilities among the Bank's employees;
- functioning of internal control over AML/CTF issues;
- ensuring of training sessions concerning AML/CTF issues.

5. The Policy on AML/CTF is based on the basic principles of prevention and counteraction:

- priority protection of legitimate interests of citizens, society and the state from damage caused by ML/TF;
- giving priority to measures to prevent the ML/TF over measures to combat them;
- application of a risk-oriented approach during financial monitoring;
- coordination of interaction of participants of intra-bank AML/CTF system;
- inevitability of measures on freezing of assets related to terrorism and its financing, proliferation of weapons of mass destruction and its financing;
- inevitability of punishment and persuasiveness and proportionality of measures of influence for violations of legislation in the field of AML/CTF;
- protection of Bank's employees from threats and other negative or discriminatory actions related to compliance with the provisions of the Law on AML/CTF;
- release from liability for damage caused in connection with fulfillment of obligations on conducting financial monitoring within the limits and in the manner prescribed by the Law on AML/CTF;
- preservation, protection of information and completeness, relevance and timeliness of information exchange;
- availability to the participants of intra-bank AML/CTF system of the information necessary for conducting financial monitoring;
- exemption from liability for providing information with limited access according to the provisions of the Law;
- cooperation and interaction in the field of AML/CTF with competent bodies, whose activities are aimed at ensuring cooperation in this field in accordance with the legislation of Ukraine.

6. The Bank's Management Board and the Compliance Officer responsible for AML ensure that all subjects of the intra-bank AML/CTF system are familiarized with the Policy. The Bank's Management Board is obliged to ensure that the employees' job descriptions define the responsibilities and powers of employees in the field of AML/CTF.

7. The Policy is not a restricted access document. The Policy or its individual provisions are published on the Bank's website.

2. DEFINITION OF TERMS AND ABBREVIATIONS

8. The following terms and abbreviations (abbreviation) are used in the Policy:

FATF - Financial Action Task Force on Money Laundering;

PEP (PEPs (plural)) - an individual who is politically exposed person, a member of his family or a person related to politically exposed person or another person, whose ultimate beneficial owner is a politically exposed person, a member of his family member or a person related to politically exposed person;

Banking Group - the banking group within the Bank, MICROCREDIT LLC and «KAPOWAI UKRAYINA» LLC;

Compliance Officer responsible for AML - the Bank's responsible employee for conducting financial monitoring;

ML/TF - legalization (laundering) of criminal proceeds, terrorist financing and financing of proliferation of weapons of mass destruction;

IRD – Bank's internal regulatory documents;

USR - the Unified State Register of legal entities, individual entrepreneurs and public formations;

UBO - an ultimate beneficial owner;

USREOU code - an identification code in the Unified State Register of enterprises and organizations of Ukraine;

National Bank – the National Bank of Ukraine;

CDD - customer due diligence;

AML/CTF - preventing and counteracting to legalization (laundering) of the criminal proceeds, terrorist financing and financing of proliferation of weapons of mass destruction;

List of terrorists - the list of persons associated with the conduct of terrorist activities or against whom international sanctions are applied, which is formed in the manner determined By the Cabinet of Ministers of Ukraine and published on the official website of a specially authorized body;

Acceptable level of ML/TF risks - risk that is managed, controlled by the Bank, can not lead to increased legal risk and reputation risk, as well as deterioration of the financial result of the Bank or harm its creditors and clients;**Reputation risk** - an existing or potential risk to revenue and capital that arises from an unfavourable perception of the Bank's image by customers, counterparties, potential investors or supervisory authorities, which affects the Bank's ability to establish new relationships with counterparties, provide new services or maintain existing relationships, and may lead the Bank (or its managers) to financial losses or decrease the client base, bringing to administrative, civil or criminal liability;

Legal risk – the existing or potential risk to the Bank's income or capital that arises from the Bank's violation or non-compliance with the requirements of the laws of Ukraine, regulatory legislative acts and may lead the Bank to financial losses, abuse, bringing the Bank and/or its managers to administrative, civil or criminal liability;

Risk-appetite (risk propensity) of the Bank in AML/CTF - the size of ML/TF risk determined in advance and within the acceptable level of ML/TF risk, in respect of which the Bank made a decision on the expediency /necessity of its maintenance in order to achieve its strategic goals and implement the business plan;

RNTRC - a registration number of the taxpayer’s registration card;

AS - Bank automation system SR;

SSU - the Security Service of Ukraine;

PFME - primary financial monitoring entity;

SAB – a specially authorised body - the Central Executive Body that implements state policy in field of AML/CTF;

9. Other terms and abbreviations used in the Policy are used in the meanings defined by the current legislation of Ukraine and regulatory legal acts of the National Bank of Ukraine.

3. REQUIREMENTS FOR THE ORGANIZATION OF THE INTRA-BANK AML/CTF SYSTEM AND CONDUCTING OF THE PRIMARY FINANCIAL MONITORING, PROPER RISK MANAGEMENT SYSTEM OF THE ML/TF

10. The Bank is the PFME of the national financial monitoring system and carries out relevant measures in the field of AML/CTF.

11. The BANK ensures proper organization and functioning of intra-bank AML/CTF system and conduct of primary financial monitoring, the functioning of a proper risk management system of ML/TF;

12. The purpose of proper organization of the intra-bank AML/CTF system and conducting of primary financial monitoring is:

1) strict compliance by the Bank's employees with the requirements of Ukrainian legislation in the field of AML/CTF;

2) detection (including in automated mode) of threshold and suspicious financial transactions with assets (suspicious activity) and notification of SAB about them;

3) preventing the use of the Bank's services and products to conduct financial transactions by clients for the purposes of ML/TF.

13. The responsibility for improper organization of intra-bank AML/CTF system and conduct of primary financial monitoring shall be born by the Bank's Chairman of the Management Board and Compliance Officer responsible for AML.

14. Proper organization of the intra-bank AML/CTF system and conducting of primary financial monitoring involves the Bank's implementation of the following measures:

1) appointment in accordance with the procedure established by the Bank's Charter and the legislation of Ukraine of the Compliance Officer responsible for AML, who heads the intra-bank AML/CTF system. The Compliance Officer responsible for AML of the Bank is the head of a separate structural unit for AML/CTF, is appointed and dismissed on the basis of a decision of the Bank's Board, is independent in his activities and directly reports to the Bank's Board;

2) creating and functioning of a separate structural subdivision for AML/CTF - Financial Monitoring Department headed by the Bank's Compliance Officer responsible for AML;

3) ensuring the functioning of an appropriate risk management system, applying a risk-oriented approach in its activities on an ongoing basis and taking appropriate measures to minimize risks;

4) development, approval and timely updating of the Bank's IRD on AML/CTF issues to the extent necessary for the effective functioning of the intra-bank AML/CTF system;

5) ensuring that the Bank's collegial management body - the Bank's Management Board considers on ongoing basis the problematic and topical issues of the functioning of the intra-bank AML/CTF system and takes response measures;

6) ensuring sufficient awareness and familiarity of the Chairman, members of the Board, the Chairman, members of the Management Board of the Bank) regarding their responsibilities in the field of AML/CTF, as well as regarding the risks of ML/TF that are inherent to risk-profile of the Bank;

7) ensuring that the Bank's managers are informed about the importance of complying with the requirements of Ukrainian legislation on AML/CTF in order to ensure an appropriate risk management system, the need to take effective measures to effectively prevent the use of the Bank's services for the purposes of the AML/CTF and understanding the consequences that the Bank is exposed to in case of non-compliance with the requirements of Ukrainian legislation on AML/CTF;

8) effective distribution of functions on AML/CTF issues between three lines of defence, ensuring proper implementation by employees of the Bank's business divisions, support divisions defined their responsibilities in the field of AML/CTF, understanding by such employees of their responsibility for failure to perform duties and/or inaction;

9) introduction and continuous improvement of internal control over AML/CTF issues, creation of conditions for timely identification by the Internal Audit Service of problematic issues and signs of an inadequate risk management system of the ML/TF;

10) the study of new products/services, including new channels for the sale, use or development of new technologies for existing or new products in order to properly assess the inherent risks of ML/TF products and to properly control the risks of ML/TF for existing products/services;

11) ensuring the implementation of training activities for Bank employees on an ongoing basis in order to understand the tasks and duties assigned to them;

12) inspection the existence of an impeccable business reputation of all employees of the Bank involved in implementation of the primary financial monitoring;

13) creating and ensuring the functioning of an effective and timely system for escalating suspicions and problematic issues in the field of AML/CTF and the procedure for their review, including reporting information/facts regarding cases of violation or possible violation of Ukrainian legislation in the field of AML/CTF;

14) ensuring sufficient resources for the functioning of the intra-bank AML/CTF system (including the Financial Monitoring Department);

15) timely detection of financial transactions subject to financial monitoring and proper information exchange with the SAB;

16) development and implementation of CDD measures in order to understand the essence of the client's activities, the purpose and expected nature of the business relationship with him, which allows the Bank to be sure that the client's financial transactions correspond to the information available in the Bank about him, his business, risk profile, including, if necessary, the source of origin of his funds/assets, establishing the UBO for the operational detection of unusual behavior and suspicious financial transactions (activities);

17) proper documentation of the Bank's employees' actions and recording of events related to the Bank's fulfillment of PFME duties;

18) storage of all documents (including electronic ones), data, information (including relevant reports, orders, files) relating to the fulfillment by the Bank of PFME duties within the terms determined by the legislation of Ukraine;

19) ensuring access to documents (or information contained therein) on AML/CTF issues, including by providing them at the request of the National Bank and at the reasonable request of law enforcement agencies, in the manner and to the scope established by the Law on Banks;

20) suspension of conducting or ensuring monitoring of the financial transaction of the relevant person in accordance with the procedure established by law by order of the SAB, provided for the purpose of fulfilling the request of the authorized body of a foreign state;

21) suspension the fulfillment of financial transactions or ensuring monitoring of the financial transaction of the relevant person in accordance with the procedure established by law by decision of the SAB;

22) conducting, in accordance with the established procedure, an internal inspection of its activities for compliance with the requirements of legislation in the field of AML/CTF: the introduction of appropriate internal control measures;

23) taking, in accordance with the legislation, measures to ensure that the Compliance Officer responsible for AML receives training in the field of AML/CTF within three months from the date of his appointment, as well as improving the qualifications of the Compliance Officer responsible for AML by completing training at least once every three years on the basis of the relevant educational institution belonging to the management sphere of the SAB and in other educational institutions in agreement with the SAB;

24) ensuring the implementation of committed on the basis, within the limits of authority and in a manner foreseen by the legislation, the requirements of the National Bank on the implementation (elimination of violations) of the requirements of the legislation in the field of AML/CTF;

25) ensuring protection of employees in connection with their notifications of the Chairman of the Management Board and/or the Compliance Officer responsible for AML, the National Bank on violation of the requirements of the legislation in the field of AML/CTF;

26) not to allow the persons who have unexpunged or unspent conviction according to the procedure established by the law for mercenary criminal offenses or terrorism, and also their accomplices in such criminal offenses and who have citizenship (nationality) of the state committing armed aggression against Ukraine, to the management, membership in the Bank's Board, in the Bank's Management Board or control bodies;

27) preventing the formation of the authorized capital of the Bank at the expense of funds whose sources of origin cannot be confirmed;

28) ensuring the continuity of the functioning of the intra-bank system of financial monitoring and interaction with the SAB, the NBU, and other state bodies in case of emergencies;

29) the introduction of an automation system (AS), which should ensure the timely and full fulfillment by the Bank of PFME obligations, taking into account the risks of ML/TF inherent in the Bank's activities in accordance with the requirements of the law.

15. The introduced AS should be aimed at:

1) ensuring to be able to process rapidly of a large amount of data on clients and their financial transactions using appropriate algorithms, scenarios, etc.;

2) strengthening internal control over the fulfillment by employees of their duties on AML/CTF issues;

3) efficient use of the Bank's resources in order to fulfill the tasks and duties of the PFME.

16. The AS shall provide:

1) freezing of assets related to terrorism and its financing, proliferation of weapons of mass destruction and its financing;

2) keeping the Bank's clients questionnaires in electronic form;

3) keeping appropriate registers of Bank's notifications;

4) keeping of information on the Bank's record as PFME;

5) timely information exchange with SAB;

6) maintaining a protocol for the work of each user, protected from modification. The protocol should display the start and end of each user's work with an indication of the time with an accuracy of a second;

7) availability of information protection system that meets the requirements of Ukrainian legislation in the field of information protection;

8) availability of information backup and storage system;

9) ongoing monitoring of clients' financial transactions in order to operational detection the indicators of suspicion of financial transactions;

10) ongoing monitoring of business relations with clients in order to operational detection the inherent risks of ML/TF and the necessity of updating by the Bank the clients' data;

11) operational informing of the Bank's authorized employees about the detected indicators of suspicion of financial transactions, ML/TF risk criteria and the necessity of updating by the Bank the clients' data, determination the priority of such notifications, taking into account their critical importance;

12) functioning of the intra-bank procedure for the escalation of suspicions by the Bank's employees in accordance with the delegated powers/duties (including documenting/recording the facts of the employees sending information notifications about suspicions, making decisions by the addressees about the further escalation of suspicion or making a final decision on the presence/absence of suspicions);

13) documentation of all events in the AS in order to fulfill the above requirements (with recording of the date, time, essence of the event);

14) implementation of other requirements of Ukrainian legislation in the field of AML/CTF and requirements of sanctions legislation.

17. The Bank's Management Board has the right to decide on the inexpediency of introducing certain areas of automation, provided that it properly fulfills all the requirements of Ukrainian legislation in the field of AML/CTF using alternative methods.

Such decision shall be duly documented and approved by the Bank's Management Board in agreement with the Compliance Officer responsible for AML, specifying all reasonable grounds and describing the essence of the available alternative methods.

18. The Bank is obliged, at the request of the National Bank, to provide the decision specified in paragraph 17 of this Policy and to ensure the explanation of the essence of such alternative methods (to demonstrate their work if necessary).

19. The relevant decision can be made in relation to the following areas of automation:

1) ongoing monitoring of business relations with clients in order to operational detection the inherent risks of ML/TF and the necessity of updating by the Bank the clients' data;

2) operational informing of the Bank's authorized employees about the detected indicators of suspicion of financial transactions, ML/TF risk criteria and the necessity of updating by the Bank the clients' data, determination the priority of such notifications, taking into account their critical importance;

3) functioning of the intra-bank procedure for the escalation of suspicions by the Bank's employees in accordance with the delegated powers/duties (including documenting/recording the facts of sending information notifications by employees about suspicions, making decisions by the addressees on the further escalation of suspicion or making a final decision on the presence/absence of suspicions).

20. The Bank ensures the existence of proper internal control (in the context of existing processes/sub-processes) and the determination of Bank employees who are responsible for fulfilling control and making decisions at different stages of control in accordance with their functional responsibilities, ensuring the principle of 'the higher position means greater power and responsibility'.

21. The Bank creates a comprehensive, adequate and effective ML/TF risk management system that meets to its size, business model, scope of activity, types, complexity of the Bank's operations and ensures detection, measurement (assessment), monitoring, reporting, control and mitigation of ML/TF risks, which takes into account the specifics of the Bank's activities and meets the following principles:

efficiency - ensuring an objective assessment of the size of ML/TF risks and the completeness of risk management measures with the optimal use of financial resources, staff and information systems for risk management of the Bank;

timeliness - ensuring timely (at an early stage) detection, measurement, monitoring, control, reporting and mitigation of ML/TF risks at all organizational levels;

structuring - clear distribution of functions, duties and powers on ML/TF risk management between all structural divisions and employees of the Bank, and their responsibility according to such distribution;

differentiation of duties (separation of the control function from the Bank's operations) - avoidance of a situation in which the same person fulfills the Bank's operations and conduct control functions;

comprehensiveness and complexity - coverage of all activities of the Bank that generate ML/TF risk at all organizational levels and in all its structural divisions;

proportionality - compliance of the ML/TF risk management system with the Bank's business model, its systemic importance, as well as the level of complexity of operations carried out by the Bank;

independence - freedom from circumstances that pose a threat to the impartial fulfillment of its functions by the Financial Monitoring Department and the Bank's The Compliance Officer responsible for AML;

confidentiality - restriction of access to information that should be protected from unauthorized acquaintance;

transparency - disclosure by the Bank of information on the risk management system and risk profile (taking into account the requirements for disclosing information on its activities in the field of AML/CTF in accordance with the requirements of the current legislation of Ukraine, regulatory requirements, market behavior standards, IRD on AML/CTF issues).

22. The procedure for ensuring certain necessary measures to create the proper organization and functioning of the intra-bank AML/CTF system and conducting primary financial monitoring, a description of the functioning of the proper risk management system of the ML/TF is set by the Bank in the Bank’S IRD on AML/CTF issues.

4. THREE LINES OF DEFENCE IN THE FIELD OF AML/CTF AND THE DISTRIBUTION OF DUTIES AND RESPONSIBILITIES BETWEEN THE BANK’S EMPLOYEES.

23. The Bank’s Board and the Management Board of the Bank are subjects of the ML/TF risk management system but are not subjects of defence. These management bodies are responsible for defining the Bank’s goals, strategies for achieving these goals and determining the optimal

organizational structure for roles and responsibilities related to ML/TF risks and are main responsible for the activities of the first, second and third lines of defence within their competence.

24. **The Bank's Board:**

1) determines the policy (general principles) of ML/TF risk management in the Bank and controls the proper organization of the intra-bank AML/CTF system, in particular, approves and proves this Policy to the Bank's Management Board and the Bank's Compliance Officer responsible for AML;

2) makes decisions on the appointment/dismissal of the Bank's Compliance Officer responsible for AML and controls on ongoing basis the compliance of the Bank's Compliance Officer responsible for AML with the requirements established by law;

3) creates a separate structural division on AML/CTF issues headed by the Compliance Officer responsible for AML;

4) defines the requirements for the risk appetite of the Bank as a whole and in the field of AML/CTF and establishes the main prohibitions/restrictions on the conduct of certain types of activities and/or the involvement of certain types of customers;

5) reviews at least once a year the report of the Bank's Compliance Officer responsible for AML on the results of the assessment of the Bank's ML/TF risk profile, problematic issues related to the creation of a proper organization of the intra-bank AML/CTF system and financial monitoring, including problematic issues related to ensuring the proper risk management system of ML/TF, approves the relevant decision on the results of such consideration and proves to the Management Board and the Bank's Compliance Officer responsible for AML for its further execution;

6) introduces and constantly improves internal control over AML/CTF issues, in particular, ensures timely detection by the audit of problematic issues and signs of an improper risk management system of the ML/TF.

25. **The Bank's Management Board:**

1) in accordance with the approved Policy, it ensures the creation and proper functioning of the intra-bank AML/CTF system, the primary financial monitoring, the functioning of the proper risk management system of the ML/TF;

2) ensures the development and approval of the Bank's IRD in the field of AML/CTF, including risk management of the ML/TF within its powers;

3) ensures that the information of the Compliance Officer responsible for AML on the functioning of the internal AML/CTF system and the adoption of response measures is reviewed at least once a quarter, in particular:

1) results of monitoring of business relations with clients, as a result of which suspicious activities of clients were detected, and proposals for taking the necessary measures in relation to such clients in order to minimize the risks of ML/TF;
2) issues related to proposals for refusal to continue business relations with clients (including in case of establishing an unacceptably high level of risk to the client);
3) problematic issues arising during conducting the CDD measures in the Bank;
4) changes in the legislation of Ukraine on AML/CTF issues and the Bank's taking the necessary measures in connection with such changes (in particular, updating the Bank's IRD on AML/CTF issues) with indicating the timing of such measures;
5) results of assessment of new banking products/services and inherent risks of ML/TF;
6) problematic issues regarding conducting of training activities for Bank employees;
7) problematic issues related to the establishment of business relations with PEPs and/or their maintenance;
8) other issues regarding the Bank's compliance with the requirements of Ukrainian legislation in the field of AML/TF, which require consideration.

4) ensures the sufficiency of resources for the functioning of the intra-bank AML/TF system;

5) ensures that all Bank employees involved in the primary financial monitoring have an impeccable business reputation.

26. **The Chairman of the Management Board:**

1) manages the work of the Management Board of the Bank;

2) grants permission to establish (maintain) business relations with the PEP (in cases that are established in the Bank's IRD on AML/CTF issues) and foreign financial institutions, delegates the authority to grant permission to establish (maintain) business relations with the PEP that have ceased to perform certain public functions (in cases that are established in the Bank's IRD on AML/CTF issues);

3) grants permission to establish relations with agents, third parties on CDD issues (subject to the Management Board's decision to allow the use of the relevant services);

4) reviews notifications of violations in the field of AML/CTF,

5) approves the training plan in AML/CTF field,

6) provides protection for employees who have reported regarding violations in the field of AML/CTF;

7) organizes proper storage of documents and preparation of reports;

8) issues orders, approves procedures, methods for practical implementation of the Bank's IRD in the field of AML/CTF, distribution of duties of employees of the 1st line of defence;

9) approves job descriptions of the Bank's employees (except for employees of divisions 2nd and 3rd lines of defense), in which, by agreement with the Compliance Officer responsible for AML, the powers and duties of employees in the field of AML/CTF are determined.

27. The defence system in AML/CTF field is based on the distribution of duties between the Bank's divisions following the model of three lines of defence:

28. **1st LINE OF DEFENCE** - at the level of business divisions and support divisions of the Bank, which are the owners of all risks arising in the sphere of their responsibility, in particular, ML/TF risks. They ensure the implementation of measures in the field of AML/CTF during the fulfillment of official duties and are responsible for detecting, assessing risks, taking certain measures to manage risks and reporting on such risks during the implementation of activities.

29. **2nd LINE OF DEFENCE** - at the level of the Financial Monitoring Department, as well as the Compliance Officer responsible for AML.

The Financial Monitoring Department carries out its activities under the supervision of the Compliance Officer responsible for AML - Head of the Financial Monitoring Department and participates in the organization and implementation of activities in the field of AML/CTF. The Compliance Officer responsible for AML is the main liaison between the Bank's divisions and the Supervisory Board within the ML/TF risk management system.

Compliance Officer responsible for AML:

1) organizes primary financial monitoring in the Bank;

2) organizes the implementation of measures to reduce the risks of ML/TF;

3) ensures the information exchange with SAB in cases established by law, as well as notification of authorized state bodies in the manner established by law, on the detection of discrepancies between the information received by the Bank as a result of the implementation of the CDD and the information on UBO and the client's ownership structure placed in the USR (in particular, on the detection of incompleteness, inaccuracies or errors in information about UBO or the ownership structure of such client contained in the USR);

4) organizes the development, submission for approval, ensuring constant updating, and control over implementation of Bank’s IRD requirements on AML/CTF issues;

5) conducts inspections of the activities of Bank’s divisions and its employees for the implementation of requirements of Bank’s IRD on AML/CTF issues;

6) ensures submission of information on financial monitoring issues at the requests of SAB and appropriate law enforcement agencies;

7) ensures execution the decisions/orders of SAB;

8) makes decision on the freezing of assets related to terrorism and its financing, proliferation of weapons of mass destruction and its financing, with subsequent notification to the SAB and the Security Service of Ukraine;

9) reports at least once a year to the Bank's Board on:

- results of assessment of the Bank's risk profile on ML/TF issues;
- problematic issues related to the creation of a proper organization of the intra-bank AML/CTF system;
- problematic issues related to the ensuring of an proper ML/TF risk management system.

10) informs the Chairman of the Management Board in accordance with the requirements of the Law on AML/CTF on detected financial transactions subject to financial monitoring and measures taken, in particular, for:

- ensuring the conducting of primary financial monitoring;
- development and updating of the Bank's IRD on AML/CTF issues;
- training of staff to comply with the requirements of the Law on AML/CTF through educational and practical work.

11) consider reports of possible violations of the requirements of the legislation, Bank'S IRD in the field of AML/CTF received from the Bank's employees through separate communication channels;

12) facilitates inspections of the Bank by authorized representatives of the National Bank to comply with the requirements of legislation in the field of AML/CTF;

13) performs other functions in accordance with the legislation of Ukraine, the Bank's IRD on AML/CTF issues, the job description of the Compliance Officer responsible for AML.

The Financial Monitoring Department performs the following functions for ML/TF risk management:

1) measures to ensure the proper organization of the intra-bank AML/CTF system, the organization of the necessary measures to comply with the requirements of the AML/CTF legislation by the Bank's employees, including the functioning of an effective and timely system for the escalation of suspicions and problematic issues on the AML/CTF issues, the functioning of an proper risk management system for the ML/TF;

2) exercise of powers that belongs exclusively within the competence of the Financial Monitoring Department and/or the Compliance Officer responsible for AML, including maintaining registers in the field of AML/CTF, determined by law, and information exchange on financial monitoring issues with the SAB, provision of information to the Security Service of Ukraine and other authorized state bodies, assessment and submission for approval to the Bank'S Board the Bank's risk profile, etc.

3) implementation of internal control measures, including further control of financial transactions, preparation of reports on issues related to risk management of AML/CTF of the Bank stipulated by the Policy;

4) methodological support of the Bank's employees on AML/CTF issues; conducting on an ongoing basis training and qualification improvement of Bank's employees and agents (their employees) [if any]

5) definition of measures and provision of proposals on the list, scope of measures and necessary additional resources in the field of AML/CTF to reduce risks based on the results of detection and assessment of relevant risks, the control over the implementation of measures;

6) other measures defined by the Bank's IRD in the field of AML/CTF.

An exhaustive list of the functions of the Financial Monitoring Department regarding the role and powers in the AML/CTF system is defined in the Regulation on the Financial Monitoring Department, as well as other IRD of the Bank, which describe the interaction of the Bank's divisions in the field of AML/CTF.

30. **3rd LINE OF DEFENCE** - at the level of the Internal Audit Service, which, on the basis of a risk-oriented approach:

1) organizes and conducts, in accordance with Article 8 of the Law, internal inspections on the Bank's compliance with the requirements of Ukrainian legislation in the field of AML/CTF (including the sufficiency of measures taken by the Bank to ensure the functioning of the proper risk management system of the ML/TF);

2) carries out an independent assessment of the internal control system created by the Bank's management over compliance by the Bank's employees with the regulatory legal acts of the National Bank and the Bank's IRD on financial monitoring issues;

3) provides the Bank's Board, the Bank's Management Board with independent objective judgments, conclusions and assessments regarding the adequacy and effectiveness of the ML/TF risk management system;

4) timely identifies problematic issues and signs of an improper ML/TF risk management system;

5) analyzes the adequacy and effectiveness of the AS introduced by the Bank to fulfill the PFME obligations of the Bank;

6) ensuring the compilation of reports, conclusions and proposals for submission to the Bank’s Board;

7) fulfilling the control over elimination of detected violations, shortcomings, comments.

31. In order to prevent violations of legislation in the field of AML/CTF, the Bank determines in the IRD the employees who make decisions at different stages of control in accordance with their functions, ensuring the principle of 'the higher position means greater power and responsibility', and establishes a clear division of duties and powers between the Bank's Board, the Chairman of the Management Board, the Management Board/members of the Management Board, the Compliance Officer responsible for AML, other employees and structural divisions of the Bank.

32. The distribution of duties, responsibility of employees, involved in the process of the Bank's activities in the field of AML/CTF, is determined in their job descriptions and/or contracts and Bank’s IRD, regulating the activities of employees, divisions, including the IRD on financial monitoring. Employees familiarize themselves with such documents against signature (including the use of an electronic signature).

33. The Chairman of the Management Board and other employees of the Bank shall facilitate the implementing by the Compliance Officer responsible for AML of his functions.

5. DETERMINATION OF RISK APPETITE OF THE BANK IN THE FIELD OF AML/CTF. MAIN PROHIBITIONS AND RESTRICTIONS

34. In its activities, the Bank applies a risk-oriented approach, which should be proportional to the nature and scale of the Bank's activities. Risk-oriented approach is applied by the Bank on a continuous basis and foreseen the determination (detection), identification, assessment/measurement (reassessment/monitoring)/and understanding of existing and potential risks of ML/TF inherent to the Bank (risk profile of ML/TF of the Bank) and its clients, as well as taking appropriate measures to manage ML/TF risks in the manner and to the scope to ensure minimization/mitigation of such risks depending on their level.

35. The risk-oriented approach of the Bank is based on a two-stage risk assessment and includes the assessment of the Bank's risk profile (including the determination of the Bank's risk appetite in the field of AML/CTF (acceptable for the Bank level of ML/TF risk) and the assessment of the client's risk profile.

36. Applying a risk-oriented approach, the Bank refrains from unreasonably applying de-risking, which contradicts the risk-oriented approach and does not promote to financial inclusion.

37. To assess ML/TF risks, the Bank uses a 4-level scale, which identifies the following risk levels:

- ✓ low
- ✓ medium

- ✓ high
- ✓ unacceptably high.

Methods for assessing the Bank's risk-profile, assessing the risk-profile of clients, the procedure for determining (identifying) and carrying out of assessment the clients' risks are defined by Management Board in Bank's IRD in the field of AML/CTF.

38. The Bank assesses its own risk profile of ML/TF taking into account the specifics of its activities and the following factors:

- the specifics, nature and scale of the Bank's activities;
- products and services provided by the Bank;
- types of clients and their risk profile;
- geographical location of the state of registration of clients or institutions through which the Bank transfers (receives) assets;
- channels/methods of providing (receiving) services;
- other significant factors related to the Bank's activities, in particular, but not exclusively, the results of the national risk assessment, the geographical location of the Bank and its separate divisions.

The Bank regularly, when updating its risk profile, reviews existing risk management measures regarding their adequacy and effectiveness and develops additional measures if, according to the results of the analysis of existing measures, it is not enough for effectively management by ML/TF risks.

39. The Bank, analyzing the risks of AML/CTF of its products and services, takes into account the features and possibilities of their use, in particular:

1) the intended use of the product and/or service:
   - whether the Bank's products and/or services allow to mask the illegal origin of funds, transfer funds to finance terrorist activities, promote the anonymity of participants in the financial transaction (hide the real final recipients of certain products and/or services);
   - whether they can be used by the client on behalf of third parties;
   - can be interesting for shell companies;
2) special opportunities for using the product and/or service: whether the product and/or service allows the Bank's client to carry out transactions with counterparties/business segment, which have increased risks in the field of ML/TF;
3) target segment for the implementation of a product and/or service: the types of clients who most/most often use a particular product and/or a particular service.

40. Based on the assessment of the Bank's inherent risks of ML/TF, the Bank determines its risk appetite (acceptable risk level) in the field of AML/TF, taking into account and determining:

- risks that the Bank is willing to accept;
- risks that the Bank can take, but only after taking measures to manage such risks (minimize them);risks that are unacceptable for the Bank.

41. The risk appetite of the Bank (exposure to risk) in the field of AML/CTF is determined in accordance with the Declaration of exposure to risks and the structure of the risk appetite of the Bank, which is approved by the Supervisory Board in accordance with internal procedures. The Bank sets limits (restrictions) for ML/TF risk management within the approved risk appetite if necessary.

42. The Supervisory Board and the Management Board of the Bank, when determining the Bank's Development Strategy and drawing up the Bank's Business Plan/Budget, take into account the amount of risk appetite specified in the Declaration of exposure to risks and the structure of the Bank's risk appetite.

43. In order to prevent exceeding the level of risk appetite (exposure to risk) in the field of AML/CTF, the Bank adheres to a policy of zero tolerance to any manifestations of illegal

activities of persons with whom the Bank enters into business (contractual) relations and/or to whom it provides services.

44. In the course of business, the Bank sets certain prohibitions/restrictions in its activities in part of establishing business relations, conducting certain transactions, taking into account their unacceptable risk for the Bank, in particular:

1) does not open and maintain anonymous (numbered) accounts;

2) does not establish correspondent relations with shell banks, as well as with banks and other non-resident financial institutions for which it is known that they maintain correspondent relations with shell banks;

3) does not carry out client and interbank financial transactions of other banks with which the correspondent has established correspondent relations through a correspondent account opened with the Bank;

4) does not establish business relations (except in cases stipulated in the UN Security Council resolutions) and does not conduct expenditure financial transactions, does not provide services directly or indirectly to the clients who are:

- persons and/or organisations included in the List of terrorists;
- persons and/or organisations acting for and on behalf of persons and/or organisations included in the List of terrorists;
- persons and/or organisations directly or indirectly owned or ultimately beneficially owned by persons and/or organisations included in the List of terrorists.

The prohibitions provided for in this sub-clause of the Policy shall also apply if the counterparty to a financial transaction or a financial institution that ensure the fulfillment of a financial transaction is a person and/or organization that is included in the List of terrorists, and the Bank became aware of this during the provision of services/execution of the transaction;

5) The Bank refuses to establish (maintain) business relations/refuses the client to open an account (servicing), including by termination of business relations, closing the account/refusal to conduct a financial transaction in case:

- if identification and/or verification of the client, and establishment of data that allow to identify the ultimate beneficial owners, is impossible or if the Bank has doubts that the person acts on own behalf;
- establishing an unacceptably high risk for the client or failure of the client to provide the documents or information necessary for the due diligence of the client;
- submission by the client or his representative to the Bank of unreliable information or submission of information for the purpose of misleading the Bank;
- detection the fact that the bank or other financial institution with which the correspondent relationship has been established is a shell bank and/or such bank or financial institution 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 carried out and establish its ultimate beneficial owner or beneficiary (beneficial owner) under the financial transaction.

6) establishes restrictions (using automation tools) on the implementation of a payment transaction in the absence of mandatory information, which should be accompanied by a payment transaction or transfer of virtual assets;

7) does not establish/maintain business relations with clients/counterparties and does not carry out financial transactions of the Bank's clients if at least one of the parties participating in the financial transaction has the appropriate registration, place of residence or location (residency) in a state/self-proclaimed territory or for fulfillment of transaction is used an account opened with financial institution registered in a state/self-proclaimed territory, or use documents issued in its name by a state/self-proclaimed territory that is on the list of territories or countries that:

- support terrorism;
- conduct military operations;

- do not comply or do not properly comply with the recommendations of international, intergovernmental organizations that carry out activities in the field of combating ML/TF;
- are self-proclaimed;
- not recognized by Ukraine.

To the list of above territories or countries, the Bank includes:

No.	Country code	Character code of the country	Name
1	364	IRN	Iran, Islamic Republic
2	408	PRK	Democratic People's Republic of Korea
3	643	RUS	Russian federation
4	104	MMR	Republic of the Union of Myanmar
5	112	BLR	Republic of belarus
6	728	SSD	Southern Sudan
7	760	SYR	Syrian Arab Republic
8	-	-	Pridnestrovien Moldavian Republic
9	-	-	Nagorno-Karabakh Republic
10	-	-	Somaliland
11	-	-	Republic of Kosovo
12	-	-	Sudan (North)
13	-	-	Republic of Abkhazia
14	-	-	South Ossetia
15	-	-	Donetsk People's Republic
16	-	-	Luhansk People's Republic
17	-	-	Crimea (a ban on business entities, as well as on persons whose residence in the territory of Crimea and Sevastopol is confirmed by a document issued not by Ukraine)

The list of territories may be expanded by order of the Chairman of the Management Board on the proposal of the Compliance Officer responsible for AML for the purpose of operational ML/TF risk management.

The Bank's Management Board is entitled to determine the list of countries with residents of which the Bank establishes business relations only with the permission of the Chairman of the Management Board.

9) the Bank does not establish/maintain business relations with clients who conduct operations/whose business activity of which is aimed at the production of narcotic drugs (except for institutions that have a state license), marijuana (except for medical cannabis allowed for circulation in Ukraine), provision of services for ‘adult entertainment’.

45. Risks that the Bank can take, but only after taking measures to manage (minimize) such risks:

✓ by decision of the Bank’s Management Board business relations are established with clients who:

- provide employment services abroad;
- trade in military weapons (does not apply to hunting weapons);
- hold lotteries and/or gambling;
- carry out activities in field of nuclear energy;
- engaged in the collection and trade in agricultural products;
- engaged in the collection and trade in scrap metal;
- engaged in trade in gas and or oil products;
- provide/participate in the circulation of virtual assets;

✓ Business relations with charitable organizations and non-resident legal entities registered in the countries listed by the Cabinet of Ministers of Ukraine as offshore zones are

established with the approval of the Compliance Officer responsible for AML and the permission of the Chairman of the Management Board.

✓ Business relations with a PEP (in the cases established in the Bank's IRD in the field of AML /CTF) and foreign financial institutions are established with the permission of the Chairman of the Management Board.

46. The Bank determines (if necessary) in its IRD on AML/CTF issues additional prohibitions/restrictions in its activities (in relation to certain types of activities and/or attracting certain types of clients for service) in order to manage risks arising during the activities.

47. All other ML/TF risks may be accepted by the Bank, including after taking risk management measures (minimize them). Taking appropriate risks, the Bank takes into account the availability of effective measures to manage them, in particular, the availability of necessary resources.

48. During the establishment of business relations, as well as during the execution of any financial transactions of the Bank's clients, operations performed in favor of the Bank's clients, as well as its own operations, the Bank checks whether the participant or beneficiary of the transaction is not included in the list of persons subject to sanctions. Relevant checks are carried out by means of AS (as far as it is possible), and include at least the following lists:

1) List of persons involved in terrorist activities;

2) National sanctions lists established by the National Security and Defence Council of Ukraine and approved by Presidential decrees and other legislative acts;

3) lists of Office of Foreign Assets Control (OFAC);

4) lists of European Union (EU);

5) lists of United Nations (UN);

6) Black list of the Bank.

6. FUNCTIONING OF INTERNAL CONTROL

49. The Bank’s internal control system should ensure sufficient confidence of the Bank’s Board and Management Board regarding the Bank's proper fulfillment of the PFME obligations and prevention of using the Bank for ML/TF.

50. All participants of the intra-bank AML/CTF system participate in ensuring internal control on AML/CTF issues, including business divisions, support divisions, the Financial Monitoring Department and the Bank's Compliance Officer responsible for AML, the Risk Department, the Compliance Department, the Internal Audit Service.

51. The functioning of the internal control system on AML/CTF issues is based on the distribution of responsibilities between the Bank's divisions, other risk management entities of the ML/TF and is based on the application of the model of three lines of defence:

- *the First line of defence* (operating, current control) includes all daily controls carried out at the individual level or the level of the responsible division, which are defined in the Bank's IRD on AML/CTF issues as ensuring the implementation of AML/CTF measures. Such controls, in particular, are: its own control (carried out by the employee on their own), automatic controls, control on the principle of "two pairs of eyes";

- *the Second line of defence* focuses on the functions of the Financial Monitoring Department and the Bank's Compliance Officer responsible for AML through their fulfillment:

✓ Ongoing control over:

- ensuring that the Bank's IRD on AML/TF issues is updated within the time limits established by law;
- updating in the AS the lists of persons subject to sanctions/restrictions determined by the legislation of Ukraine;
- training of Bank’s employees involved in the AML/TF system;

✓ Selective periodic further control over:

- proper compliance with the requirements of legislation and established processes for the purpose of CDD by employees, business divisions, support divisions;
- detection of threshold financial transactions;
- preparation of reporting, including data on ML/TF risks;
- other control measures regarding the proper organization of the intra-bank AML/CTF system and the fulfillment of primary financial monitoring, risk management in the field of AML/CTF.

- *the Third line of defence* is provided by the Internal Audit Service, which carry out inspections of the effectiveness of the internal control system, in particular, ensures the timely detection of problematic issues and signs of an improper ML/TF risk management system.

The Financial Monitoring Department and other divisions of second line of defence interact with each other in part of determination of levels and types of risk that the Bank intends to accept or should avoid in order to achieve its business goals, detect operational risk incidents and compliance risk.

52. Responsibility for compliance by the Bank's employees with the requirements of the AML/CTF legislation is assigned to each employee of the Bank (within the job duties determined by job descriptions), as well as its direct chief, the Bank’s managers and Bank's Compliance Officer responsible for AML (a person temporarily exercising the powers of the Bank's Compliance Officer responsible for AML in his absence), as well as other employees involved in the implementation of these measures, in case of violation of the requirements on AML/CTF issues are responsible in accordance with the law.

53. Responsibility for organizing, ensuring and controlling the implementation of the requirements of the Policy (processes and operations regulated by the Policy) is assigned to the Chairman of the Management Board and the Bank's Compliance Officer responsible for AML. Support and current control of the processes defined by the Policy is carried out by the Financial Monitoring Department, which is the owner of the process.

54. The responsibility for control of organization the compliance with the requirements of the Policy and the result of the process is assigned to the Bank's Board and the Bank's Compliance Officer responsible for AML.

7. PROVISION OF TRAINING ACTIVITIES ON AML/CTF ISSUES

55. In order to properly comply with requirements of the legislation in AML/CTF the Bank engages competent persons to perform functions and duties, ensures the maintenance of an proper level of employees' qualification, in particular by conducting training activities in AML/CTF issues.

The Compliance Officer responsible for AML on an ongoing basis keeps his level of knowledge in AML/CTF issues at the proper level, including through AML/CTF training, as well as advanced training.

The content of the Bank's training activities takes into account the specific of employees' job descriptions, their powers and responsibilities, as well as the level of knowledge and qualifications required for such employees in order to properly fulfill their duties in AML/CTF.

56. The Compliance Officer responsible for AML ensures awareness of the Management Board and the Bank employees involved in the AML/CTF procedures with changes in legislation, guidelines of world organizations in AML/CTF and changes in the Bank's IRD on AML/CTF issues.

57. Measures to organize training and advanced training of employees are taken by the Bank on an ongoing basis.

58. The purpose of staff training is to ensure the proper level of their professional background for a thorough understanding of their responsibilities and procedures, for timely detection of transactions subject to financial monitoring, and to prevent attempts to use the Bank's system for ML/TF.

59. Training activities, if necessary, are completed by a test of knowledge with subsequent assessment of the results of inspections by management.

60. The description of the intraq-bank financial monitoring system, in particular, the set effective risk-oriented procedures that are sufficient for the proper organization and functioning of the AML/CTF system and conducting primary financial monitoring is defined in the Bank's IRD on financial monitoring. The main requirements for development of the Bank's IRD on financial monitoring issues are defined in section 8 of the Policy.

61. The Bank pays considerable attention to the training of the Bank's Compliance Officer responsible, employees of the Financial Monitoring Department and employees of the Internal Audit Service in order to maintain their proper level of knowledge and qualifications in the field of AML/CTF.

8. BANK'S REGULATORY DOCUMENTS ON AML/CTF ISSUES

62. The Bank develops and approves IRD on AML/TF issues in scope necessary for the effective functioning of the intra-bank AML/TF system.

63. In accordance with the requirements for construction an intra-bank AML/CTF system established in the legislation and this Policy, the Bank develops internal documents of a regulatory and administrative nature (regulations, instructions, methods, rules, directives, decisions, orders, job descriptions, description of procedures and operational processes, other internal documents regulating the activities of the Bank). The Management Board of the Bank should develop, approve and ensure the implementation and control over the implementation of in particular:

- Financial Monitoring Rules of the Bank;
- Program for implementation of due diligence measures for the Bank's clients;
- Risk management programs for financial monitoring of the Bank;
- Training and advanced training program for the Bank's employees on issues of preventing the legalization (laundering) of criminal proceeds, financing of terrorism, financing of the proliferation of weapons of mass destruction;
- Procedure for accompanying of payment transactions or transfers of virtual assets with the necessary information;
- Procedure for implementation of special economic and other restrictive measures (sanctions).

The Bank's IRD on AML/CTF issues of a regulatory nature are approved by the Bank's authorized management bodies.

The Bank's Management Board has the right to develop and approve other documents on AML/CTF issues in order to improve the AML/CTF system.

The Chairman of the Management Board has the right to approve methods, temporary procedures, distribution of powers between employees of divisions of the 1st line of defence, job descriptions of employees in order to resolve practical issues of implementing the requirements of the Bank's IRD on AML/CTF issues.

The Compliance Officer responsible for AML develops guidelines, clarifications, other documents to ensure proper application by the employees the Bank's IRD on AML/CTF issues and proper fulfillment by the the Bank the duties of PFME.

64. The basic principles for the development and implementation of Bank's IRD on AML/CTF issues are:

- proper organization and functioning of the effective intra-bank AML/CTF system and conducting primary financial monitoring, functioning of proper ML/TF risk management system;
- introduction of a risk-oriented approach during implementation of AML/CTF procedures;
- fulfilling by the Bank of all duties in AML/CTF field stipulated by the legislation;
- taking into account all types and activities of the Bank;
- introduction of AML/CTF culture in the Bank and ensuring the direct participation of each employee (within his competence) in the implementation of AML/CTF procedures;

- clear division of duties and powers between the Bank's Board, the Chairman of the Management Board, members of the Management Board, the Compliance Officer responsible for AML, other employees and structural divisions of the Bank in order to prevent violations of the legislation on AML/CTF field;

- the existence of proper internal control (for different types of services/products, types of clients, the level of clients' risks, the amount of financial transactions) and determination of the Bank's employees who make decisions at different stages of control in accordance with their functions for ensuring the principle of 'the higher position means greater power and responsibility';

- establishing a detailed and as clear as possible the understandable procedure for the Bank's employees during implementation by them the AML/CTF procedures;ensuring the secrecy of financial monitoring and confidentiality of information about information exchange with the SAB, including the fact of transmitting information about the client's financial transaction to the SAB;

- ensuring confidentiality of information about IRD on AML/CTF issues;

- ensuring the confidentiality of information about clients, their accounts and financial transactions, as well as other information that constitutes Bank secrecy;

- prevention of involvement of the Bank employees in ML/TF.

65. The Policy does not define an exhaustive list of Bank's IRD on AML/CTF issues. At the same time, in order to carry out its activities, the Bank must take into account the peculiarities and directions of activity, the peculiarities of different types of clients, as well as the need to implement a risk-oriented approach in the field of AML/CTF, and the Bank's IRD on issues of AML/CTF must contain:

- determination of the Bank's division(s) and/or Bank employees responsible for implementation of CDD measures and distribution of responsibilities between them;

- the procedure that ensures the implementation of all measures for the CDD (in particular, measures for identification and verification, identification of an UBO, monitoring of business relations and financial transactions, updating client's data);

- the procedure for detection of PEP and the procedure for taking required supplementary measures;

- the procedure for evaluating/revaluing the Bank's risk profile, risk profile of clients and taking meaures to minimize ML/TF risks;

- the procedure for detection of ML/TF risk criteria and indicators of suspicious financial transactions;

- the procedure for taking necessary extra measures for establishment of correspondent relations with a foreign financial institution;

- the procedure for keeping an electronic questionnaire, which will ensure the timeliness, completeness and reliability of the information entered into the client's electronic questionnaire;

- the procedure for the Bank's refusal to establish (maintain) business relationship/open an account (servicing), including by terminating a business relationship, closing an account/refusing to conduct a financial transaction in cases foreseen by the Law on AML/CTF;

- the procedure for the Bank to detect the discrepancies between the information about the UBO contained in the USR and the information received by the Bank as a result of CDD;

- the procedure for using the reliance tool (if the Bank decides to use this tool);

- the procedure for involving agents by the Bank, conducting training activities for them (their employees) and conducting control over their activities (if the Bank decides to involve agents);

- the procedure for entering relevant information into the notification registers;

- the procedure for using the AS;

- the procedure for information exchange with the SAB and fulfilling of relevant SAB's decisions/instructions;

- the procedure for freezing assets related to terrorism and its financing, proliferation of weapons of mass destruction and its financing;

- the procedure for suspension by the Bank the operations in cases defined by the Law;

- the procedure for Bank's accompanying of payment transactions or transfers of virtual assets with relevant information in accordance with the requirements established by the Law;

- the procedure for controlling the relevant limits in case the Bank applies simplified methods of identification and verification of the client (client's representative);

- the procedure for ensuring the secrecy of financial monitoring, confidentiality of other information;

- the procedure for informing the SSU in cases stipulated by the legislation in AML/CTF field;

- the procedure for conducting training activities for the Bank employees;

- the procedure for familiarising the Bank's employees with the Bank's IRD on AML/CTF issues;

- the procedure for storing all documents/information on the Bank's compliance with the requirements of legislation in AML/CTF field.

66. The Bank shall independently determine and document the procedure for classifying the Bank's IRD on AML/CTF issues as restricted documents and the procedure for access to them by the Bank's employees and third parties.

67. The Bank's IRD on AML/TF issues should be relevant, consider events that may affect the Bank's ML/TF risks. Renewal (updating) of the Bank's IRD on AML/CTF issues is carried out on an ongoing basis, but not later than three months from the date of entry into force of amendments to the legislation of Ukraine on AML/CTF issues and/or the establishment by the Bank of events that may affect the risks of the ML/TF.

68. In case of changes in the legislation, detection of schemes, typologies of transactions that carry increased risks of ML/TF before updating the Bank's IRD and in order to prevent the Bank from violating the legislation or involving the Bank in the ML/TF, the Compliance Officer responsible for AML shall have the right to issue orders for changes in certain procedures for the functioning of the AML/CTF system in terms of strengthening controls, prohibiting certain transactions, refraining from actions, etc.

9. FINAL PROVISIONS

69. The Policy is indefinite, comes into force after its approval by the Bank's Board and is valid until its cancellation, or the approval by the Bank's Board of a new Policy, with the entry into force of which the previous one loses the strength.

70. With the entry into force of this Policy, the Policy of Preventing and Counteracting to Legalization (Laundering) of the Proceeds from Crime, Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction of JSC «BANK 3/4», approved by the Bank’s Board decision from 21.09.2023 (Protocol No. 15), loses the strength.

71. The Policy is reviewed, if necessary, but at least once a year. Based on the results of the revision, the Bank's Board is entitled to decide on the inexpediency of amending the Policy. Amendments and/or additions to this Policy shall be made by their approval by the Bank's Board in due course.

72. In case of non-compliance of any part of this Policy with the current legislation of Ukraine and regulatory legal acts of the National Bank, including in connection with the adoption of new regulatory legal acts and/or amendments to existing ones, this Policy will operate only in the part that does not contradict the current legislation and regulatory legal acts of the National Bank. Prior to making appropriate changes to this Policy, employees of the Bank in their work should be guided by the norms of the current legislation of Ukraine.