[COPY]

APPROVED

By the decision of the Supervisory Board of
JSC “CRYSTALBANK”
Minutes No. 80
dd. August “20”, 2020

Chairman of the Supervisory Board

/signature/ V.A. Kopylov

POLICY
of JSC “CRYSTALBANK”
on preventing and countering to legalization (laundering) of the proceeds of crime, terrorist financing and financing proliferation weapons of mass destruction

Kyiv

2020

INTERNAL DOCUMENT RECORD CARD

<table>
<tr><td>The document title</td><td colspan="4">Policy of JSC “CRYSTALBANK” on preventing and countering to legalization (laundering) of the proceeds of crime, terrorist financing and financing proliferation weapons of mass destruction</td></tr>
<tr><td>Decision on the document approval</td><td colspan="4">Minutes of the Supervisory Board of JSC “CRYSTALBANK” No.80 dd. August 20, 2020</td></tr>
<tr><td rowspan="2">The requirement to submit the document to regulatory and monitoring authorities</td><td rowspan="2">yes</td><td colspan="3">Name of the authority</td></tr>
<tr><td colspan="3">In case of request from the National Bank of Ukraine</td></tr>
<tr><td>Department – compiler/owner of the document</td><td colspan="4">Financial Monitoring Service</td></tr>
<tr><td rowspan="2">The document completed by</td><td colspan="2">Title</td><td>Signature</td><td>Name</td></tr>
<tr><td colspan="2">Head of the Financial Monitoring Service</td><td>/signature/</td><td>Ya.V. Korzhenivskyi</td></tr>
<tr><td rowspan="4">The document agreed by</td><td colspan="2">Deputy Chairman of the Management Board</td><td>/signature/</td><td>I.M. Zhabska</td></tr>
<tr><td colspan="2">Head of the Compliance Control Service</td><td>/signature/</td><td>S.O. Kondrasheva</td></tr>
<tr><td colspan="2">Head of the Department of Methodology of Internal Documentation</td><td>/signature/</td><td>L.Ye. Vystoropska</td></tr>
<tr><td colspan="2">Director of the Risk Management Department</td><td>/signature/</td><td>O.P. Lazarenko</td></tr>
<tr><td>The access level</td><td colspan="4">Information for internal use only</td></tr>
<tr><td>The document revision:</td><td>Revision</td><td>No. and date of approval</td><td colspan="2">Brief description of amendments</td></tr>
<tr><td>Policy of JSC “CRYSTALBANK” on preventing and countering to legalization (laundering) of the proceeds of crime, terrorist financing and financing proliferation weapons of mass destruction</td><td>1</td><td>Decision of the Supervisory Board of the Bank, Minutes No. 80 dd. August 20, 2020</td><td colspan="2">First version</td></tr>
<tr><td>Place of storage of the original document before handing over to the archive</td><td colspan="4">- the appendices to the decision of the Supervisory Board of the Bank on approval (Corporate Secretary)</td></tr>
<tr><td>Entered in the information database of internal documents of JSC “CRYSTALBANK”</td><td>Date</td><td>Name of the network resource</td><td colspan="2">The file name</td></tr>
<tr><td>Full name: L.Ye. Vystoropska</td><td>21.08.2020</td><td>W:/ Internal regulations of CRYSTALBANK</td><td colspan="2">\1General document\5Policies\7Policy of financial monitoring</td></tr>
</table>

CONTENT

I. General Provisions

1.1. The policy of JSC "CRYSTALBANK" on preventing and countering to legalization (laundering) of the proceeds of crime, terrorist financing and financing proliferation weapons of mass destruction (hereinafter referred to as the Policy) is developed to prevent the use of JSC "CRYSTALBANK" (hereinafter referred to as the Bank) for the legalization (laundering) of proceeds from crime, terrorist financing and financing of the proliferation of weapons of mass destruction.

1.2. The Policy is developed taking into account the requirements of the 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" (hereinafter – the Law on AML/CFT), the Regulation on financial monitoring by banks approved by Resolution of the Board of the National Bank of Ukraine No. 65 dd. 19.05.2020 (hereinafter – Regulation No. 65), statutory instruments of the National Bank of Ukraine, Ministry of Finance of Ukraine adopted for implementation and in accordance with the Law on AML/CFT, recommendations of the Financial Action Task Force on Money Laundering (FATF), the Basel Committee on Banking Supervision, the results of the National Risk Assessment and risk profile of the Bank, recommendations of the National Bank of Ukraine and typology studies of the central executive authority implementing the state policy in the field of preventing and countering to legalization (laundering) of the proceeds from crime, terrorist financing and financing proliferation weapons of mass destruction (hereinafter referred to as the Designated Authority, the DA).

1.3. The Policy determines the general principles of the Bank regarding compliance with the requirements of the legislation of Ukraine on preventing and countering to legalization (laundering) of the proceeds from crime, terrorist financing and financing proliferation of weapons of mass destruction (hereinafter – AML/CFT).

1.4. The Policy is determined and approved by the Bank's Supervisory Board (hereinafter referred to as the Board).

1.5. The Policy is brought to the attention of the Bank's Management Board and the Bank employee responsible for conducting financial monitoring (hereinafter referred to as the responsible employee of the Bank) in order to form a clear understanding of the Board's expectations regarding:

1) proper organization and functioning of the intrabank AML/CFT system and conducting primary financial monitoring, functioning of the proper risk management system for legalizing (laundering) proceeds of crime, terrorist financing and financing proliferation of weapons of mass destruction (hereinafter - ML/FT);
2) the Bank's risk appetite in the field of AML/CFT (including, if any, established prohibitions/restrictions on certain types of activities and/or attracting certain types of clients for service);
3) the scope of internal documents of the Bank to be developed and approved on AML/CFT issues;
4) requirements for the development of three lines of defence in the field of AML/CFT and the distribution of responsibilities and liability among the Bank employees;
5) functioning of internal control on AML/CFT issues;
6) ensuring the conduct of training events on AML/CFT issues.

1.6. The terms and concepts used in the Policy are applied in the meanings defined in the Law on AML/CFT, Regulation No. 65 and this Policy.

II. Requirements for the proper organization and functioning of the intrabank AML/CFT system and conducting primary financial monitoring, the functioning of the proper ML/FT risk management system

2.1. The Bank ensures proper organization of the intrabank AML/CFT system and primary financial monitoring.

The purpose of proper organization of the intrabank AML/CFT system and primary financial monitoring is:

1) compliance with the requirements of the legislation of Ukraine in the field of AML/CFT;
2) the ability to properly identify threshold and suspicious financial transactions (activities) and report them to the designated authority;
3) prevention of using the Bank's services and products by clients to conduct financial transactions for the purpose of ML/FT.

2.2. The Bank takes, in particular, the following measures in order to properly organize the intrabank AML/CFT system and conduct primary financial monitoring:

1) appointing the responsible employee of the Bank in accordance with the requirements of the legislation of Ukraine in the field of AML/CFT at the level of the Bank's management. The responsible employee of the Bank is the Head of the Financial Monitoring Service;
2) establishing a separate structural division for AML/CFT headed by the responsible employee of the Bank. The Bank has established the Financial Monitoring Service;
3) ensuring the functioning of the ML/FT risk management system;
4) developing and approving internal documents of the Bank on issues of AML/CFT to the extent required for the effective functioning of the intrabank AML/CFT system and understanding by the Bank employees of their duties and powers in the field of AML/CFT;
5) ensuring the functioning on an ongoing basis of a collegial body for consideration of problematic and topical issues of the functioning of the intrabank AML/CFT system. The Bank has established the Financial Monitoring Committee;
6) providing sufficient resources for the functioning of the intrabank AML/CFT system (including the separate structural division for AML/CFT);
7) ensuring sufficient awareness of the Chairman, Members of the Board and Management Board of the Bank regarding their responsibilities in the field of AML/CFT, as well as the risks inherent in the Bank's risk profile of ML/FT;
8) ensuring that the Bank's managers are informed about the importance of the requirements of the legislation of Ukraine on AML/CFT in order to ensure the proper risk management system, the need to take measures to effectively prevent the use of the Bank's services for the purpose of ML/FT and understand the consequences that the Bank is exposed to in case of non-compliance with the requirements of the legislation of Ukraine on AML/CFT;
9) effectively distributing functions on AML/CFT issues among three lines of defence, ensuring proper awareness and performance by the Bank employees, including employees of business divisions, of the duties assigned to them in the field of AML/CFT, understanding by such employees of their liability for non-performance of duties and/or inactivity;
10) introducing and continuously improving the internal control on AML/CFT issues, in particular, ensuring timely identification by the internal audit of problematic issues and signs of an improper ML/FT risk management system;
11) examining new products/services, including new sales channels, the use or development of new technologies for the existing or new products, in order to properly assess the inherent ML/FT risks and properly monitor the ML/FT risks for the existing products/services;
12) ensuring that training activities are carried out on an ongoing basis for the Bank employees and, if there are the Bank agents (their employees), in order to understand their responsibilities and the procedure for actions;
13) ensuring that all Bank employees involved in conducting primary financial monitoring have an impeccable business reputation (when hiring an employee in the Bank - before such an employee starts performing their duties);

14) creating and ensuring the functioning of an effective and timely system of escalation of suspicions and problematic issues in the field of AML/CFT and the procedure for their consideration, including reporting information/facts concerning cases of violation or possible violation of the legislation of Ukraine in the field of AML/CFT, in accordance with the procedure provided for by the Bank internal documents;
15) introducing an automation system (hereinafter – the AS) that ensures timely and full performance by the Bank of the duties of the primary financial monitoring entity (hereinafter – the PFME) (in particular, identification of financial transactions subject to financial monitoring, freezing of assets related to terrorism and/or its financing/proliferation of weapons of mass destruction and/or its financing, making it impossible for persons from the list of terrorists to carry out transactions);
16) ensuring timely identification of financial transactions subject to financial monitoring and proper information exchange with the DA;
17) developing and implementing measures for the client due diligence (hereinafter – the CDD) in order to understand the essence of the client's activities, the purpose and expected nature of business relations with him/her that allows the Bank to be sure that the client's financial transactions correspond to the information available in the Bank about him/her, his/her business, risk profile, including, if necessary, the sources of origin of his/her funds/fortune, the establishment of the ultimate beneficial owner (hereinafter – the UBO) for prompt identification of unusual behavior and suspicious financial transactions (activities);
18) properly documenting the actions of the Bank employees and recording events related to the performance by the Bank of the PFME's obligations;
19) storing all documents, data, and information (including relevant reports, orders, and files) related to the performance by the Bank of the PFME's obligations within the time limits determined by the legislation of Ukraine;
20) promptly and in full submitting to the requests of the National Bank of Ukraine the necessary documents/information/explanations/arguments that properly confirm the Bank's compliance with the requirements of the legislation of Ukraine on AML/CFT;
21) taking measures to continuously improve the intrabank AML/CFT system.

2.3. The Chairman of the Bank's Management Board, as well as the responsible employee of the Bank, are responsible for the proper organization of the intrabank AML/CFT system and conducting primary financial monitoring.

2.4. The Bank has established a separate committee – the Financial Monitoring Committee (hereinafter referred to as the Committee), which ensures at least once a quarter (no later than the 20th day of the month following the quarter) the consideration of the following issues in the field of AML/CFT:

1) the results of monitoring business relations with clients that revealed suspicious client activity, and suggestions for the Bank to take the necessary measures against such clients in order to minimize the ML/FT risks;
2) issues related to proposals for refusal to continue business relations with clients (including if the client is set an unacceptably high level of risk);
3) problematic issues that arise during the implementation of the CDD in the Bank;
4) changes in the legislation of Ukraine on AML/CFT and adoption by the Bank of necessary measures in connection with such changes (in particular, updating the Bank's internal documents on AML/CFT) indicating the time period for taking such measures;
5) results of evaluation of new banking products / services and their inherent ML/FT risks;
6) problematic issues related to conducting training events for the Bank employees, Bank agents (their employees);
7) problematic issues related to the establishment of business relations with individuals who are politically exposed persons, their family members or persons associated with politically exposed persons or other persons whose ultimate beneficial owner is a politically exposed person, a member of his/her family or a person associated with a politically exposed person (hereinafter - PEP in the singular, PEPs in the plural) and/or their service;

8) other issues related to the Bank's compliance with the requirements of the legislation of Ukraine in the field of AML/CFT that need to be considered.

The powers of the Committee, the procedure for developing and making decisions are determined in the regulations on the Committee. The Chairman of the Committee is the Chairman of the Bank's Management Board.

2.5. The responsible employee of the Bank reports to the Board at least once a year (no later than February 20 of the year following the reporting year) on:

1) results of assessment of the Bank's risk profile;
2) problematic issues related to the development of a proper organization of the intrabank AML/CFT system and the conduct of primary financial monitoring;
3) problematic issues related to ensuring the proper ML/FT risk management system.

2.6. The responsible employee of the Bank must constantly maintain his/her level of knowledge on AML/CFT issues at the proper level, including by completing training in the field of AML/CFT, as well as advanced training in accordance with the procedure and within the time limits established by the Law on AML/CFT.

2.7. The Financial Monitoring Service, in order to ensure the secrecy of financial monitoring, as well as other confidential information in the field of AML/CFT, must be located in a separate room(s) and must function in accordance with the regulations on this structural division, approved by the Board in accordance with the requirements of the internal documents of the Bank.

2.8. The Internal Audit Division of the Bank, based on a risk-based approach, organizes and conducts internal audits in accordance with Article 8 of the Law on AML/CFT regarding the Bank's compliance with the requirements of the legislation of Ukraine in the field of AML/CFT (including the sufficiency of measures taken by the Bank to ensure the functioning of the proper ML/FT risk management system).

When conducting internal audits, the Bank's Internal Audit Division must analyze the sufficiency and effectiveness of the AS implemented in the Bank for the Bank to fulfill the PFME's obligations.

2.9. The Bank's Internal Audit Division prepares reports, opinions and suggestions based on the results of its internal audits and monitors the elimination of identified violations.

No later than 15 business days from the date of approval of the audit report by the Board, the Financial Monitoring Service draws up an action plan to eliminate identified violations of the legislation of Ukraine and/or shortcomings in the field of AML/CFT in order to minimize the ML/FT risks and prevent violations in the future (hereinafter referred to as the risk mitigation plan).

The Bank is obliged to take measures to implement the risk mitigation plan within the time limits specified in it.

At the request of the National Bank of Ukraine, the Bank is obliged to submit to it an electronic version of the risk mitigation plan with a cover letter signed with a qualified electronic signature of the Chairman of the Bank's Management Board.

The National Bank of Ukraine has the right to submit suggestions and comments to the risk mitigation plan, which are mandatory for the Bank to take into account and implement.

2.10. The Bank is obliged to submit an electronic version of audit reports, opinions and suggestions with a cover letter signed with a qualified electronic signature of the Chairman of the Management Board of the Bank to the structural division of the central office of the National Bank of Ukraine, whose competence includes issues of supervision in the field of preventing and combating ML/FT, no later than the twentieth business day from the date of their approval, ensuring guaranteed delivery and confidentiality.

2.11. The Bank, taking into account the specifics of its activities (in particular, the nature and scope of its activities, types of services provided, types of clients served, the use of the latest technologies) and the ML/FT risks inherent in its activities, introduces an appropriate automation system (the AS).

The Bank uses the B2 automated banking system (hereinafter referred to as the ABS B2) in order to meet the requirements of the legislation of Ukraine in the field of AML/CFT.

2.12. The AS is used to ensure:

1) freezing of assets related to terrorism and its financing, proliferation and financing of weapons of mass destruction;
2) maintaining the Bank client profiles in electronic form;
3) maintaining relevant registers of the Bank notifications;
4) maintaining information about the Bank's registration as an PFME;
5) timely information exchange with the DA;
6) maintaining a log of activity of each of the users protected from modification. The log should include the start and end of each user's activity indicating time to the nearest second;
7) availability of an information security system that meets the requirements of the legislation of Ukraine in the field of Information Protection;
8) availability of an information backup and storage system;
9) ongoing monitoring of clients' financial transactions to quickly identify indicators of suspicious financial transactions;
10) ongoing monitoring of business relations with clients in order to quickly identify the criteria inherent in the ML/FT risk and the need for the Bank to update client data;
11) promptly informing the authorized employees of the Bank about the identified indicators of suspicious financial transactions, ML/FT risk criteria and the need for updating client data by the Bank, determining the priority of such notifications, taking into account their critical importance;
12) functioning of the intrabank procedure for escalating suspicions by the Bank employees in accordance with delegated powers/responsibilities (including documenting/recording the facts of sending notifications about suspicions by the employees, making decisions by addressees on further escalation of suspicion or making a final decision on the presence/absence of suspicions);
13) documenting all events in the AS in order to meet the above requirements (with recording the date, time, and the event);
14) implementation of other requirements of the legislation of Ukraine in the field of AML/CFT.

2.13. The Bank implements sub-clauses 10-12 of clause 2.12 of this Policy depending on the capabilities of the ABS B2. If a decision is made on the inexpediency of automating these areas, the Bank simultaneously decides on the use of alternative methods, provided that all the requirements of the legislation of Ukraine in the field of AML/CFT are properly met.

Such a decision should be properly documented, indicating all reasonable grounds and describing the essence of the available alternative methods.

At the request of the National Bank of Ukraine, the Bank is obliged to provide such a decision and provide an explanation of the essence of such alternative methods (demonstrate their operation if necessary).

2.14. The Bank uses a risk-based approach in its activities.

The risk-based approach is applied by the Bank continuously and provides detection, identification, assessment of all existing and potential ML/FT risks inherent in the Bank's activities (risk profile of the Bank) and its clients, as well as provides for timely development of measures for managing ML/FT risks, their minimization.

The Bank documents the process of applying the risk-based approach in such a way as to be able to demonstrate: its essence (in particular, what is the difference in approaches); the decisions taken by the Bank during its application and the justification of such decisions; the compliance of measures taken during the application of the risk-based approach with the requirements of the legislation of Ukraine on AML/CFT.

The process of applying the risk-based approach by the Bank, the essence of measures to apply the risk-based approach is described in the Bank's internal documents on AML/CFT issues, in particular, in the ML/FT risk management program.

2.15. The Bank, applying the risk-based approach, refrains from unjustified use of de-risking. This approach contradicts the risk-based approach and does not promote financial inclusion.

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

1) assessment of the Bank's risk profile:

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

2) assessment of the client's risk profile:

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

2.17. The Bank assesses its own risk profile, taking into account the specifics of its activities and such factors:

- the nature and scope of the Bank's activities;
- products and services provided by the Bank;
- types of clients and their risk profile;
- geographical location of the Bank, 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 important factors related to the Bank's activities.

2.18. When analyzing the AML/CFT risks of its products and services, the Bank takes into account the specifics and possibilities of their use, in particular:

1) intended use of the product and/or service:

- whether the Bank's products and/or services allow masking the illegal origin of funds, transferring funds to finance terrorist activities, and promoting anonymity of participants to a financial transaction (hiding the real ultimate recipients of certain products and/or services);
- whether they can be used by the client on behalf of third parties;
- whether they can be of interest for shell-corporations;

2) special opportunities for using the product and/or service: whether the product and/or service allows the Bank's client to perform operations with counterparties/business segment that are characterized by higher risks in the ML/FT sector;

3) target segment for product and/or service implementation: types of clients who most often use a particular product and/or service.

2.19. Analyzing the channels/methods of providing (receiving) its products and/or services, the Bank pays special attention to the risks inherent in the latest technologies (in particular, remote establishment of business relations with the client), the presence of agents, and the use of information from other PFMEs.

2.20. The Bank takes into account geographical risk criteria, paying, in particular, special attention to states (territories) that do not comply with the FATF recommendations, or that have strategic shortcomings in the field of AML/CFT (according to the FATF statements), states that carry out armed aggression against Ukraine in the meaning given in Article 1 of the Law of Ukraine "On Defence of Ukraine", the presence/absence of military conflicts, terrorist groups and/or organizations on the territory of the state (territory).

The Bank's geographical risk criteria should also take into account the location of the Bank (its parent institution, branches, representative offices, subsidiaries) and the geography of provision of its products and/or services by the Bank.

2.21. When determining its risk profile, the Bank also takes into account the presence and nature of sanctions that are applied to it.

2.22. When updating its risk profile, the Bank regularly reviews the existing risk management measures in the Bank regarding their sufficiency and effectiveness and develops additional

measures, if the results of the analysis of the existing measures are not sufficient for the effective ML/FT risk management.

2.23. The risk criteria are determined by the Bank independently, taking into account the risk criteria established in the Law on AML/CFT, Regulation No. 65, as well as taking into account the typology studies of the DA, the results of the National Risk Assessment, as well as the recommendations of the National Bank of Ukraine.

The Bank determines the priority/significance of the developed risk criteria, taking into account the possible consequences/impact of such risks, and sets their appropriate relative share for further risk assessment.

2.24. The Board reviews the results of the Bank's risk profile assessment, approves the relevant decision based on the results of such review and informs it to the Bank's Management Board and the responsible employee of the Bank for its further implementation.

2.25. The Bank takes into account the results of the Bank's risk profile assessment when developing risk criteria for assessing the risk of business relations (a financial transaction without establishing a business relationship) with the clients and the ML/FT risk management measures.

2.26. The Bank assesses the risk of business relations (a financial transaction without establishing a business relationship) with the clients before establishing a business relationship with the client/conducting a financial transaction without establishing a business relationship.

2.27. Based on the results of assessing business relations (a financial transaction without establishing a business relationship) with the client, the Bank sets the level of risk using a risk scoring model that takes into account the presence of risk criteria inherent in the client's activities (including those expected at the stage of establishing a business relationship with the client).

2.28. The scale for classifying the risk levels of business relations (a financial transaction without establishing a business relationship) used in the Bank contains low, medium, high and unacceptably high (subcategory of high risk, which is the highest possible risk that cannot be accepted by the Bank) risk levels.

The Bank introduces its own risk scoring model and independently determines the input data and information sources for conducting the risk assessment, the algorithm (model) for conducting the risk assessment, and the scale for determining risk levels.

The Bank, developing risk criteria taking into account its risk appetite in the field of AML/CFT, determines the relevant quantitative limits for those criteria that contain quantitative characteristics (in particular, 'significant increase', 'large volumes', 'regularity').

The Bank develops algorithms containing quantitative and/or qualitative characteristics that make it possible to identify and establish the existence of an appropriate risk criterion inherent in the client and business relations with him/her (a financial transaction without establishing a business relationship).

2.29. The Bank has introduced a multi-level system for assessing the risk of business relations (a financial transaction without establishing a business relationship) with the client that provides for determining the primary level of risk of business relations (a financial transaction without establishing a business relationship) with the client and assessing the level of risk of business relations with the client in the process of servicing him/her in the Bank.

2.30. The Bank constantly takes measures to keep up to date (including re-assessment of the risk level if necessary):

1) its own risk profile - in case of a change in the business model, introduction of new products or services that significantly differ from the existing ones, taking into account the inherent ML/FT risks, but at least once a year;

2) the client's risk profile:

- when implementing measures to update the client's data;
- in case of identification of new risk criteria inherent in business relations (a financial transaction without establishing a business relationship) with the client - no later than the fifteenth day of the month following the month, in which the new risk criterion was identified.

2.31. The Bank takes measures at least once a quarter to identify the risk criteria inherent in business relations (a financial transaction without establishing a business relationship) with the client using the appropriate software modules, analyzing the information obtained as a result of the CDD and the client's financial transactions performed.
2.32. The Bank documents the list of risk criteria inherent in a specific business relationship (a financial transaction without establishing a business relationship) with the client as of the relevant date, as well as the list of the ML/FT risk management measures taken by the Bank in order to mitigate the level of primary risk to the residual risk established by the Bank.
2.33. The ML/FT risk management measures, in particular, include:

1) clear distribution of responsibilities and liability among the Bank employees and constant internal control;

2) preliminary analysis of new products/services of the Bank in order to identify their inherent potential ML/FT risks;

3) application of limits or other tools that restrict the use of a particular service/product;

4) introduction of a diversified approach to obtaining permission to establish (continue) business relations (conducting a one-time financial transaction for a significant amount without establishing a business relationship) with the client, applying the risk-based approach (according to the principle: the higher risk is, the higher ex officio authorized employee of the Bank provides his/her permission, including the Bank's managers);

5) obtaining an additional permission from an authorized employee of the Bank/Head of the Bank to conduct certain financial transactions with a high level of risk within the established business relationship;

6) implementation of the automated modules for monitoring business relations with the client that will make it possible to quickly identify the relevant inherent risk criteria;

7) implementation of the client due diligence measures (including enhanced ones if necessary) and application of the "know your client" principle, including obtaining additional necessary information to understand the scope of the client's activities and/or the essence of the financial transaction;

8) increasing the level and nature of monitoring of business relations with high-risk clients;

9) regular and objective informing of the Bank's management about the identified ML/FT risks and measures to manage such risks;

10) ensuring a deep understanding by the Bank employees of their responsibilities in the field of AML/CFT, including by conducting training events.

2.34. The Bank organizes its work in such a way as to avoid any signs of an improper risk management system. The signs of an improper risk management system are:

1) improper implementation of a comprehensive assessment/re-assessment of the Bank's ML/FT risks, including those inherent in its activities (the risk profile of the Bank), documenting their results, monitoring measures, risk control and maintaining the risk profile of the Bank up-to-date in order to minimize the use of the Bank's services for the purposes of ML/FT;

2) failure to implement the CDD, improper assessment/re-assessment of the risk of business relations (a financial transaction without establishing a business relationship) with clients (the client risk profiles), documenting their results, monitoring measures, risk control and maintaining the risk profiles of the Bank's clients up-to-date in order to minimize the use of the Bank's services for the purposes of ML/FT;

3) improper application of the risk-based approach, which consists in the Bank's improper understanding of the ML/FT risks that its client exposes to, failure to take effective measures proportional to the identified risks to minimize them (the simplified CDD for low-risk clients and enhanced CDD for high-risk clients), lack of a differentiated (multi-level) risk-based procedure for coordinating business relations with clients;

4) failure to take timely and proper measures to minimize the identified ML/FT risks to an acceptable level of ML/FT risks;

5) lack of effective tools to prevent/eliminate multiple, large-scale financial transactions (activities) by the clients that are suspected of using the Bank for ML/FT or committing another

crime, in particular monitoring business relations with the clients and financial transactions of the clients carried out in the course of such business relations;

6) lack of the effective internal control on financial monitoring issues, late detection by the internal audit of problems and shortcomings in the intrabank AML/CFT system and signs of the improper ML/FT risk management system;

7) lack of an effective system for escalating suspicions and problematic issues in the field of AML/CFT that makes it impossible to consider them in a timely and effective manner, including reporting information/facts related to cases of violation or possible violation of the legislation of Ukraine in the field of AML/CFT;

8) lack of a proper PEPs detection system that led to the Bank's failure to properly take additional measures in relation to them, determined 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 actions of the Bank employees and record events related to the Bank's performance of PFME's functions;

11) the presence of facts of repeated, large-scale financial transactions, in respect of which there are suspicions of using the Bank for ML/FT or committing another crime, resulting from non-compliance with AML/CFT measures.

III. Risk appetite of the Bank in the field of AML/CFT

3.1. Based on the assessment of the 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 - there is no need for additional actions to enhance monitoring/control;

2) risks that the Bank can take, but only after taking measures to manage such risks (minimize them) – there is a need for enhanced monitoring/control, identifying factors that have an adverse impact on the risk and developing measures to mitigate it;

3) risks that are unacceptable for the Bank – there is a need to implement immediate decisions/actions to mitigate it.

3.2. When determining risk appetite in the field of AML/CFT, the requirements of the Statement on risk propensity and risk appetite structure of JSC "CRYSTALBANK", approved by the Board's decision dd. 30.01.2020, Minutes No. 12, are taken into account.

3.3. The risk appetite parameters may be changed based on the results of reviewing the report of the responsible employee of the Bank on the results of assessing the Bank's risk profile.

3.4. The Bank takes comprehensive measures to avoid risks in the field of ML/FT. The Bank has set zero tolerance for them. If they occur and are detected during the monitoring, the responsible employee of the Bank informs the Bank's Management Board and, if necessary, the Board, and makes recommendations on measures to be taken to mitigate the risks to an acceptable level of the ML/FT risk.

3.5. The ML/FT risks that are unacceptable for the Bank are:

- service of clients (individuals) in respect of whom the Bank is unable to fulfill the obligations determined by the Law on AML/CFT or minimize the identified risks associated with the client or financial transaction;
- service of clients (individuals) in respect of whom there are reasonable suspicions based on the results of studying the client's suspicious activities that such activities may be fictitious;
- service of clients (individuals) in respect of whom the Bank, based on the results of studying the client's activities, has reasonable suspicions about their implementation of ML/FT transactions and other crimes;
- service of clients (individuals) in respect of whom the Bank has the reason to believe that they are shell-corporations;

- service of clients (individuals) who did not provide the necessary documents or information for proper verification of the client at the Bank's request;
- service of clients (individuals) in respect of whom, under the due diligence, it is established that the client or his/her representative submitted false information or submitted information in order to mislead the Bank;
- service of clients, for whom it is impossible to identify and/or verify and/or establish data that allows you to identify the ultimate beneficial owners, or if the Bank has doubts that the individual acts on his/her own behalf;
- carrying out financial transactions, if it is impossible to identify the individual on whose behalf or in whose interests the financial transaction is being conducted and establish its ultimate beneficial owner or beneficiary for the financial transaction;
- establishing/maintaining correspondent relations with other banks or financial institutions that are shell-banks and/or maintain correspondent relations with shell-banks;
- service of individuals and/or organizations that are included in the list of individuals and entities associated with carrying out terrorist activities or against whom international sanctions have been applied (hereinafter referred to as the list of individuals and entities);
- service of individuals and/or organizations acting on behalf of the individuals and/or organizations included in the list of individuals and entities;
- service of individuals and/or organizations that are directly or indirectly owned or whose ultimate beneficial owners are individuals and/or organizations that are included in the list of individuals and entities.

3.6. The ML/FT risks that the Bank can accept, but only after taking measures to manage such risks (minimize them), are risks managed by the Bank.

The conditions, under which the Bank employees are required to take risk management measures (mitigation to a minimum level), are defined in the Bank's internal documents on the recommendation of the responsible employee of the Bank. Such conditions provide for the existence of limits/appropriate circumstances, after which actions against the client must be agreed with the Financial Monitoring Service (in particular, establishing business relationships/opening an account/conducting operations without opening an account and/or performing operations that have certain characteristics and/or are carried out for an amount greater than a certain amount).

If necessary, the responsible employee of the Bank takes the initiative to amend the internal documents of the Bank and establish prohibitions/restrictions, in particular, regarding certain types of activities and/or attracting certain types of clients for service.

3.7. There are no the ML/FT risks that the Bank is ready to accept.

IV. Requirements for the scope of internal documents of the Bank to be completed and approved on AML/CFT issues

4.1. The Bank, following this Policy, develops and approves the internal documents in order to comply with the requirements of the legislation of Ukraine in the field of AML/CFT, which must contain the effective risk-oriented procedures, procedures sufficient for the proper organization and functioning of the intrabank AML/CFT system and conducting primary financial monitoring, the functioning of the proper ML/FT risk management system.

4.2. The internal documents of the Bank on AML/CFT issues are developed by the Bank taking into account the requirements of the laws of Ukraine regulating AML/CFT, Regulation No. 65, statutory instruments of the National Bank of Ukraine, the Ministry of Finance of Ukraine, recommendations of the FATF, the Basel Committee on Banking Supervision, the results of the National Risk Assessment and risk profile of the Bank, recommendations of the National Bank of Ukraine and typology studies of the DA.

4.3. The basic principles of development and implementation of the internal documents of the Bank on AML/CFT issues are:

1) proper organization and functioning of the intrabank AML/CFT system and conducting primary financial monitoring, functioning of the proper ML/FT risk management system, ensuring the functioning of an effective intrabank AML/CFT system;

2) introduction of the risk-based approach implementing the AML/CFT procedures;

3) fulfillment by the Bank of all the requirements defined by the legislation of Ukraine in the field of AML/CFT;

4) taking into account all types and areas of the Bank's activities;

5) introduction of AML/CFT culture in the Bank and ensuring the direct participation of each employee (within their competence) in the process of implementing the AML/CFT procedures;

6) clear distribution of duties and powers among the Board, the Chairman of the Management Board of the Bank, members of the Management Board of the Bank, the responsible employee of the Bank, other employees and structural divisions of the Bank in order to prevent violations of the legislation of Ukraine in the field of AML/CFT in the Bank's operation;

7) the presence of proper internal control (for different types of services/products, types of clients, the level of risks of clients, the amount of financial transactions) and the identification of Bank employees who make decisions at different stages of control in accordance with their functional responsibilities, ensuring the principle of "the higher position is, the greater powers and responsibility are assigned";

8) establishing a detailed and understandable procedure for the Bank employees when performing the AML/CFT procedures;

9) ensuring the secrecy of financial monitoring and confidentiality of information about information exchange with the DA, including the fact of transmitting information about the client's financial transaction to the DA;

10) ensuring confidentiality of information about the Bank's internal documents on AML/CFT issues;

11) ensuring confidentiality of information about the clients, their accounts and financial transactions, as well as other information constituting a bank secret;

12) prevention of involvement of the Bank employees in ML/FT.

4.4. The Bank's internal documents on AML/CFT issues must contain:

1) determination of the Bank's division(s) and/or the Bank employees responsible for implementing the CDD activities, and distribution of responsibilities among them;

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

3) the procedure for identifying PEPs and the procedure for taking the necessary additional measures against them;

4) the procedure for assessment/re-assessment of the Bank's risk profile and the client risk profile and taking measures to minimize the ML/FT risks;

5) the procedure for identifying the ML/FT risk criteria and indicators of suspicious financial transactions;

6) the procedure for taking the necessary additional measures to establish correspondent relations with a foreign financial institution;

7) the procedure for maintaining an electronic form, which will ensure the timeliness, completeness and reliability of the information entered in the client's electronic form;

8) the procedure for actions regarding the Bank's refusal to establish (maintain) business relations / open an account (service), including by terminating the business relationship, closing the account / refusing to conduct a financial transaction in cases stipulated by the Law on AML/CFT;

9) the procedure for the Bank to identify discrepancies between the information about the UBO contained in the Unified State Register of Legal Entities and the information received by the Bank as a result of the CDD;

10) the procedure for using the assignment procedure (if the Bank decides to use it);

11) the procedure for using agents by the Bank, conducting training events for them (their employees) and monitoring their activities (if the Bank decides to involve agents);

12) the procedure for entering relevant information in the notification registers;

13) the procedure for using the AS;

14) the procedure for information exchange with the DA and performance of relevant decisions/instructions of the DA;

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

16) the procedure for suspension of transactions by the Bank in cases defined by the Law on AML/CFT;

17) the procedure for the Bank to support money transfers with relevant information in accordance with the requirements defined in Article 14 of the Law on AML/CFT;

18) the procedure for controlling the relevant limits if the Bank uses simplified methods of identification and verification of the client (the client's representative);

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

20) the procedure for informing the SSU in cases defined by the legislation of Ukraine in the field of AML/CFT;

21) the procedure for conducting training events for the Bank employees;

22) the procedure for familiarizing the Bank employees with the Bank's internal documents on AML/CFT issues;

23) the procedure for storing all documents/information on the Bank's compliance with the requirements of the legislation of Ukraine in the field of AML/CFT.

4.5. The Bank ensures that the Bank's internal documents on AML/CFT issues are up-to-date, taking into account amendments to the legislation of Ukraine in the field of AML/CFT and events that may affect the Bank's ML/FT risks.

The Bank updates the Bank's internal documents on AML/CFT issues continuously, but not later than three months from the date of entry into force of amendments to the legislation of Ukraine on AML/CFT and/or the Bank establishes events that may affect the ML/FT risks.

4.6. The Bank independently determines and documents the procedure for classifying the internal documents on AML/CFT issues as documents with restricted access and the procedure for access to them by the Bank employees and third parties.

4.7. The Bank provides familiarization with the Bank's internal documents on AML/CFT issues of the Bank employees (depending on their duties) against signature or by electronic means in the event of:

1) employment of an employee to the Bank, before the employee starts performing his/her duties;

2) approval, making changes to the Bank's internal documents on AML/CFT issues, no later than 20 business days from the date of approval, making changes.

4.8. The internal documents of the Bank on AML/CFT issues (except for this Policy) are approved by the Bank's Management Board in accordance with the procedure established by the Bank's constituent documents, on the recommendation of the responsible employee of the Bank.

V. Requirements for the development of three lines of defence in the field of AML/CFT, the distribution of responsibilities and liability among the Bank employees, as well as the functioning of internal control on AML/CFT issues

5.1. The Bank applies the internal control system in the field of AML/CFT based on the distribution of responsibilities among the Bank's divisions, except for functions that fall within the exclusive competence of the Bank's Board/Management Board/Committees in accordance with the provisions of the legislation of Ukraine, statutory instruments of the National Bank of Ukraine.

This distribution is based on the application of a model of three lines of defence, namely:

1) the first line of defence is at the level of business units and support units of the Bank's activities. These divisions conduct and show transactions, accept risks in the course of their activities, and are responsible for the current management of these ML/FT risks. The first-line

divisions exercise their powers within the limits defined by the regulations on divisions and job descriptions;

2) the second line of defence is at the level of the risk management division, the Compliance Control Service and the Financial Monitoring Service. These divisions provide the Bank's managers with confidence that the risk control and management measures implemented by the first line of defence have been developed and are functioning properly. The Financial Monitoring Service controls the implementation of relevant measures by the first line units;

3) the third line of defence is at the level of the Internal Audit Division, which performs an independent assessment of the effectiveness of the first and second lines of defence and a general assessment of the effectiveness of the internal control system.

5.2. The Bank determines in its internal bank documents the procedures and control measures applied by the divisions of each of the three lines of defence.

5.3. The Bank's internal control system on AML/CFT issues consists of the following components: control environment of AML/CFT, management of the AML/CFT risks inherent in the Bank's activities, control activities in the Bank on AML/CFT issues, control over information flows and communications of the Bank on AML/CFT issues, monitoring the effectiveness of the Bank's internal control system on AML/CFT issues.

5.4. The Bank develops a comprehensive, effective and proper internal control system for AML/CFT issues in compliance with the following principles:

1) comprehensiveness and complexity;
2) effectiveness;
3) adequacy;
4) prudence;
5) risk-based approach;
6) integration;
7) earliness;
8) independence;
9) continuity;
10) privacy policy.

5.5. The principle of comprehensiveness and complexity provides that the Bank has implemented each of the five components of the internal control system on AML/CFT issues and ensures their implementation in a mutually integrated way, that is, the results of the implementation of such a component are used in the implementation of other components of the internal control system; internal control procedures on AML/CFT issues (hereinafter referred to as the control procedures) are integrated into the Bank's processes at all organizational levels.

5.6. The principle of effectiveness establishes that internal control measures for AML/CFT (hereinafter referred to as the control measures) implemented in the Bank are effective and ensure that the Bank achieves certain business goals and is reasonably confident that:

1) the transactions performed by the Bank are effective and shown correctly in the Bank's information systems/record-keeping systems;

2) financial, statistical, managerial and other reporting on AML/CFT issues is reliable;

3) the Bank complies with the requirements of the legislation of Ukraine on AML/CFT, statutory instruments of the National Bank of Ukraine, the internal documents;

4) the Bank employees have the necessary information about the components of the internal control system on AML/CFT issues and ensure the implementation of these components within the limits of their competence and powers defined in job descriptions;

5) the Bank shall identify and assess the shortcomings of the internal control system on AML/CFT issues and take timely, proper and sufficient corrective measures to correct such shortcomings.

5.7. The principle of adequacy provides that the Bank's internal control system on AML/CFT issues corresponds to the specifics of its activities, including the volume, business model, scale of activity, types, complexity of transactions, and risk profile of the Bank.

5.8. The principle of prudence establishes that the Bank provides sufficient confidence of the Bank's managers regarding the Bank's achievement of the goals of its activities on AML/CFT issues, based on conservative assumptions and taking into account a certain probability of erroneous judgments or decisions of the Bank's managers and/or employees.
5.9. The principle of risk-based approach provides that the Bank ensures the organization and functioning of the internal control system on AML/CFT issues, based on the risk-based approach that provides for the application of more in-depth and frequent control measures to those areas of the Bank's activities that are characterized by higher risks.
5.10. The principle of integration establishes that the control procedures for AML/CFT issues are an integral part of all processes of activity and corporate governance of the Bank.
5.11. The principle of earliness provides that the Bank's internal control system on AML/CFT issues is able to ensure that potential threats of adverse impact on the Bank's activities are identified before such threats actually arise.
5.12. The principle of independence establishes that the Bank avoids circumstances that may pose a threat to the impartial performance by actors of its internal control system of their functions on AML/CFT issues.
5.13. The principle of continuity provides that the Bank's implementation of the internal control activities on AML/CFT issues makes it possible to prevent, identify and eliminate shortcomings of the internal control system on AML/CFT issues on an ongoing basis and in a timely manner.
5.14. The principle of confidentiality stipulates that the Bank does not allow disclosure of information on AML/CFT to individuals and entities who do not have the authority to receive it.
5.15. The Bank determines the order and procedures for:

1) vertical interaction used in the implementation of the internal control among units and divisions of various lines of defence;

2) horizontal interaction applied in the case of the internal control within the same division and/or among units of the same line of defence.

5.16. The Bank implements the control procedures for AML/CFT issues:

1) organizationally by:

distribution within the Bank's organizational structure of powers, responsibilities and liability for the internal control over AML/CFT issues among divisions, managers and employees of the Bank. Subordination, duties, rights and responsibilities of the employees are determined in their job descriptions;

introduction of the necessary control procedures and restrictions that ensure the effective functioning of the internal control system on AML/CFT issues;

descriptions contained in the regulations for divisions of the control functions performed by each of them on AML/CFT issues;

conducting regular risk assessment of the Bank on AML/CFT issues and measures to control the Bank;

ensuring information security and organizing proper exchange of information on AML/CFT issues;

monitoring the effectiveness of the internal control system on AML/CFT issues, including evaluating its effectiveness by conducting inspections by the Internal Audit Division;

2) methodologically by describing the internal control system on AML/CFT issues in the internal documents, including the frequency and timing of implementation of the control measures, officials who are assigned the control;

3) technologically by automating the control procedures for AML/CFT issues in the Bank's information systems, taking into account the Bank's judgment on the economic feasibility of automating such procedures.

5.17. The Bank ensures that there is proper internal control in the field of AML/CFT, including for various types of services/products, types of clients, the level of risks of clients, the amount of financial transactions and the identification of the Bank employees who make decisions at different stages of control in accordance with their functional responsibilities, ensuring the principle of "the higher position is, the greater powers and responsibility are assigned".

5.18. In order to exercise the internal control, the Bank periodically conducts further monitoring of financial transactions in accordance with the procedure established in the Bank's internal documents on AML/CFT issues, in order to identify financial transactions that are subject to financial monitoring, but for certain reasons were not detected in a timely manner.

VI. Requirements for ensuring the conduct of training events on AML/CFT issues

6.1. The responsible employee of the Bank, as well as other employees of the Bank involved in the AML/CFT intrabank system, must constantly maintain their level of knowledge on AML/CFT issues at the proper level, including through training in the field of AML/CFT and/or self-education, as well as advanced training in accordance with the procedure and within the time limits established by the Law on AML/CFT and internal documents of the Bank on AML/CFT issues.
6.2. The responsible employee of the Bank must complete training in the field of AML/CFT within three months from the date of his/her appointment, as well as undergo advanced training by completing training at least once every three years on the basis of the relevant educational institution belonging to the management sphere of the designated authority.
6.3. The Bank develops the internal documents on AML/CFT issues, which determine the procedure for conducting trainings for the Bank's employees. The internal documents on AML/CFT define the relevant structural divisions of the Bank, whose employees must be trained in AML/CFT.
6.4. When developing the content of trainings, the specifics of employees' duties, their powers and responsibilities, as well as the level of knowledge and qualifications necessary for such employees, are taken into account in order for them to properly perform their duties in the field of AML/CFT. The result of the training should be an understanding by the employees of the Bank's expectations and their responsibilities/role in the field of AML/CFT.
6.5. The Bank annually develops a plan for conducting trainings on AML/CFT that should contain:

1) the planned intrabank trainings (developed and conducted by the Bank's internal human resources and/or with the involvement of external lecturers/teachers);

2) the planned external trainings (the Bank employees attend the external trainings/pass appropriate certifications in the field of AML/CFT);

3) familiarization of the Bank employees with the requirements of the Bank's internal documents on AML/CFT issues before they start performing their duties (including in the event of a significant change in them) and in the event of changes to the Bank's internal documents on AML/CFT issues.

The plan for conducting trainings on AML/CFT issues shall be approved by the Chairman of the Bank's Management Board.
6.6. The intrabank training activities should include at least the following:

1) requirements of legislation and the Bank's internal documents on AML/CFT issues;

2) liability provided for by the legislation for violation of the requirements of the legislation on AML/CFT issues;

3) the highest risk zones of the Bank based on the results of the Bank's risk profile assessment;

4) examples of violations of relevant sanctions by banks and other entities;

5) the Bank's existing escalation/notification procedures (in particular, regarding its suspicions, possible violations, identified indicators of suspicious financial transactions, risk criteria, and other problematic issues on AML/CFT);

6) practical aspects of working with the Bank's software modules in order to meet the requirements of the legislation and the Bank's internal documents on AML/CFT issues.

6.7. After the Bank employees pass the appropriate training, testing of the level of knowledge acquired by employees is carried out, and repeated training is provided for those employees who received unsatisfactory results based on the results of testing.
6.8. The facts of conducting the relevant trainings should be documented, in particular, with the following information:

1) type of trainings and name of the training course;

2) surname, first name and patronymic (if any), title of the person who has completed the training;

3) surname, first name and patronymic (if any), title of the person who conducted the training (in the case of conducting an internal banking training, except for electronic courses);

4) place of training (in case of attending an external training);

5) data of the person who conducted an external training;

6) date of the training;

7) test results and/or a copy of the certificate (if any).

The plan for conducting trainings on AML/CFT issues, as well as the information specified in this paragraph, is stored by the Bank for at least five years from the date of the relevant training.

6.9. The content of trainings should be updated periodically, taking into account changes in the Bank's internal documents on AML/CFT issues, internal processes and procedures, and the results of assessing the Bank's risk profile.

6.10. The Bank provides an opportunity for the Bank employees to receive appropriate explanations and answers to questions related to the performance of their duties in the field of AML/CFT.

6.11. Considerable attention should be paid to training the responsible employee of the Bank, employees of the Financial Monitoring Service and employees of the Internal Audit Division in order to maintain their proper level of knowledge and qualifications in the field of AML/CFT.

6.12. The Bank's training programs should include training at least once a year for the Bank managers and employees of the Internal Audit Division in order to understand the international standards on AML/CFT and trends in the field of AML/CFT.

6.13. If a decision is made to involve agents, the Bank develops the internal documents on AML/CFT issues, which should provide for trainings for agents (their employees) and monitoring their activities.

6.14. When entering into contracts with agents to identify and verify the clients (representatives of the clients), the Bank constantly ensures that trainings are held for agents (their employees) in order to maintain an appropriate level of their knowledge regarding the requirements for the procedure for identifying and verifying the clients (representatives of the clients) of the Bank in accordance with the Bank's internal documents on AML/CFT issues. The Bank provides documentation of the fact of conducting trainings, their content and the list of agents (their employees) who have received appropriate training.

6.15. Trainings for the Bank employees are held on an ongoing basis in order for them to understand their responsibilities and the procedure for actions.

6.16. If a decision is made on the use of video verification, the Bank ensures that authorized employees of the Bank pass the appropriate and proper training for video verification prior to performing their duties related to ensuring the video verification process.

6.17. During the implementation of training activities on PEPs, special attention is paid to the concept of sources of fortune (wealth), in order to prevent cases when the Bank employees have a false assumption that the status of PEP itself is a rational and logical explanation for such a person to possess significant fortune (wealth) due to the presence of access to significant funds (assets) in connection with the performance of public functions.

6.18. If the Bank employees are involved in the analysis of financial transactions (including those that were detected using the automated modules) with the delegation of appropriate functional responsibilities and rights to them, training activities are provided for them in such a way that such employees are able to identify unusual and suspicious activities of the clients.

VII. Final Provisions

7.1. This Policy comes into force on the next business day after the date of its approval by the Board.

7.2. Amendments and additions to the Policy shall be approved by a decision of the Board and executed by amendments to this Policy or by setting out a new version of the Policy.

7.3. In case of non-compliance of any part of the Policy with the current legislation of Ukraine, in particular, statutory instruments of the National Bank of Ukraine, including in connection with the adoption of new laws of Ukraine or statutory instruments of the National Bank of Ukraine, this Policy shall apply only in the part that does not contradict the current legislation of Ukraine.
7.4. The Policy is an internal document of the Bank and is binding on all employees of the Bank within the scope of their duties.
7.5. The Financial Monitoring Service is responsible for keeping this Policy up-to-date.

TRUE COPY

*[Total numbered, bound, signed and sealed 22 pages*Director of the Legal Department*L.O. Myronova]*

[Bound, numbered and signed Chairman of the Supervisory Board*/signature/ V.A. Kopylov]*

*/Seal: Joint-Stock Company "CRYSTALBANK"*identification code: 39544699*Kyiv*Ukraine /*