ASIA ALLIANCE BANK

Combating Money Laundering, Terrorism Financing and Financing Proliferation of Weapons of Mass Destruction and Sanctions Policy

(Compliance program)

Tashkent – 2024

I. General rules

This Policy establishes and regulates the basic rules, principles and measures aimed at ensuring compliance of the activities of ASIA ALLIANCE BANK with combating the legalization of proceeds from criminal activity, the financing of terrorism, the financing of the proliferation of weapons of mass destruction and sanctions, and also establishes the relevant functions and obligations of the divisions of ASIA ALLIANCE BANK.

2. The following key concepts are used in this Policy:

bank – JSCB "ASIA ALLIANCE BANK";

front office – employees, including senior employees of the bank's divisions, directly involved in customer service and responsible for customers' banking operations;

regulatory document – a bank's regulatory legal act (policy, regulation, procedure, instruction, etc.) that defines the main standards and approaches to the bank's activities in the following areas;

CDD – customer due diligence;

ML – money laundering;

rules – Internal control rules for combating money laundering, terrorism financing and the financing of the proliferation of weapons of mass destruction in commercial banks (registration of the Ministry of Justice of the Republic of Uzbekistan No. 2886 dated May 23, 2017);

risk appetite protocol – "ML/FT and sanctions risk appetite" protocol.

training program – a training program for the preparation and retraining of bank employees on AML/CFT and FPWMD issues;

Watch list – a list of individuals and legal entities provided by the SASB and associations for combating international economic crimes

ROBS – regional office of banking services;

SASB – specially authorized state body (Department for Combating Economic Crimes under the Prosecutor General's Office of the Republic of Uzbekistan); ;

Sanction – a coercive measure applied by states or international organizations to a state, legal entities and individuals who have violated international law;

FPWMD – financing the proliferation of weapons of mass destruction;

FT – terrorist financing;

Central Bank – the Central Bank of the Republic of Uzbekistan;

client – an individual or legal entity that carries out banking financial transactions;

bank account - an account opened by a bank for a client in accordance with an agreement under which the bank undertakes to accept and credit funds received on its account, to carry out the client's instructions to transfer and issue the corresponding funds and to carry out other operations on the account;

one off transaction - transactions carried out by clients on a one-time basis without opening a bank account, not repeated within one month;

escalation - notification of a higher level of the bank about questionable cases identified in the course of combating AML/CFT and FPWMD.

3. This Policy is mandatory for application in all divisions of the bank.

4. The Bank undertakes to comply with the legislation of the Republic of Uzbekistan, the Rules, sanctions, this Policy, as well as the following regulatory documents of the Bank:

Regulations on the Bank's Compliance Control Department;

Know Your Customer (KYC) Procedure;

Risk Assessment Procedure (RA);

Transaction Monitoring and Reporting Procedure (TM);

Sanctions Screening Procedure (SS).

5. The objectives of this Policy are:

effective detection and suppression of operations aimed at ML/FT and FPWMD;

prevention of intentional or unintentional involvement of the bank in criminal activity, penetration of criminal capital into its authorized capital, as well as penetration of criminal persons into the management of the bank;

detection, assessment, documentary recording and mitigation of risks;

ensuring strict compliance with the requirements of the legislation on AML/CFT and FPWMD;

compliance with sanctions in the manner prescribed by the bank's regulatory documents.

6. In the event that the requirements of the Government of the Republic of Uzbekistan, the Central Bank and the SASB are not provided for by this Policy, then the requirements established by the Government of the Republic of Uzbekistan, the Central Bank and the SASB shall apply. In this case, appropriate changes and additions must be made to this Policy based on the requirements of the Government of the Republic of Uzbekistan, the Central Bank and the SASB.

7. This Policy also sets out the management principles and standards for protecting the bank from money laundering, terrorist financing, sanctions violations and financing the proliferation of weapons of mass destruction.

II. Management and control of compliance with AML/CFT, FPWMD and sanctions requirements

8. The Bank shall make every effort to ensure the adoption of measures aimed at combating the legalization of proceeds from criminal activity, the financing of terrorism and the proliferation of weapons of mass destruction.

9. The Bank undertakes to conduct continuous and systematic monitoring of employees in terms of their compliance with the legislation of the Republic of Uzbekistan, this Policy and other regulatory documents of the Bank.

10. the Bank's Supervisory Board’s authority includes:

monitoring compliance with legislation and regulations related to AML/CFT and sanctions compliance; reviewing materials on the study of the implementation of this Policy and the Bank's compliance with sanctions, submitted by the management and the Internal Audit Department, and making decisions on them;

ensuring that the Bank's senior management has the necessary qualifications and appropriate authority to manage ML/FT risks and sanctions; approving the Bank's AML/CFT policy and monitoring its implementation;

appointing and dismissing employees of the Compliance Control Department; evaluating and providing material incentives for the activities of the Compliance Control Department employees.

The Bank's Supervisory Board serves as a high-level escalation point for consultations on AML/CFT and sanctions compliance.

11. The authority of the Internal Audit Department includes:

conducting an independent and periodic assessment of risk control over the implementation of the AML/CFT program and compliance with sanctions;

creating a methodological audit base for assessing the effectiveness of the implementation of the AML/CFT program and compliance with sanctions; providing materials on the study of the results of the internal audit and proposals for eliminating deficiencies to the Supervisory Board of the bank and relevant stakeholders.

Depending on the risk profile of the bank, additional audits may be assigned, including through the involvement of third parties.

12. The authority of the Chairman of the Management Board of the Bank includes:

ensuring the development of the draft AML/CFT and Sanctions Compliance Policy;

monitoring the assessment and revision of the AML/CFT and Sanctions Compliance Policy;

proposing for consideration and approval by the Supervisory Board of the Bank candidates who have the appropriate qualifications and independence for the effective implementation of the AML/CFT and sanctions compliance program;

ensuring the allocation of resources at the appropriate level for AML/CFT and sanctions compliance activities.

13. The authority of the Bank's Management Board includes:

conducting, together with the Compliance Control Department, ongoing monitoring of the implementation and evaluation of the effectiveness of the AML/CFT program and sanctions compliance by the bank;

coordinating the effectiveness of the bank's senior management ("Tone from the top");

reviewing and discussing the AML/CFT and sanctions compliance program within the scope of its responsibilities;

assessing and eliminating risks and deficiencies identified as a result of the compliance test and independent audit of the AML/CFT and sanctions compliance policy, bringing the bank's regulatory documents into compliance;

establishing appropriate procedures for the implementation of the AML/CFT and sanctions compliance policy subject to subsequent approval by the Bank's Supervisory Board; making amendments and additions to the regulatory documents defining the procedure for the AML/CFT policy and sanctions compliance, within the timeframes and in the manner established by the legislation of the Republic of Uzbekistan;

allocation of sufficient and necessary resources to ensure the activities of the bank's divisions in AML/CFT compliance and sanctions compliance at the proper level.

The bank's management serves as the first-level escalation point for consultation on the AML/CFT program and sanctions compliance.

14. The authority of the heads of departments and other equally important divisions of the bank includes:

compliance with and implementation of this Policy, as well as other regulatory documents of the bank;

strict fulfillment of compliance requirements established by the bank's management;

regular review and ensuring compliance of business processes with the AML/CFT program and sanctions compliance.

Front office managers must have compliance skills and ensure control over ML/FT risk management and control over sanctions compliance for the relevant areas, including clients and transactions.

15. The authority of the Head of the Compliance Control Department includes:

development of the draft AML/CFT and Sanctions Compliance Policy;

ensure implementation and assessment of the AML/CFT and Sanctions Compliance Policy;

submission of a report on AML/CFT, including compliance with the Know Your Customer (KYC) program;

“Risk Assessment Procedure” (RA); “Transaction Monitoring and Reporting Procedure” (TM); Sanctions Verification Procedure (SS) to the Management Board and the Supervisory Board of the bank;

ensure control over compliance by the bank's divisions with this Policy and related regulatory documents;

ensure strengthening the responsibility of employees responsible for ensuring compliance with the AML/CFT and sanctions program, and establishing a periodic reporting system;

reduction of ML/FT and sanctions risks when developing new products, services and introducing technologies, creation and implementation of an effective system for managing them;

maintaining relevant records in the AML/CFT and sanctions compliance program;

creation and implementation of the Know Your Employee (KYE) system;

conducting training sessions for employees on the AML/CFT and sanctions compliance program;

regularly assessing and correcting the effectiveness of AML/CFT and sanctions compliance in the bank, as well as providing the Supervisory Board of the bank with a report on the results of tests and corrections once every three months;

providing the head of the Supervisory Board of the bank with information on the process in the compliance system, changes in it and compliance risks in electronic form at least once a week;

distribution of duties and tasks among the employees of the Compliance Control Department taking into account the volume and complexity of financial transactions;

The Head of the Compliance Control Department is a member of the Management Board of the bank.

16. The authority of the Deputy Head of the Compliance Control Department includes:

assisting the Head of the Department in the performance of the functions and tasks assigned to the Department;

ensuring the performance of the functions and tasks assigned to the Compliance Control Department in resolving compliance issues together with authorized government agencies on the AML/CFT and sanctions compliance program.

In the temporary absence of the Head of the Compliance Control Department from the workplace, his functions and tasks shall be assigned to the Deputy Head of the Department.

17. The authority of the Compliance Control Department includes:

creation, implementation and evaluation of the AML/CFT and sanctions compliance program;

control and coordination of the daily implementation of the AML/CFT and sanctions compliance program in accordance with this Policy and related regulatory documents;

monitoring the implementation of the bank's AML/CFT training program and sanctions compliance;

bringing this Policy and related regulatory documents to the attention of each responsible employee.

The Compliance Control Department is the second-level escalation point for AML/CFT and sanctions compliance issues of the bank

18. The authority of the ROBS managers includes:

responsibility for the compliance of all financial transactions carried out in the ROBS with the requirements of this Policy and regulatory documents;

should have the necessary competence to manage AML/CFT risks and sanctions compliance, as well as ensure control over the progress of compliance by the ROBS employees with the requirements of this Policy;

coordination of activities jointly with the Compliance Control Department on issues of compliance with AML/CFT requirements and sanctions compliance.

19. The authority of the front office employees includes:

obtaining information related to the identification of the client when establishing practical working relationships, etc.;

conducting checks at the appropriate level in accordance with the client's risk level;

monitoring transactions, notifying the Compliance Control Department of questionable and suspicious transactions identified during monitoring; notifying the Compliance Control Department in the event of receiving an initial signal related to AML/CFT and compliance with sanctions, namely a trigger event;

Responsible front office employees serving clients and carrying out financial transactions on behalf of and at the direction of clients, as well as senior employees, are the bank's main link in identifying and preventing cases of money laundering.

III. Risk-oriented approach

20. The Bank implements a risk-based approach to identifying and assessing the risks of money laundering, terrorist financing, proliferation of weapons of mass destruction and sanctions.

At the same time, the Bank, in order to reduce the main risk, strengthens compliance with internal controls and allocates appropriate and necessary resources. For the preliminary active prevention of potential threats, the Bank establishes a "Risk Appetite" in terms of the AML/CFT program and sanctions compliance.

The Bank carries out an assessment of ML/FT and sanctions risks for the purpose of continuously studying, identifying, assessing, reducing and monitoring ML/FT and sanctions risks in accordance with the Risk Appetite protocol in accordance with Appendix No. 1 to this Policy.

21. Bank employees are required to take into account the Risk Appetite Protocol when performing their official duties and making various decisions.

The main principle for the bank based on the ML/FT and sanctions risk appetite protocol is: the bank considers its main goal to be the implementation of requirements for all requests and instructions of the control committee, and strives to maintain relations with them;

the bank in its activities takes into account the possible risk of FPWMD, terrorist financing and sanctions, as well as the emergence of a high level of risk for some types of activities and clients of the bank.

At the same time, in order to maintain an average risk profile, the bank takes measures to effectively manage and reduce all risks at a high level.

The draft ML/FT and sanctions risk appetite protocol is developed by the Compliance Control Department for each financial year and submitted for approval to the Supervisory Board of the bank.

a) AML/CFT and Sanctions Risk Assessment

22. The primary objective of the AML/CFT and Sanctions Risk Assessment is to identify the bank's AML/CFT and sanctions risks, taking into account factors such as customers, products and services, geographic location, channels and transactions, and to effectively address the residual risk through the AML/CFT and sanctions compliance program.

23. In accordance with this Policy, the Compliance Control Department shall:

at least once a year assess the level of ML/FT risk and sanctions;

develop strategies and action plans for areas of activity to reduce residual risks;

provide plans for eliminating the main risks and control deficiencies identified during the assessment to the bank's management bodies;

develop necessary measures for the priority implementation and elimination of identified deficiencies or control deficiencies.

After their implementation, these measures may have a significant positive impact on the overall residual risk of the bank.

24. When assessing the level of ML/FT risk and non-compliance with sanctions, the following must be carried out:

study, analysis, identification, assessment, monitoring, management, documentation and risk mitigation;

identification of deficiencies in the AML/CFT and sanctions compliance program, and study of opportunities for its improvement;

study of the risk profiles of each area of the bank's activity, including the factors of the impact of new products and services on the risk profile of the bank and individual front offices, as well as their potential impact;

assistance to the Bank in making strategic decisions, including the development or revision of the Risk Appetite Protocol, resource allocation, implementation of enhanced control, improvement of technologies and systems, etc.

25. The bank's management and relevant departments must pay serious attention to the status of implementation of actions to correct the identified deficiencies and receive regular reports from the Compliance Control Department.

26. In order to assess the possible impact on the level of residual risk (ideally, reduction), the bank must take all measures to eliminate the identified deficiencies before the next assessment of the risk of ML/FT and non-compliance with sanctions.

The Front Office ensures compliance with ML/FT risks and sanctions.

b) New products, services or technologies

27. Before introducing new products and services, business operations or new or developing technologies, the bank shall assess the products and services of this type for ML/FT risks and sanctions.

28. Before introducing any new product, service or technology, the bank unit implementing such services (products) shall be responsible for studying the compliance of the existing risks with the requirements of the compliance policy and shall take into account the following minimum requirements:

identification and assessment of the capabilities of the bank's responsible units to manage the specific risk of the new product, service or technology, and the levels of risk associated with it;

before introducing a new product, service or technology, ensure that the proposed new product, service or technology has been assessed by the Compliance Control Department for ML/FT risk and non-compliance with sanctions;

adopting appropriate measures by the bank unit and the Compliance Control Department to monitor and mitigate these risks; the need to provide information on the results of the measures to the Bank's Management Board.

29. Before making changes and additions to existing products, services and technologies, the bank takes into account the minimum requirements described above, based on the specific risk profile of the bank.

30. Risk identification and assessment are carried out by the bank's division implementing new types of services (new technologies) jointly with the Compliance Control Department.

In this case, the implementation of a new service (new technologies) into practice is carried out after the deficiencies identified during the assessment of this service (new technology) have been eliminated and measures have been taken to reduce risks.

The bank's division implementing new types of services (new technologies) and the Compliance Control Department must take appropriate measures to monitor and reduce these risks.

Before implementing a new product, service or technology, the bank's division implementing new types of services (new technologies) completes and provides information in the form in accordance with Appendix No. 2 to this Policy.

IV. Policy for establishing practical business relationships with clients.

31. The Bank operates on the basis of the Know Your Client (KYC) procedure established by the Bank, which includes the procedures and processes necessary for establishing practical business relationships with clients, and enters into practical relationships with clients that meet its requirements.

a). Prohibited clients and types of prohibited activities

32. This Bank Policy prohibits the establishment of practical business relationships, including conducting one-off transactions, with any individual/legal entity designated as a "Prohibited type of client" and "Prohibited type of activity" under the Know Your Client (KYC) procedure.

b). Know Your Client (KYC)

33. This Bank Policy ensures work with clients who are engaged in legitimate business activities and receive their income, funds and investment assets from legitimate sources.

The Bank aims to enter into transactions only with clients known to the Bank through risk-based due diligence.

If the Bank does not have the ability to properly verify clients, the Bank prohibits the establishment of relationships with clients and the execution of one-off transactions. The Bank performs the KYC procedure before executing all financial transactions.

34. Front office employees continuously check all clients, including related parties, for compliance with the Watch List during the Know Your Client (KYC) procedure.

In the event that it is established that the data of a potential client completely matches the data of a person included in the Watch List, the Bank employee is obliged to inform the Compliance Control Department about this fact.

The Compliance Control Department conducts an analysis and verification of the client and sets appropriate recommendations.

35. The risk level of the Bank's clients is formed as a result of a combination of such indicators as the type of client, origin (country), banking products and services used, communication channels, etc.

The Bank conducts a process of client risk assessment for all clients.

36. Clients are divided into separate categories depending on the risk level. The client's risk level is verified during the course of the client interaction, as well as on an ongoing, periodic or event-driven basis.

c) Client Due Diligence

37. The concept of customer due diligence includes the processes of identifying and verifying customers. CDD is used during customer onboarding, account opening and periodic or event-based reviews.

38. The customer CDD process includes at least the following:

identification and verification (where appropriate of any persons acting on behalf of the customer);

identification of beneficial owners and related parties;

examination of the business and purpose; ongoing monitoring and updating of identification information;

identifying suspicious activity and reporting it to the CMS.

39. The CDD programme includes the following methods:

simplified due diligence (SDD) for lower-risk customers;

general due diligence (CDD) for customers not considered subject to simplified due diligence;

enhanced due diligence (EDD) for high-risk customers.

Special enhanced due diligence (SEDD) for certain types of customers and accounts that are distinguished by the unique nature of the customer and account, in accordance with the Know Your Customer (KYC) procedure.

40. The Bank is obliged to inform the customer about insufficient information to identify its customers under the Know Your Customer (KYC) procedure and about the failure of verification (for example, opening of an account or rejection of a transaction).

d). Know your employee (KYE)

41. In order to prevent the involvement of employees, including persons hired by the bank under civil law contracts, in ML/FT, the Know Your Employee (KYE) program is being implemented.

The Know Your Employee (KYE) check is conducted for all employees every year to determine the involvement of the bank's employees in ML/FT activities.

In the event that any employee is found to be involved in a recorded criminal act, the bank's management will immediately take measures against this employee in accordance with the legislation of the Republic of Uzbekistan.

42. If necessary, the Compliance Control Department may conduct additional Know Your Employee (KYE) checks.

d). Personnel qualifications

43. The Bank is obliged to conduct regular training, preparation and retraining of the employees of the Compliance Control Department, front office, legal services, internal audit and security services in order to ensure that employees are informed about the latest developments, including information on modern AML/CFT and FPWMD techniques, methods and trends, and a clear explanation of all aspects of the legislation and AML/CFT and FPWMD obligations.

44. The Compliance Control Department, together with the relevant divisions of the Bank, shall annually develop a training program.

The training program must provide for the following: the procedure for conducting training, preparation and retraining, their forms (initial briefing, scheduled and unscheduled training) and deadlines;

appointment of persons responsible for organizing the training, preparation and retraining; the procedure for intermediate and final knowledge testing. The training program is approved by the Management Board of the Bank.

e). Client Termination Policy

45. In the event that a new or existing client poses an unacceptable level of risk to the bank based on the Risk Appetite Protocol indicators, the bank will consider refusing the transaction and/or terminating the relationship with this new or existing client, and will inform the SASB of the reasons for terminating the relationship.

46. The bank will consider refusing a transaction and/or terminating the relationship with clients at least in the following cases:

when the client refuses to provide information for the KYC process; when the client or its related parties are subject to sanctions;

when it is discovered that the client is involved in activities with prohibited clients. The list of prohibited types of clients is defined in the bank's Know Your Customer (KYC) procedure.

47. In the event that a client is identified as the object of refusing a transaction and/or terminating the relationship, the Head of Compliance Control must be informed about this.

The Head of Compliance Control Department studies the matter and submits the information to the Chairman of the Management Board of the bank for further analysis.

The final decision on relations with clients is made by the Chairman of the Board of the Bank.

V. Sanctions Compliance Program

48. All Bank employees are required to comply with sanctions programs that restrict trade or other economic activity with certain jurisdictions, individuals, entities, organizations, products or countries.

It is the Bank’s policy to comply with all applicable sanctions requirements. The Bank screens all customers, employees, suppliers of products and services, certain related parties and transactions for sanctions compliance when establishing and maintaining banking relationships.

49. Bank employees are prohibited from establishing business relationships with sanctioned persons (customers), opening new accounts or entering into business relationships with them, except as provided in the Bank’s Sanctions Screening (SS) Procedure.

VI. Suspicious Activity Monitoring and Reporting Program

50. In the event of detection of questionable and/or suspicious situations related to AML/CFT and FPWMD, front office employees must immediately escalate such situations directly to their manager and employees of the Compliance Control Department in the form according to Appendix No. 3 to this Policy.

In order to determine whether the activity is suspicious or not, the Compliance Control Department conducts an analysis and investigation, and takes appropriate measures.

51. The head of the Compliance Control Department is responsible for timely informing the Bank's Management Board, the Central Bank and the SASB about suspicious activity in accordance with the legislation of the Republic of Uzbekistan.

52. Any involvement of employees in ML/FT, violation of sanctions or other illegal activity through ignorance or deliberate inaction (inaction) is strictly prohibited.

53. The Compliance Control Department identifies dubious and suspicious transactions of clients on the basis of AML/CFT and informs the SASB about this in accordance with the established procedure.

VII. Confidentiality

54. All employees of the Bank shall maintain strict confidentiality of all activities related to external regulatory reporting. Information related to any external reporting shall not be disclosed.

VIII. Record Keeping

55. The Bank may provide the necessary information in accordance with the Law of the Republic of Uzbekistan "On Bank Secrecy".

The Bank is required to collect, store and maintain certain types of information. These data are as follows: customer information, including documents and evidence submitted to meet the requirements of the "Know Your Customer (KYC)" procedure;

money transfer transactions, including domestic and international money transfers;

AML/CFT and sanctions documents, regulations and instructions of the Bank confirming their compliance;

bank account files and correspondence on activities, as well as the results of any analysis performed;

correspondence with regulatory authorities;

reports of suspicious financial transactions.

56. The Compliance Control Department strictly adheres to the requirements for maintaining all records related to AML/CFT and sanctions compliance. All records related to AML/CFT and sanctions compliance are stored for at least 5 years.

Electronic versions of documents are recorded, archived, on electronic media and stored by the Head of the Compliance Control Department together with the necessary documents in a fireproof safe.

Upon expiration of the storage period, the documents are transferred to the bank's archive in accordance with the established procedure.

57. The Compliance Control Department limits the use by front office personnel of information related to AML/CFT and sanctions compliance, including documents stored in the bank's archive.

The Compliance Control Department ensures non-disclosure of information received by bank employees in the course of performing their duties.

IX. Compliance Stress Test

58. The Head of the Compliance Control Department develops and implements a stress testing plan for the AML/CFT and Sanctions Compliance Policy in accordance with the risk-based approach.

The Compliance Control Department identifies, assesses, diagnoses and monitors risks associated with compliance with the bank's AML/CFT and sanctions requirements, and prepares reports on the relevant tests and their results.

59. The AML/CFT and sanctions compliance stress test is conducted at least annually and includes an assessment of compliance with regulatory requirements, as well as internal

policies, procedures and controls. A report on the diagnostic results of the compliance stress test is submitted to the Supervisory Board of the bank.

X. Internal Audit Review

60. The Internal Audit Department of the Bank develops and maintains a plan for audits of the Compliance Control Department.

Internal audit is conducted at least once a year. External audit is conducted on a voluntary basis to assess the effectiveness of the AML/CFT and Sanctions Program of the Compliance Control Department and this Policy.

The results of the AML/CFT and sanctions review will be presented to the Supervisory Board of the Bank.

XI. Reporting to the Supervisory Board of the Bank

61. The Compliance Control Department maintains the necessary and proper records of its AML/CFT and sanctions compliance program and provides regular quarterly reports to the Supervisory Board of the Bank.

XII. Transaction Monitoring System

62. In order to effectively implement the tasks defined by this Policy and its procedures, the Compliance Control Department creates and implements a transaction monitoring system (TMS).

The system automatically identifies transactions that meet the criteria that are recorded in the "Transaction Monitoring and Reporting" procedure. If it is impossible to automatically determine whether transactions meet the criteria, the determination is carried out manually by the employees of the Compliance Control Department.

XIII. Appendix

Information	Name	File
Appendix No. 1	ML/FT Risk Appetite and Sanctions Protocol	
Appendix No. 2	New products and services	
Appendix No. 3	Escalation form	