AML / KYC POLICY

ALTN Limited

(Registered in the Astana International Financial Centre, regulated by AFSA)

1. POLICY STATEMENT

ALTN Limited (the Company) is committed to full compliance with the Law of the Republic of Kazakhstan dated August 28, 2009 'On Counteracting the Legalisation (Laundering) of Proceeds from Crime and the Financing of Terrorism' (KZ AML/CFT Law), AIFC Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Rules No. FR0008 of 2017 (AIFC AML Rules), Guidance (Requirements) applicable to the Rules of Internal Control for the purposes of counteracting the legalisation (laundering) of proceeds from crime and the financing of terrorism for financial monitoring entities of the Astana International Financial Centre (the Relevant Persons) dated May 21, 2020 (Guidance), and applicable best international standards and practices, e.g. Financial Action Task Force (FATF) standards and other applicable law and documentation. The Company has adopted and will enforce the provisions set forth in ('AML Regulations') in order to prevent and detect money laundering, terrorist financing and other illegal activities.

If the Company, its personnel and/or premises are inadvertently used for money laundering or other illegal activities, the Company can be subject to potentially serious civil and/or criminal penalties. Therefore, it is imperative that every member, officer, director, and employee (each, an "employee") is familiar with and complies with the policies and procedures set forth in this Policy.

This Compliance Statement is designed to assist all Clients in adhering to the Company's policy and procedures, which, if followed diligently, are designed to protect themselves, the Company, its employees, its facilities and its activities from money laundering or other illegal activities.

To ensure that the Company's policies and procedures are adhered to, the Company shall designate an Anti-Money Laundering Compliance Officer (the "Compliance Officer"). The Compliance Officer is responsible for establishing and conducting employee training programs to ensure that all appropriate employees are aware of the applicable Anti-Money Laundering Regulations, the Company's Anti-Money Laundering Policies & Procedures and their responsibilities with respect to these policies.

2. OBJECTIVES

– Comply with all Anti-Money Laundering Rules & Regulations of the jurisdictions in which **ALTN Limited** operates.
– Require all employees to prevent, detect and report to the Compliance Officer all potential instances in which the Company or its employees, its facilities or its activities have been or are about to be used for money laundering, terrorist financing and other illegal activity.
– Provide for a Compliance Officer who shall ensure adherence to the Company's Anti-Money Laundering Policies and Procedures.
– Require all appropriate employees to attend anti-money laundering training sessions, so that all such employees are aware of their responsibilities under the Company's policies and procedures;

this Policy; and as affected by current developments with respect to anti-money laundering events.

3. MONEY LAUNDERING DEFINITION

Money laundering involves the placement of illegally obtained money into legitimate financial systems so that monetary proceeds derived from criminal activity are transformed into funds with an apparently legal source.

Money laundering has many destructive consequences both for society as a whole and for those entities involved in money laundering activities. With respect to society as a whole, money laundering may provide resources for drug dealers, terrorists and other criminals to operate and expand their criminal activities.

With respect to entities, any involvement, whether to instigate, assist, conceal, or ignore the source, nature, location, ownership or control of money laundering activities, can lead to both civil and criminal proceedings against both the individual and the entity involved. Additionally, the adverse effects, including the adverse publicity to **ALTN Limited** associated with involvement in money laundering events, cannot be emphasized enough.

Money laundering transactions may include:
a. Engaging in any activity while willfully or recklessly disregarding the source of the funds or the nature of the Client's transaction;
b. Engaging in any activity designed to hide the nature, location, source, ownership or control of proceeds of criminal activity;
c. Dealing in funds to facilitate criminal activity; or
d. Dealing in the proceeds of criminal activity.

Money laundering can involve the proceeds of drug dealings, terrorist activities, arms dealings, mail fraud, bank fraud, wire fraud or securities fraud, among other activities.

4. CONTROLS TO PREVENT MONEY LAUNDERING

a. Put in place internal controls and policies to ensure continuing compliance with the Rules & Regulations.
b. Appoint a **Money Laundering Reporting Officer (Compliance Officer)**.
c. Establish / enhance record keeping systems for:
   i. All transactions;
   ii. The verification of Client's identity.
d. Establish internal suspicion reporting procedures.
e. Educate and train all staff with the main requirements of the Rules & Regulations.

Internal controls and policies should be established and recorded in order to:
a. Ensure that anyone who suspects money laundering knows how to report this information to their Compliance Officer.
b. Provide the Compliance Officer with the means by which the reasonableness of the suspicion can be judged, and thereby assess which suspicious matter should be reported to the **Financial Monitoring Agency (FMA)** of the Republic of Kazakhstan.

The obligation to report does not depend on the amount involved or the seriousness of the offence.

5. RECORD KEEPIN

All records verifying the identity of **ALTN Limited**'s Clients must be**Financial Monitoring Agency (FMA)** must be retained for 7 years from the time of the report. Records of who has been trained and the timing and form of training sessions must be kept for 6 years from the time of the training session.

6. PROHIBITION ON RELATIONSHIPS WITH SHELL BANKS

The MLRO of **ALTN Limited** is responsible for monitoring and must not allow setting up any business relationships with Shell Banks (5.1.6 AML Rules).

7. ANTI-MONEY LAUNDERING – COMPLIANCE OFFICER – MLRO

Any employee of **ALTN Limited** shall immediately notify the MLRO if he/she suspects or has any reason to suspect that any potentially suspicious activity has occurred or will occur if a transaction is completed. Employees are encouraged to seek the assistance of the MLRO and Compliance Officer with any questions or concerns they may have with respect to the Company's Anti-Money Laundering Policies or Procedures.

Appointment of MLRO
The Board of Directors will appoint an individual as MLRO, with responsibility for implementation and oversight of its compliance with the AML Rules, who has an appropriate level of seniority and independence to act in the role. The MLRO must have independence and authority within the organization to carry out their responsibilities effectively. This includes having access to necessary resources, support from management, and the ability to escalate any concerns or issues related to AML/CFT compliance. The MLRO may directly report to the Board of Directors.

Deputy MLRO – is a role within the organization responsible for assisting and supporting the MLRO in carrying out their duties related to AML/CFT activities. The Deputy MLRO acts as a deputy or second-in-command to the MLRO and helps ensure compliance with relevant AML/CFT laws, regulations, and internal policies. In the absence of the MLRO, the Deputy MLRO temporarily executes the functions of the MLRO.

Responsibilities of the MLRO
The MLRO will implement and oversee, and is responsible for, the following matters:
a. the day-to-day operations for compliance by the Company with its Policy, procedures, systems and controls;
b. acting as the point of contact to receive notifications from the Company's employees under 5.2. of this Policy;
c. acting as the point of contact within the Company for the AIFC, the AFSA, and any other competent authority regarding money laundering issues;
d. responding promptly to any request for information made by the AIFC, the AFSA, and any other competent authority;
e. registering in the FMA reporting system for submitting SARs, STRs, TTRs before the

commencement of its business activities;
f. creation of risk management procedures associated with AML/CFT and the financing of the proliferation of weapons of mass destruction;
g. conducting internal risk assessment related to AML/CFT and the financing of the proliferation of weapons of mass destruction;
h. development of internal rules of compliance in accordance with the AML Rules, and submitting them for approval to the CEO and Board of Directors of the Company;
i. making a reasoned decision to assign a different final level of risk to the work with the customer;
j. identification among the customers of the Company of persons in respect of which measures should be taken to freeze funds and/or block financial transactions;
k. making a decision on recognizing a financial transaction as suspicious (non-suspicious) and submitting (non-submitting) information about it to AFSA and FMA;
l. making a decision to refuse to carry out a financial transaction in cases provided for by the AML/CFT Law, and this Policy;
m. obtaining and updating the list of terrorists, sanction lists, list of financing weapon of mass destruction and list of financial pyramids;
n. tracking and analyzing changes in legislation in the field of prevention of money laundering, financing of terrorist activities and financing of the proliferation of weapons of mass destruction, as well as the gathering of relevant information on the prevention of money laundering, financing of terrorist activities and financing of the proliferation of weapons of mass destruction received from state bodies;
o. filling in, signing SARs and STRs with an electronic digital signature and their timely submission to the FMA and AFSA in the form of an electronic document;
p. ensuring the systematic study (monitoring) of the Recommendations (positions) of the FATF regarding the prevention of legalization of proceeds from crime, the financing of terrorist activities or the financing of the proliferation of weapons of mass destruction in the course of activities similar to that carried out by the Company;
q. consulting employees of the Company on issues arising from the implementation of internal control rules, risk management procedures, identification, verification of customers and preparation of information to the financial monitoring body;
r. organizing and conducting scheduled training, other types of training, as well as testing the knowledge of the employees of the Company on AML/CFT and the financing of the proliferation of weapons of mass destruction;
s. making proposals to the CEO of the Company on improving and increasing the efficiency of the internal control system, as well as proposals on the need to make changes and/or additions to the internal control rules;
t. submission of AML Return report to AFSA, on an annual basis, no less than 2 months after the end of the calendar year, as per 13.7. AML Rules;
u. other functions in accordance with official duties, this Policy, applicable laws of the AIFC, AML/CFT Law and other local regulatory legal acts of the Company, and the requirements of AML Rules in preventing the legalization of proceeds from crime, financing terrorist activities and financing the proliferation of weapons of mass destruction.

For the implementation of the functions, the MLRO has the right to receive from the employees of the Company the necessary documents and information.

With the prior approval of AFSA, the Company will appoint and change the MLRO.

Obligations of Co-operation
The MLRO will deal with AFSA in an open, responsive, and co-operative manner and will

disclose appropriately any information of which AFSA would reasonably be expected to be notified.

Reporting
The Company will complete AFSA's AML Return form on an annual basis and submit such form to AFSA within 2 months of its financial year end.

Responsibilities of the Compliance Officer include the following:
a. Developing and regularly reviewing the Company's AML/CFT systems to ensure they are up-to-date, meet legal and regulatory requirements, and effectively manage the risks associated with money laundering and terrorist financing;
b. Monitoring and supervising all aspects of the Company's anti-money laundering and counter-terrorist financing systems, including assessing their effectiveness and making necessary improvements to the controls and procedures;
c. Communicating important anti-money laundering and counter-terrorist financing issues to senior management, including significant compliance deficiencies, if applicable;
d. Ensuring that the training provided to staff members regarding anti-money laundering and counter-terrorist financing is sufficient, appropriate, and effective in equipping them with the necessary knowledge and skills.

9. PRE-TRANSACTION REPORTING TO THE FINANCIAL MONITORING AGENCY

If a pre-transaction Suspicious Activity Report (SAR) is made by the MLRO to the relevant criminal authority, no business may be conducted with or for the Client until the MLRO receives “consent” from the relevant criminal authority. Dealing with or advising a Client before receiving consent from the relevant criminal authority may constitute one of the offences, that is concealing, arrangements, or acquisition.

If a SAR is submitted to the FMA, no related transaction or activity is allowed to proceed until the Company has been contacted by the relevant FMA or a law enforcement agency.

The MLRO will inform whether the FMA consents to you dealing with the Client or not. Please liaise directly with the MLRO who will provide guidance on what information may be provided to the Client or potential Client.

10. POST-TRANSACTION REPORTING TO THE FINANCIAL MONITORING AGENCY

Since the FMA cannot provide consent after a transaction or activity has already occurred, it will provide an acknowledgment of receipt of a SAR to the MLRO. In the absence of an indication to the contrary from the MLRO, you may deal with the Client as normal. However, you must inform the MLRO of every interaction with the Client and seek guidance on how to deal with that Client.

11. DECISION NOT TO REPORT TO THE FINANCIAL MONITORING AGENCY

Until the MLRO informs you that no SAR to the FMA is to be submitted, any further transactions or activity in respect of the suspected Client must be reported to the MLRO as soon as they arise.

12. CONTACT WITH THE CLIENT AND THIRD PARTIES

Any contact from the Client questioning the delay in processing their transaction needs to be handled very carefully. In these circumstances, please liaise closely with the MLRO.

Whether or not the relevant criminal authority allows you to proceed with a transaction, you may not tip off the Client that a disclosure to the authorities has been made. Neither may you disclose that such a disclosure has been made in response to a data protection request.

Unless specifically authorized to do so, you must not discuss any reports of suspicions of money laundering with third parties. Any requests for information from third parties, such as the Police or Customs, must be immediately referred to the MLRO.

13. CLIENT DUE DILIGENCE

13.1. Obligation to Undertake Client Due Diligence

The Company must:
a. undertake Client due diligence (hereinafter – "CDD") under 13.6 a) for each of its Clients; and
b. in addition to a), undertake Enhanced due diligence (hereinafter – "EDD") under 36 in respect of any Client it has classified as high risk.

13.2. Establishment of Business Relationship

The Company will apply CDD measures:
a. when establishing a business relationship with a Client; and
b. after establishing a business relationship with a Client.

13.3. After the Establishment of a Business Relationship

The Company will also undertake appropriate CDD if, at any time:
a. in relation to an existing Client, it doubts the veracity or adequacy of documents, data, or information obtained for the purposes of CDD;

13.3. After the Establishment of a Business Relationship

The Company will also undertake appropriate CDD if, at any time:
a. in relation to an existing Client, it doubts the veracity or adequacy of documents, data, or information obtained for the purposes of CDD;
b. it suspects money laundering; or
c. there is a change in the risk rating applied by the Company to an existing Client, or it is otherwise warranted by a change in circumstances of the Client.

For the purposes of (a), examples of situations which might lead the Company to have doubts about the veracity or adequacy of documents, data, or information previously obtained could include:

- where there is a suspicion of money laundering in relation to that Client;

- where there is a material change in the way that the Client's account is operated, which is not consistent with the Client's business profile; or
- where it appears to the Company that a person other than the Client is the real Client.

13.4. Establishing a Business Relationship Before CDD is Complete

The Company may establish a business relationship with a Client before completing the verification if the following conditions are met:
a. deferral of the verification of the Client or beneficial owner is necessary in order not to interrupt the normal conduct of a business relationship;
b. there is little risk of money laundering occurring and any such risks identified can be effectively managed by the Company;
c. in relation to a bank account opening, there are adequate safeguards in place to ensure that the account is not closed and transactions are not carried out by or on behalf of the account holder (including any payment from the account to the account holder) before verification has been completed; and
d. subject to (c), the relevant verification is completed as soon as reasonably practicable and, in any event, no later than 30 days after the establishment of a business relationship.

Such situations might include, for example:

- accepting subscription monies during a short offer period;
- executing a time-critical transaction, which if not executed immediately, would or may cause a Client to incur a financial loss due to price movement or loss of opportunity; or
- when a Client seeks immediate insurance cover.

13.5. Inability to Complete CDD

Where the Company is not reasonably able to comply with the 30-day requirement in 13.4 d), it will, prior to the end of the 30-day period:
a. document the reason for its non-compliance;
b. complete the verification in 13.4 as soon as possible; and
c. record the non-compliance event.

13.6. Identification and Verification of Clients

The MLRO must, in the first place, be obliged to identify, beyond a reasonable doubt, the identity of persons enabled to conduct transactions on our exchange. For this reason, the Company collects ID scans, the authenticity of which is verified using specialized software from professional external providers. The Company requires the submission of a “selfie” or Client video recording with the ID document to prevent the possibility of someone else using the Client’s documents. Verification of the Client’s likeness to the ID photo is carried out using specialized software from professional external providers or, in case of doubt, manually by the Company’s Client Support team.

If any doubts arise, the Client Support team will contact the Client to clarify concerns and resolve the issue. If the Company cannot determine, beyond a reasonable doubt, that the provided documents belong to the Client and are authentic, no transactions will be permitted.

a. In undertaking CDD required by 13.1, the MLRO must:

- verify the identity of the Client and any beneficial owner based on original or properly certified documents, data, or information issued by or obtained from a reliable and independent source;
- understand the Client's sources of funds;
- understand the Client's sources of wealth; and
- undertake ongoing due diligence of the Client's business relationship under section 14.

b. The Company will, in complying with a) i) above and adopting the Risk-Based Approach (RBA), obtain, verify, and record for every Client who is a natural person the following identification information:
i. full name (including any alias);
ii. date of birth;
iii. nationality;
iv. legal domicile; and
v. current residential address (not a P.O. box).

Items i) to iii) must be obtained from a valid passport, or if unavailable, from an official identification document containing a photograph. "Domicile" refers to the place a person regards as their permanent home, with which they have the closest ties or which is their place of origin.

c. For all legal entities (companies), the procedure is more stringent and depends on the company's structure, country, etc. The Company must establish who owns the company, who represents it, where it is based, and what its business is. Since governmental documentation standards differ between countries, verification is done manually and is more time-consuming. The following information is required for all Clients that are legal persons:
i. full business name and any trading name;
ii. registered or business address;
iii. date of incorporation or registration;
iv. place of incorporation or registration;
v. copy of the certificate of incorporation or registration;
vi. valid commercial or professional license;
vii. identity of directors, partners, trustees, or equivalent executive authority; and
viii. for a trust — certified copy of the trust deed, documentation on the nature and purpose of the trust, and evidence of the appointment of current trustees.

d. If original documents cannot be obtained, the Company will obtain certified copies signed by a person of good standing (e.g., registered lawyer or notary, chartered accountant, bank manager, police officer, embassy/consulate employee, or similar). Downloading publicly available information from an official source (e.g., regulator or government website) is also acceptable. Information from reputable companies or reporting agencies, banking references, or reliable public/commercial databases may be used for lower-risk Clients. For higher-risk situations, identification must be independently verified using both public and non-public sources.

e. Understanding the Client's source of funds means identifying where the funds for a specific service or transaction originate (e.g., a specific bank or trading account) and whether this aligns with their source of wealth. This is usually obtained during onboarding. The CEO and Senior Management will keep evidence, such as account opening forms, Client questionnaires (Annex 1 for individuals, Annex 2 for legal entities), or memos of calls with financial institutions.

f. Understanding the Client's source of wealth for a natural person may involve application form questions, Client questionnaires, discussions with relationship managers, or information from reliable public sources (e.g., published accounts or reputable media). While a complete

breakdown of global wealth is not required, sufficient detail must be gathered to confirm legitimacy and support ongoing due diligence. The Company will clearly document this understanding.

g. Understanding the Client's sources of funds and wealth is essential for ongoing due diligence under a) iv). Initial funding from unknown or unexpected sources may pose risks. This knowledge also supports the Company's transaction monitoring program.

h. For life insurance or similar policies, the Company will:
i. verify the identity of any named beneficiaries; and
ii. verify the identity of persons in any class of beneficiary, or, where unidentified, ensure sufficient information is obtained to verify their identity at payout.

Life policy equivalents include life-related protection, pensions, or investment products that pay out upon a specific event or redemption.

13.7. Identification and Verification of Beneficial Owners

a. In determining whether an individual meets the definition of a beneficial owner or controller, the Company will consider all circumstances of the case.

b. When identifying beneficial owners, the Company applies a substantive approach to CDD for legal persons, focusing on the money laundering risks of the Client and the services provided, rather than solely on the legal form of an arrangement or fixed percentage thresholds for identifying beneficial owners.

c. The Company will take all reasonable steps to establish and understand a corporate Client's legal ownership and control structure and to identify the beneficial owner. Using the Risk-Based Approach (RBA), the Company will act on reasonable grounds in a manner proportionate to the risks identified.

d. In some situations, no percentage threshold will be applied when identifying beneficial owners, particularly where it is necessary to identify all underlying beneficial owners to ensure there are no undisclosed associations or connections. This may be relevant when there are a small number of investors in an account or fund, each holding a significant financial interest, and the Client-specific risks are higher. For lower-risk Clients and services, a percentage threshold may be applied to determine "control" for the purposes of identifying a beneficial owner.

e. For a widely-held retail investment fund, where investors contribute through pensions and there are no individuals with material control or ownership, the fund manager is not expected to identify underlying investors. However, for a closely-held fund with a small number of large shareholders or investors, the Company will identify and verify each beneficial owner based on its risk-based assessment. For a corporate health policy with defined benefits, beneficial owners are not required to be identified.

f. When identifying and verifying actual and potential beneficial owners of a trust, the Company will include the trustee, settlor, protector, enforcer, beneficiaries, any person with authority to appoint or remove a trustee, and any person entitled to receive a distribution, whether named as a beneficiary or not.

13.8. Client is a Politically Exposed Person (PEP)

a. Where a Client, or a beneficial owner of the Client, is identified as a Politically Exposed Person (PEP), the Company will ensure that, in addition to the measures outlined in 13.6 a), it will:
i. increase the degree and nature of monitoring of the business relationship to determine whether the Client's transactions or activities appear unusual or suspicious; and
ii. obtain the approval of senior management before commencing a business relationship with the Client.

b. Individuals who hold, or have held, a high political profile or public office may pose a higher risk of money laundering due to their potential exposure to corruption. This risk extends to their immediate family members and close associates. While PEP status does not itself incriminate an individual or entity, it places the Client in a higher risk category.

c. Foreign PEPs typically present a higher money laundering risk, as they may be more likely to place funds offshore to avoid recognition as a PEP and to make it harder for law enforcement authorities in their home jurisdiction to confiscate or freeze illicit assets.

d. The risk of corruption-related money laundering increases when dealing with PEPs. Corruption may involve serious criminal offences and is an area of heightened global scrutiny. Relationships with family members or close associates of PEPs carry risks similar to those of the PEPs themselves.

e. Former PEPs may continue to pose a higher money laundering risk if they retain political influence—either directly or indirectly—or otherwise present a risk of involvement in corruption.

14. ON-GOING CLIENT DUE DILIGENCE

a. When undertaking on-going CDD under 13.6 a), the Company must, using the risk-based approach:
i. monitor transactions undertaken during the course of its Client relationship to ensure that the transactions are consistent with the Company's knowledge of the Client, its business, and its risk rating;
ii. pay particular attention to any complex or unusually large transactions or unusual patterns of transactions that have no apparent or visible economic or legitimate purpose;
iii. enquire into the background and purpose of the transactions in ii);
iv. periodically review the adequacy of the CDD information it holds on Clients and beneficial owners to ensure that the information is kept up to date, particularly for Clients with a high-risk rating; and
v. monthly review each Client to ensure that the risk rating assigned to a Client remains appropriate for the Client in light of the money laundering risks.

b. In complying with a) the Company will undertake a periodic review to ensure that non-static Client identity documentation is accurate and up-to-date. Examples of non-static identity documentation include passport number and residential/business address and, for a legal person, its share register or list of partners.

c. The Company will undertake a review under a) iv) particularly when:
i. the Company changes its CDD documentation requirements;
ii. an unusual transaction with the Client is expected to take place;
iii. there is a material change in the business relationship with the Client; or
iv. there is a material change in the nature or ownership of the Client.

d. The degree of the on-going due diligence to be undertaken will depend on the Client risk assessment carried out.

15. FAILURE TO CONDUCT OR COMPLETE CLIENT DUE DILIGENCE

15.1. Prohibitions
a. Where, in relation to any Client, the Company is unable to conduct or complete the requisite CDD in accordance with 13.6 a), it must, to the extent relevant:
i. not carry out a transaction with or for the Client through a bank account or in cash;
ii. not open an account or otherwise provide a service;
iii. not otherwise establish a business relationship or carry out a transaction;
iv. terminate or suspend any existing business relationship with the Client;
v. return any monies or assets received from the Client; and
vi. consider whether the inability to conduct or complete CDD necessitates the making of a Suspicious Activity Report.

This applies to both existing and prospective Clients. For new Clients, it may be appropriate for the Company to terminate the business relationship before a service is provided. However, for existing Clients, while termination of the business relationship should not be ruled out, suspension may be more appropriate depending on the circumstances. Whichever route is taken, the Company should be careful not to "tip off" the Client.

b. The Company adopts the RBA for CDD of existing Clients. For example, if the Company considers that any of its existing Clients have not been subject to CDD at an equivalent standard to that required by this Policy, it will adopt the RBA and take remedial action in a manner proportionate to the risks and within a reasonable period of time whilst complying with 15.1 a).

15.2. Exceptions
The Company is not obliged to comply with 15.1 a) (i) to (v) if to do so would amount to "tipping off" the Client, in breach of the Law of the Republic of Kazakhstan “On Counteraction Legalization (Laundering) of Proceeds Obtained through Criminal Means and Financing of Terrorism” (hereinafter — “AML Law”); or if the Financial Monitoring Agency of the Ministry of Finance (the "FMA") directs the Company to act otherwise.

16. ENHANCED DUE DILIGENCE

16.1. Procedure where Enhanced Due Diligence is required
Below is the procedure whereby risk assessment of Client due diligence instigates the Company to conduct EDD:

a. The Company shall annually prepare a compliance status report, whereby the net traded/investment value (value bought less value sold) is equal to or greater than the following thresholds:
i. For Corporate Entities — minimum threshold is $10,000,000;
ii. For Individual Investors — minimum threshold is $1,000,000.

b. If any Client is in non-compliance with the above-specified threshold limits, then EDD will be conducted for that Client, and a Suspicious Transaction Report will be initiated. The same will be kept on record, and a trail will be maintained at all material times.

c. The Company will also maintain a summary report of the investors who fall under the above category. The summary report covers the following details:
i. At Client Level: name, address, contact number, email address, profession;
ii. At Risk Category Level: initial risk level and any revisions made;
iii. Compliance Status;
iv. Action initiated, if any required.

16.3. Conducting Enhanced Due Diligence

a. EDD measures are mandatory only to the extent applicable to the relevant Client or the circumstances of the business relationship, and to the extent that the risks reasonably require them. Therefore, the CEO will determine the extent of additional measures on a case-by-case basis.

b. For high-risk Clients, the Company will apply a greater degree of diligence throughout the Client relationship, aiming to understand the nature of the Client's business and assess whether it is consistent and reasonable.

c. The Company must be satisfied that a Client's use of complex legal structures and/or trust and private investment vehicles has a genuine and legitimate purpose.

d. For EDD, where there is a beneficial owner, verification of the Client's source of funds and wealth may require investigating the beneficial owner's source of funds and wealth, as the source would normally be the beneficial owner rather than the Client.

e. Verification of sources of funds might include obtaining independent corroborating evidence, such as proof of dividend payments connected to a shareholding, bank statements, salary/bonus certificates, loan documentation, and proof of a transaction which generated the payment into the account.

f. A Client should be able to demonstrate and document how the relevant funds are connected to a particular event that generated the payment into the account or the source of funds for a transaction.

g. Verification of sources of wealth might include obtaining independent corroborating evidence such as share certificates, publicly-available registers of ownership, bank or brokerage account statements, probate documents, audited accounts and financial statements, reputable news items, and other similar evidence. For example:
i. for a legal person — obtaining its financial or annual reports published on its website, or news articles and press releases reflecting its financial situation or business profitability;
ii. for a natural person — obtaining documents that corroborate answers to questions on sources of wealth in an application form or Client questionnaire. For example, if wealth is attributed to inheritance, the Client may be asked to provide a copy of the will or grant of probate. Alternatively, sufficient bank or salary statements covering several years may be requested to establish a picture of the Client's sources of wealth.

h. The Company may commission a third-party report to obtain further information on a Client or transaction, or to investigate a Client or beneficial owner in very high-risk cases. This may be particularly useful when there is little or no publicly-available information on a person or legal arrangement, or when the Company has difficulty obtaining and verifying information.

i. Circumstances in which it may be applicable to require the first payment made by a Client to open an account with the Company to be carried out through a bank account in the Client's name with a financial institution specified in 16.2(f) include:
i. where, after applying other EDD measures, the Company is not satisfied with the results of due diligence; or
ii. as an alternative measure, where one of the measures in section 14 cannot be carried out.

17. CLIENT IDENTIFICATION AND CLASSIFICATIONS

The Company's anti-money laundering (AML) policies and procedures are designed to ensure that, before accepting funds from Clients, all reasonable and practical measures are taken to verify the Clients' identities.

The Company will also verify that any third party it relies upon for Client identification—such as a bank, other financial intermediary, or any other entity—adheres to equivalent identification standards.

Funds from a new or existing Client will only be accepted when:
a. The Company has confirmed the Client's identity and verified that the Client is acting as a principal, not on behalf of any third party, unless a specific disclosure to that effect has been made; or
b. If the Client is acting on behalf of others, the Company has confirmed the identities of the underlying third parties.

The Client Identification Procedures are applied in consideration of the specific characteristics of each Client. The MLRO may also apply Enhanced measures for reasons other than those set out under "High-Risk Clients."

As a reference tool, the Company uses an Individual Client KYC Checklist. Employees are encouraged to submit any proposed revisions to the MLRO. The MLRO will retain copies of all reviewed documents and completed checklists in accordance with the Company's Client Records Retention policies.

18. CLIENT CLASSIFICATION CRITERIA

a. **Retail Client**
b. **Professional Client**
c. **Market Counterparty**

Professional Clients may be classified as **"Deemed"** or **"Assessed"** Professional Clients in accordance with the criteria set out in the AIFC Collective Investment Scheme and Conduct of Business Rules.

19. HIGH-RISK CLIENTS

The MLRO will maintain and regularly update a list of Client types considered **high risk**, requiring enhanced due diligence beyond standard Client Identification Procedures.

Examples of high-risk Clients include:

a. **A Senior Manager**, any member of a **Senior Foreign Political Figure's Immediate Family**, or any **Close Associate** of a Senior Foreign Political Figure.

b. **Any Client** residing in, or incorporated/chartered under the laws of, a **Non-Cooperative Jurisdiction**.
Note: A Non-Cooperative Jurisdiction is any foreign country designated by an intergovernmental body, such as the **Financial Action Task Force on Money Laundering (FATF)**, as non-cooperative with international anti-money laundering standards.

c. **Any Client** suspected of having funds originating from, or routed through, an account at an **offshore bank** or a bank incorporated under the laws of a **Non-Cooperative Jurisdiction**.

d. **Any Client** for whom the MLRO has reason to believe that the source of funds may be **illegitimate** or potentially linked to **terrorist activities**.

20. ENHANCED CLIENT IDENTIFICATION PROCEDURES FOR 'HIGH-RISK' NATURAL PERSONS

Enhanced Client Identification Procedures for Clients classified as **high risk** and who are natural persons include, but are not limited to, the following:

a. Identifying how the Client's wealth was generated and determining the source of the specific funds intended for the investment.

b. Reviewing publicly available information, including media reports, to verify whether the Client has been the subject of any criminal or civil enforcement actions.

c. Assessing the Client's business reputation by reviewing financial or professional references, publicly available media reports, or other credible sources.

d. Considering the origin of the Client's wealth, including the economic activities that generated it, and verifying the source of the funds intended for the investment.

e. Reviewing publicly available information to determine whether the Client has been involved in any criminal or civil enforcement actions related to violations of anti-money laundering laws or regulations, or any investigation, indictment, conviction, or enforcement action related to the financing of terrorism.

f. Conducting a face-to-face meeting with the Client to discuss and confirm the account opening documentation.

All enhanced due diligence measures undertaken for high-risk Clients must be **fully documented in writing**, and any questions or concerns regarding such Clients must be referred to the **MLRO**.

21. ENHANCED CLIENT IDENTIFICATION PROCEDURES FOR 'HIGH-RISK' CORPORATIONS, PARTNERSHIPS, TRUSTS AND OTHER LEGAL ENTITIES

Enhanced Client identification procedures for Clients classified as **high risk** and operating as corporations, partnerships, trusts, or other legal entities include, but are not limited to, the following:

a. Assessing the Client's business reputation by reviewing financial or professional references, publicly available media reports, or other credible sources.

b. Reviewing any recent changes in the ownership structure or senior management of the Client.

c. Conducting an on-site visit to the Client's place of business and holding a face-to-face meeting to discuss and confirm the account application, the intended purpose of the account, and the source of the Client's assets.

d. Reviewing publicly available information to determine whether the Client has been involved in any criminal or civil enforcement actions related to violations of anti-money laundering laws or regulations, or any criminal investigation, indictment, conviction, or enforcement action related to the financing of terrorism.

22. GENERAL REPORTING PROCEDURES

a. A designated individual within the organization is appointed to receive disclosures under this regulation (the "Compliance Officer" or "Money-Laundering Reporting Officer" – MLRO).

b. Any employee who, during the course of their work, obtains information that causes them to suspect that a person is engaged in money laundering must report it to the MLRO and/or Compliance Officer.

c. Upon receiving such a disclosure, the MLRO must review the information in the context of any other relevant data available to the Company and determine whether it creates a suspicion of money laundering.

d. If the MLRO, in consultation with Senior Management, determines that the suspicion is valid, the matter must be reported to the Regulatory Authority after obtaining independent legal advice.

e. In most cases, before deciding to submit a report, the MLRO will have access to relevant business information, which may include:

- Financial circumstances of the customer or beneficial owner, or any person on whose behalf the customer acts;
- Characteristics of the transactions, including the jurisdictions in which they occur;
- Underlying CDD documentation and copies of source materials related to the customer.

f. Additionally, the MLRO may:

- Assess the completeness of the customer's identity information and review any available details about their personal circumstances;
- Examine patterns and volumes of transactions, the length of the business relationship, and existing identification records.

Suspicious Activity Reports (SARs) or Suspicious Transaction Reports (STRs) must be submitted to the Financial Monitoring Agency (FMA) in accordance with the procedure outlined in Order No. 13 of the FMA Chairman dated 24 February 2022.

When preparing a SAR or STR, if the Company knows or suspects that the funds involved belong to a third party rather than the customer, this fact and the Company's intended course of action should be included in the report.

SARs and STRs must be submitted electronically via the FMA's WEB SFM Portal (https://websfm.kz) within **24 hours** of the transaction or activity being deemed suspicious. The AFSA must also be notified in writing of the suspicious transaction or activity as soon as possible.

23. OTHER OFFENCES – FAILURE TO REPORT OFFENCES

a. It is an offence for any individual working in the regulated sector to fail to promptly inform either the Regulatory Authority or the Company's MLRO if they have knowledge, suspicion, or reasonable grounds to know or suspect that another person is engaged in money laundering.

b. It is an offence for the MLRO, in the regulated sector, to fail to make the required report to the Regulatory Authority as soon as practicable if, after receiving an internal report, they know or suspect that a person is engaged in money laundering

24. CLIENT RECORDS RETENTION

The Company will retain copies of all documents related to its Client Identification Procedures for a period at least equal to that required by applicable laws or regulations.

These records include:

- Copies of documents reviewed during Client Identification or Enhanced Due Diligence procedures;
- Client identification checklists or similar due diligence documentation;
- Any other documents required under applicable anti-money laundering legislation.

All documents will be kept for the entire duration of the Client's relationship with the Company and for a minimum of six years after the relationship has ended.

25. REVIEW OF EXISTING CLIENT BASE AND DETECTION OF SUSPICIOUS ACTS

The MLRO will coordinate a periodic review of the Company's existing Client list to ensure the adequacy of due diligence performed on all Clients.

The Company's policies, procedures, and controls will also include mechanisms to detect potentially suspicious activity. If detected, such activity will undergo further review to determine whether it is indeed suspicious.

Examples of activities that, while not inherently suspicious, may require further investigation include:
a. A Client shows unusual concern about the Company's compliance processes, especially regarding identity, business type, and assets, or is unwilling to provide required business information, or presents unusual or suspect identification or documents;
b. The Client seeks to make investments inconsistent with their stated investment strategy;
c. The Client, or a publicly associated person, is mentioned in news reports involving possible criminal, civil, or regulatory violations;
d. The Client appears to act for another entity but refuses, without a valid commercial reason, to disclose information about it;
e. The Client struggles to describe their business or demonstrates limited knowledge of the industry they claim to be in;
f. The Client makes unusually frequent investments, redemptions, withdrawals, or transfers without clear justification;
g. The Client conducts unusual or frequent wire transfers, especially to unknown or unrelated bank accounts;
h. The Client sends funds to jurisdictions other than their home jurisdiction;
i. The Client requests transactions in cash or cash equivalents.

Any employee who detects or suspects suspicious activity must immediately report it to their supervisor and to the MLRO and Compliance Officer.

Important: Employees are prohibited by law from discussing suspicious activity or the fact that it has been reported with the Client involved.

The MLRO and Compliance Officer, in consultation with higher management, will decide whether to report the matter to relevant law enforcement authorities (e.g., the Financial Monitoring Unit) within **7 working days** of identifying the suspicious activity, as required by law.

26. REGULAR REVIEW/AUDIT OF THE POLICY

The Company will conduct regular reviews of this Policy to ensure it is functioning as intended. These reviews may be carried out by either internal or external resources and must be supported by a formal assessment or written report.

If regulatory requirements regarding the reporting of suspicious activities are amended, the Company will promptly update this Policy to ensure full compliance.

To maintain ongoing compliance and the effectiveness of AML measures, evaluations of the Policy will be conducted **at least annually** or whenever requested by Senior Management.

27. RECORD KEEPING

This section outlines the Company's record-keeping procedures to ensure compliance with anti-money laundering (AML) and counter-terrorism financing (CTF) obligations.

Maintaining complete and accurate records enables the Company to:
a. Provide an audit trail for all advice given and actions undertaken on behalf of a Client;
b. Supply adequate information to law enforcement agencies to support investigations;
c. Monitor Client activity against expected behavior;

d. Identify and report suspicious activity;
e. Demonstrate compliance with all statutory and regulatory obligations.

The following records must be retained:
a. Client information, including proof of identity;
b. Details of all transactions conducted by each Client;
c. Internal and external suspicion reports;
d. MLRO annual report and any other compliance-related reports;
e. Information received but not acted upon;
f. Transaction monitoring records;
g. Records of training provided and evaluations of training effectiveness.

All such records must be readily available to competent authorities in the context of any relevant criminal investigations or prosecutions.

28. IDENTIFICATION RECORDS

Client identification records must be retained for a minimum of six (6) years from the date the Client relationship ends. This is defined as the later of:

- the date of the last transaction with the Client, or
- the date of closure of the Client's account.

29. TRANSACTION RECORDS

Transaction records must be retained for a minimum of six (6) years from the date of the transaction.
They must be maintained in a manner that ensures a clear and complete audit trail, allowing for the full reconstruction of all transactions carried out through the Company.

30. THIRD PARTY RECORD KEEPING

When the Company engages an agent or third party to perform activities on its behalf, it remains the Company's responsibility to ensure that such agents comply with the Company's record keeping requirements.
This includes the obligation to retain relevant records for a minimum of six (6) years.
The same principle applies to third-party service providers, such as introducers and/or administrators.

31. REFUSED BUSINESS RECORDS

If a prospective business relationship is declined due to failure to meet Client identification, verification, or CDD/KYC standards, the Company must retain a record of such refusal for a minimum period of six (6) years.

32. WIRE TRANSFER AND ELECTRONIC PAYMENT RECORDS

The Company must retain all electronic payment messages for a minimum of six (6) years. These records must contain sufficient information to identify all parties involved in the transaction, including both the originator (payer) and the beneficiary. The required information includes full names, addresses, and account numbers of each party.

If such details cannot be included in the electronic payment message itself, complete records containing this information must be maintained separately in accordance with the Company's record-keeping requirements.

33. SANCTIONS SCREENING

The United Nations Sanctions regulations implement measures decided by the UN Security Council. It is a criminal offence to provide or solicit financial or related services for any Client who is a person or entity designated in UN sanctions lists.

33.1. Sources of sanctions and terrorist financing lists

The Company refers to the lists maintained by:

- The UN Security Council and its Sanctions Committees;
- The Agency of Financial Monitoring of the Republic of Kazakhstan (AFM).

Individuals and entities on these lists (designated persons or entities) are subject to financial restrictions to prevent access to and use of funds for terrorism and related purposes.

Relevant resources:

- UN Sanctions Consolidated List: https://www.un.org/securitycouncil/content/un-sc-consolidated-list
- AFM Anti-Money Laundering section: https://afmrk.gov.kz/ru/

33.2. Frequency of name checks

- The Company conducts name checks of each Client, and, based on a risk-based approach, may also screen beneficial owners, against the latest UN, AFSA, FATF, and AFM sanctions lists before establishing any business relationship.
- Ongoing sanctions screening is performed regularly for the entire Client base.
- UN sanctions list updates are reviewed on a monthly basis, with immediate action for high ML/TF risk cases.

33.3. Notification obligation

If the Company suspects that any property is owned or controlled by a designated person or entity, or is otherwise terrorist property, it must immediately cease dealing with such property and report the matter to the AFM (as per the "Reporting of Suspicious Transactions" section).

33.4. Reporting of suspicious transactions

- All Company principals and staff are required to report any knowledge or suspicion of money laundering, bribery, tax evasion, or terrorist financing, whether it relates to Clients or third parties.
- Failure to report such suspicion constitutes a criminal offence under both domestic law and the United Nations (Anti-Terrorism Measures) Ordinance.

- Before dismissing a potentially suspicious activity, the Company must consider whether all available information, taken together, provides reasonable grounds for knowledge or suspicion.

34. INTERNAL AND EXTERNAL SUSPICIOUS ACTIVITY REPORTS

The Company must retain records of all reports concerning suspicions of money laundering, regardless of whether the MLRO ultimately submitted a report to the relevant criminal authority. These records include:

a. Documentation of actions taken under both internal and external reporting requirements;
b. Cases where the MLRO reviewed an internal report and decided not to escalate it to the relevant criminal authority;
c. A complete record of all information considered during the review process;
d. Copies of Suspicious Activity Reports (SARs) submitted to the relevant criminal authority.

Retention period:

- All such records must be kept for **6 years** from the date the report is made.
- If the Company is aware that the relevant criminal authority or another law enforcement agency is conducting an investigation into a Client, all related records must be retained until confirmation is received that the case has been closed.
- If, within 6 years of the disclosure, no notification of an ongoing investigation is received, the Company may destroy the records.

Important: It is a criminal offence to destroy any documentation that may be relevant to a money laundering investigation.

35. EXAMPLES OF SUSPICIOUS ACTIVITY

Below is a non-exhaustive list of activities that may indicate potential money laundering or terrorism financing. These examples do not automatically constitute suspicious activity but will often warrant further enquiry. It remains the responsibility of the person identifying the activity to determine whether a report of suspicion should be made.

Possible suspicious circumstances include:

a. Transactions with no clear purpose, lacking economic rationale, or appearing designed/structured to avoid detection;
b. Transactions requested without reasonable explanation that fall outside the normal range of services provided or outside the Company's typical experience with that customer;
c. Transactions whose size or pattern, without reasonable explanation, deviates significantly from previously established activity or appear deliberately structured to avoid detection;
d. A customer's refusal to provide requested information without a valid explanation;
e. A new customer using the relationship for a single transaction or only for a very short duration;
f. Extensive use of offshore accounts, companies, or structures where such arrangements are not supported by the customer's legitimate economic needs;

g. Unnecessary routing of funds through third-party accounts;
h. Submission of documents that appear fraudulent, unofficial, or otherwise suspicious;
i. Unusual transactions with no apparent profitable motive;
j. Any other transactions or circumstances as described in Article 4 of the AML/CFT Law.

36. ON-GOING RELATIONSHIPS WITH SUSPICIOUS CLIENTS

The Company will not maintain relationships with Clients where it believes its services may be used for money laundering.

If a Client has been involved in suspicious activity, the MLRO and Senior Management will jointly decide whether to continue or terminate the relationship. If the decision is to maintain the relationship, enhanced monitoring measures will be applied to the Client's account.

Where a Client has been the subject of a Suspicious Activity Report (SAR) to the relevant criminal authority, no action to terminate the relationship may be taken without informing the MLRO. In such cases, the MLRO must consult with the relevant criminal authority and obtain permission before closing the Client's account.

37. OBLIGATION TO REPORT AND FINDINGS

All employees, whether AFSA-approved or not, must submit a formal report to the MLRO if, during their work, they know, suspect, or have reasonable grounds to know or suspect money laundering or terrorism financing. This obligation applies to any person, regardless of whether they are a Client of the Company.

If an employee identifies that a Client's name appears on a sanctions list, they must first verify the accuracy of this information. If confirmed, the employee must:
a. Suspend all bank transactions involving the Client;
b. Suspend any existing professional relationship with the Client;
c. Refuse to provide any services;
d. Submit a report to the FMA within one business day;
e. Immediately notify AFSA.

All reports to the FMA must be submitted in the prescribed format and through the official channels required by AML Law and related regulations.

FREEZING OF FUNDS AND/OR BLOCKING FINANCIAL TRANSACTIONS OF PERSONS

a. The Company will refuse to conduct operations with money and/or other assets (freeze and/or block) and/or terminate business relationships with a Client if there are suspicions that such relationships are being used for money laundering or terrorism financing.

b. Within twenty-four hours from the publication on the FMA website of an updated list of individuals involved in terrorist activities, organizations or individuals associated with the financing of terrorism and extremism, or the financing of the proliferation of weapons of mass destruction, the Company must immediately take measures to freeze any financial transactions involving money and/or other assets of such persons.

c. To prevent money laundering and terrorism financing, the Company must immediately report any suspicious transaction to the FMA and AFSA before its execution. No operations with money and/or other assets shall be conducted until the FMA or AFSA issues a decision to suspend or confirms there is no need to suspend the transaction.

d. If the Company does not receive a decision from the authorized body within twenty-four hours from the moment of reporting the suspicious transaction, the operation shall be carried out unless other grounds under the laws of the Republic of Kazakhstan require its suspension.

DISCLOSURE

The Company must disclose to AFSA any information if it has reasonable grounds to believe that:

a. There is a breach or likely breach of a provision of AFSA legislation;
b. There is a failure or likely failure to comply with any obligations to which the Company is subject under such legislation; or
c. Any other matters as may be prescribed by AFSA Rules.

38. SUSPICIOUS ACTIVITY REPORTING

Obligation to Report
Every member of staff, whether AFSA-approved or not, is required to make a formal report to the MLRO if, in the course of their employment, they know, suspect, or have reasonable grounds for knowing or suspecting money laundering or terrorism financing.

This obligation applies in respect of any person, whether the Company's Client or not, and exists even if:

- A potential Client does not conduct any business through the Company; or
- The Company declines the business.

Reports must be submitted using the **Escalation Form** available in the AIFC Policies section on the website.

39. FAILURE TO MAKE A REPORT

In addition to any legal or regulatory sanctions, the Company will take disciplinary action against any member of staff who fails to report a suspicion without a reasonable excuse.

40. OBJECTIVE TEST

The Company may be found guilty of failing to report even if no actual suspicion existed, but where it ought to have been suspected. The key measure is whether an honest and reasonable person, working in the financial services industry, would have formed a suspicion based on the facts available at the time. To meet this test, the Company must have sufficient knowledge of the Client, their business, and the rationale for their instruction, activity, or transaction. Failure to make adequate enquiries or to assess relevant facts will not protect against the application of the objective test of reasonable suspicion.

41. REPORTING

The Compliance Officer (CO) must produce a Compliance Report at least annually. The CO is also required to report regularly to the Management Body and Committee on compliance matters. Reports should reference the compliance risk assessment conducted during the reporting period, including any changes to the compliance risk profile based on relevant performance indicators, summarize identified breaches and/or deficiencies, recommend corrective measures, and provide updates on corrective measures already implemented. The reporting format should align with the Company's compliance risk profile and scope of activities.

For the purposes of this manual, breaches and deficiencies are classified as such if they meet any of the following criteria:
a. Criminal or fraudulent events (all such events must be reported, regardless of the loss amount);
b. Material breaches of applicable laws, regulations, or standards;
c. Incidents causing material reputational damage;
d. Regulatory sanctions.

Reports must be submitted as soon as reasonably practicable.

42. DISCHARGE OF INDIVIDUAL RESPONSIBILITY

By submitting a report of suspicions to the MLRO, an individual discharges their personal responsibility and is thereby protected from criminal prosecution for the offence of failure to disclose. After making such a report, the individual must ensure they receive a formal written acknowledgment from the MLRO and retain it for their own records.

43. CONSULTATION WITH A COLLEAGUE OR LINE MANAGER

It is permissible to discuss suspicions with a Line Manager. However, if after such consultation suspicions remain, it is the individual's responsibility to ensure a report is submitted to the MLRO.

A Line Manager may provide comments on the proposed report but has no authority to block or attempt to block any report to the MLRO. If there is any attempt to prevent a report from being made, the matter must be raised directly with the MLRO.

If a colleague, including a Line Manager, is consulted, they will also have knowledge of the matter and must consider whether they should make a report to the MLRO. To avoid duplicate reporting, the consulted colleague should only submit a report if reasonably satisfied that the original individual will not do so.

To minimise the risk of inadvertently tipping off a Client, discussions should be limited to as few people as possible.

44. CONTINUOUS OBLIGATION TO REPORT

Submitting a report does not remove the obligation to inform the MLRO of any further suspicions that may arise regarding the same or a different Client. If new suspicions occur, separate and additional reports must be submitted to the MLRO.

45. TRANSACTION MONITORING

A combination of AML and CTF training and commercial awareness should enable staff to detect, recognise, and report suspicious activities.

The rationale behind a Client's transaction or activity must be understood. When identifying unusual or potentially suspicious activity, staff should apply their knowledge of the Client and determine what would be considered normal under the given circumstances.

In monitoring Client accounts, staff should take into account the following considerations, alongside other factors outlined in this Policy:
a. Whether the financial performance of an enterprise aligns with the nature and scale of its business, and whether the services sought appear legitimate in that context.
b. The unusual nature of a transaction, such as abnormal size or frequency for that Client or category of Client.
c. The nature of a series of transactions, for example, multiple cash payments.
d. The geographic origin or destination of a payment, particularly if involving a high-risk jurisdiction.
e. The parties involved, such as payments to or from individuals or entities listed on a Sanctions List.

While staff training is essential, it is not a complete substitute for transaction monitoring. The Financial Crime Surveillance and Intelligence Team will conduct formal reviews of transactions on a risk-based approach to ensure no money laundering has occurred or been facilitated.

All evidence of transaction monitoring carried out by the Company must be retained for at least six years from the date of review.

46. UP-TO-DATE CLIENT INFORMATION

Client information must be kept current through regular reviews, with frequency based on the Client's risk category:
a. Low-risk Clients: re-assessment every three years.
b. High-risk Clients: re-assessment annually.

The purpose of these reviews is to detect significant changes in the Client's corporate structure, management, or activities. Unless otherwise determined by the MLRO, it is not always necessary to re-obtain all account opening information or re-verify all identification documents.

An overall review of the Client's activity during the period should also be performed to assess whether any changes could be considered unusual given the existing knowledge of the Client.

If any staff member becomes aware of changes in a Client's circumstances — such as alterations in ownership structure or entry into a new business area — this must be recorded in the Client's file immediately. If such changes may affect the Client's risk assessment, the MLRO must be informed to decide whether a reassessment is necessary.

Identification, assessment, and assignment of the final risk level for working with the Client shall be carried out in accordance with Annex 3 to this Policy.

47. AML & CTF TRAINING RECORDS

Records relating to AML and CTF training must be retained for a minimum of six years from the date the training materials were issued. Such records shall include:

a. Date(s) on which AML training was conducted.
b. All AML and CTF training materials provided to staff, including the nature and content of courses and presentations.
c. Names of attendees who participated in the training.
d. Results of any tests taken, if applicable.

48. MLRO REPORT

The following records must be retained for a minimum of six years:
a. The annual MLRO report to the Board, along with any other reports submitted to senior management.
b. Records documenting the consideration of these reports and any actions taken as a result.

49. MLRO'S DETERMINATION

The MLRO (or, in their absence, a member of the Head of Financial Crime Surveillance and Intelligence Team) will review the suspicion report and all relevant circumstances to decide whether a Suspicious Activity Report ("SAR") should be submitted to the relevant criminal authority. If a SAR is to be filed, it must be done as soon as practicable.

To complete the SAR, the MLRO may require additional information or access to Client records. The MLRO must be granted unrestricted access to all Client documentation. If further information is needed from the Client or an intermediary, it should normally be requested by the staff member responsible for the Client relationship to reduce the risk of alerting the Client or intermediary to a potential disclosure.

The MLRO must maintain a record of all internal enquiries made in connection with the suspicion report and document the rationale for the decision to file, or not to file, a SAR with the relevant criminal authority.

Failure to submit a SAR when there are reasonable grounds for suspicion may constitute assistance in money laundering. If a disclosure to the MLRO results in the MLRO having knowledge or reasonable grounds to suspect money laundering, and the MLRO fails to submit a SAR, this will amount to the offence of failure to disclose.

50. FORMAT AND RETRIEVAL OF RECORDS

The Company may maintain records in any of the following formats:
a. Original documents;
b. Photocopies of original documents;
c. Scanned copies;
d. Computerised or electronic form.

Where possible, records should be retained on the Company's business premises. However, in compliance with statutory requirements and to reduce storage volume, records may be kept offsite or outside Kazakhstan, provided the Company ensures that all required records can be made available without undue delay and remain compliant with Kazakhstan's regulatory requirements.

Regardless of format or storage location, the Company must ensure that all records can be retrieved within 48 hours.

51. COURT ORDERS

Any evidence to be presented in court must be obtained under a court order. The types of orders that may be served on the Company as part of an investigation include:
a. Production order;
b. Disclosure order;
c. Client information order;
d. Account monitoring order;
e. Search and seize warrant;
f. Order for financial information under the Terrorism Act.

All such orders must be forwarded immediately to the MLRO, who will coordinate with the Company's legal advisers as appropriate.

52. SANCTIONS AND PENALTIES

The purpose of the Regulations is to define the arrangements companies must establish to prevent and deter operations related to money laundering and terrorism financing.

The Company's business activities fall within the scope of these Regulations and must therefore maintain appropriate policies and procedures covering:
a. Client due diligence;
b. Politically Exposed Persons;
c. Reporting;
d. Record keeping;
e. Internal control;
f. Risk assessment and management;
g. Compliance management; and
h. Communication.

AFSA may initiate proceedings for offences under the Regulations related to money laundering. Failure to comply constitutes an offence punishable by imprisonment, a fine, or both.

A breach of the Regulations can be established regardless of whether money laundering has actually occurred. The Company may be sanctioned for not having adequate procedures in place.