GUIDELINES FOR ANTI-MONEY LAUNDERING/COUNTERING TERRORIST FINANCING POLICIES AND PROCEDURES

1. Introduction

These Guidelines are not a standalone document; it does not attempt to set out all applicable requirements and should be read in conjunction with existing laws, rules and other AIFC guidance on Anti-Money Laundering and Countering Terrorist Financing (AML/CTF). If there is a discrepancy between this guide and any applicable legal requirements, the provisions of the relevant requirement prevail. If firms have any doubt about a legal or other provision or their responsibilities under the AIFC AML Rules or other relevant legislation or requirements, they should seek appropriate professional advice. The purpose of this document is simply to assist potential AIFC Applicants in drafting their AML/CFT policies and procedures.

Requirement to establish AML policies and procedures

AIFC AML Rule 4.1.1 requires Relevant Persons to take appropriate steps to identify and assess the risks of money laundering and terrorist financing to which its business is exposed; and establish and maintain policies and procedures to mitigate and manage the risks identified.

It is important to note that adequate internal controls are a prerequisite for the effective implementation of policies and processes to mitigate and manage ML/TF risks identified. Internal controls include appropriate governance arrangements where responsibility for AML/CFT is clearly allocated. It also includes controls to monitor the integrity of staff, in accordance with the applicable local legislation, especially in cross-border situations, the national risk assessment; and compliance and controls to test the overall effectiveness of the policies and processes to identify, assess and monitor risk. As a bare minimum, we would expect the AML/CFT Procedures to cover the following topics below:

2. Organisational structure and Governance

Firms' **organisational structures** to combat financial crime and terrorist financing may differ. Some large firms will have a single unit that coordinates efforts and which may report to the head of risk, the head of compliance or directly to the CEO. Other firms may spread responsibilities more widely. There is no one 'right answer' but the firm's structure should promote coordination and information sharing across the business.

- Who has **overall responsibility** for establishing and maintaining effective AML/CFT controls? Are they sufficiently senior?

- Do senior management receive **informative, objective information** that is sufficient to enable them to meet their AML/CFT obligations?
- How regularly do senior management commission **reports** from the **MLRO**? (This should be at least annually.) What do they do with the reports they receive? What **follow-up** is there on any recommendations the MLRO makes?
- How are senior management involved in **approving relationships** with high risk customers, including politically exposed persons (PEPs) and the customers' Ultimate Beneficial Owners (UBO)?
- Who has ultimate responsibility for financial crime matters, particularly: a) anti-money laundering; b) fraud prevention; c) data security; d) countering terrorist financing; e) anti-bribery and corruption and f) financial sanctions?
- Do staff have appropriate seniority and experience, along with clear reporting lines?
- Does the structure promote a coordinated approach and accountability?
- Are the firm's financial crime teams adequately resourced to carry out their functions effectively? What are the annual budgets for dealing with financial crime, and are they proportionate to the risks?
- In smaller firms: do those with financial crime responsibilities have other roles? (It is reasonable for staff to have more than one role, but consider whether they are spread too thinly and whether this may give rise to conflicts of interest.)

3. MLRO

Firms (Relevant Persons include: Authorised Firms, Authorised Market Institutions, DNFBPs and Registered Auditors – (please refer to the AIFC Glossary) must appoint an individual as MLRO. The MLRO is responsible for oversight of the firm's compliance with its anti- money laundering obligations and should act as a focal point for the firm's AML activity. In the absence of the MLRO, there should be someone who can stand in i.e. a Deputy MLRO. Also, a Relevant Person may outsource the role of MLRO and the outsourced service provider's obligations should be clearly documented in a binding agreement.

- Does the MLRO have sufficient resources, experience, access and seniority to carry out their role effectively?
- Do the firm's staff, including its senior management, consult the MLRO on matters relating to money-laundering?
- Does the MLRO escalate relevant matters to senior management and, where appropriate, the board?
- What awareness and oversight does the MLRO have of the highest risk relationships?
- Who is the Deputy MLRO?
- Does the firm intend to appoint an MLRO or will it outsource the MLRO?

4. Business Risk assessment

The assessment of money laundering risk is at the core of the firm's AML effort and is essential to the development of effective AML policies and procedures. Firm's must assess the business risk of each client individually. A firm should identify and assess the financial crime risks to which it is exposed as a result of, for example, (i) the products and services it offers, (ii) the jurisdictions it operates in, (iii) the types of customer it attracts, the complexity and volume of transactions, and (iv) the distribution channels it uses to service its customers. As a minimum, the client business risk assessment must include an assessment of the risks attached to the products and services, jurisdiction, type of customer and distribution channel. Firms can then target their financial crime resources on the areas of greatest risk.

Firms should regularly review both their business-wide and individual risk assessments to ensure they remain current.

- What are the main financial crime risks to the business?
- How does your firm seek to understand the financial crime risks it faces?
- When did the firm last update its risk assessment? How do you identify new or emerging financial crime risks?
- What kind of measures can be taken by the MLRO to mitigate and manage the risks identified?
- Is there evidence that risk is considered and recorded systematically, assessments are updated and sign-off is appropriate?
- Who challenges risk assessments and how? Is this process sufficiently rigorous and well-documented?
- How do procedures on the ground adapt to emerging risks? (For example, how quickly are policy manuals updated and procedures amended?)

5. Customer Due Diligence

Firms must **identify** their customers and, where applicable, their beneficial owners, and then **verify** their identities. Firms must also understand the **purpose** and **intended nature** of the customer's relationship with the firm and collect information about the customer and, where relevant, beneficial owner. This should be sufficient to obtain a complete picture of the risk associated with the business relationship and provide a meaningful basis for subsequent monitoring.
In situations where the money laundering risk associated with the business relationship is increased, firms must carry out additional, enhanced due diligence (EDD).

- Does your firm apply **customer due diligence** procedures in a risk- sensitive way?

- Do your CDD processes provide you with a **comprehensive understanding** of the risk associated with individual business relationships?
- How does the firm **identify** the customer's **beneficial owner**(**s**)? Are you satisfied that your firm takes risk-based and adequate steps to verify the beneficial owner's identity in all cases? Do you understand the rationale for beneficial owners using complex corporate structures?
- Are procedures **sufficiently flexible** to cope with customers who cannot provide more common forms of identification (ID)?
- What kind of CDD measures will be adopted by the firm when establishing non face-to-face business relationships with its customers?

Examples of EDD include:

- obtaining more information about the customer's or beneficial owner's business
- obtaining more robust verification of the beneficial owner's identity based on information from a reliable and independent source
- gaining a better understanding of the customer's or beneficial owner's reputation and/or role in public life and assessing how this affects the level of risk associated with the business relationship
- carrying out searches on a corporate customer's directors or other individuals exercising control to understand whether their business or integrity affects the level of risk associated with the business relationship
- establishing how the customer or beneficial owner acquired their wealth to be satisfied that it is legitimate
- establishing the source of the customer's or beneficial owner's funds to be satisfied that they do not constitute the proceeds from crime.

6. STRs/SARs

Firms must have a **Money Laundering Reporting Officer (MLRO)**. The nominated officer has a legal obligation to **report any knowledge or suspicions** of money laundering to the FIU (Financial Intelligence Unit) through a 'Suspicious Activity Report', also known as a 'SAR'. Staff must report their concerns and may do so to the firm's MLRO, who must then consider whether a report to FIU is necessary based on all the information at their disposal.

- Is it clear who is **responsible** for different types of liaison with the authorities?
- How does the **decision-making** process related to **SARs** work in the firm?
- Are procedures clear to staff?
- Do staff report suspicions to the **nominated officer**? If not, does the nominated officer take steps to identify why reports are not being made? How does the nominated officer deal with reports received?

- What evidence is there of the rationale **underpinning decisions** about whether a SAR is justified?
- Is there a documented process for responding to **Production Orders**, with clear timetables?

7. Sanctions

A firm should have effective, up-to-date screening systems appropriate to the nature, size and risk of its business. Although screening itself is not a legal requirement, screening new customers and payments against the Sanctions List (this includes United Nations Security Council sanctions lists and any other Kazakhstan Sanctions List), and screening existing customers when new names are added to the list, helps to ensure that firms will not breach the sanctions regime.

- When are customers screened against **lists**, whether the Sanctions List, internal watchlists maintained by the firm, or lists from commercial providers? (Screening should take place at the time of customer take-on. Good reasons are needed to justify the risk posed by retrospective screening, such as the existence of general licences.)
- If a customer was **referred** to the firm, how does the firm ensure the person is not listed? (Does the firm screen the customer against the list itself, or does it seek assurances from the referring party?)
- How does the firm become **aware of changes** to the Sanctions List? (Are there manual or automated systems? Are customer lists rescreened after each update is issued?)
- What kind of measures will be taken by the firm against persons on Sanction Lists?

8. Training and Awareness

Firms must employ staff who possess the skills, knowledge and expertise to carry out their functions effectively. They should review employees' competence and take appropriate action to ensure they remain competent for their role. Vetting and training should be appropriate to employees' roles.

- What is your approach to **vetting** staff? Do vetting and management of different staff reflect the financial crime risks to which they are exposed?
- How does your firm ensure that its employees are aware of financial crime risks and of their **obligations** in relation to those risks?
- Do staff have access to training on an **appropriate range** of financial crime risks?
- How does the firm ensure that training is of **consistent quality** and is **kept up to date**?

- Is training **tailored** to particular roles?
- How do you assess the **effectiveness** of your training on topics related to financial crime?
- Is training material relevant and up to date? When was it last reviewed?

9. Record-keeping

Firms must keep copies of any documents and information obtained to meet CDD requirements and sufficient supporting records for transactions for **six years** after the business relationship ends or five years after an occasional transaction.

- Can your firm retrieve records **promptly in response to law enforcement agencies'/regulators' request**?
- If the firm **relies on others** (Reliance and Outsourcing – please see Chapter 9 of AIFC AML Rules) to carry out AML checks, is this within the limits permitted by the *AML/CTF Rules*? How does it satisfy itself that it can rely on these firms?