COMPLIANCE POLICIES AND PROCEDURES APPLICABLE TO MEMBERS
(ITS CENTRAL SECURITIES DEPOSITORY LIMITED)

1. Members' Policy

Members of the ITS Central Securities Depository Limited ("Company") have an obligation to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities ("AML") by complying with requirements hereunder and all applicable AML laws and regulations in jurisdictions they operate.

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets.

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment.

The Company's Members shall have AML policies, procedures and internal controls designed to ensure compliance with all applicable regulations and rules and must be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in regulations and changes in Members' business.

The Company's Member shall certify regularly to the Company's Accreditation and Registration Department that it has implemented its anti-money laundering program and that it will perform (or its agent will perform) specified requirements of the customer identification program and suspicious transaction reporting.

2. AML Compliance Person Designation and Duties

The Company's Members must designate a senior staff person as their Money Laundering Reporting (MLRO).

The MLRO must be qualified by experience, knowledge and training. The duties of the MLRO will include monitoring the Member's compliance with AML obligations, overseeing communication and training for employees. The MLRO will also ensure that the Member keeps and maintains all of the required AML records and will ensure that Threshold Transactions Reports (TTR) are filed with a respective financial intelligence unit ("FIU") when appropriate. The MLRO is vested with full responsibility and authority to enforce the Member's AML program.

Member firms will provide the Company's Accreditation and Registration Department with contact information for the MLRO, including: name; title; mailing address; email address; telephone number; and facsimile number and will keep the Company informed of any change in this information and will review, and if necessary update, this information upon request of the Company.

3. Risk-based approach and Customer Identification Program

The Company's Member should identify, assess, and understand the money laundering and terrorist financing risks emerging from launch of new product, service or relationship with client. Based on that assessment, the Company's Member should apply a risk-based approach. Measures to prevent or mitigate the consequences of money laundering and terrorist financing should be commensurate with the identified risks.

The Company's Members are required to have and follow reasonable procedures to document and verify the identity of their customers who open new accounts. These procedures must address the types of information the Member will collect from the customer and how it will verify the customer's identity.

The Company's Member's customer identification program must be in writing and be part of the Member's AML compliance program.

4. Identification of Customer

The Company's Members will verify customer identity through documentary means. Appropriate documents for verifying the identity of customers include the following:

- For an individual, an unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as passport;

- For a person other than an individual, documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement or a trust instrument

The risk that members may not know the customer's true identity may be heightened for certain types of accounts, such as an account opened in the name of a corporation, partnership or trust that is created or conducts substantial business in a jurisdiction that has been designated by FATCA as a primary money laundering jurisdiction, a terrorist concern, or has been designated as a non-cooperative country or territory.

The Company's Members must not establish a business relationship with a customer which is a legal person if the ownership or control structure of the customer prevents the Company's Members from identifying all of the customer's beneficial owners. The Company's Members must not establish or maintain a business relationship with a Shell Bank.

5. Failure to conduct or complete Customer Due Diligence

Where, in relation to any customer, the Company's Members is unable to conduct or complete the requisite CDD it must, to the extent relevant:

- not carry out a transaction with or for the customer through a bank account or in cash;

- not open an account or otherwise provide a service;

- not otherwise establish a business relationship or carry out a transaction;

- terminate or suspend any existing business relationship with the customer;

- consider whether the inability to conduct or complete CDD necessitates the making of a STR.

The Company is prohibited from knowingly maintaining anonymous accounts or accounts under deliberately fictitious names.

6. Obligation to keep records

The Company's Members must maintain the following records:

- a copy of all documents and information obtained in conducting initial and on-going CDD;

- the supporting records (consisting of the original documents or certified copies) in respect of the customer business relationship, including transactions;

- STRs and any relevant supporting documents and information, including internal findings and analysis;

- any relevant communications with the FIU;

- for at least six years from the date on which the notification or report was made, the business relationship ends or the transaction is completed, whichever occurs last.

The Company ensures the safety and availability of documents to the responsible person in order to provide the necessary information at the request of the AFSA.

7. Reliance and outsourcing

The Company's Members may, under the following circumstances, rely on the performance by another financial institution (including an affiliate) of some or all of the elements of their CIP with respect to any customer that is opening an account or has established an account or similar business relationship with the other financial institution to provide or engage in services, dealings or other financial transactions:

- when such reliance is reasonable under the circumstances;
- when the other financial institution is subject to a rule implementing the antimoney laundering compliance program requirements and is regulated in a jurisdiction which has comparable AML standards; and
- when the other financial institution has entered into a contract with the Company's Member requiring it to certify regularly to the Company's Member that it has implemented its anti-money laundering program and that it will perform (or its agent will perform) specified requirements of the customer identification program.

The Company's Member will not be held responsible for the failure of the other financial institution to fulfill adequately its CIP responsibilities, provided that the Company's Member can establish that its reliance was reasonable and it has obtained the requisite contracts and certifications.

The Company's Member should conduct appropriate due diligence to assure itself of the suitability of a service provider and should ensure that the provider's obligations are clearly documented in a binding agreement.

8. General Customer Due Diligence

The Company's Members must obtain sufficient information about each customer to allow them to evaluate the risk presented by that customer and to detect and report suspicious activity. When they open an account for a customer, the due diligence they perform may be in addition to customer information obtained for purposes of the CIP.

Such information should include:

- the customer's business;
- the customer's anticipated account activity (both volume and type);
- the source of the customer's funds.

The Company's Members conducts enhanced due diligence - EDD (Enhanced Due Diligence) in relation to:

1. A client classified as high risk;
2. Transactions with persons from countries with high geographical risk factors.

For accounts that are deemed to be higher risk, the Company's Members will obtain the following information:

- the purpose of the account;
- the source of funds and wealth;
- the beneficial owners of the accounts;
- the customer's (or beneficial owner's) occupation or type of business;

- financial statements;
- banking references;
- domicile (where the customer's business is organized);
- description of customer's primary trade area and whether international transactions are expected to be routine;
- description of the business operations and anticipated volume of trading;
- explanations for any changes in account activity.

9. Due Diligence for Politically Exposed Persons (PEPs)

The policies, procedures, systems and controls adopted by the Company's Members must enable it to determine whether a customer or a beneficial owner is a Politically Exposed Person ("PEP").

Where a customer, or a beneficial owner of the customer, is a PEP, the Company's Members must ensure that, in addition to CDD it also:

- increases the degree and nature of monitoring of the business relationship, in order to determine whether the customer's transactions or activities appear unusual or suspicious; and
- obtains the approval of senior management to commence a business relationship with the customer.

10. Sanctions

The Company's Members must establish and maintain effective systems and controls to ensure that on an on-going basis it is properly informed as to, and takes reasonable measures to comply with, relevant resolutions or sanctions issued by the UNSC or by the Republic of Kazakhstan.

The Company's Members must comply with prohibitions from conducting transactions with designated persons and entities, in accordance with the obligations set out in the relevant resolutions or sanctions issued by the UNSC or by the Republic of Kazakhstan.

The Company's Members must freeze without delay and without prior notice, the funds or other assets of designated persons and entities pursuant to relevant resolutions or sanctions issued by the UNSC or by the Republic of Kazakhstan.

11. Monitoring Accounts for Suspicious Activity

The Company's Members must establish and maintain policies, procedures, systems and controls to monitor and detect suspicious activity or transactions in relation to potential money laundering.

The Company's Members must register in the FIU reporting system for submitting TTRs before the commencement of its business activities.

12. Suspicious Transactions Reporting

The Company's Members must establish and maintain policies, procedures, systems and controls to monitor and detect transactions above defined thresholds and submit threshold transactions reports ("TTRs") to the FIU in accordance with the AML Law.

The Company's Members will not notify any person involved in the transaction that the transaction has been reported.

13. AML Recordkeeping

The Company's Member's MLRO and his or her designee will be responsible for ensuring that AML records are maintained properly for at least six years from the date on which the notification or report was made, the business relationship ends or the transaction is completed, whichever occurs last.

14. AML training

All relevant employees of the Company's Members be given appropriate AML training as soon as reasonably practicable after commencing employment. A relevant employee means a member of the senior management or operational staff, any employee with customer contact, or any employee who handles (or may handle) customer monies or assets, and any other employee who might encounter money laundering in the business.

AML training should be provided by the Company's Members to each of its relevant employees at intervals appropriate to the role and responsibilities of the employee at least annually.

AML training provided by the Company's Members need not be in a formal classroom setting, rather it may be via an online course or any other similarly formal and documented manner.