ADS Securities Hong Kong Limited

Prevention of Money Laundering and Terrorist Financing Policy

1. Policy Statement

1.1 Policy

ADS Securities Hong Kong Limited (the "**Company**" or "**ADSS HK**") is fully committed to comply with all applicable laws and regulations in relation to the prevention of money laundering and counter-terrorist financing. This Prevention of Money Laundering and Terrorist Financing Policy (this "**Policy**") incorporates measures to combat money-laundering and terrorist financing activities and to generate a level of awareness of the obligations and responsibilities of employees on the prevention of money laundering and counter-terrorist financing.

1.2 Acknowledgement Form

The Company and its directors, officers, employees and any other of its representatives must adhere to this policy as a condition of their employment or engagement and must sign an acknowledgement form (Employee Undertaking Form).

2. Introduction

2.1 Money Laundering

(i) Money laundering ("**ML**") means an act intended to have the effect of making any property:

(a) that is the proceeds obtained from the commission of an indictable offence under the laws of Hong Kong, or of any conduct which if it had occurred in Hong Kong would constitute an indictable offence under the laws of Hong Kong; or

(b) that in whole or in part, directly or indirectly, represents such proceeds,

not to appear to be or so represent such proceeds.

(ii) There are three common stages in the laundering of money, and they frequently involve numerous transactions. The Company and all employees must be alert to any such sign for potential criminal activities. These stages are:

(a) Placement - the physical disposal of cash proceeds derived from illegal activities;

(b) Layering - separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the source of the money, subvert the audit trail and provide anonymity; and

(c) Integration - creating the impression of apparent legitimacy to criminally derived wealth. In situations where the layering process succeeds, integration schemes effectively return the laundered proceeds back into the general financial system and the proceeds appear to be the result of, or connected to, legitimate business activities.

2.2 Terrorist Financing

(i) Terrorist financing ("**TF**") means:

(a) the provision or collection, by any means, directly or indirectly, of any property-

(1) with the intention that the property be used; or

(2) knowing that the property will be used, in whole or in part, to commit one or more terrorist acts (whether or not the property is actually so used); or

(b) the making available of any property or financial (or related) services, by any means, directly or indirectly, to or for the benefit of a person knowing that, or being reckless as to whether, the person is a terrorist or terrorist associate; or

(c) the collection of property or solicitation of financial (or related) services, by any means, directly or indirectly, for the benefit of a person knowing that, or being reckless as to whether, the person is a terrorist or terrorist associate.

(ii) Terrorists or terrorist organisations require financial support in order to achieve their aims. There is often a need for them to obscure or disguise links between them and their funding sources. It follows then that terrorist groups must similarly find ways to launder funds, regardless of whether the funds are from a legitimate or illegitimate source, in order to be able to use them without attracting the attention of the authorities.

2.3 Legislation and Guidelines

The main pieces of legislation and guideline in Hong Kong concerning money laundering, terrorist financing, financing of proliferation of weapons of mass destruction and financial sanctions that are applicable to the Company and all employees are:

(i) Anti-Money Laundering and Counter-Terrorist Financing Ordinance **("AMLO")** – This Ordinance imposes legal requirements relating to customer due diligence ("**CDD**") and record-keeping on licensed corporations ("**LCs**"). It also provides regulators including the SFC with the power to supervise compliance with those requirements.

(ii) Guideline on Anti-Money Laundering and Counter-Terrorist Financing **("AML Guideline")** – This Guideline is issued by the Securities and Futures Commission and sets out the relevant anti-money laundering and counter-financing of terrorism ("**AML/CFT**") statutory and regulatory requirements, and the AML/CFT standards which LCs should meet in order to comply with the statutory requirements under the AMLO and the Securities and Futures Ordinance ("**SFO**").

The AML Guideline also provides practical guidance to assist LCs and their senior management in designing and implementing their own policies, procedures and controls in the relevant operational areas, taking into consideration their special circumstances so as to meet the relevant AML/CFT statutory and regulatory requirements.

(iii) Drug Trafficking (Recovery of Proceeds) Ordinance **("DTROP")** - This Ordinance contains provisions for the investigation of assets that are suspected to be derived from drug trafficking activities, the freezing of assets on arrest and the confiscation of the proceeds from drug trafficking activities upon conviction. In particular, section 25A imposes a legal obligation that any person, who knows or suspects any property represents proceeds of crime or terrorist property, shall make a report to the Joint Financial Intelligence Unit ("**JFIU**").

(iv) Organized and Serious Crimes Ordinance **("OSCO")** - This Ordinance gives the Police and Customs and Excise Department the ability to investigate the activities of organized crime and triad activities, gives the Courts of Hong Kong jurisdiction to confiscate the proceeds of organized and serious crimes, and creates an offence of ML in relation to the proceeds of indictable offences. In particular, section 25A imposes a legal obligation that any person, who knows or suspects any property represents proceeds of crime or terrorist property, shall make a report to the JFIU.

(v) United Nations (Anti-Terrorism Measures) Ordinance **("UNATMO")** - This Ordinance is principally directed towards implementing decisions contained in relevant United Nations Security Council Resolutions ("**UNSCRs**") aimed at preventing the financing of terrorist acts and combating the threats posed by foreign terrorist fighters. Besides the mandatory elements of the relevant UNSCRs, the UNATMO also implements the more pressing elements of the Financial Action Task Force ("**FATF**") Recommendations specifically related to TF. The UNATMO also criminalises the provision or collection of property and making any property or financial (or related) services available to terrorists or terrorist associates.

(vi) Weapons of Mass Destruction (Control of Provision of Services) Ordinance **("WMD(CPS)O")** – This Ordinance controls the provision of services that will or may assist the development, production, acquisition or stockpiling of weapons capable of causing mass destruction or that will or may assist the means of delivery of such weapons. The WMD(CPS)O also prohibits a person from providing any services where he believes or suspects, on reasonable grounds, that those services may be connected to PF. The provision of services is widely defined and includes the lending of money or other provision of financial assistance.

(vii) Code of Conduct for Persons Licensed by or Registered with the SFC **("Code of Conduct")** – This Code of Conduct includes guidance for establishing the true and full identity of clients in the know-your-client ("**KYC**") process.

2.4 Procedures

The Company needs to establish and maintain appropriate procedures for:

(i) identifying clients and their beneficial owners;

(ii) verifying clients' identities;

(iii) identifying suspicious transactions;

(iv) performing screening against new or updated terrorist and sanctions designations, and other adverse information and cases;

(v) monitoring business relationships continuously;

(vi) reporting knowledge or suspicion of ML;

(vii) maintaining adequate CDD information, transaction records and other necessary records relating to the client and account; and

(viii) providing appropriate AML/CFT trainings.

2.5 Risk Areas

The area of the Company's business which are most susceptible to ML risk is when large sums of money from private individuals are being dealt with. In particular, the Company needs to pay more attention when reviewing transactions relating to individuals or

organizations in countries where it is difficult to obtain information about the client and which have deficiencies in their legal and regulatory systems regarding the prevention of ML, e.g. non-FATF member countries[1]. Warning messages and other relevant information from FATF (including high risk and non-cooperative jurisdictions[2]) must be taken into account in these circumstances.

2.6 Consequences of non-compliance

(i) According to the AMLO, it would in certain circumstances be a criminal offence for the financial institution if it knowingly contravenes a specified provision or with intent to defraud any relevant authority, contravenes a specified provision. If an employee or the management of a financial institution knowingly causes or knowingly permits the financial institution to contravene a specified provision, then the person also commits an offence and is liable for fines and imprisonment; and

(ii) In addition, a failure by the Company or any of its licensed representatives to comply with the AML Guideline (i) will be admissible in evidence in a court proceeding under the AMLO and (ii) will reflect on the fitness and properness as well as (iii) may be considered to be misconduct.

3. Responsibilities

3.1 Senior Management

The responsibilities of senior management include:

(i) ensuring that on an ongoing basis, the Company's AML/CFT systems are effective and are capable of adequately addressing the ML/TF risks which exist in the Company's business;

(ii) appointing:

(a) a Compliance Officer ("**CO**") at the senior management level to have the overall responsibility for the establishment and maintenance of the FI's AML/CFT systems;

(b) a senior member of the Company as the Money Laundering Reporting Officer **("MLRO")**[3] to act as the central reference point for suspicious transaction reporting; and

(c) a senior member of the Company (usually the MLRO) to act as the Manager-In-Charge of AML/CFT to principally be responsible for managing the AML/CFT core function;

(iii) ensuring, to the extent that is practical, the CO and the MLRO, as well as their authorized delegates, are independent of all operational and business functions and have sufficient level of seniority and authority;

(iv) maintaining sufficient direct contact with the CO and the MLRO to be satisfied that the Company is implementing and maintaining sufficiently robust measures to protect itself against the risk of ML/TF; and

[1] FATF member list is available at: http://www.fatf-gafi.org/countries/
[2] The list of countries is available at: http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/
[3] Senior management may decide that the functions of CO and MLRO should be performed by the same staff member, after considering the size and businesses of the Company.

(v) ensuring that the CO and the MLRO are fully conversant with the Company's statutory and regulatory obligations and the ML/TF risks arising from the Company's business, as well as have full access to all necessary and available information (both from internal source such as CDD records and external sources such as screening results from third-party data base) that allows them to carry out their duties and fulfill the regulatory obligations in that position.

3.2 Compliance Officer

The responsibilities of the CO include:

(i) disseminating updated news/circulars/regulations covering ML/TF to all employees to raise their awareness;

(ii) reviewing AML/CFT policies and procedures regularly and where necessary, and making all necessary updates and communicating key AML/CFT issues with senior management;

(iii) ensuring that all employees adhere to AML/CFT policies and procedures;

(iv) performing regular independent reviews on transactions concluded with customers/counterparts regularly and where necessary, in order to identify whether there is any issue that may give rise to a suspicion of ML or TF activity;

(v) mitigating ML/TF risks which arise from business relationships and transactions with persons from countries which do not or insufficiently apply the FATF recommendations; and

(vi) providing or arranging AML/CFT trainings to employees regularly and where necessary.

3.3 Money Laundering Reporting Officer

The responsibilities of the MLRO include:

(i) reviewing, analyzing and conducting further investigation on suspicious transactions as reported by employees;

(ii) reporting any suspicious transactions to the JFIU;

(iii) maintaining a register to keep all records of reports made by employees, whether they are valid or invalid case with reasons, together with the reports made to the JFIU;

(iv) providing guidance on how to avoid "tipping off" where a disclosure is made to the JFIU in the event of a suspicion of ML/TF; and

(v) acting as the main point of contact with the JFIU and any other competent authorities in relation to AML/CFT.

3.4 Manager-In-Charge ("**MIC**") of Core Function

(i) The definition of MIC by the SFC is an individual appointed by an LC to be principally responsible for managing one or more of the eight core functions.

(ii) In the context of AML/CFT, the MLRO will usually be appointed as the MIC for AML/CFT, and will be principally responsible for managing the AML/CFT core function of the Company.

3.5 Employees

The responsibilities of employees are to:

(i) comply with this policy to ensure appropriate measures are implemented in practice to prevent ML/TF activities, which include but are not limited to reporting suspicious transactions internally to the MLRO;

(ii) be aware of and comply with the legislation and guidelines that are related to AML/CFT; and

(iii) cooperate with the CO and the MLRO so that he or she can liaise appropriately with the relevant law enforcement authorities, including but not limited to timely disclosure of information.

4. General Requirements

4.1 Requirements

The Company is obliged to establish and verify the true and full identity of each client, as well as the true and full identity of any beneficial owners of the subject trading account and. The Company also need to establish each client's financial situation, investment experience and investment objectives at the time when the business relationship is established with the client (the identity verification requirement however can be waived in certain situations subject to (i) any risk of ML/TF arising from the delayed verification of the client's or beneficial owner's identity can be effectively managed; (ii) it is necessary not to interrupt the normal conduct of business with the client; and (c) verification of identity is completed as soon as reasonably practicable.). The relevant requirements are set out below.

4.2 Beneficial Owner

A beneficial owner for the purposes of a **corporate** client means an individual who:

(i) owns or controls, directly or indirectly, including through a trust or bearer share holding, more than 25% of the issued share capital of the corporation;

(ii) is, directly or indirectly, entitled to exercise or control the exercise of more than 25% of the voting rights at general meetings of the corporation; or

(iii) exercises ultimate control over the management of the corporation.

A beneficial owner for the purposes of a **partnership** client means an individual who:

(i) is entitled to or controls, directly or indirectly, more than a 25% share of the capital or profits of the partnership;

(ii) is, directly or indirectly, entitled to exercise or control the exercise of more than 25% of the voting rights in the partnership; or

(iii) exercises ultimate control over the management of the partnership.

For the definition of a beneficial owner in the context of a **trust** client, please refer to paragraph (ii).

In relation to a client which is not a corporation, partnership or trust, beneficial owner means any individual who ultimately owns or controls the person.

Wherever a client is **acting on behalf of another person**, that other person will also be a beneficial owner.

4.3 Anonymous / Fictitious Accounts

Anonymous or fictitious accounts must not be maintained for any new or existing customers.

4.4 List Checking and Database Maintenance

For AML/CFT purposes, the SFC issues circulars to licensed corporations to provide updated information on relevant persons or entities. The Company needs to maintain a database which contains the names and particulars of terrorist suspects and designated parties or the Company can make appropriate arrangements with a third party database provider. Employees need to screen new clients against current terrorist and sanction designations at the establishment of the relationship and thereafter when new sanction lists are published. The results of the screening of clients must be fully investigated and documented. Employees must report any transactions or relationships they have or have had with any named individuals or entities to the MLRO who would then decide whether to report to the JFIU.

5. Timeframe

5.1 Before Relationship

The Company should identify and verify the client and any beneficial owners before establishing any relationship with the client or effecting any transactions.

5.2 Exceptions

The approval of senior management must be obtained for a decision to delay such verification, and such approval may only be granted on the basis that:

(i) the risk of ML/TF arising from the delayed verification of the client's or beneficial owners' identifies can be effectively managed;

(ii) this is necessary so that the normal business with the client would not be interrupted;

(iii) all other necessary CDD information has been obtained;

(iv) the client has been advised of the Company's obligation to terminate the relationship at any time on the basis of non-completion of the verification measures;

(v) limits on the number of transactions and types of transactions are placed on the client; and

(vi) no funds can be paid out to any third party unless:

(a) there is no suspicion of money laundering or terrorist financing;

(b) the risk of money laundering and terrorist financing is assessed to be low;

(c) the transaction is approved by senior management after taking into account of the nature of the business of the client; and

(d) the names of recipients do not match with watch lists such as those for terrorist suspects and politically exposed persons.

5.3 No Delay Permitted

However, no delay in verification should be allowed if there is:

(i) knowledge or a suspicion of money laundering or terrorist financing;

(ii) these is any doubt about the identify or intentions of the client or the beneficial owner; or

(iii) the business relationship is assessed to pose a high risk.

5.4 Suspension / Termination

The verification of the client's identity and that of any beneficial owners should be concluded within a reasonable timeframe and in any case:

(i) such verification should be completed no later than 30 working days after the establishment of business relations;

(ii) business relations with the client should be suspended and the Company should refrain from carrying out further transactions (except to return funds to their sources) if such verification remains uncompleted 30 working days after the establishment of business relations; and

(iii) business relations with the client should be terminated if such verification remains uncompleted 120 working days after the establishment of business relations.

5.5 Senior Management Updates

The CO is responsible for monitoring relationships with clients pending completion of the verification and providing updates to senior management of any pending cases on a regular basis.

6. Customer Due Diligence ("CDD") (Standard Identification Procedures)

6.1 CDD Measures - General

The Company is required to undertake the following CDD measures in relation to each customer:

(i) identify each customer and verify the customer's identity using reliable, independent source documents, data or information;

(ii) if there is a beneficial owner in relation to the customer (see paragraph 4.2 above), identify and take reasonable measures to verify the beneficial owner's identity so that the Company is satisfied that it knows who the beneficial owner is, including, where the customer is a legal person or trust, measures as to enable the financial institution to understand the ownership and control structure of the legal person or trust;

(iii) obtain information on the purpose and intended nature of the business relationship established with the Company (unless obvious);

(iv) if a person purports to act on behalf of the customer:

(a) identify the person and take reasonable measures to verify the person's identity; and

(b) verify the person's authority to act on behalf of the customer.

6.2 CDD Measure - Specific

The CDD measures applicable for the different categories of client are set out below. Deviations from these requirements can only be made with the written approval of the CO and this approval will only be granted in exceptional circumstances e.g. where the CO has been able to confirm with an independent third party in writing that the relevant requirement is inapplicable in the case of the prospective client and that there is no relevant equivalent.

6.3 Individual Clients

(i) Before opening an account, satisfactory evidence of the identity of the client must be obtained. Positive identification of a client must be obtained from documents issued by reliable sources and file copies should be retained and reference numbers and other relevant details recorded. All prospective customers should be interviewed personally unless the CO waives this requirement in writing before the account is opened.

(ii) The following documents and information should be obtained for all individual clients:

(a) full name (can be obtained from passport or identity card (or where the person is not a Hong Kong resident and not physically present in Hong Kong for verification purposes, driver's licence);

(b) permanent address and residential address if different (can be verified against recent utility or rates bill);

(c) date of birth (can be obtained from passport, identity card (or where the person is not a Hong Kong resident and not physically present in Hong Kong for verification purposes, driver's licence);

(d) nationality (not required for HKID card holder);

(e) identity document type and number;

(f) occupation;

(g) beneficial ownership and control (to determine whether the account is beneficially owned by the client and if not, the same details should be obtained for the beneficial owner(s)); and

(h) where relevant, identification document of any person purporting to act on behalf of the client and written authority.

(iii) If a client has not been physically present for identification purposes, the Company must carry out at least one of the following measures: -

(a) further verifying the customer's identity on the basis of documents, data or information referred to in section 2(1)(a) of Schedule 2 of the AMLO but not previously used

for the purposes of verification of the customer's identity under that section;

(b) taking supplementary measures to verify all the information provided by the customer; and

(c) ensuring that the payment or, if there is more than one payment, the first payment made in relation to the customer's account is carried out through an account opened in the customer's name with an authorized institution or a licensed bank in a FATF jurisdiction.

6.4 Companies and Other Incorporated Entities

(i) In respect of companies and other incorporated entities, it is important to identify the directors, the account signatories and the nature of its business.

(ii) Unless a corporate client is eligible for simplified customer due diligence ("SDD") measures under paragraph 7, the Company must obtain copies of the following documents and information:

(a) the full name and address of the client;

(b) the country of incorporation of the client;

(c) a copy of the certificate of incorporation or other constitutive documents (such as memorandum and articles of association or incorporation);

(d) a copy of the client's licence certificates from the local regulatory body (if any);

(e) an authorized signatories list;

(f) a copy of the Business Registration Certificate or equivalent;

(g) a copy of the Board of Directors resolution (or equivalent) authorizing the transaction;

(h) a list of the directors of the client (or equivalent) and copies of their identification documents;

(i) identification information for all beneficial owners;

(j) identification documents (to permit verification of identity) for those beneficial owners;

(k) confirmation as to whether the account is beneficially owned by the client and / or a third party;

(l) where the client is incorporated in Hong Kong, a company search report from the Hong Kong Companies Registry; and

(m) where the client is incorporated overseas, obtain (i) a company report (similar to a company search) form the local registry in the place of incorporation; or (ii) a certificate of incumbency or equivalent, issued by the client's registered agent in its place of incorporation or (iii) a similar or comparable document to a company search report or a certificate of incumbency certified by a

professional third party in the relevant jurisdiction, in each case issued within the last six months.

(iii) The Company should understand the ownership structure of the client and determine its source of funds. Special care should be taken in dealing with companies that have nominee shareholders and companies which have a significant proportion of capital in the form of bearer shares.

6.5 Partnerships and Other Unincorporated Bodies

(i) In respect of partnerships or other unincorporated body clients, it is important to identify the partners etc, the account signatories and the nature of the business.

(ii) The Company must obtain copies of the following documents and information, unless the client is eligible for SDD (see paragraph (iv)):

(a) the full name and address of the client;

(b) the names of all partners and individuals who exercise control over the management of the partnership or unincorporated body;

(c) the names of all individuals (for a partnership) who are entitled to or exercise control more than 25% of the capital or profits or of the voting rights;

(d) if the partnership or unincorporated body acts on behalf of another person, identity information of the other person;

(e) a mandate authorizing the opening of the account and conferring authority on those who will operate it (for a partnership);

(f) the partnership agreement / deed; and

(g) identification documents (see above) of the partners and individuals exercising ultimate control over the management for the purpose of verification of identity; and

(h) identification documents (see above) of the partners and individuals who are entitled to or exercise control over 25% or more of the capital or profits or of the voting rights of the client management for the purpose of verification of identity.

(iii) The Company should understand the ownership structure and determine the source of funds.

6.6 Trusts

(i) A trust does not possess a separate legal personality. It is the trustee who / which acts on behalf of the trust that should be considered to be the customer of the Company.

(ii) In relation to a trust, a beneficial owner is:

(a) an individual who is entitled to a vested interest in 25% or more of the capital of the trust property, whether the interest is in possession or in remainder or reversion and whether it is defeasible or not;

(b) the settler of the trust;

(c) a protector or enforcer of the trust; and

(d) any individual who has ultimate control over the trust.

(iii) The Company must obtain copies of the following documents and information:

(a) trust deed;

(b) date of establishment / settlement;

(c) the identification number (if any) granted by any applicable official bodies;

(d) identity information of trustee, settlor, protector or enforcers (if any) and beneficial owners (same as those set out under “Individual Clients” or Companies and other incorporated entities” as the case may be); and

(e) identification documents (to permit verification of identity) of trustee, settlor, protector, enforcers and for those beneficial owners with 25% or greater interest.

6.7 Limited Partnerships - Private Equity Funds

Funds, especially private equity funds, are sometimes structured as limited partnerships. If a fund is an "investment vehicle" eligible for SDD measures, the following documents and information will need to be obtained in relation to the fund itself, but nothing will need to be obtained in relation to any of its beneficial owners (i.e. limited partners):

(i) full name, and date and place of establishment;

(ii) certificate of registration of the fund or equivalent;

(iii) confirmation from a relevant person that the investment vehicle has reliable systems and controls in place to conduct the CDD (including identification and verification of the identity) on all underlying investors in accordance with the requirements of Schedule 2 of the AMLO;

(iv) purpose and intended nature of the business relationship between the fund and the Company (if not obvious);

(v) all relevant identification information for the general partner (and the Company will need to take reasonable measures to verify the general partner's identity); and

(vi) evidence of the general partner's authority to act on behalf of the fund.

6.8 Anonymous Accounts

Anonymous accounts are prohibited.

6.9 Pre-existing Clients

The Company must perform due diligence measures on a one-off basis in respect of any client with whom / which a business relationship was established prior to 1 April 2012, when:

(i) a transaction which takes place with regard to the client, which is by virtue of the amount or nature of the transaction, unusual or suspicious; or is not consistent with the Company's knowledge of the client or the client's business or risk profile, or with its knowledge of the source of the client's funds;

(ii) a material change occurs in the way in which the client's account is operated;

(iii) the Company suspects that the client or the client's account is involved in ML/TF; or

(iv) the Company doubts the veracity or adequacy of any information previously obtained for the purpose of identifying the client or for the purpose of verifying the client's identity.

7. Simplified Customer Due Diligence ("SDD")

7.1 Low Risk

The Company is permitted to apply SDD procedures where the Company is satisfied that the risk of ML/TF is low.

7.2 Types of Clients

SDD will suffice in relation to a client which is:

(i) a financial institution ("**FI**") as defined under the AMLO; or

(ii) an institution that:

(a) is incorporated or established in a jurisdiction that is a member of the FATF (other than Hong Kong) or a jurisdiction that imposes AML / CTF requirements similar to those imposed under the AMLO (an "equivalent jurisdiction"); and

(b) carries on a business similar to that carried on by an FI; and

(c) has measures in place to ensure compliance with requirements similar to those imposed under the AMLO; and

(d) is supervised for compliance with those requirements by an authority in that jurisdiction that performs functions similar to those of the SFC; or

(iii) a corporation listed on any stock exchange;

(iv) an investment vehicle (e.g. a legal person / trust / collective investment scheme / other investment entity) where the person responsible for carrying out measures that are similar to the CDD measures, in relation to all the investors of the investment vehicle, is:

(a) an FI; or

(b) an institution incorporated or established in Hong Kong, or in an equivalent jurisdiction that:

- has measures in place to ensure compliance with requirements similar to those imposed under the AMLO; and
- is supervised for compliance with those requirements; or

(v) the Government or any public body in Hong Kong; or

(vi) the government of an equivalent jurisdiction or a body in an equivalent jurisdiction that performs functions similar to those of a public body.

7.3 SDD Measures

In order to justify the SDD approach, the following information must be documented and kept:

(i) evidence of the place of incorporation of the client and a print out of its status e.g. listed or regulated; and

(ii) Where relevant and if applicable, confirmation from certain client that it has measures in place to comply with AML requirements similar to the Hong Kong AML requirements[4].

When SDD measures are applicable, the Company only has to:

(i) identify the client and verify the client's identity (and does not need to identity or verify the identity of any beneficial owners);

(ii) obtain information on the purpose and intended nature of the business relationship with the Company (if not obvious); and

(iii) obtain the identification documents and written authority of the person purporting to act on behalf of the client.

7.4 Nominee Companies / Investment Vehicles

The Company may apply SDD to a client that is an FI which opens an account:

(i) in the name of a nominee company for holding fund units on its behalf or its underlying customers, or

(ii) in the name of an investment vehicle in the capacity of a service provider (such as manager or custodian) to the investment vehicle where the underlying investors have no control over the management of the investment vehicle's assets;

provided that the FI described above:

(i) has conducted CDD:

(a) in the case where the nominee company holds fund units on behalf of the client or the client's underlying customers, on its underlying customers; or

(b) in the case where the client acts in the capacity of a service provider (such as manager or custodian) to the investment vehicle, on the investment vehicle in accordance with the provisions of the AMLO; and

[4] If the client is an FI and the Company is in doubt for some reasons, the Company should also obtain a confirmation from the client that it has not had any negative comments from its regulator in relation to any deficiencies in its AML measures, e.g. during a routine inspection

(ii) is authorized to operate the account as evidenced by contractual document or agreement.

8. Risk Situations / Enhanced Due Diligence

8.1 High Risk Situations

The Company must, in any situation specified by the SFC in a notice in writing given to the Company and in any situation that by its nature presents a higher risk of ML/TF, take additional measures to mitigate the risk of ML/TF.

8.2 Non-FATF Jurisdictions

The Company should also give particular attention to, and exercise extra care by performing additional measures in respect of business relationships and transactions with persons from or in jurisdictions that do not or insufficiently apply the FATF Recommendations[5]. The Company will monitor and implement the latest update of the FATF country list, non-FATF country list, and the list of high-risk and other monitored countries.

In addition, the FATF will also from time to time identify countries which have strategic AML/CFT deficiencies and have not committed an action plan developed with the FATF to address the deficiencies[6], where the Company will also closely monitor and implement the latest update of these specific countries.

There is extremely high risk involved (reputational risk in particular) in taking on clients from any of the non-FATF countries, high-risk and other monitored countries, and countries which have strategic AML/CFT deficiencies.

In principle[7], senior management has determined not to conduct business with clients from certain countries, the list which will be updated from time to time and distributed within the Company.

For clients from countries which are included in the lists other than the FATF country list, senior management has determined that if the Company is being approached and wishes to deal with a client from one of those countries, the Company must obtain specific senior management approval with full reasons documented before taking on the client and perform the additional steps as set out below.

8.3 Additional Measures

Additional measures or enhanced due diligence **("EDD")** may usually include:

(i) obtaining the approval of senior management to commence or continue the business relationship;

(ii) taking reasonable measures to establish the relevant client's or beneficial owner's source of wealth and the source of the funds that will be involved in the business relationship;

(iii) obtaining additional information on the client (e.g. occupation, volume of assets, information available through public databases, internet, etc.) and updating more regularly the identification data of client and beneficial owner;

[5] The list of the high risk and non-cooperative jurisdictions is available at FATF's official website and will be updated from time to time

[6] The lists of the countries with strategic AML/CFT deficiencies is available at FATF's official website and will be updated from time to time

[7] The SFC does not ban these jurisdictions outright but this is a recommended practice in a risk-based approach

(iv) obtaining additional information on the intended nature of the business relationship (e.g. anticipated account activity);

(v) obtaining information on the reasons for intended or performed transactions; and

(vi) increasing the number and timing of the controls applied and selecting patterns of transactions that need further examination.

9. Politically Exposed Persons ("PEPs")

9.1 PEPs

EDD measures must be undertaken on all PEPs (whether "foreign" or "domestic") and others who are classified as a high risk for ML/TF.

9.2 Measures

When the Company knows that a particular client or beneficial owner is a PEP, it should, before (i) establishing a business relationship or (ii) continuing an existing business relationship, apply all the following measures:

(i) obtain approval from senior management for establishing or continuing such business relationship;

(ii) take reasonable measures to establish the client's or the beneficial owner's source of wealth and the source of the funds; and

(iii) conduct enhanced ongoing monitoring on that business relationship based on the level of assessed risk.

10. Intermediaries / Agents

10.1 Specified Intermediaries

The Company can rely on the due diligence measures (i.e. measures to identify each client and verify the client's identity) taken by any of the following institutions **("specified intermediaries")** subject to the following provisions:

(i) an authorized institution, a licensed corporation etc.; or

(ii) a financial institution in a FATF or FATF equivalent jurisdiction that:

(a) is locally registered or licensed or is regulated under the law of that jurisdiction;

(b) has measures in place to ensure compliance with CDD measures similar to the Hong Kong requirements; and

(c) is supervised locally for compliance with CDD measures similar to the Hong Kong requirements.

10.2 Formal Agreement

In order for the Company to be able to rely on the measures taken by a specified intermediary, that intermediary would need to confirm in writing that it agrees:

(i) to act as the Company's intermediary and perform which part of the CDD measures specified in section 2 of Schedule 2 of the AMLO;

(ii) to provide to the Company immediately the data or information the intermediary has obtained (e.g. name and address) in the course of carrying out the CDD measures; and

(iii) to provide, on request, a copy of any document or a record of any data or information obtained by the intermediary in the course of carrying out the CDD measures.

The intermediary should also confirm in writing that where documents and records are kept by the intermediary, it agrees to keep all underlying CDD information throughout the continuance of the Company's business relationship with the client and for at least five years beginning on the date on which the business relationship of a client with the Company ends or until such time as may be specified by the SFC.

10.3 Company Liable

The Company would remain liable under the AMLO for any failure by the intermediary to conduct any of its CDD measures so it is important that any such intermediary comply with all requirements to which it is subjected to.

10.4 Record Keeping

The intermediary must also be obliged to pass copies of all documents and records to the Company, where the intermediary is about to cease trading or does not act as an intermediary for the Company anymore.

10.5 Testing

The Company must conduct sample testing on the intermediary and if it has doubts, take reasonable steps to review the intermediary's ability to perform its CDD duties.

Whenever termination of the relationship between the Company and the intermediary is required, the Company should obtain all CDD information from the intermediary.

11. Suspicious Transactions

11.1 Obligation

The Company has an obligation to report where there is knowledge or suspicion of ML/TF.

11.2 Knowledge

Generally speaking, knowledge is likely to include:

(i) actual knowledge;

(ii) knowledge of circumstances which would indicate facts to a reasonable person; and

(iii) knowledge of circumstances which would put a reasonable person on inquiry.

11.3 Suspicion

Suspicion is personal and subjective and falls far short of proof based on firm evidence. However, suspicion goes beyond mere speculation. It is "a degree of satisfaction and not necessarily amounting to belief but at least extending beyond speculation as to whether an event has occurred or not".

11.4 Examples

These are general examples of situations that might give rise to suspicion in certain circumstances:

(i) transactions or instructions which have no apparent legitimate purpose and/or appear not to have a commercial rationale;

(ii) transactions, instructions or activity that involve apparently unnecessary complexity or which do not constitute the most logical, convenient or secure way to do business;

(iii) where the transaction being requested by the customer, without reasonable explanation, is out of the ordinary range of services normally requested, or is outside the experience of the financial services business in relation to the particular customer;

(iv) where, without reasonable explanation, the size or pattern of transactions is out of line with any pattern that has previously emerged;

(v) where the customer refuses to provide the information requested without reasonable explanation or who otherwise refuses to cooperate with the CDD and/or ongoing monitoring process;

(vi) where a customer who has entered into a business relationship uses the relationship for a single transaction or for only a very short period without a reasonable explanation;

(vii) the extensive use of trusts or offshore structures in circumstances where the customer's needs are inconsistent with the use of such services;

(viii) transfers to and from high risk jurisdictions 59 without reasonable explanation, which are not consistent with the customer's declared business dealings or interests; and

(ix) unnecessary routing of funds or other property from/to third parties or through third party accounts.

11.5 Employee/Agent Conduct

The following are all examples of employee/agent conduct which may indicate a suspicious situation:

(i) changes in employee characteristics (e.g. lavish life styles);

(ii) changes in employee or agent performance, (e.g. an employee sells products for cash and has a remarkable or unexpected increase in performance);

(iii) any dealing with an agent where the identity of the ultimate beneficiary or counterparty is undisclosed, or contrary to normal procedures for the type of business concerned; and

(iv) the use of an address that is not the client's permanent address, (e.g. using the employee's office or home address for the dispatch of customer documentation).

11.6 High Risk Accounts

(i) The most common accounts used for money laundering are remittance agencies, moneychangers, casinos, accounts with members of secretarial companies as authorized signatories, accounts of shelf companies and nominee client accounts.

(ii) Greater attention should be paid to any clients where any of the above applies.

11.7 Inclusion of Client on List

Particular care should be taken when a client is on a list described under paragraph 4.4.

11.8 Guidelines on Recognition of Suspicious Transactions

(i) If an employee receives instructions from a client to carry out a transaction with any of the suspicious indicators listed above, the employee should request an explanation for the transaction from the client.

(ii) The employee should consider whether the client has provided a reasonable and legitimate explanation of the financial activity. If not, the matter should be discussed with the MLRO for further action.

(iii) If the client is unwilling or refuses to answer questions or gives replies that appear to be untrue, the employee should refer the matter to the MLRO as this may be a further indication of a suspicious transaction.

11.9 Reporting

(i) The obligation to report under the DTROP, OSCO or UNATMO rests with any individual who becomes suspicious of a person and/or transaction.

(ii) If an employee identifies any of the transaction types described above, he or she must report it immediately to the MLRO by writing and list out all the suspicions and details of the subject transaction. The reporting employee must not disclose the matter to any other person to avoid contravening the regulatory requirement that there should be no tipping-off. The MLRO will then initiate the following course of action:

(a) consider appropriate questioning of the client;

(b) review information already known about the client to decide if the apparently suspicious activity should be expected from that client;

(c) make a subjective decision about whether the client's activity is suspicious or not; and

(d) if he or she decides that the activity is suspicious, report the transaction appropriately.

(iii) If in the opinion of the MLRO a report needs to be filed, it should be done through the Suspicious Transaction Report and Management System ("**STREAMS**") of the JFIU.

(iv) The MLRO should keep a register of all suspicious transaction reports made by employees and all reports made to the JFIU.

Dos and Don'ts – Summary

DO	report any suspicious transactions or solicitations to the MLRO immediately.
DO	keep a full record of all conversations and any relevant circumstances underlying the suspicions. These should be passed immediately to the MLRO.
DO	be aware of abnormal transactions or dealing patterns, even from existing clients.
DO NOT	do anything which may lead the person with whom employees are dealing to conclude that any of the employees are suspicious of him or her - "tipping off" is a criminal offence.
DO NOT	undertake any business with new clients until their identity has been verified in accordance with this policy.

12. Record Keeping

12.1 Records

(i) The JFIU needs to ensure a satisfactory audit trail for suspected laundered money is kept in order to establish a financial profile of the suspect account.

(ii) To satisfy these requirements, the Company is required to retain the following information:

(a) the beneficial owner(s) of the account;

(b) the volume of the funds flowing through the account; and

(c) for each transaction:

(1) the origin of the funds;

(2) the form in which the funds were offered or withdrawn, e.g. cash, cheques, etc.;

(3) the identity of the person undertaking the transaction;

(4) the destination of the funds; and

(5) the form of instruction and authority.

12.2 Retention of Records

(i) All records on transactions (including those set out in paragraph 12.1 above, both domestic and international, should be maintained for at least 5 years after the completion of a transaction, regardless of whether the business relationship ends during the period. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currencies involved, if any) so as to provide, if necessary, evidence for prosecution of criminal behavior.

(ii) Customer identification records (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence should be kept for at least 5 years after the account is closed.

(iii) In situations where the records relate to on-going investigations or transactions which have been the subject of disclosure, they should be retained until it is confirmed that the case has been closed.

13. Periodic Monitoring

13.1 The Company is required to monitor on an ongoing basis, its business relations with each client and observe the transactions they undertake to ensure that the transactions are consistent with the Company's knowledge of the client, its business and risk profile and where appropriate, the source of funds.

13.2 Where transactions that are complex, large or unusual, or patterns of transactions which have no apparent economic or lawful purpose, are noted, the Company should examine the background and purpose, including, where appropriate, the circumstances, of the transactions. The findings and outcomes of these examinations should be properly documented in writing and be available to assist investigations from the JFIU, the SFC, or other relevant authorities. Proper records of decisions made, by whom, and the rationale for them will help the Company demonstrate that it is handling unusual or suspicious activities appropriately.

13.3 All high-risk clients must be reviewed at least on an annual basis.

14. Education and Training

14.1 Training on AML/CFT will be provided for new employees during orientation to ensure that they are aware of their personal obligations under the relevant legislation and guidelines and that they can be personally liable should they fail to report as required.

14.2 Refresher training will be provided regularly to generate and maintain a level of awareness and vigilance to enable suspicious transactions to be recognized and reported.

14.3 The frequency, content and techniques used for the purpose of the ongoing training needs to be determined by the CO and the MLRO based on the needs of the business at the time and in accordance with the AML Guideline. The effectiveness of the training must be monitored by testing, so that further training needs can be identified.

14.4 The Company should monitor and maintain records showing who has done training, when, and the type of the training. These records should be maintained for a minimum of 3 years.

15. Branches and Subsidiary Undertakings outside Hong Kong

15.1 The Company must ensure that any:

(i) branches; and

(ii) subsidiary undertakings that carry on the same business as a FI in a place outside Hong Kong,

have procedures in place to ensure compliance with, to the extent permitted by the law of that place, requirements similar to those imposed under the AMLO that are applicable to the Company.

15.2 The Company must inform the SFC accordingly and take additional measures to mitigate the risk of ML/TF faced by the branch or subsidiary as a result of any inability to comply with the requirements.

16. Forms

All employees and licensed persons are required to complete Employee Undertaking Form in relation to this Policy when they join the Company and at least annually thereafter.

REVISION HISTORY

Version	Content	Revision Type	Date	Updated By
1.0 (2014)	Adopted from Deacon Compliance Manual	New	04/11/2014	Phyllis Cheung
2.0 (2017)	Revision	Revision	Feb 2017	Catherine Ng
3.0 (2019)	Update contents	Revision	Feb 2019	Derek Hong