Example AML / CTF policies and procedures

Note: *This example policy is a modified version of the example policy set out as "T01 Example policies and procedures" in the AML Procedures Manual published by the Institute for a practice that chooses not to adopt "good practices". The following policies and procedures should be further tailored to the circumstances of your practice before use in practice.*

Practice Unit: _____
Money Laundering Reporting Officer: _____
AML Compliance Officer: _____

A. Policy statement

The practice has a policy of zero tolerance to any involvement in money laundering, including tax evasion, when dealing with the practice's own or our client's affairs. All principals, employees and any sub-contractors used by the practice are therefore required to comply with relevant legislation on anti-money laundering and counter-terrorist financing (see Section I below on staff training and hiring) and the code of ethics of the Hong Kong Institute of Certified Public Accountants (HKICPA) and in particular, Part F of the code, "Guidelines on Anti-Money Laundering and Counter-Terrorist Financing for Professional Accountants". Accordingly, it is the policy of the practice to apply suspicious transaction reporting and financial sanctions related procedures to all clients but all other policies and procedures, in particular the customer due diligence (CDD) and ongoing monitoring procedures specified in Sections F and G below, only to clients, whether new or existing clients, whose engagements involve the following:

(a) buying and selling of real estate;
(b) managing of client money, securities or other assets;
(c) management of bank, savings or securities accounts;
(d) organisation of contributions for the creation, operation or management of companies;
(e) creation, operation or management of legal persons or arrangements;
(f) buying and selling of business entities.
(g) forming corporations or other legal persons;
(h) acting as, or arranging for another person to act as, a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
(i) providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
(j) acting as, or arranging for another person to act as, a trustee of an express trust or similar legal arrangement; or
(k) acting, or arranging for another person to act, as a nominee shareholder for a person other than a corporation whose securities are listed on a recognised stock market.

All principals, employees and any sub-contractors are expected to report any

knowledge or suspicions of money laundering, including tax evasion, to the practice's Money Laundering Reporting Officer (MLRO) in accordance with their statutory obligations.

B. Risk assessment and management

Among the risks facing the practice are:

- Involvement of clients in:
    - Tax evasion such as that specified in Section 82 of the Inland Revenue Ordinance.
    - Fraud or false accounting under Sections 16A or 19 respectively of the Theft Ordinance.
    - Dealing in property known or believed to represent the proceeds of an indictable offence under Section 25(1) of the Organized and Serious Crimes Ordinance ("OSCO",) or drug trafficking under Section 25(1) of the Drug Trafficking (Recovery of Proceeds) Ordinance ("DTROP") (and "property" has a broad definition under the relevant legislation)
    - Various bribery offences under the Prevention of Bribery Ordinance.
    - Breaches of targeted financial sanctions

- Failure to report to the practice's MLRO suspicion or knowledge of such involvement by a principal, employee or sub-contractor of the practice.

- Failure to implement and apply appropriate policies and procedures.

Whilst the likelihood of encountering instances of money laundering other than tax evasion may not be high, principals, staff and sub-contractors must still remain alert to such eventuality.

Principals, staff and sub-contractors must also be alert for complex or unusually large transactions and unusual patterns of transactions which have no apparent economic or visible lawful purpose.

Similarly, principals, staff and sub-contractors must identify situations where the client is using products and transactions which might favour anonymity (such as companies in offshore jurisdictions where transparency may be lacking (e.g., Panama)), recognise the increased risk of money laundering or terrorist financing that these products and transactions produce, and take additional measures, where appropriate.

Where applicable, all know your client forms and customer due diligence forms should record the client's risk profile.

C. Financial sanctions and terrorist financing

The United Nations Sanctions Ordinance (Cap. 537) empowers the Chief Executive of Hong Kong to make regulations to implement sanctions decided by the United Nations ("UN") Security Council. It is an offence to provide or solicit financial or related services to a client who is a person or entity designated in UN sanctions lists.

(a) Sources of the lists of the financial sanctions and terrorist financing

We will refer to the lists maintained by the UN Security Council and its Sanctions Committees [and the United States' Office of Foreign Assets Control ("US OFAC") *(note: not mandatory, see 650.1.6)*]. The entities and individuals on those lists (referred to as designated persons or entities) are subject to financial restrictions. The purpose of the sanctions is to prevent access to and use of funds for terrorism and terrorist purposes.

The UN sanctions consolidated list is available from:
https://www.un.org/securitycouncil/content/un-sc-consolidated-list

[The US OFAC sanctions list is available from: https://sanctionssearch.ofac.treas.gov]

We will also refer to the Anti-money laundering section of the HKICPA website (at: https://www.hkicpa.org.hk/en/Standards-and-regulation/Anti-money-laundering) as well as the HKICPA's monthly technical e-newsletter 'Techwatch' (See http://www.hkicpa.org.hk/en/standards-and-regulations/technical-resources/techwatch/) and the weekly e-circular for information on the latest sanctions lists.

(b) Frequency of conducting name checks

We will conduct a name check of a client and consider, based on a risk approach, extending the check to the client's beneficial owners against the latest UN [and US OFAC] sanction lists before the establishment of a business relationship with that client, regardless of what service is to be provided and perform ongoing screening of our client base regularly thereafter.

We will check for updates of UN sanction lists on a [weekly] [monthly] basis as it [has] [does not have] cases with high money laundering/terrorist financing ("ML /TF") risks.

(c) Reporting obligation

When we come across situations where we suspect that property belongs to a designated person or entity or is otherwise terrorist property, we have a responsibility to stop dealing with the property and report to the Joint Financial Intelligence Unit (see Section D "Reporting of suspicious transactions" for details).

D. Reporting of suspicious transactions

All principals and staff must report knowledge or suspicion of money laundering (including bribery and tax evasion) or terrorist financing, whether it relates to clients or other parties. It is a criminal offence under OSCO, DTROP and also the United Nations (Anti-Terrorism Measures) Ordinance to fail to report where the requisite knowledge or suspicion exists. Before deciding that a potentially suspect activity is not suspicious, you should consider whether the information that you have, taken in its entirety, might provide "reasonable grounds for knowledge or suspicion", i.e. in the eyes of a third

party.

If in doubt, discuss your concerns with the practice's MLRO *[name of MLRO]* or deputy MLRO *[name of deputy MLRO].*

E. Avoiding tipping off

In the event of a report being made to the MLRO or to Joint Financial Intelligence Unit (JFIU), under no circumstances must the client be informed. This means that the client must not be made aware that a report has been made. It also means that the client should not be made aware if an investigation into allegations that a money laundering offence has been committed is being contemplated or carried out.

Generally, disclosure, not only to the client but to any other person, of any matter that is likely to prejudice an investigation, once a report is known or suspected to have been made, is a criminal offence. If it appears to be necessary to disclose the existence of a report or an actual or contemplated investigation to any other person (i.e. not the client) then the MLRO must be consulted before any disclosure is made.

F. Customer due diligence measures (where applicable)

Where applicable, the standard approach to verifying the identity of individuals will be (in order of preference):

For Hong Kong residents:
- A Hong Kong identity card

For others:
- a valid international passport or other travel document;
- a current national (i.e., government or state-issued) identity card bearing the photograph of the individual;
- a current valid national (i.e., government or state-issued) driving licence incorporating photographic evidence of the identity of the applicant, issued by a competent national or state authority;
- other documents as appropriate; or
- online checks carried out through _____(enter name of service).

When carrying out enhanced due diligence (EDD) on individuals, the standard approach should be enhanced with at least one additional piece of evidence of identity.

For new clients, generally before any activity for the client is undertaken standard CDD requires that staff should check that:

1. A risk assessment has been completed and updated where necessary.
2. Up-to-date evidence of identification for the client has been provided.
3. An up-to-date list of principals (directors, partners, trustees, etc.) has been provided.
4. Depending on the risk assessment in '1', the file contains adequate information to satisfy us on the identity of the principals.

5. Where the client has beneficial owners, the details of all beneficial owners are fully recorded and up to date.
6. Depending on the risk assessment in '1', the file contains adequate information to satisfy us that we know who any beneficial owners are.
7. Know-your-client forms exist and are up to date.
8. The client's risk assessment in '1' remains up to date and appropriate.

For pre-existing clients (i.e., those with which/whom the practice established a business relationship before 1 March 2018) CDD measures should be performed when:

(a) a transaction takes place with regard to the client that is unusual or suspicious by virtue of its nature or size, or which is otherwise not consistent with the practice's understanding of the client's business
(b) there is a material change in the way in which the client's business is conducted
(c) there is doubt about the veracity or adequacy of information previously obtained for the purposes of identifying or verifying the identity of the client, or there is a suspicion that the client may be involved in money laundering or terrorist financing.

As part of the practice's CDD procedures, consideration must be given to establishing whether the client is a politically exposed person (PEP) (including whether they are a domestic PEP), or a family member or close associate of a PEP or is included on a sanctions list.

Where a client or beneficial owner is known or subsequently found to be a foreign PEP or is otherwise assessed as being high risk and EDD applied the approval of senior management should be obtained for establishing or continuing a business relationship.

Because of the increased risk involved the practice will not seek to rely on CDD evidence obtained by others. Instead, where we are acting for a mutual client who has already provided adequate CDD to a financial or credit institution, practice of accountants or a lawyer, we should seek certified copies of that information in an attempt to avoid requiring the client to produce identification evidence again.

Similarly, we will caution other practices not to rely just on our CDD information. However, if we are acting for a mutual client we will normally provide the other practice with certified copies should they ask for them.

G. Ongoing monitoring (where applicable)

Where applicable, we will maintain appropriate ongoing monitoring of all client transactions to prevent activities related to money laundering and terrorist financing. This applies even where the client qualifies for simplified customer due diligence (SDD) measures and pre-existing clients.

In future years, steps 1 to 8 in the CDD above will be followed to ensure the information held on clients, beneficial owners, etc. is still appropriate and up to date. This review will be recorded on the relevant sections of the "Know your client" and risk assessment forms. [T05 to T07 in this manual].

In high risk situations, where EDD has been applied, the information will be reviewed annually.

In normal and low risk situations where CDD and SDD have been applied the information will be reviewed every [x years] and [y years], respectively. A review of the risk category of normal and low risk clients will be performed annually.

Trigger events

Apart from conducting periodic on-going monitoring of all clients' transactions following the above timeframes, we will take steps to ensure that the client information obtained for the purposes of CDD is up to date and relevant when any of the following trigger events occurs:

(a) a significant or unusual activity or transaction is to take place;
(b) a material change occurs in a client's ownership and/or activities;
(c) there is a substantial change in client documentation standards; or
(d) we are aware that there is insufficient information about a particular client.

(Note: the above trigger events are examples from section 620.10.7 of the AML Guidelines.)

H. Record keeping

We will keep full records of:

- CDD checks
- details of beneficial ownership
- know-your-client forms
- evidence of staff training
- internal reports to the MLRO
- external reports to JFIU
- the practice's risk assessment
- the practice's compliance checks
- transaction files

to the extent that they are applicable under this policy. All such records will be retained for at least [five] years from the end of the business relationship or the date of the transaction as applicable. The latest records of CDD checks, details of beneficial ownership and know-your-client forms for clients with whom we had a business relationship will be kept for at least [five] years from the end of the relationship.

I. Training and hiring

All relevant staff must receive adequate training on:

- Guidelines on Anti-Money Laundering and Counter-Terrorist Financing for Professional Accountants issued by the HKICPA;

- Applicable sections of the following ordinances:
  - AMLO - Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions and Designated Non-Financial Businesses and Professions) Ordinance (Cap. 615);
  - DTROP - Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405)
  - OSCO - Organised and Serious Crimes Ordinance (Cap. 455);
  - UNATMO - United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575);

- For entities controlled by the practice that offer trust or company services, also the Guideline on Compliance of Anti-Money Laundering and Counter-Terrorist Financing Requirements for Trust or Company Service Providers, issued by the Companies Registry.

They should also be made aware of the practice's policies and procedures to prevent money laundering and combat terrorist financing.

Staff should also be given regular updates on identifying and dealing with suspicious transactions. This will generally be at least annually.

The practice will only engage staff who appear capable of understanding and complying with the practice's policies and procedures on the prevention and detection of money laundering and terrorist financing. New staff should receive introductory training as part of their induction process, unless they can demonstrate adequate knowledge as a result of training in previous practices. Nevertheless, they must be made fully aware of the practice's policies and procedures.

J. Internal control, monitoring and management of compliance

The MLRO and the AML Compliance Office (CO) (who may be the same person) remain responsible for managing the practice's reporting procedures, liaising with JFIU where consent is required, keeping the practice's policies and procedures up-to-date and communicating those policies and procedures to principals, staff and sub-contractors. The CO or MLRO/CO also has overall responsibility for ensuring that the practice's policies and procedures are complied with and are sufficient to meet the requirements of the law and the HKICPA Guidelines. This will involve periodic testing (at least annually) of the practice's systems, including reviewing relevant records to ensure that the policies and procedures are operating properly.

All principals and managers are responsible for ensuring that these policies, together with the accompanying procedures in the manual are followed for their clients.

The staff principal is responsible for ensuring that all principals and relevant staff have received adequate training and are aware of the practice's policies and procedures.

K. Internal communication of such policies and procedures

The practice's procedures are to be found on / at … [specify location, and whether in electronic or paper form].

All principals, staff and sub-contractors will sign an annual “Awareness of money laundering procedures” form to confirm that they have had the relevant training and will comply with the practice’s procedures. [T03 in this manual]