

## **TEMPLATE – FOR REFERENCE ONLY**

According to the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance, Chapter 615, Laws of Hong Kong, it is the responsibility of each financial institution to put in place its own policies, procedures and controls to mitigate the risks of Money Laundering and Terrorist Financing.

Please note that each financial institution has its own features of company structure, staff responsibilities and customer base, etc. Therefore, its Policy Statement may not be the same as others. The attached sample policy statement provides a set of simple and basic policy statement that may be of reference value to a financial institution with comparatively simple structure.

# Policy Statement

On

## Anti-Money Laundering and Counter-Terrorist Financing

My Company's Name:      XXXXX

Address:      XXXXX

Telephone:      XXXXX

Holder of MSO Licence numbered:      XXXXX

### Company Structure:

Sole Proprietor  / Partnership  / Corporation

Number of Staff Employed:      \_\_\_\_\_

### Nature of Money Service:

Money Changing Service  /

Remittance Service  /

Both Money Changing Service and Remittance Service

### Customer Profile:

customer in a business relationship  /

passing trade  /

customer of same sector

customer identity verification: Yes  / No  / Not necessary

Please insert a "v" in the appropriate box

## **(1) Culture and Values**

"My company takes all reasonable measures to ensure that proper safeguards exist to mitigate the risks of Money Laundering (ML) and Terrorist Financing (TF) and to prevent a contravention of any requirement under the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance, Chapter 615, Laws of Hong Kong (AMLO) and the related Guideline on Anti-Money Laundering and Counter-Terrorist Financing (AML Guideline).

(We have made reference to AML Guideline Chapter 2.1 and related requirements)

My company establishes and implements adequate and appropriate Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) policies, procedures and controls taking into account factors including types of customers, products and services offered, delivery channels and geographical locations involved.

(We have made reference to AML Guideline Chapter 2.2 and related requirements)"

## **(2) Allocation of Responsibilities**

"My company's senior management undertakes its assessment of the risks the firm faces and how the ML/TF risks are to be managed and ensures all relevant staff are trained and made aware of the law and their obligations under it.

My company appoints a Compliance Officer (CO) (named \_\_\_\_\_) to act as a focal point for the oversight of all activities relating to the prevention and detection of ML/TF and providing support and guidance to the senior management to ensure that ML/TF risks are adequately managed.

(We have made reference to AML Guideline Chapter 2.14 and related requirements)

My company appoints a Money Laundering Reporting Officer (MLRO) (named \_\_\_\_\_) as a central reference point for reporting suspicious transactions to the Joint Financial Intelligence Unit of the Hong Kong Police Force. The MLRO receives full co-operation from all staff and full access to all relevant documentation enabling him/her to perform his/her functions.

(We have made reference to AML Guideline 2.15 and 7.19 – 7.30 and related requirements)

My company adopts appropriate measures letting frontline staff know the responsible areas and to judge whether a transaction is suspicious and to report them promptly to CO or MLRO."

### **(3) Risk Identification and Assessment**

"My company applies a risk-based approach to assess which customers are to be of higher risks of ML/TF. The followings are some risk factors to be identified:

1. types of customers and behaviour;
2. products and services offered;
3. delivery channels; and
4. customer's business organisation/geographical locations involved  
(see Annex)

My company takes enhanced measures (including customer due diligence and on-going monitoring) to manage those customers with higher risks and knows that simplified measures may be applied to customers with lower risks.

(We have made reference to AML Guideline Chapter 3.1 and related requirements)"

### **(4) Customer Due Diligence (CDD), Record Keeping and Ongoing Monitoring**

"My company should carry out CDD according to the conditions as stated in the AML Guideline Chapter 4.1.9 and Chapter 11.

My company should apply the CDD measures as stated in the AML Guideline Chapter 4.1.3.

My company adopts a risk-based approach to adopt appropriate controls and oversight and accordingly to determine the extent of due diligence to be performed and the level of ongoing monitoring to be applied.

(We have made reference to AML Guideline Chapter 3.2 and related requirements)

My company should monitor the business relationship with our customers under the conditions stated in the AML Guideline Chapter 5.1.

My company should keep the documents obtained in the course of identifying and verifying the identity of the customer and maintain the documents obtained in connection with the transactions for six years.

(We have made reference to AML Guideline Chapter 8.3 – 8.6 and related requirements)"

## **(5) Staff Awareness to AML/CFT**

"My company provides training to all relevant staff (including new staff) in order to ensure they are made aware of the AMLO and providing appropriate AML/CFT training to them regularly facilitating them to recognize suspicious activities/transactions.

(We have made reference to AML Guideline Chapter 9.5 and 9.6 and related requirements)

elaborate how /what /when training is provided to new employees /existing staff

My company will keep training records/records of relevant courses or seminars attended for inspection by regulator."

## **(6) Reporting Suspicious Activities/Transactions**

"My company will give sufficient guidance to all relevant staff to enable them to take appropriate actions when detecting suspicious transactions and to report the suspicious activities/transactions to CO / MLRO as soon as possible.

(We have made reference to AML Guideline Chapter 7.5 and 7.7 and related requirements)"

## **(7) Internal Monitoring System**

"My company carries out regular assessments of the adequacy of our systems and controls to ensure that we manage the ML and TF risks effectively and are compliant with the AMLO and the AML Guideline."

## **(8) Regular Review**

"My company keeps the policies and procedures under regular review and assesses that the risk mitigation procedures and controls are working effectively.

(We have made reference to AML Guideline Chapter 3.7 and related requirements)"

## **Others**

### **(9) Personal Data (Privacy) Ordinance**

"According to Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong, my company shall protect the privacy of the customer / individual with respect to personal data and shall use the personal data for which they were originally collected or a directly related purpose unless the data subject has given prior consent."

|

**(10) Money Changers Ordinance**

"My company shall operate the money changing business according to the provisions of Money Changers Ordinance, Chapter 34, Laws of Hong Kong."

**(11) Cooperation with Regulator and Law Enforcement Agencies**

"My company shall cooperate with the Customs & Excise Department about their routine inspection or investigation. My company will also cooperate with other law enforcement agencies wherever required under the laws of Hong Kong."

"My company shall implement the above policies, procedures and controls to mitigate the risks of money laundering and terrorist financing."

\_\_\_\_\_  
Company Chop and Signature

Name of Signatory: \_\_\_\_\_

Date: \_\_\_\_\_

### Possible high risk situations for MSOs

The list below includes examples of the types of risk factors that may be regarded as involving high risk in money laundering or terrorist financing.

#### Risk factors – customer types and behaviour

- Customers with businesses that handle large amount of cash
- Customers with complex business ownership structures with the potential to conceal underlying beneficiaries
- Customers who are in a public position which could create a risk of exposure to the possibility of corruption
- Customers based in or conducting business in, or through, a high-risk jurisdiction, or a jurisdiction with known higher levels of corruption, organised crime or drug production/distribution
- Customers who are not local to the business
- New customers carrying out large transactions
- Customers carrying out regular large transactions
- A number of transactions below the amount requiring ID checks carried out by the same customer within a short span of time
- A number of customers sending money to the same individual
- Non face-to-face customers
- Situations where the source of funds cannot be easily verified
- Customers that are carrying out transactions or business with countries where the FATF has highlighted deficiencies in systems to prevent money laundering and terrorist financing

#### Risk factors – product/transaction types

- Complex or unusually large transactions
- Unusual patterns of transactions which have no apparent economic or visible lawful purpose
- Uncharacteristic transactions which are not in keeping with the customer's known activities
- A sudden increase in business from an existing customer
- A high level of transactions for amounts just below the amount requiring ID checks
- Peaks of activity at particular locations or at particular times

### **Risk factors – delivery channels**

- Sales through online, postal or telephone channels (non-face-to-face)
- Business sold through intermediaries – business relationship between customer and MSO may become indirect

### **Risk factors – business organisation/geographical area of operation**

- Large number of branches
- Large number of agents
- Geographical locations of operation
- Number of employees and turnover of staff
- Money sent to or received from areas known to have high levels of criminality or terrorist activity

Note: This list is not exhaustive. MSOs will need to add any other relevant risk factors which are appropriate in individual and particular case.