TEMPLATE – FOR REFERENCE ONLY

Under the Anti-Money Laundering and Counter-Terrorist Financing Ordinance, Chapter 615, Laws of Hong Kong, it is the responsibility of each Money Service Operator (MSO) to establish and maintain effective policies, procedures and controls to mitigate the risks of money laundering and terrorist financing.

Please note that each MSO has its own features of company structure, staff responsibilities, customer base and particular risk profiles, 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 an MSO with comparatively simple structure.

Policy Statement on
Anti-Money Laundering and
Counter-Financing of Terrorism

Company Name : _____

Principal Address : _____

Telephone Number : _____

MSO Licence Number : _____

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 ☐ **/**

Walk-in customer ☐ **/**

Customer of same sector ☐

Please insert a "√" in the appropriate box

(1) Culture and Values

"This 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 Ordinance, Chapter 615, Laws of Hong Kong (AMLO) and the related Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (AML Guideline).
(Reference has been made to AML Guideline Paragraph 3.1 and related requirements)

This company adopts a risk-based approach (RBA) in the design and implementation of the Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) policies, procedures and controls (AML/CFT Systems) with a view to managing and mitigating ML/TF risks.
(Reference has been made to AML Guideline Paragraphs 2.1, 3.1 and related requirements)"

(2) Risk Identification, Institutional ML/TF Risk Assessment (IRA) and Customer Risk Assessment (CRA)

"This company conducts an IRA to identify, assess and understand the ML/TF risks in relation to:

1. the customers;
2. the countries or jurisdictions the customers are from or in ;
3. the countries or jurisdictions this company has operations in; and
4. the products, services, transactions and delivery channels (see Annex)

(Reference has been made to AML Guideline Paragraphs 2.2 to 2.9 and related requirements)

This company conducts a CRA to assess the ML/TF risks associated with the customers in order to differentiate between the risks of individual customers and business relationships, as well as apply appropriate and proportionate customer due diligence (CDD) and risk mitigating measures.

This company applies enhanced due diligence measures and on-going monitoring to manage those customers with higher risks and knows that simplified due diligence measures may be applied to customers with lower risks.
(Reference has been made to AML Guideline Paragraphs 2.12 to 2.15, 4.8, 4.9 and related requirements)"

(3) Allocation of Responsibilities

"This 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.

This 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.
(Reference has been made to AML Guideline Paragraphs 3.5 to 3.9 and related requirements)

This company appoints a Money Laundering Reporting Officer (MLRO) (named_____) as a central reference point for reporting suspicious transactions to the Joint Financial Intelligence Unit (JFIU) of the Hong Kong Police Force. The MLRO is of a sufficient level of seniority and authority within the company and capable of accessing all relevant documentation enabling him/her to discharge his/her responsibilities effectively.

(Reference has been made to AML Guideline Paragraphs 3.5 to 3.10 and 7.9 to 7.23 and related requirements)

This company adopts appropriate measures to enable frontline staff to know their responsibilities, to judge whether a transaction is suspicious and to report suspicion to CO or MLRO in a timely manner."

(4) CDD, Record Keeping and Ongoing Monitoring

"This company carries out CDD measures under the conditions as stated in the AML Guideline Paragraph 4.2.1 and Chapter 11.

This company applies the CDD measures as stated in the AML Guideline Paragraph 4.1.3.

This company adopts a RBA 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.
(Reference has been made to AML Guideline Chapter 2 and related requirements)

This company monitors the business relationship with the customers under the conditions stated in the AML Guideline Paragraph 5.1. This company also reviews all customers that present high ML/TF risks annually or more frequently if deemed necessary to ensure the CDD information retained remains up-to-date and relevant.
(Reference has been made to AML Guideline Paragraphs 5.1 to 5.3 and related requirements)

This company keeps the documents obtained in the course of identifying and verifying the identity of the customer and maintains the documents obtained in connection with the transactions for at least 5 years.
(Reference has been made to AML Guideline Paragraphs 8.3 to 8.6 and related requirements)"

(5) Combating TF and Financing of Proliferation of Weapons of Mass Destruction (PF)

"This company establishes and maintains effective policies, procedures and controls to ensure compliance with the relevant regulations and legislation on TF, financial sanctions and PF. The legal and regulatory obligations of this company and those of the staff are well understood and adequate guidance and training are provided to the staff.

This company maintains a database or subscribe to a database maintained by a third party service provider of names and particulars of terrorists and designated parties, which consolidates the various lists that have been made known to this company and take appropriate measures (e.g. conduct sample testing periodically) to ensure the completeness and accuracy of the database. An effective screening mechanism is implemented to avoid establishing business relationship or conducting transactions with any terrorist suspects and possible designated parties.
(Reference has been made to AML Guideline Chapter 1, Chapter 6 and related requirements)"

(6) Staff Awareness of AML/CFT

"This company provides ongoing training to all relevant staff (including new staff) in order to ensure they are made aware of the AMLO. This company also provides appropriate AML/CFT training to them regularly facilitating them to identify suspicious activities / transactions.
(Reference has been made to AML Guideline Paragraphs 9.2 and 9.4 and related requirements)

This company will keep training records/records of relevant courses or seminars attended for a minimum of 3 years and for inspection by regulator.
(Reference has been made to AML Guideline Paragraph 9.7 and related requirements)"

(7) Reporting Suspicious Activities/Transactions

"This 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 MLRO as soon as possible.
(Reference has been made to AML Guideline Paragraphs 7.5 and 7.10 and related requirements)"

(8) Internal Monitoring System

"This company carries out assessments of the adequacy of the systems and controls on a regular basis to ensure that this company manage the ML and TF risks effectively and are compliant with the AMLO and the AML Guideline."

(9) Regular Review

"This company establishes an independent audit function to keep the AML/CFT Systems under regular review and assesses whether the risk mitigation procedures and controls are working effectively.
(Reference has been made to AML Guideline Paragraphs 3.11 to 3.13 and related requirements)"

Others

(10) Personal Data (Privacy) Ordinance

"Under the Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong, this 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."

(11) Money Changers Ordinance

"This company shall operate the money changing business in accordance with the provisions of Money Changers Ordinance, Chapter 34, Laws of Hong Kong."

(12) Cooperation with Regulator and Law Enforcement Agencies

"This company shall cooperate with the Customs & Excise Department about their routine inspection or investigation. This company will also cooperate with other law enforcement agencies wherever required under the laws of Hong Kong. (Reference has been made to AML Guideline Paragraphs 7.31 to 7.35 and related requirements)"

"This company shall implement the above AML/CFT Systems to mitigate the ML and TF risks."

_____
Company Chop and Signature

Name of Signatory: _____

Date: _____

Annex

Possible high-risk situations for MSOs

The list below includes examples of the types of risk factors that may present a high risk of 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 large transactions regularly
- 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
- Transactions which are not consistent with the MSO's knowledge of the customer's business
- A sudden increase in business from an existing customer
- A high level of transactions for amounts just below the amount requiring ID checks
- A large quantity of transactions carried out 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 a high level 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.