恒基兆業地產有限公司
HENDERSON LAND DEVELOPMENT COMPANY LIMITED
Incorporated in Hong Kong with limited liability
(Stock Code : 12)

# Anti-Money Laundering and Counter-Terrorist Financing Policy

## 1. FOREWORD

Henderson Land Development Company Limited (the "**Company**", together with its subsidiaries, collectively referred to as the "**Group**") is committed to combat money laundering ("**ML**") and terrorist financing ("**TF**") and has put in place this policy (the "**Policy**") to comply with the requirements of the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Chapter 615 of the laws of Hong Kong) (the "**AMLO**"). The Policy is revisited periodically and amended from time to time based on prevailing industry standards and the applicable rules and regulations. All directors, senior management and staff of the Group, in particular, those staff members who have direct dealings with customers in the first instance or handle transactions settlement, are required to get familiar with the Policy.

## 2. DEFINITIONS OF ML AND TF

### 2.1 Money Laundering

The term "**money laundering**" is defined in section 1 of Part 1 of Schedule 1 to the AMLO and 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.

There are three common stages in the laundering of money, and they frequently involve numerous transactions. The Company should 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

The term "**terrorist financing**" is defined in section 1 of Part 1 of Schedule 1 to the AMLO and means:

(a) the provision or collection, by any means, directly or indirectly, of any property:-
   (i) with the intention that the property be used; or
   (ii) 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.

## 2.3 Criminal Offences

Both ML and TF are criminal offences under the laws of Hong Kong. Under the Drug Trafficking (Recovery of Proceeds) Ordinance (Chapter 405 of the laws of Hong Kong) ("**DTROP**") and the Organized and Serious Crimes Ordinance (Chapter 455 of the laws of Hong Kong) ("**OSCO**"), a person commits the offence of ML if he deals with any property, including money, which he knows or has reasonable grounds to believe to be proceeds of drug trafficking or an indictable offence. Under the United Nations (Anti-Terrorism Measures) Ordinance (Chapter 575 of the laws of Hong Kong) ("**UNATMO**"), a person commits the offence of TF if he provides or collects any property knowing or with the intention that such property will be used to commit a terrorist act.

# 3. AML/CTF SYSTEMS

To fulfil obligations under the AMLO, the Group should assess the ML/TF risk of its practices and businesses, and develop and implement policies, procedures and

controls ("**AML/CTF systems**") on:

(a) risk assessment;
(b) customer due diligence measures;
(c) continuous monitoring of customers;
(d) suspicious transactions reporting;
(e) record keeping; and
(f) staff training.

Each department of the Company should be responsible for establishing and implementing its own AML/CTF systems (including customer acceptance policies and procedures) taking into account factors including services offered, types of customers and geographical locations involved. The department heads have to ensure their AML/CTF systems are capable of mitigating the ML/TF risks identified.

The head of Audit Department is designated as the Group's Compliance Officer who is responsible for the Group's overall compliance with the anti-money laundering ("**AML**")/counter-terrorist financing ("**CTF**") requirements and acts as the focal point within the Group for the oversight of all activities relating to the prevention and detection of ML/TF. The Compliance Officer will also assume the role of the Money Laundering Reporting Officer who is responsible for reviewing suspicious transactions identified by each department and determine whether or not such transactions should be reported to the Joint Financial Intelligence Unit ("**JFIU**")[1].

As regards joint ventures in the People's Republic of China ("**PRC**") where the joint venture partners control the daily operations, the joint venture partners should be responsible for the local AML/CTF matters. For all other operations in the PRC where the Group is directly responsible, training of the PRC staff for AML/CTF has to be arranged by the relevant department heads.

## 4. RISK ASSESSMENT

As regards AML/ CTF, ML/TF can be performed in many ways and even regular business operations may be used for ML/TF. The Company has, therefore, adopted a risk-based approach for combating ML/TF in formulating the Policy, proportionate to those risks faced by the relevant business of the Group.

Under this risk-based approach, each department of the Company should assess the risks that its practice or business may be used for ML/TF, and put in place appropriate measures to manage and mitigate those risks.

The general principle is that where customers are assessed to be of higher ML/TF

[1] The JFIU manages the suspicious transaction reporting regime for Hong Kong and its role is to receive, analyse suspicious transaction reports and to disseminate them to the appropriate law enforcement agencies in or outside Hong Kong, or financial intelligence units worldwide.

risks, the relevant department should take enhanced measures to manage and mitigate those risks, and where the risks are lower, simplified measures may be applied. In determining the risk rating of customers, the following factors may be considered:

(a) customer risk (e.g. resident or non-resident, type of customers, occasional or one-off, legal person structure, types of politically exposed person, types of occupation, etc.);
(b) country/geographic risk (e.g. customers with residence in or connection with high-risk jurisdictions e.g. countries identified by the Financial Action Task Force ("**FATF**")[2] as having deficient systems to prevent ML/TF, etc);
(c) service risk (e.g. services that inherently have provided more anonymity, large cash payments, payments received from unassociated or unknown third parties, etc.); and
(d) delivery channel risk (e.g. on-line or other non face-to-face, cross boundary service etc.).

Each department should consider all the relevant risk factors before determining the appropriate risk level and type of mitigation to be applied, and should keep records and document their risk assessment.

## 5. CUSTOMER DUE DILIGENCE ("CDD")

Each department should conduct CDD to ensure that the identities of all customers are verified to a reasonable level of certainty. The CDD information may be used as an important tool to recognise whether there are grounds for ML/TF activities. CDD is particularly relevant to those departments which have direct dealings with customers in the first instance like the Sales Department and Portfolio Leasing Department.

### 5.1 CDD Measures

The following CDD measures should be adopted:

(a) identifying the customer and verifying the customer's identity using documents, data or information from reliable and independent source;
(b) where there is a beneficial owner in relation to the customer, identifying the beneficial owner (i.e. an individual who owns or controls, directly or indirectly, 25% or more interest in a corporation, partnership or trust property) and take reasonable measures to verify the beneficial owner's identity;
(c) obtaining information on the purpose and intended nature of the business relationship (if any) established with the Group; and
(d) if a person purports to act on behalf of the customer:
    (i) identifying the person and taking reasonable measures to verify the

[2] FATF is an inter-governmental body established in 1989 that sets international standards on combating ML/TF.

person's identity using documents, data or information from reliable and independent source; and

(ii) verifying the person's authority to act on behalf of the customer.

## (A) Identification and verification of a customer

The identification information required varies between different kinds of person which can be divided into the following categories:

### *(1) Customer that is a natural person*

For a customer that is a natural person, the Company shall identify the customer by obtaining at least the following identification information:

(a) full name;
(b) date of birth;
(c) nationality; and
(d) unique identification number (e.g. identity card number or passport number) and document type.

In verifying the identity of a customer that is a natural person, the Company should verify the name, date of birth, unique identification number and document type of the customer. The Company should do so by reference to documents, data or information provided by a reliable and independent source, examples of such documents, data or information include:

(a) Hong Kong identity card or other national identity card bearing the individual's photograph;
(b) valid travel document (e.g. unexpired passport); or
(c) other relevant documents, data or information provided by a reliable and independent source (e.g. document issued by a government body).

The Company should retain a copy of the individual's identification document for record.

### *(2) Customer that is a legal person*

For a customer that is a legal person, the Company should identify the customer by obtaining at least the following identification information:

(a) full name;
(b) date of incorporation, establishment or registration;
(c) place of incorporation, establishment or registration (including address of registered office);
(d) unique identification number (e.g. incorporation number or business registration number) and document type; and
(e) principal place of business (if different from the address of registered office).

In verifying the identity of a customer that is a legal person, the Company should normally verify its name, legal form, current existence (at the time of verification), and powers that regulate and bind the legal person. The Company should do so by reference to documents, data or information provided by a reliable and independent source, examples of such documents, data or information include:

(a) certificate of incorporation;
(b) record of companies registry;
(c) certificate of incumbency;
(d) certificate of good standing;
(e) record of registration;
(f) partnership agreement or deed;
(g) constitutive document; or
(h) other relevant documents, data or information provided by a reliable and independent source (e.g. document issued by a government body).

***(3) Customer that is a trust or other similar legal arrangement***

The Company shall also regard the trustee as its customer if the trustee enters into a business relationship or carries out occasional transactions on behalf of the trust, which is generally the case if the trust does not possess a separate legal personality. In such a case, the Company should identify and verify the identity of the trustee in line with the identification and verification requirements for a customer that is a natural person or, where applicable, a legal person.

For a customer that is a trust or other similar legal arrangement, the Company shall identify the customer by obtaining at least the following identification information:

(a) the name of the trust or legal arrangement;
(b) date of establishment or settlement;
(c) the jurisdiction whose laws govern the trust or legal arrangement;
(d) unique identification number (if any) granted by any applicable official bodies and document type (e.g. tax identification number or registered charity or non-profit organisation number); and
(e) address of registered office (if applicable).

In verifying the identity of a customer that is a trust or other similar legal arrangement, the Company should normally verify its name, legal form, current existence (at the time of verification) and powers that regulate and bind the trust or other similar legal arrangement. The Company should do so by reference to documents, data or information provided by a reliable and independent source, examples of such documents, data or information include:

(a) trust deed or similar instrument;

(b) record of an appropriate register in the relevant country of establishment;
(c) written confirmation from a trustee acting in a professional capacity;
(d) written confirmation from a lawyer who has reviewed the relevant instrument; or
(e) written confirmation from a trust company which is within the same group as the Company, if the trust concerned is managed by that trust company.

## (B) Identification and verification of a beneficial owner

A beneficial owner is normally a natural person who ultimately owns or controls the customer or on whose behalf a transaction or activity is being conducted. The Company must identify any beneficial owner in relation to a customer, 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. However, the verification requirements under the AMLO are different for a customer and a beneficial owner.

### *(1) Beneficial owner in relation to a natural person*

In respect of a customer that is a natural person, there is no requirement on the Company to make proactive searches for beneficial owners of the customer in such a case, but they should make appropriate enquiries where there are indications that the customer is not acting on his own behalf.

### *(2) Beneficial owner in relation to a legal person*

The AMLO defines beneficial owner in relation to a corporation as:

(a) 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; or
(b) if the corporation is acting on behalf of another person, means the other person.

For a customer that is a legal person, the Company identify any natural person who ultimately has a controlling ownership interest (i.e. more than 25%) in the legal person and any natural person exercising control of the legal person or its management, and take reasonable measures to verify their identities. If there is no such natural person (i.e. no natural person falls within the definition of beneficial owners), the Company should identify the relevant natural persons who hold the position of senior managing official in the legal person, and take reasonable measures to verify their identities.

### *(3) Beneficial owner in relation to a trust or other similar legal arrangement*

The AMLO defines the beneficial owner, in relation to a trust as:

(a) an individual who is entitled to a vested interest in more than 25% 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 settlor of the trust;
(c) a protector or enforcer of the trust; or
(d) an individual who has ultimate control over the trust.

For trusts, the Company should identify the settlor, the protector (if any), the enforcer (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate control over the trust (including through a chain of control or ownership), and take reasonable measures to verify their identities. For other similar legal arrangements, the Company should identify any natural person in equivalent or similar positions to beneficial owner of a trust as stated above and take reasonable measures to verify the identity of such person. If a trust or other similar legal arrangement is involved in a business relationship and the Company does not regard the trustee (or equivalent in the case of other similar legal arrangement) as its customer (e.g. when a trust appears as part of an intermediate layer), the Company should also identify the trustee (or equivalent) and take reasonable measures to verify the identity of the trustee (or equivalent) so that the Company is satisfied that it knows who that person is.

For a beneficiary of a trust designated by characteristics or by class, the Company shall obtain sufficient information concerning the beneficiary to satisfy the Company that it will be able to establish the identity of the beneficiary at the time of payout or when the beneficiary intends to exercise vested rights.

## (C) Ownership and control structure

Where a customer is not a natural person, the Company shall understand its ownership and control structure, including identification of any intermediate layers (e.g. by reviewing an ownership chart of the customer). The objective is to follow the chain of ownerships to the beneficial owners of the customer.

Similar to a corporation, a trust or other similar legal arrangement can also be part of an intermediate layer in an ownership structure, and should be dealt with in similar manner to a corporate being part of an intermediate layer.

Where a customer has a complex ownership or control structure, the Company should obtain sufficient information for the Company to satisfy itself that there is a legitimate reason behind the particular structure employed.

**(D) Identification and verification of a person purporting to act on behalf of the customer**

If a person purports to act on behalf of the customer, the Company must:

(a) identify the person and take reasonable measures to verify the person's identity by reference to documents, data or information provided by a reliable and independent source:
  (i) a governmental body;
  (ii) the relevant authority;
  (iii) an authority in a place outside Hong Kong that performs functions similar to those of the relevant authority; or
  (iv) any other reliable and independent source that is recognised by the relevant authority; and
(b) verify the person's authority to act on behalf of the customer.

The Company should verify the authority of each person purporting to act on behalf of the customer by appropriate documentary evidence (e.g. board resolution or similar written authorisation).

**(E) Purpose and intended nature of business relationship**

Unless the purpose and intended nature of the business relationship are obvious, the Company shall obtain satisfactory information from all new customers as to the intended purpose and reason for establishing the business relationship, and record the information on the account opening documentation. The information obtained by the Company should be commensurate with the risk profile of the customers and the nature of the business relationships. Information that might be relevant may include:

(a) nature and details of the customer's business/occupation/employment;
(b) the anticipated level and nature of the activity that is to be undertaken through the business relationship (e.g. what the typical transactions are likely to be);
(c) location of customer;
(d) the expected source and origin of the funds to be used in the business relationship; and
(e) initial and ongoing source(s) of wealth or income.

## 5.2 Timing

(a) CDD process must be conducted before establishing any business relationship or carrying out an occasional transaction that involves an amount of an

aggregate value of HK$120,000 or above.

(b) Any department that carries out verification after establishing a business relationship with a customer must complete the verification as soon as reasonably practicable.

**Delayed identity verification during the establishment of a business relationship**

The Company shall verify the identity of a customer and any beneficial owner of the customer before or during the course of establishing a business relationship or conducting transactions for occasional customers. However, the Company may, exceptionally, verify the identity of a customer and any beneficial owner of the customer after establishing the business relationship, provided that:

(a) any risk of ML/TF arising from the delayed verification of the customer's or beneficial owner's identity can be effectively managed;
(b) it is necessary not to interrupt the normal conduct of business with the customer; and
(c) verification is completed as soon as reasonably practicable.

If the Company allows verification of the identity of a customer and any beneficial owner of the customer after establishing the business relationship, it should adopt appropriate risk management policies and procedures concerning the conditions under which the customer may utilise the business relationship prior to verification. These policies and procedures should include:

(a) establishing a reasonable timeframe for the completion of the identity verification measures and the follow-up actions if exceeding the timeframe (e.g. to suspend or terminate the business relationship);
(b) placing appropriate limits on the number, types, and/or amount of transactions that can be performed;
(c) monitoring of large and complex transactions being carried out outside the expected norms for that type of relationship;
(d) keeping senior management periodically informed of any pending completion cases; and
(e) ensuring that funds are not paid out to any third party. Exceptions may be made to allow payments to third parties subject to the following conditions:
    (i) there is no suspicion of ML/TF;
    (ii) the risk of ML/TF is assessed to be low;
    (iii) the transaction is approved by senior management, who should take account of the nature of the business of the customer before approving the transaction; and
    (iv) the names of recipients do not match with watch lists, such as those for terrorist suspects and politically exposed person.

## 5.3 Failure to complete CDD

Where a department is unable to complete the CDD process, the relevant department:

(a) must not establish a business relationship or carry out any occasional transaction with that customer;
(b) must terminate the business relationship as soon as reasonably practicable if it has already established a business relationship with that customer; and
(c) should assess whether failure to complete the CDD process provides grounds for knowledge or suspicion of ML/TF and consider reporting the case to the Compliance Officer to follow up.

## 5.4 Simplified CDD ("SCDD")

Pursuant to section 4(3) of Schedule 2 to the AMLO, the Company may apply SCDD if the customers is:

(a) an financial institutions as defined in the AMLO;
(b) an institution that-
  (i) is incorporated or established in an equivalent jurisdiction;
  (ii) carries on a business similar to that carried on by the Company as defined in the AMLO;
  (iii) has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2; and
  (iv) is supervised for compliance with those requirements by an authority in that jurisdiction that performs functions similar to those of any of the relevant authorities;
(c) a corporation listed on any stock exchange;
(d) an investment vehicle 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-
  (i) an financial institutions as defined in the AMLO;
  (ii) an institution incorporated or established in Hong Kong, or in an equivalent jurisdiction that-
    i. has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2; and
    ii. is supervised for compliance with those requirements.
(e) the Government or any public body in Hong Kong; or
(f) the government of an equivalent jurisdiction or a body in an equivalent jurisdiction that performs functions similar to those of a public body.

Where SCDD applies, the department concerned is not required to identify and verify the ultimate beneficial owner. Nevertheless, other aspects of customer

due diligence must be undertaken.

### 5.5 Enhanced CDD ("ECDD")

Section 15 of Schedule 2 to the AMLO provides that in a situation that by its nature may present a high risk of ML/TF, the Company must, before establishing a business relationship or continuing an existing business relationship, among others, apply all the following ECDD measures:

(a) obtaining approval from the senior management; and
(b) either taking reasonable measures to establish the customer's or the beneficial owner's source of wealth and the source of funds that will be/are involved in the business relationship or taking additional measures to mitigate the risk of ML/TF.

Examples of additional measures, for illustration purposes, may include:

(a) obtaining additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.) and updating more regularly the identification data of customer and beneficial owner;
(b) obtaining additional information on the intended nature of the business relationship (e.g. anticipated account activity);
(c) obtaining information on the reasons for intended or performed transactions; or
(d) increasing the number and timing of the controls applied and selecting patterns of transactions that need further examination.

High-risk situations for which ECDD apply include:

(a) customer not physically present for identification purposes;
(b) customer or his beneficial owner being a politically exposed person, an individual who is or has been entrusted with a prominent public function in a place outside the PRC (e.g. a head of state, head of government, senior politician, etc.);
(c) customer from or transaction connected with a jurisdiction that does not adopt or insufficiently adopts the recommendations issued by FATF; and
(d) any situation that by its nature may present a higher risk of ML/TF.

## 6. CONTINUOUS MONITORING

Each department must continuously monitor the business relationship with a customer by:

(a) reviewing from time to time information relating to the customer that have been obtained for the purpose of complying with CDD requirements to ensure that

they are up-to-date and relevant;
(b) conducting appropriate scrutiny of transactions carried out for the customer to ensure that they are consistent with the Group's knowledge of the customer and the customer's business, risk profile and source of funds; and
(c) identifying transactions that are complex, unusually large in amount or of an unusual pattern or that have no apparent economic or lawful purpose, and examining the background and purposes of those transactions and recording his findings in writing.

The Audit Department should review the overall implementation of the AML/CTF controls to ensure effectiveness. The frequency and extent of the review should be commensurate with the risks of ML/TF and the size of the Group's business.

**Transaction monitoring systems and processes**

The Audit Department shall establish and maintain adequate systems and processes (e.g. the use of large transactions exception reports which help the Company to stay apprised of operational activities) to monitor transactions. The design, degree of automation and sophistication of transaction monitoring systems and processes should be developed appropriately having regard to the following factors:

(a) the size and complexity of its business;
(b) the ML/TF risks arising from its business;
(c) the nature of its systems and controls;
(d) the monitoring procedures that already exist to satisfy other business needs; and
(e) the nature of the products and services provided (which includes the means of delivery or communication).

The Company shall ensure that the transaction monitoring systems and processes can provide all relevant staff who are tasked with conducting transaction monitoring and investigation with timely and sufficient information required to identify, analyse and effectively monitor customers' transactions.

In designing transaction monitoring systems and processes, including (where applicable) setting of parameters and thresholds, the Audit Department should take into account the transaction characteristics, which may include:

(a) the nature and type of transactions (e.g. abnormal size or frequency);
(b) the nature of a series of transactions (e.g. structuring a single transaction into a number of cash transactions);
(c) the counterparties of transactions;
(d) the geographical origin/destination of a payment or receipt; and
(e) the customer's normal account activity or turnover.

## 7. CASH TRANSACTIONS AND TRANSFERS TO THIRD PARTIES

Where cash transactions or transfers to third parties are being proposed by a customer and such requests do not accord with the customer's known pattern of practice, the relevant staff member should be cautious and makes relevant further enquiries. The relevant staff member, having made the necessary enquiries, does not consider the cash transaction or third party transfer reasonable, he/she must escalate the case to the department head who should consider referring the case to the Compliance Officer. This is particularly relevant to those departments which frequently handle transactions involving cash settlement, such as the Sales Department, Commercial and Industrial Properties Department, Portfolio Leasing Department and the Cashier Department.

## 8. REPORTING SUSPICIOUS TRANSACTIONS

When conducting CDD and continuous monitoring process, the staff identify or suspect that a transaction is related to ML/TF activity or a property in the transaction represents the proceeds linked to ML/TF activity, they must escalate the case to their respective department heads who should consider reporting such case to the Compliance Officer. The Compliance Officer should make a suspicious transactions report to the JFIU if necessary.

The JFIU will acknowledge receipt of a suspicious transaction report made by a person under section 25A of both the DTROP and the OSCO, and section 12 of the UNATMO. If there is no need for imminent action e.g. the issue of a restraint order on an account, consent will usually be given under the provisions of section 25A(2) of both the DTROP and the OSCO, and section 12(2B)(a) of the UNATMO. An example of such a letter is given at the Appendix to this Policy. On the contrary, consent will not be given by JFIU for dealing with the funds as per the sample letter contained in the Appendix to this Policy.

## 9. TIPPING OFF

It is an offence for a person, knowing or suspecting that a disclosure has been made to the JFIU, to reveal to any other person any matter which is likely to prejudice any investigation. Therefore, the department concerned and the Compliance Officer should keep the relevant case strictly confidential.

## 10. RECORD KEEPING

10.1 In respect of each customer, the department concerned must keep:

(a) the original or a copy of the documents, and a record of the data and information for identifying and verifying the identity of the customer or any beneficial owner of the customer;
(b) the original or a copy of the files relating to the customer's business

relationship and business correspondence with the customer and any beneficial owner of the customer; and

(c) the records as referred to in (a) and (b) above throughout the continuance of the business relationship with the customer and for a period of at least 5 years beginning on the date on which the business relationship ends.

10.2 In respect of each transaction, the department concerned must keep:

(a) the original or a copy of the documents, and a record of the data and information obtained in connection with the transaction; and

(b) the relevant records for a period of at least 5 years beginning on the date on which the transaction is completed.

10.3 Copies of any suspicious transaction reports, together with any supporting documentation shall be kept for 5 years form the date of filing with the relevant government authority.

## 11. STAFF TRAINING

Focused training for appropriate staff or groups of staff on supervisory level will enable the Group to implement the AML/CTF systems effectively.

The heads of each department should organise appropriate training and seminars catering for such department's learning needs. In particular, the front-line staff dealing with customers directly and the back-office staff handling settlements or payments process should be given continuous training to keep abreast of AML/CTF requirements/developments. The Compliance Officer, being also the Money Laundering Reporting Officer, should receive higher level training covering all aspects of Hong Kong's AML/CTF regime.

All staff members of the Group should attend relevant training and their attendance records of participating in AML/CTF training should be sent to the Compliance Officer for records.

November 2020

**APPENDIX**

CONFIDENTIAL 機密

Joint Financial Intelligence Unit

G.P.O. Box No. 6555, General Post Office,
Hong Kong

**Tel : 2866 3366 Fax : 2529 4013**
**Email : jfiu@police.gov.hk**

**Date: 2012-XX-XX**

Money Laundering Reporting Officer,
XXXXXXX.

**Fax No. : XXXX XXXX**

Dear Sir/Madam,

**Suspicious Transaction Report ("STR")**

| JFIU No. | Your Reference | Date Received |
|---|---|---|
| XX | XX | XX |

I acknowledge receipt of the above mentioned STR made in accordance with the provisions of section 25A(1) of the Drug Trafficking (Recovery of Proceeds) Ordinance (Cap 405) / Organized and Serious Crimes Ordinance (Cap 455) and section 12(1) of the United Nations (Anti-Terrorism Measures) Ordinance (Cap 575).

Based upon the information currently in hand, consent is given in accordance with the provisions of section 25A(2) of the Drug Trafficking (Recovery of Proceeds) Ordinance and Organized / Serious Crimes Ordinance, and section 12(2) of United Nations (Anti-Terrorism Measures) Ordinance.

Should you have any queries, please feel free to contact Senior Inspector Mr. XXXXX on (852) 2860 XXXX.

Yours faithfully,

(XXXXX)
*for* Head, Joint Financial Intelligence Unit

**APPENDIX**

CONFIDENTIAL 機密

PERSONAL DATA

Joint Financial Intelligence Unit

G.P.O. Box No. 6555, General Post Office,
Hong Kong
**Tel : 2866 3366 Fax : 2529 4013**
**Email : jfiu@police.gov.hk**

Our Ref. :
Your Ref :

2012-XX-XX

Money Laundering Reporting Officer,
XXXXXX
Fax No. : XXXX XXXX

Dear Sir/Madam,

**Drug Trafficking (Recovery of Proceeds) Ordinance/**
**Organized and Serious Crimes Ordinance**

I refer to your disclosure made to JFIU under the following reference:

| JFIU No. | Your Reference | Dated |
|---|---|---|
| XX | XX | XX |

Your disclosure is related to an investigation of 'XXXXX' by officers of XXXXX under reference XXXXX.

In my capacity as an Authorized Officer under the provisions of section 25A(2) of the Organized and Serious Crimes Ordinance, Cap. 455 ("OSCO"), I wish to inform you that you do NOT have my consent to further deal with the funds in the account listed in Annex A since the funds in the account are believed to be crime proceeds.

As you should know, dealing with money known or reasonably believed to represent the proceeds of an indictable offence is an offence under section 25 of OSCO. This information should be treated in strict confidence and disclosure of the contents of this letter to any unauthorized

**APPENDIX**

CONFIDENTIAL 機密

person, including the subject under investigation which is likely to prejudice the police investigation, may be an offence under section 25A(5) OSCO. Neither the accounts holder nor any other person should be notified about this correspondence.

If any person approaches your institution and attempts to make a transaction involving the account, please ask your staff to immediately contact the officer-in-charge of the case, and decline the transaction. Should the account holder or a third party question the bank as to why he cannot access the funds in the accounts he should be directed to the officer-in-charge of the case, without any further information being revealed.

Please contact the officer-in-charge, Inspector XXXXX on XXXX XXXX or the undersigned should you have any other query or seek clarification of the contents of this letter.

Yours faithfully,

( XXXXXXX )
Superintendent of Police
Head, Joint Financial Intelligence Unit

c.c. OC Case

**APPENDIX**

CONFIDENTIAL 機密

**Annex A**

| S/N | Account holder | Account Number |
|---|---|---|
| 1. | | |