WHARF

Established 1886

THE WHARF (HOLDINGS) LIMITED

Stock code: 0004

ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING POLICY

Anti-Money Laundering and Counter-Terrorist Financing Policy (the "Policy")

I. Introduction

1. The Wharf (Holdings) Limited (the "Company") and its subsidiaries (collectively, the "Group") are committed to upholding high standards of business ethics and corporate governance. The Group has zero tolerance towards any involvement in money laundering ("ML") and terrorist financing ("TF") in its operations and complies with all relevant anti-money laundering ("AML"), counter-terrorist financing ("CTF") and applicable sanction laws and regulations in the jurisdictions in which the Group operates.

2. Violation of AML and CTF laws could lead to civil or criminal penalties. The purpose of this Policy is to set out the principles and basic requirements for the Group and employees to comply with the requirements of the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615 of the laws of Hong Kong) (the "AMLO") and other applicable AML and CTF laws and regulations, as well as to monitor and report for suspicious transactions. Business Units should establish and maintain their own AML and CTF policies and procedure documents in alignment with this Policy, subject to the laws and regulations in the jurisdictions in which they operate.

II. Scope of Application

1. This Policy applies to all employees, including employees at all levels and others who may act on behalf of the Group. Employees should familiarise themselves with this Policy. Failure to adhere to this Policy may result in disciplinary action (which may include summary dismissal) and/or referral to law enforcement.

III. Definitions

1. <u>Money laundering</u>

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

1.2 There are three common stages in money laundering:

(a) Placement - 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. Terrorist Financing

2.1 The term "terrorist financing" is defined in section 1 of Part 1 of Schedule 1 to the AMLO as:

(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.

IV. AML/CTF Systems

1. To fulfill the obligations to mitigate the risk of ML and TF, and ensure legal compliance under the AMLO, the Group should assess the risk of the businesses, develop and implement policies, procedures and controls (collectively, "AML/CTF systems") on:

(a) risk assessment;

(b) customer/counterparty due diligence ("CDD") measures;

(c) ongoing monitoring of customers/counterparties;

(d) suspicious transactions reporting;

(e) record keeping;

(f) staff training; and

(g) independent audit function.

2. Business Units should establish and implement adequate and appropriate AML/CTF systems (such as business relationship acceptance policies and procedures) taking into account factors including, *inter alia*, products and services offered, types and level of risks of customers/counterparties and geographical locations involved. The persons-in-charge of each Business Unit should ensure the AML/CTF systems can address the ML and TF risks identified and confirm annually to the Group's Risk Management and Internal Control Committee.

3. Risk Assessment
   (a) The Group adopts a risk-based approach to identify, assess and take action to mitigate ML and TF risks. Control and oversight adopted, including the extent of CDD, the level of ongoing monitoring and the risk mitigation measures, should be appropriate in view of the customer/counterparty's ML and TF risks identified.

   (b) In determining the ML and TF risk rating of a customer/counterparty, the Group considers a range of risk factors relevant to the specific circumstance. The following factors may be considered[1]:
      (i) Country/geographic risk
         - Customers/Counterparties with residence in or connection with high-risk jurisdictions (e.g. those that have been identified by Financial Action Task Force ("FATF") as jurisdictions with strategic AML/CTF deficiencies, or countries subject to sanctions, embargos or similar measures issued by the United Nations, etc.)

      (ii) Customer risk
         - Some customers, by their structure, nature or behavior, might present a higher risk of ML/TF. Factors might include involvement in cash-intensive businesses; nature, scope and location of business activities generating the funds/assets, having regard to sensitive or high-risk activities, etc.

[1] Guideline on Compliance of Anti-Money Laundering and Counter-Terrorist Financing Requirements for Licensed Money Lenders (June 2023)

(iii) Product/service risk
- Might include services that inherently have provided more anonymity; and ability to pool underlying customers/funds.

(iv) Delivery/distribution channel risk
- Transactions through online, postal or telephone channels where a non-face-to-face approach is used to establish business relationship, etc.

(c) Depending on the risk circumstances and how it evolves, the Group adjusts its risk assessment from time to time and reviews the extent of CDD, level of ongoing monitoring and risk mitigation measures to be applied to reasonably control ML and TF risks.

(d) Each Business Unit should keep records and relevant documents of the risk assessment conducted.

4. Customer/counterparty Due Diligence ("CDD")

(a) The Group carries out CDD measures to identify and evaluate the potential risks before establishing business relationship or entering into transactions.

(b) Each Business Unit should implement appropriate CDD measures according to its business activities for customer/counterparty identification and verification, ongoing monitoring (if applicable) and reporting of suspicious activity. Save as otherwise provided in the AML and CTF policies and procedure documents maintained by each Business Unit, the CDD measures should include at least the following steps:

(i) obtaining the basic information of customer/counterparty ("CCD Information"), such as trade or business nature, identity and ownership structure;

(ii) verifying the identity of customer/counterparty, and its beneficial owner(s) or controller(s) in case of non-natural person, by using reliable and independent sources of information, such as official documents and databases, or third-party verification services where necessary;

(iii) if an agent purports to act on behalf of the customer/counterparty, identifying the agent and taking reasonable measures to verify the agent's identity and his/her authority to act on behalf of the customer/counterparty;

(iv) requesting customer/counterparty to make update if there is any subsequent change to its CCD Information;

(v) screening name of customer/counterparty against certain sanctions lists issued by but not limited to the UN and HK, and the competent authority in the jurisdiction in which the Group operates, if any customer/counterparty or its beneficial owner/controller/agent found to be locating, residing, domiciling, organised in any countries/regions listed thereon, reporting to the management in accordance with the procedure of section 6. Suspicious Transactions Reporting as set out below.

(c) Employees must follow all due diligence procedures implemented in their respective Business Units to conduct assessment.

(d) Knowing your customer/counterparty procedures are not generally required for individual hotel guests of the Group's hotels, the Group's restaurant patrons, the Government of PRC and HK and their respective departments, banks, and any company under the Group.

(e) There are situations that additional measures or enhanced due diligence ("EDD") should be taken. Such situations may include:
   (i) customer/counterparty is not physically present for identification purposes;
   (ii) customer/counterparty or its beneficial owner being a politically exposed person, an individual who is or has been entrusted with a prominent public function in a place outside of Hong Kong and his/her close family members ("PEP");
   (iii) corporate customer/counterparty which has issued bearer shares;
   (iv) customer/counterparty from or transaction connected with a jurisdiction identified by the FATF as having strategic AML/CTF deficiencies; and
   (v) any situation by its nature presenting a higher ML and TF risk.

(f) Business Units should establish procedures for EDD and viable additional measures for employees to follow. The additional measures or EDD taken should be proportionate, appropriate and discriminating based on the nature and level of ML and TF risks.

(g) Where applicable, when a particular customer/counterparty or its beneficial owner is a non-Hong Kong PEP[2], all the following EDD measures should be applied:
   (i) obtaining approval from the senior management; and
   (ii) taking reasonable measures to establish the customer/counterparty's or the beneficial owner's source of wealth and the source of funds that will be/are involved in the business relationship.

(h) The Group and its employees shall only proceed with transactions with customer/counterparty where it is satisfied that the transactions would not be in breach of the Policy or the Business Unit's own AML and CTF policies, and would not be involved in any ML and TF activities.

5. Ongoing Monitoring
   (a) Adopting a risk-based approach, appropriate ongoing monitoring of the business relationship and transactions with new and existing customer/counterparty is applied, where applicable. The measures may include:

[2] Please refer to section 19(1) of Part 2 of Schedule 2 to the AMLO

(i) from time to time review documents, data and information related to the customer/counterparty obtained for the purpose of CDD to ensure that they are up-to-date and relevant;
(ii) conduct appropriate scrutiny of transactions to ensure that they are consistent with the Group's knowledge of the customer/counterparty and its business, risk profile and source of funds; and
(iii) identify transactions that are complex, unusually large in amount or of an unusual pattern or that have no apparent economic or lawful purpose and which may indicate ML and/or TF.

(b) The frequency of review and the extent of monitoring should be proportionate with the risk profile of the customer/counterparty through the risk assessment. Review should also be conducted when triggering events such as below occur:
(i) a significant transaction (i.e. in terms of monetary value or where the transaction is unusual or not in line with the Group's knowledge of the customer/counterparty) is to take place;
(ii) a material change occurs in the customer/counterparty's ownership;
(iii) customer/counterparty documentation standards change substantially; or
(iv) the Group is aware that it lacks sufficient information about the customer/counterparty concerned.

6. Suspicious Transactions Reporting
(a) When employees identify or suspect that a transaction is related to ML and TF activity, they must report the case to their respective department heads who should evaluate to report to Business Units' person-in-charge and to Top Management of the Group. If applicable, a suspicious transaction report will be made to Joint Financial Intelligence Unit of HKSAR Government ("JFIU").

(b) It is a criminal offence under the Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405 of the laws of Hong Kong) ("DTRPO"), the Organised and Serious Crimes Ordinance (Cap. 455 of the laws of Hong Kong) ("OSCO") and also the United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575 the laws of Hong Kong) ("UNATMO") if a person fails to report where the requisite knowledge or suspicion exists.

(c) In the event of a report being made to the JFIU, it is an offence if an employee discloses to the customer/counterparty and any other person any matter which is likely to prejudice any investigation which might be conducted following the disclosure (commonly referred to as "tipping-off"). Therefore, the employees concerned shall keep the relevant case strictly confidential.

7. Record Keeping
   (a) Business Units must maintain the original or a copy of all relevant records of customers/counterparties, transactions, etc. to meet the record-keeping requirements under the AMLO and other relevant regulatory requirements.

   (b) All of the abovementioned records must be kept for at least 5 years from the end of the business relationship or the date of the transaction as applicable and following the Business Units' own documentation policies.

8. Staff Training
   (a) All employees of the Group should be informed of the Policy, and all relevant employees must familiarise themselves with the Policy, their obligations under AMLO and the AML/CTF systems applied in their respective Business Units.
   (b) Employees should be made aware of the Group's statutory obligations and their own personal statutory obligations and the possible consequence for failure to report suspicious transactions under the OSCO, DTROPO and the UNATMO.

   (c) Focused and on-going training for appropriate employees or groups of employees should be held by Corporate Units and Business Units, as appropriate. Areas to be covered in training should be adjusted and tailored according to the groups of employees (e.g. new employees should receive introductory training as part of their induction process, and front-line employee who deal with customers directly should be provided with training on policies and procedures of CDD, etc.). Regular updates on identifying and dealing with suspicious transactions will generally be given at least annually.

   (d) Training records including the date and type of training received by **each employee** should be maintained for a minimum of 3 years and be available to the Internal Audit Department on demand.

Note

This Policy will be reviewed and updated from time to time to ensure its relevance and effectiveness. The latest version of this Policy is posted on the Group's website.

In the event of any inconsistency or conflict between the English and the Chinese version of this Policy, the English version shall prevail.