CK Asset Holdings Limited

Anti-Money Laundering Policy

Anti-Money Laundering Policy

I. OBJECTIVE AND SCOPE

(a) CK Asset Holdings Limited ("CKA" or the "Company") is committed to upholding high ethical and legal standards in its operations. This includes complying with applicable AML Laws in Hong Kong and any other jurisdictions in which it may operate.

(b) Doing business in violation of AML Laws could lead to civil or criminal penalties and significant reputational risks for the Company. Employees and other persons connected to the Company could also face civil or criminal penalties.

(c) The purpose of this Anti-Money Laundering Policy ("Policy") is to set out the main areas of money laundering risks facing the Company and the principles that the Company applies to comply with applicable AML Laws. The Company has adopted this Policy to help its employees comply with these anti-money laundering requirements and applicable AML Laws.

(d) All Employees, including those who deal with Counterparties located anywhere in the world, must adhere to this Policy. Failure to comply with the Policy by an Employee may result in disciplinary action up to and including termination of employment or referral to law enforcement.

(e) This Policy should be read alongside with the CKA Code of Conducts which sets out the standards of conduct and professionalism applicable to all Employees acting for or on behalf of the Group (as defined in paragraph (f) below).

(f) This Policy is applicable only to the Company and its subsidiaries in Hong Kong and PRC (for the purpose of the application of this Policy only, the "Group"), subject to and in compliance with any applicable legal and regulatory requirements. CKA's overseas operating subsidiaries, joint venture companies, affiliates and associates, shall as applicable adopt and maintain their own independent anti-money laundering policy in alignment with the principles adopted under this Policy, but subject to and in compliance with the legal and regulatory requirements of the jurisdictions in which they each operate.

(g) Capitalized terms used in this policy which are not otherwise defined are set out and defined in **Annex A**.

II. DEFINITION OF MONEY LAUNDERING

(a) Money laundering is the criminal practice of handling or possessing criminal property, which is a benefit a person receives from criminal conduct. Criminal property can include money, securities, tangible property or intangible property. Money laundering does not necessarily involve cash or cash equivalents at every stage of the laundering process.

(b) Money laundering can be a very simple process. For example, a person uses money raised from an illegal activity to purchase a clean asset, and in doing so, distancing the benefit of the illegal activity from the illegal activity itself, and enabling the launderer to enjoy the benefit of his crime.

(c) Money laundering can also be highly complex. Most complex money laundering schemes follow three stages that may occur separately or simultaneously in order for money laundering to occur:

(i) **Placement** is the initial placement of illegally-derived (criminal) money into a legitimate financial context (usually with the aim of avoiding the attention of financial institutions or law enforcement). For example, profits derived from a corruptly procured contract, which are mixed with untainted funds a company holds.

(ii) **Layering** involves the distancing of illegal proceeds from their criminal source through the creation of layers of financial transactions, for example, via offshore companies. Possible examples of layering include unnecessary currency exchange, exchanging monetary instruments for larger or smaller amounts or wiring or transferring funds to and through numerous accounts in one or more financial institutions.

(iii) **Integration** occurs when the criminal money ultimately becomes absorbed into the economy in a way that appears to have been derived from a legitimate source, for example by investing that money.

III. PROHIBITION ON ACCEPTING PROCEEDS FROM BELIEVED ILLEGAL ACTIVITY

(a) The Group, including through its Employees, will not accept or become involved in any arrangement concerning money that is known or suspected to be the proceeds of illegal activity or money laundering.

(b) The head of each department is responsible for conducting AML due diligence and assessing AML risks (as set out in Section IV below) for the transactions that his or her department proposes to undertake, subject to the principles that:

(i) the Group will only proceed with transactions where it is satisfied that the transactions would not involve illegal activity or money laundering or be in breach of this Policy; and

(ii) the Group will only acquire or make any investment where it is satisfied that it is not acquiring, or becoming involved in an arrangement that involves money laundering (including enabling the transfer of criminal property).

IV. AML DUE DILIGENCE

(a) AML due diligence means (i) taking steps to identify and assess the potential money laundering risks that may arise before entering into transactions with Counterparties, and (ii) reviewing the nature and information about transactions with the Counterparties and background of Counterparties in order to assess any evidence of money laundering.

Red Flag Indicators and Green Light Indicators

(b) During the process of AML due diligences, Employees should take into account the "Red Flag Indicators" and the "Green Light Indicators" below in order to identify the risks of money laundering. The purpose of the Red Flag Indicators is to prompt the Group and its Employees to identify potential high-risk instances of money laundering.

(c) Any transaction that is proposed to be undertaken with a significant number of Red Flags should prompt the Group and its Employees to exercise significant caution with that Counterparty.

(d) To the extent there are Red Flags identified or otherwise an Employee considers it helpful to perform a risk assessment to identify the presence or absence of risk factors associated with a transaction, Employees should collate the information set out in the Group's AML and Sanctions Transaction Assessment Form (see **Annex C**).

(e) The Red Flag Indicators include:

(i) the potential for impropriety in the way a Counterparty conducts its core business, for example suspicion that it has acquired its market position, and hence its transaction value, by making corrupt payments;

(ii) requests from Sellers to purchase Potential Investments through an unusual or unnecessarily complex deal structure;

(iii) requests from Counterparties to use unusual payment methods, such as the use of large amounts of cash; multiple or sequentially numbered money orders; traveller's cheques or other cash equivalents; cashier's cheques; precious metals or gems; physical inventory; cryptocurrency; or payment from/to third parties (including extension of credit, debt, or guarantees to such parties);

(iv) requests from Counterparties to conduct transactions through multiple banks, unknown financial institutions, or institutions outside of the country where the transaction is occurring (or to avoid the formal banking system / SWIFT transactions altogether in favour of using money exchange houses, cryptocurrencies or Hawala methods of payment);

(v) unwillingness by Counterparties to provide complete or accurate contact information, financial references, or business affiliations;

(vi) attempts by Counterparties to maintain an unusual degree of secrecy with respect to the transaction, for example requests that normal business records not be kept;

(vii) involvement of known or suspected criminals, including through press speculation involving the Counterparty;

(viii) purchases or sales that are unusual for that type of Counterparty, or unusual for that particular Counterparty (for example, in terms of frequency, transaction size, currency denomination, or involvement of "round numbers"); and

(ix) transacting business in regions that the Group has identified as a high risk for economic crime or known for drug trafficking, terrorism or other criminal activities (see: (i) Annex B for the latest list of countries identified by the Financial Action Task Force list as high-risk and other monitored jurisdictions for the purposes of AML; and (ii) the Basel Institute on Governance index rank of countries according to AML risk (https://www.baselgovernance.org/basel-aml-index/public-ranking)).

(f) The presence of Red Flags should be balanced against certain factors relating to a transaction which indicate lower risk ("Green Light Indicators"), including but not limited to:

(i) the proposed transaction or Investment has a simple deal structure and the deal structure has a clear commercial rationale;

(ii) the Counterparties request payment to a large financial institution registered in a low-risk jurisdiction and there is otherwise no presence of any unusual payment methods;

(iii) the Counterparties respond convincingly to questions about the financial aspects of the proposed transaction;

(iv) the Counterparties provide complete and accurate contact information, financial references and/or business affiliations, by for exampling warranting that the information provided is true and directly addressing and responding to any questions posed;

(v) the proposed business is in line with well-established business conducted by the Counterparties; and

(vi) customer due diligence measures have already been conducted against the Counterparties by an Intermediary provided that such Intermediary is able to satisfy the Group that it has adequate procedures in place to prevent money laundry and is required to comply with the requirements set out in Schedule 2 to AMLO or other applicable law and regulations with respect to customers.

V. REPORTING ACTUAL OR SUSPECTED MONEY LAUNDERING

(a) Employees must report any knowledge or suspicion of actual or potential Money Laundering (including Red Flags referred to Section IV above) in relation to the Group's dealings with Counterparties, as soon as reasonably practicable to his/her department head who will consider whether to engage the Company Secretarial department, the Internal Audit department and/or external counsel to form an investigation team (the "Investigation Team") to conduct further investigation.

(b) The Group will keep complaints, investigations, and the terms of its resolutions confidential to the fullest extent practicable but cannot guarantee complete confidentiality consistent with the need to undertake a full investigation or provide details to authorities as and when required by law.

(c) The Investigation Team will assess the report of suspicious activity using the "**SAFE**" approach as soon as reasonably practicable:

(i) **Screen**: screen the facts for suspicious indicators (i.e., identify the actual or potential Money Laundering Red Flags reported);

(ii) **Ask**: ask the relevant Seller's, Investor's or Customer's appropriate questions;

(iii) **Find**: find out the Seller's, Investor's or Customer's records (ie, review the information already known when considering whether the reported activity is suspicious); and

(iv) **Evaluate**: evaluate all of the above information and consider whether the activity or transaction is suspicious.

For more information on the SAFE approach, please see the Hong Kong Government's Joint Financial Intelligence Unit website at https://www.jfiu.gov.hk/en/str.html.

(d) Having considered the reported activity or transaction following the process in paragraph (c) above, if the Investigation Team know or suspect the reported property is the proceeds of money laundering, they will report their findings to the Chairman ofthe Group and the Group shall, as soon as reasonably practicable, submit a suspicious transaction report with the Hong Kong Government's Joint Financial Intelligence Unit in accordance with the procedure specified at https://www.jfiu.gov.hk/en/str.html.

(e) The Group and its Employees should not disclose any information to any other person about any report they have made under this Policy and which is likely to prejudice any investigation which might be conducted following a report to the Government's Joint Financial Intelligence Unit described in paragraph (d) above.

VI. COUNTERPARTY DUE DILIGENCE

(a) Counterparty due diligence means taking steps to assess the potential risks that may arise in relation to transactions with Counterparties, before entering into such transactions.

(b) Counterparty due diligence also involves assessing Potential Investments so that the Group can be satisfied that it is not acquiring, or becoming involved in an arrangement that involves money laundering (including enabling the transfer of criminal property).

(c) Employees are required to follow all due diligence procedures in force by their department (if any) (the "DEPT's DD Procedures") to assess the Counterparty and keep the diligence information obtained up-to-date.

(d) Employees shall comply with procedures to prevent involvement of the Group in money laundering, prior to engaging in transactions with a Counterparty (including receiving dividends or interest from Current Investments). In addition to DEPT's DD Procedures, these procedures include the following: -

(i) applying "know your counterparty" procedures on Counterparties which involve (I) the identification of beneficial owners and Ultimate Beneficial Owners of Counterparties; (II) identifying whether a Counterparty is a PEP (or an associate of a PEP); and (III) establishing the source of funds used during the business relationship or transaction. Note that known PEPs within the Group, any of its subsidiaries, joint venture companies, affiliates or associates should not raise red flags; Note that KYC procedures do not generally need to be conducted for the following entities: -

(1) individual hotel guests of the Group's hotels; or

(2) patrons of the Group's restaurant; or

(3) the Hong Kong Government or a governmental body of it; or

(4) any banks, credit or financial institutions, insurance companies' licensed corporations, appointed insurance agents or authorized insurance broker or insurance brokers licensed in Hong Kong or their equivalents in any G-10 country; or

(5) any qualified accountants or lawyers, where the business relationship solely involves the obtaining of their professional advice or services; or

(6) any company under the CK Group (including entities controlled jointly by two or more companies under the CK Group), except in circumstances where the Group is intending to increase its shareholding from a non-controlling to a controlling stake of such entities.

(ii) requesting confirmation from Current Investments that the dividends and interest do not comprise the proceeds of crime, if the Employee is suspicious that the payment received from the Current Investments is unusual; and

(iii) gathering information on the Counterparties, including through screening for press speculation about illegal or high-risk activities involving the Counterparties and using screening software, where considered appropriate.

(e) The riskier a Counterparty is assessed as, during the due diligence process, the more stringent the due diligence process that must be undertaken by the Group (including by its Employees).

(f) The Group and its Employees must only proceed with transactions involving Counterparties` where it is satisfied that the transactions would not be in breach of this Policy or involve illegal activity or money laundering. Such transactions include receiving dividends and interest from Current Investments.

VII. ANTI-MONEY LAUNDERING TRAINING

(a) Training is a key aspect of compliance, and all Employees should be informed about this Policy.

(b) This Policy should be made available (whether in hard copy or online) to all Employees who deal with Counterparties, in addition to all Employees with responsibilities within the Group's Treasury, Compliance and Finance functions.

(c) Training or briefing session should be held, as appropriate, by the Company Secretarial Department to inform the Employees specified in paragraph (b) above of their obligations under this Policy. A record of such training or briefing sessions should be maintained by the Company Secretarial Department.

VIII. RECORD KEEPING

(a) Employees must maintain proper book, record, or account that relates to the business of the Counterparties, or the transactions conducted by the Group. The falsification of any book, record or account is prohibited.

(b) All of the above records must be kept for a minimum of seven years or such other longer period as required under each department's own document retention policy or practice.

IX. REPORTING VIOLATIONS OF THIS POLICY

The Group expect its Employees to report any suspected or actual violations of this Policy pursuant to the procedure set out in the CKA Whistleblowing Policy.

X. ENQUIRIES

Any question by employees regarding the AML compliance assessment procedures of individual department and this Policy should be addressed to the head of department, and any questions raised by head of departments should be addressed to the Company Secretarial Department.

Annex A

Definition

AML Laws means the laws, regulations, rules and other stipulations relating to anti-money laundering or counter-terrorism financing of Hong Kong, People's Republic of China, the United Kingdom, the European Union, the United States, Canada, Australia, and New Zealand.

AMLO means Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Chapter 615, Laws of Hong Kong).

Audit Committee means the audit committee of the Company.

Borrowers include third party companies and individuals the Group lends money to.

CKA Code of Conduct means the CKA's Employment Terms and Conditions: Clause 12.7 Code of Conduct.

CKA Whistleblowing Policy means the "Procedures for Reporting Possible Improprieties in Matter of Financial Reporting, Internal Control or Other Matters" of the Group.

Counterparty means: any Investment, Joint Venture Partner, Seller, Purchaser, Supplier, Customer, Borrower or Lender.

Customers include (i) companies and individuals the Group provides or sells goods/property or services to, including trade customers; and (ii) companies and individuals the Group leases property to.

Employees means: all employees, officers, and directors of the Group (whether full or part-time).

G10 means "The Group of Ten" which is made up of eleven industrial countries (Belgium, Canada, France, Germany, Italy, Japan, the Netherlands, Sweden, Switzerland, the United Kingdom and the United States) which consult and co-operate on economic, monetary and financial matters.

Intermediaries includes (a) accounting professional, estate agents, legal professionals and TCSP licencees as defined in Part 2, Schedule 1 of AMLO; (b) authorized institutions as defined in Section 2 of Banking Ordinance (Chapter 155, Laws of Hong Kong); (c) licensed corporations as defined in Part 1, Schedule 1 of Securities and Futures Ordinance (Chapter 571, Laws of Hong Kong); (d) authorized insurers and licensed insurance intermediaries as defined in Section 2 of Insurance Companies Ordinance (Chapter 41, Laws of Hong Kong); or their equivalents in any G10 country.

Investments include (i) assets or companies that the Group is considering investing in or acquiring ("Potential Investments"); and (ii) assets or companies that the Group has investedin or acquired ("Current Investments").

Joint Venture Partners include companies or individuals who are co-investors or joint venture partners of the Group for the Investments.

Lenders include third party companies and individuals the Group borrows money from.

PEP means "politically exposed person" who, in simple terms, is an individual entrusted with a prominent public function, such as head of state, head of government, senior politician, senior government, judicial or military official, senior executive of a stated-owned corporation and an important political party official, their spouses, partners, children or parents, or their close associates. For further details, please refer to Schedule 2 of the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Chapter 615 of the laws of Hong Kong).

Purchasers include third party companies or individuals who are or were involved in purchasing or attempting to purchase any of CKA's Current Investments.

Sellers include third party companies or individuals who are or were involved in selling or attempting to sell Investments to the Group.

Suppliers include third party companies or individuals the Group purchases goods or services or leases property.

Ultimate Beneficial Owner of a legal entity means an individual person who: (i) holds minimum 25% equity in the legal entity's capital; (ii) can exercise, directly or indirectly, minimum 25% of the voting rights at the general meeting of shareholders of the legal entity; or (iii) is the indirect beneficiary of minimum 25% of the legal entity's capital.

Annex B: Financial Action Task Force: high risk and other monitored jurisdictions (March 2020)

High Risk Jurisdiction		Monitored Jurisdiction	
Democratic People's Republic of Korea	●	Iran	●
Albania	●	Bahamas	●
Barbados	●	Botswana	●
Cambodia	●	Ghana	●
Iceland	●	Jamaica	●
Mauritius	●	Mongolia	●
Myanmar	●	Nicaragua	●
Pakistan	●	Panama	●
Syria	●	Uganda	●
Yemen	●	Zimbabwe	●