CK Infrastructure Holdings Limited

Anti-Money Laundering Policy

Table of Contents

1. Policy Statement

1.1 CK Infrastructure Holdings Limited ("**CKI**" or the "Company") is committed to uphold the highest ethical and legal standards in its operations. This includes complying with applicable laws and regulations prohibiting money laundering in jurisdictions in which it operates.

1.2 This anti-money laundering policy ("**Policy**") is to help the Employees to comply with the anti-money laundering requirements.

1.3 Doing business in violation of AML Laws could lead to civil or criminal penalties and significant reputational risks for CKI. Employees and other persons connected to CKI could also face civil or criminal penalties.

1.4 Failure to follow this policy may result in disciplinary action, up to and including termination of employment or agency.

1.5 For the purposes of this Policy, **AML Laws** means the laws, regulations, rules and other stipulations relating to anti-money laundering or counter-terrorism financing of Hong Kong, the United Kingdom, the European Union, the United States, Canada, Australia, New Zealand and Bermuda.

1.6 If you have any questions or become aware of any conduct you believe may violate this Policy or applicable AML Laws, you should immediately raise the issue with your supervisor and department head or otherwise contact the audit committee of CKI ("**Audit Committee**"). CKI will not tolerate any form of retaliation against an employee that raises any such concerns and does so in good faith.

2. Purpose

2.1 The purpose of this Policy is to set out the main areas of money laundering risks facing CKI and the principles that CKI must apply to ensure its compliance with applicable AML Laws. CKI has adopted this Policy to help Employees to comply with these anti-money laundering requirements and applicable AML Laws.

2.2 The Company is committed to conducting its business abiding by the fundamental principles set out under the CKI's Employment Terms and Conditions: Clause 12.7 Code of Conduct ("***CKI Code of Conduct***") which provides that each Employee is expected to observe the highest standard of ethical, personal and professional conduct. This includes abiding by best regulatory practices.

2.3 This Policy should be read alongside the CKI Code of Conduct. It sets out the standards of conduct and professionalism applicable to all employees, officers, and directors of CKI (***Employees***) acting for or on behalf of the Company to ensure their compliance with this Policy and applicable anti-money laundering laws and regulations.

2.4 All Employees must comply with this Policy and will be provided with a copy of this Policy upon their employment or engagement. A copy of this Policy can also be found on the CKI intranet or requested from the internal audit department or legal department.

3. Investments, Sellers, Customers and Purchasers

3.1 "***Investments***" include:

(a) companies that CKI is considering investing in or acquiring ("***Potential Investments***"); and

(b) companies that CKI has invested in or acquired ("***Current Investments***").

3.2 "***Sellers***" include third party companies or individuals who are or were involved in selling or attempting to sell Investments to CKI.

3.3 "***Customers***" include:

(a) companies and individuals CKI provides or sells goods or services to, including trade customers;

(b) companies and individuals CKI leases property to; and

(c) companies and individuals CKI lends money to.

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

3.5 This Policy applies to Employees who deal with Sellers, Investments, Customers and Purchasers located anywhere in the world.

Application of this Policy

3.6 This Policy is applicable only to CKI. CKI subsidiaries, joint venture companies, affiliates, associates and operating companies, shall, as applicable adopt and maintain their own independent AML policy in alignment with the principle adopted under this Policy but subject to and in compliance with the legal and regulatory requirements of the jurisdictions in which they each operate.

3.7 CKI expects that each of its Current Investments shall commit that prior to the payment of any dividends or interest on any intra-company loans that are owed to CKI, they will take steps to ensure that the monies used for such payments are not the benefit or proceeds from any illegal activity, money laundering, or otherwise in breach of AML Laws.

4. Definition of Money Laundering

4.1 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.

4.2 Money laundering could be a very simple process. For example, someone using 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 their crime.

4.3 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:

(a) **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.

(b) **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.

(c) **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.

5. Prohibition on Accepting Proceeds from Believed Illegal Activity

5.1 CKI and 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.

6. Red Flag Indicators and Green Light Indicators

6.1 The Company expects that each Employee shall review the nature and information about transactions with counterparties in order to assess any evidence of money laundering. 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 Company and its Employees to identify potential high-risk instances of money laundering. Where any Red Flags arise each Employee should take the necessary steps to report the instances of money laundering.

6.2 Any transaction that is proposed to be undertaken with a significant number of Red Flags should prompt the Company and its Employees to exercise significant caution with that counterparty.

6.3 To assist in assessing the risks associated with a transaction, Employees should collate the information set out in CKI’s AML and Sanctions Transaction Assessment Form (see Annex C).

6.4 The Red Flag Indicators include:

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

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

(c) requests from Sellers, Customers or Purchasers 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);

(d) requests from Sellers, Customers or Purchasers 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);

(e) unwillingness by Sellers, Customers or Purchasers to provide complete or accurate contact information, financial references, or business affiliations;

(f) attempts by Sellers, Customers or Purchasers to maintain an unusual degree of secrecy with respect to the transaction, for example requests that normal business records not be kept;

(g) involvement of known or suspected criminals, including through press speculation involving the Sellers, Investments, Customers or Purchasers;

(h) purchases or sales that are unusual for that type of Sellers, Customers or Purchasers, or unusual for that particular Seller, Customer or Purchaser (for example, in terms of frequency, transaction size, currency denomination, or involvement of "round numbers"); and

(i) transacting business in regions that CKI 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)).

6.5 Employees should balance the presence of Red Flags against certain factors relating to a transaction which indicate lower risk ("***Green Light Indicators***"), including but not limited to:

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

(b) the Sellers, Customers or Purchasers request payment to a large financial institution registered in a low-risk jurisdiction and there is otherwise no presence of any unusual payment methods;

(c) the Sellers, Customers or Purchasers respond convincingly to questions about the financial aspects of the proposed transaction;

(d) the Sellers, Customers or Purchasers 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; and

(e) the proposed business is in line with well-established business conducted by the Sellers, Customers or Purchasers.

7. Investment, Seller, Customer and Purchaser Due Diligence

7.1 Investment, Seller, Customer and Purchaser due diligence means taking steps to assess the potential risks that may arise in relation to transactions with Investments, Sellers, Customers or Purchasers before entering into such transactions.

7.2 Investment, Seller, Customer or Purchaser due diligence also involves assessing Potential Investments so that CKI 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).

7.3 Employees are required to follow internal CKI due diligence procedures and ensure that the diligence information obtained is kept up-to-date.

7.4 Employees shall comply with procedures to prevent involvement of CKI in money laundering, prior to engaging in transactions with an Investment, Seller, Customer or Purchaser (including receiving dividends or interest from Current Investments). These procedures include the following:

(a) applying “know your client” procedures, including Potential Investment, Seller, Customer or Purchaser verification which involves the identification of beneficial owners and ultimate beneficial owners of Potential Investments, Sellers, Customers or Purchasers. Note that KYC procedures do not need to be conducted on any entity that CKI directly or indirectly owns or controls (for example, CKI subsidiaries, joint venture companies, affiliates, associates and operating companies), except in circumstances where CKI is intending to increase its shareholding from a non-controlling to a controlling stake of such entities;

(b) identifying whether a Seller, Customer or Purchaser is a “politically exposed person” (***PEP***) (or an associate of a PEP) and establishing the source of funds used during the business relationship or transaction. Note that known PEPs within any CKI subsidiaries, joint venture companies, affiliates, associates and operating companies should not raise Red Flags;

(c) identifying whether an Investment is involved with a PEP (or an associate of a PEP);

(d) 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;

(e) gathering information on the Investment, Seller, Customer or Purchaser including through screening for press speculation about illegal or high-risk activities involving the Seller, Investment, Customer or Purchaser and using screening software, where considered appropriate; and

(f) gathering information on the purpose and intended nature of the business relationship with the Customer and using screening software, where considered appropriate.

7.5 The riskier an Investment, Seller, Customer or Purchaser is assessed as, during the due diligence process, the more stringent the due diligence process that must be undertaken by CKI (including by its Employees).

7.6 CKI and its Employees must only proceed with transactions involving Investments, Sellers, Customers or Purchasers 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.

8. Reporting Actual or Suspected Money Laundering

8.1 Employees must report any knowledge or suspicion of actual or potential Money Laundering (including Red Flags referred to Section 6.1 above) in relation to CKI's dealings with Sellers, Investments, Customers, Purchasers, as soon as reasonably practicable to his/her department head who will consider whether to engage the Internal Audit department, the Company Secretarial department and/or external counsel to form an investigation team (the **"Investigation Team"**) to conduct further investigation.

8.2 CKI 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.

8.3 The Investigation Team will then assess the report of suspicious activity using the "SAFE" approach as soon as reasonably practicable:

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

(b) **Ask**: ask the relevant Sellers, Investments, Customers or Purchasers appropriate questions;

(c) **Find**: find out the Seller's, Investment's, Customer's or Purchaser's records (i.e., review the information already known when considering whether the reported activity is suspicious); and

(d) **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.

8.4 Having considered the reported activity or transaction following the process in section 8.3 above, if the Investigation Team knows or suspects the reported property is the proceeds of money laundering, they will report the finding to Group Managing Director of the Company and the Company 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.

8.5 CKI 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 8.4 above.

9. Anti-Money Laundering Training

9.1 Training is a key aspect of ensuring that all Employees understand their requirements and responsibilities under this Policy.

9.2 Anti-money laundering training should be provided to all existing and new Employees who deal with Sellers, Investments, Customers or Purchasers, in addition to all Employees with responsibilities within CKI's Treasury, Compliance and Finance functions.

9.3 The internal audit department and legal department are responsible for monitoring anti-money laundering training is adequately provided to all existing and new Employees specified in section 9.2 above, in addition to maintaining a record of this training.

9.4 The training must be sufficient to ensure that the Employees specified in section 9.2 are aware of their obligations under this Policy, including its annexures.

10. Record Keeping

10.1 Employees must not intentionally misclassify or falsify any book, record, or account that relates to the business of CKI Sellers, Investments, Customers, Purchasers or the disposition of CKI's assets. This includes, but is not limited to, intentionally omitting or misclassifying any transaction as to accounts, departments, or accounting periods.

10.2 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.

11. Reporting Violations of this Policy

11.1 CKI expect its Employees to report any suspected or actual violations of this Policy pursuant to the procedure set out in the "Procedures for Reporting Possible Improprieties in Matter of Financing Reporting, Internal Control or Other Matters" of CKI.

12. Enquiries

12.1 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 internal audit department or legal department.

Annex A: Case studies to illustrate identification of Red Flags and escalation

Investments

CKI is contemplating acquiring a company that operates in the water sanitation sector in Indonesia (the "**Target**"). The transaction team conducts initial due diligence on the Target. The Seller provides you with copies of the local government licences that it has acquired to carry out water sanitation. You notice that the payments made for the licences do not appear to be made to Indonesian state treasury accounts, but instead are to accounts in the names of private individuals in Singapore.

RED FLAGS:

- The Target may have acquired its market position, and hence its transaction value, by making corrupt payments
- Indonesia is a region that has a high-risk of economic crime

This transaction should be escalated for further consideration.

Sellers

A well-known private equity house offers to sell you a portfolio company. You have dealt with them before, in a similar sector and if you complete this transaction they have requested that you remit the transaction proceeds through a different method to the way you have paid them before: they ask you to split the consideration up into 4 separate payments, into 4 accounts held at 4 separate banks. They explain that they recently restructured, and that for tax reasons they now arrange their affairs in this way, and participated in an interview that satisfied you that this was the *bona fide* rationale.

RED FLAGS:

- requests from Seller to purchase Potential Investments through an unusual deal structure
- requests from Seller to conduct transactions through multiple banks

GREEN LIGHTS:

- the Seller responds convincingly to questions about the financial aspects of the proposed transaction
- the proposed business is in line with well-established business conducted by the Seller

This transaction, when considered in the round, may not need to be escalated further.

Customers

You are approached by your subsidiary (the ***Subsidiary***) in relation to potential capital expenditure. The capital expenditure is in line with the Subsidiary's general line of business. The Subsidiary provides clear and detailed information relating to the nature and purpose of the proposed capital expenditure. Your Subsidiary asks for an intra-group loan to carry out the capital expenditure.

Note that prior to the payment of the intra-group loan, the Subsidiary has not informed you of any pending, threatened or expected investigation into its conduct by any authority for breach of applicable laws.

RED FLAGS:

- N/A

GREEN LIGHTS

- The Subsidiary has given detailed information about the proposed business.
- There is no indication from the Subsidiary that there is any pending, threatened or expected investigation into its conduct for breach of applicable laws.
- The Subsidiary has produced consistent financial statements over the last few financial years.

This transaction, when considered in the round, should not be escalated further.

Annex B: Financial Action Task Force: high risk and other monitored jurisdictions (October 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	●

Annex C: Transaction Assessment Form

CK Infrastructure Holdings Limited

Anti-Money Laundering and Sanctions Transaction Assessment Form

AML AND SANCTIONS TRANSACTION ASSESSMENT FORM

Section (A) Basic Information

Counterparty Name:) _____ Today's date:) _____

_____ Your name:) _____

Customer Contract Details:) _____ Office:) _____

) _____

Section (B) Transaction Information

(1) Transaction Categorisation Tick-Box and Description

Investment ☐ _____

Supplier Transaction ☐ _____

Other ☐ _____

Section (B) Transaction Information			
(2) Direct counterparty details			
Counterparty name(s)	Counterparty jurisdiction(s)	Contact name	Contact details

Section (B) Transaction Information			
(3) Any other third party details?			
Third party name(s)	Third-party jurisdiction(s)	Contact name	Contact details

Section (C) Transaction Information – Red Flag identification	
(1) Red flag identifier tick box **The red flag indicators below are not exhaustive of all potential red flags. Please consider the elements of the transaction being undertaken in the round and consider carefully any factors which give rise to suspicion or which merit further enquiry. Please describe the details of these factors in Section C(2) below.**	
Does a counterparty to the transaction or the proposed merger & acquisition, joint venture or investment target, have significant operations in a country subject to broad economic sanctions, including, Iran, Crimea, Syria, North Korea and/or Cuba (see Annex C of CKI's Sanctions Compliance Policy)?	
Does a counterparty or proposed acquisition target, joint venture partner or investment opportunity have an opaque and complex ownership structure, which may hide or conceal the true ownership of a potential asset?	

Has the counterparty to a proposed transaction, merger or acquisition, joint venture or investment provided insufficient information to enable you to assess compliance with financial sanctions?	
Has there been a rapid change that you know of the financial sanctions regime which means that you suspect that the new sanctions in force capture the transaction being contemplated?	
Has the counterparty hidden, concealed, made unclear or provided inconsistent or incomplete information as to the ownership structure of the counterparty or ownership of the asset to which the transaction relates?	
Have you been notified or otherwise become aware that the name of the proposed counterparty matches or is similar to an individual on a sanctions list?	
Does the transaction involve a complex, unusual or unexpectedly changed financing arrangements?	
Has the counterparty requested that payment must be received in an unusual method, such as the use of large amounts of cash; multiple or sequentially numbered money orders; traveler'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)?	
Has the counterparty requested that payment is received by multiple different methods?	
Is the transaction unusual or out of the ordinary for the business that is being contracted with?	
Is there any other factor which is causing suspicion or raising red flags on your part about the counterparty or transaction?	

Section (C) Transaction Information – Red flag identification	
(2) Further information if any red flags appear	
Please provide further details regarding any of the red flags identified in the section above? Are there any factors which indicate that the transaction is generally low risk? If so, please provide details? Please consult the CKI AML and Sanctions Policies if required.	_____ _____ _____ _____ _____

Section (D) Sanctions screening	
Do any of the parties identified in Section B appear on any sanctions lists? Please leave blank if sanctions screening has not taken place.	Y/N
If so, please provide details?	_____ _____ _____ _____

Section (E) Escalation to Group Legal	
Does this transaction require escalation to Group Legal?	Y/N
If yes, please explain basis of escalation?	_____ _____ _____ _____