GLOBAL FRAUD POLICY

Name of Policy	Global Fraud Policy
Policy Owner	Group Legal, Secretariat & Compliance
Version	1
Effective Date of Policy / Change in Version	March 2026
Version superseded	-

Contents

1. INTRODUCTION

1.1 CapitaLand Investment Limited, and its subsidiary entities (whether direct or indirect) as well as any associated entities or joint ventures over which it, or any of its subsidiaries, exercise management control (collectively, "**CapitaLand**", "**CLI**" or the "**Group**") is committed to a strong anti-fraud culture and to preventing, detecting, and responding to fraud.

1.2 The Global Fraud Policy establishes guidelines and responsibilities for CLI and its subsidiaries to aid in the prevention of, detection of, and response to fraud against the Group or its clients. It applies to all directors, officers, employees, subsidiaries, joint ventures, and third parties acting on behalf of the Group (collectively **"CLI Persons"**).

1.3 Any actual fraud or suspicions of fraud must be reported as set out in this Policy.

1.4 Any CLI Persons who have any questions whatsoever concerning the requirements of the this Policy should consult with the Compliance team.

2. POLICY

2.1 It is Group policy to conduct all business in an honest and ethical manner.

2.2 The Board and senior management take a zero-tolerance stance toward fraud and are committeed to acting professionally, fairly and with integrity in all business dealings and relationships, implementing and maintaining effective systems to counter fraud.

2.3 CLI takes its responsibilities very seriously and will uphold all laws relevant to fraud in all the jurisdictions in which it operates.

3. FRAUD

3.1 Fraud[1] is the use of deception with intention of obtaining an advantage, avoiding an obligation or causing loss to another party. Fraud can be perpetuated by employees, third parties or a collusion between employees and third parties.

3.2 Management is responsible for the detection and prevention of fraud, misappropriations, and other irregularities.

3.3 Actions that constitute fraud may include the following:

a. Misappropriation or theft of company funds, properties, supplies or assets, including the removal, misuse or destruction of the same for illegal, improper or unethical purpose;

b. Impropriety in the handling or reporting of money or financial transactions which include false accounting and misleading disclosures;

c. Forgery or unauthorized alteration of any company documents;

[1] Definition of Fraud, Asset Misappropriation, Fraudulent Statement Fraud, Corruption and Bribery are adopted from Association of Certified Fraud Examiners ("ACFE") and ISO37001 standards. The definition of these terms may vary across jurisdictions.

d. Improper/unauthorized disclosure, use and/or manipulation of confidential, proprietary, commercially sensitive or material non-public information;

e. Profiteering as a result of insider knowledge of company activities or information;

f. E-crime using computers and technology to defraud and commit crimes (e.g. phishing, hacking, social engineering frauds, fake websites); and

g. Any similar or related irregularities for any of the above.

4. FRAMEWORK

CLI's Fraud risk management framework consists of three pillars:

1) Prevention: Internal controls, segregation of duties, pre-employment screening, manage third parties, training and conflict-of-interest declarations.

2) Detection: Transaction monitoring, red-flag indicators (non-exhaustive examples at Annex A), independent reviews/audit and whistleblowing.

3) Response: Investigation protocols, disciplinary actions, recovery of losses and disclosure to authories where required.

4.1 **Prevention:**

4.1.1 Internal Controls

Internal controls are embedded within various policies/processes to help minimize the occurrence of fraud. Broadly, such controls include:

a. Proper authorization of transactions and activities;
b. Verification and approval of work/ services/ transaction by relevant approval mechanism;
c. Adequate supporting documentation on approvals for payments;
d. Management oversight over material transactions;
e. Adequate segregation of duties;
f. Training;
g. Pre-employment screening;
h. Mandatory block leave for certain functions;
i. Avoiding or reducing conflicts of interest; or
j. Maintaining user access controls.

4.1.2 Third party risk

For legal, regulatory and reputational reasons, the Group needs to know who it is doing business with. It is the Group's policy to conduct due diligence and KYC processes on third parties who have enter into a business relationship with the Group (including investors, joint venture partners, suppliers/vendors, service providers, agents, advisors, consultants and third parties acting on the Group's behalf) and conduct ongoing monitoring.

Employees must refer to the CapitaLand Third Party Due Diligence Policy for detailed requirements.

4.1.3 Managing Conflicts of Interest

The Group has implemented a Global Conflicts of Interest Policy setting out guidance and requirements for the management of actual or potential conflicts of interest.

In essence all Employees are required to act in the best interests of clients and to avoid situations where their personal interests could be, or potentially be in conflict with the Group and/or its clients.

Please refer to the Global Conflicts of Interest Policy for detailed information.

4.2 Detection

4.2.1 Transaction monitoring

Irregularities that occur in processes that deviate from day-to-day operations could be potential signs of fraud. Greater attention paid to irregularities can provide early warning that something is not quite right and increase the likelihood of fraud being discovered. Employees should maintain a healthy amount of professional skepticism and believe that fraud is always a possibility.

Some ways through which irregularities could be observed and detected include:

a. Being alert to fraud red flag indicators (see non-exhaustive examples at Annex A) on third parties and transactions;
b. Ongoing and ad-hoc due diligence and monitoring of transactions entered;
c. Internal controls in processes such as regular reviews (e.g., bank reconciliation, project costs tracking reconciliation) by independent employees; and
d. Benchmarking by comparing business processes or performance/ results, over time, or against best practices & standards.

Should employees detect any irregularities and/or have reasonable grounds for suspicion that warrant further investigations, they must escalate the issue to their supervisor, HOD or report via the Whistleblowing channel as outlined in section 6 below. Where a statutory right exists, employees may contact a government whistleblowing channel if they feel necessary.

4.2.2 Independent Review & Audit

The internal and external auditors conduct reviews of the adequacy and effectiveness of the material internal controls in the Group.

Material non-compliance or lapses in internal controls together with corrective measures recommended by the internal and external auditors are reported to and reviewed by Audit Committee.

4.3 Response

4.3.1 Investigation

The Group has put in place an investigation procedure to manage malpractice or impropriety at the workplace. Employees must not attempt to personally conduct any investigation, interview or interrogation.

4.3.2 Insurance & Recovery

Where practicable, attempts should be made to recover any financial losses via various means including insurance claims and/or legal action. Reporting of any incident should be made as soon as possible to ensure that the Group's rights to indemnity under the policies are preserved.

4.3.3 Contact with Authorities

Any contact from or to any authorities must be coordinated with the Legal & Compliance department.

Under no circumstances are CLI Persons to respond to anyone claiming to be from an authority such as a regulator, stock exchange, police or other investigative authority without first consulting the Legal & Compliance Departments. The Group General Counsel or the Group Head of Compliance will advise the Employee on the appropriate course of action.

5. RESPONSIBILITIES

The prevention, detection and reporting of fraud is everyone's resposibility and all CLI Persons are to act at all times with the highest degree of honesty, integrity and accountability when they perform their duties for the Group.

5.1 Specifically, all CLI Persons are to:

a. Comply with this Policy;
b. Act with propriety in the use of the Group resources and the handling of funds and in dealing with clients, vendors and suppliers;
c. Be alert to the possibility of unusual events or transations that could be indicators of fraud;
d. Report details immediately if you suspect fraud or see any suspicious acts as outlined in Section 6 below; and
e. Co-operate fully during internal audits, review or investigations.

6. REPORTING AND WHISTLEBLOWING

Confidential channels are available for CLI Persons and external parties to report suspected fraud. If there is doubt whether a particular act constitutes fraud or is otherwise unlawful, CLI Persons should consult with the Compliance Department.

6.1 Reporting Actual and Suspected Fraud

6.1.1 Report to immediate supervisor or Head of Department ("**HOD**")

a. Employees who are aware of or have reasonable grounds to suspect any actual or potential fraud incident or breach of this Policy must report and escalate their suspicions to their immediate supervisor or HODs.
b. For potential fraud incidents that may involve their immediate supervisor or HOD or any other party, employees should report the incident via the Whistleblowing Channel.

6.1.2 Reporting via Whistleblowing Channel

a. The Whistleblowing Channel[2] is a trusted avenue for employees and external parties who believe that they may have discovered malpractice or impropriety in the workplace to report with confidence**.** Employees who make reports of malpractice or impropriety in the workplace in good faith will not be dismissed, penalised or discriminated against by the Group because of the making of such reports. In all circumstances, timely reporting is essential. Doing so will allow the Group an opportunity to deal with the issue promptly before the consequences escalate.

b. Supervisors or HODs who have come into knowledge of any fraud incident must report and escalate the incident to Senior Management or via the Whistleblowing Channel, as they deem appropriate.

c. The Audit Committee Chairman and Head of Group Internal Audit will ensure that investigation will be independently conducted.

d. To make a report via Whistleblowing Channel please send an email to: Whistleblowing.ACChair@capitaland.com.

7. RECORD KEEPING

7.1 All financial and business transaction information must be accurately recorded and retained in the relevant entity's books, records and accounts, in a timely manner and with necessary details.

7.2 All due diligence materials, reports, assessments and checklists must be retained for at least 7 years from the end of the business relationship, or such other length of time prescribed by law.

7.3 Detailed records for whistle blowing cases, Anti-Bribery & Corruption ("**ABC**") due diligence results, ABC-related policies and procedures must be properly kept by the policy and/or business process owners.

7.4 Employees must not destroy, amend, remove, damage or corrupt files and records subject to any report or investigation. If an Employee is found to have acted improperly, they will be subject to disciplinary action as set out in Section 9.

8. TRAINING AND AWARENESS

8.1 Training on fraud risk management forms part of the onboarding process to employees, depending upon job title, current responsibilities and potential risks associated with that role, as required. CLI Persons will receive regular, relevant training on how to implement and adhere to this policy.

8.2 CLI's zero-tolerance approach to fraud must be communicated to all suppliers, contractors and business partners at the outset of the business relationship with them and as appropriate thereafter.

8.3 Regular fraud awareness and compliance training for all employees, with targeted sessions for high-risk roles

[2] For more information on the procedures of whistle blowing, please refer to the Whistleblowing policy on intranet.

9. CONSEQUENCES FOR NON-COMPLIANCE

CLI Persons who commit fraud or act in contravention with this Policy will be subject to disciplinary action, including possible termination of employment and potential civil and criminal liabilities for individuals and the Group.

Disciplinary actions could also be taken against CLI Persons who have knowledge of such violations but have concealed them from the Group, or who take detrimental or retaliatory actions against other employees who report such non-compliance.

Any third party who is found to have committeed fraud will have the business relationship terminated immediately and be reported to the relevant authorities for potential civil and criminal liabilities.

ANNEX A: RED FLAG SITUATIONS

Examples of “red flags” situations may include, among other things, the following:

a. **Unusual patterns:** Sudden spikes in activity, multiple transactions in a short timeframe, or transactions that seem to have no clear business purpose.

b. **High-risk activity:** Frequent cross-border transfers or transactions involving high-risk jurisdictions

c. **Structuring:** Breaking down large transactions into smaller ones to stay below reporting thresholds.

d. **Inconsistent details**: Mismatches between billing and shipping addresses, or inconsistencies in trade documents, such as names, addresses, or ports of call.

e. **Unexplained activity**: Unexplained deposits into an account or frequent, profitable trades just before major company announcements.

f. **Duplicate payments**: Frequent duplicate payments to a vendor.

g. **Inconsistent information:** Discrepancies in information or lack of transparency in transactions.

h. **Account takeover attempts:** Indicators of an account being taken over, such as multiple failed login attempts or unusual activity following a login.

i. **Unfamiliarity with business:** A business principal who is unfamiliar with their own business operations.

j. **Inaccurate information:** Payment orders with inaccurate information or the use of pseudonyms or numbered accounts for commercial transactions.

k. **Pressure to act:** Being pressured to act immediately, often using scare tactics or threats.

l. **Lifestyle changes:** An employee living beyond their means or experiencing excessive gambling or debt.

m. **Lack of transparency:** A lack of transparency in transactions or with business partners.

n. **Organizational issues:** Financial difficulty, tight deadlines, unclear governance, or pressure to meet results.

o. **Missing documents:** Frequent reporting of missing documents, particularly from critical departments.

p. **Excessive adjusting entries:** A high number of adjusting entries in the books of accounts.

q. **Unsuitable provider:** Third party appears to lack sufficient capability or employee qualifications to provide the services or goods for which it is being engaged (based on years in business, types of service performed, etc.).

r. **Evasive:** Third party is reluctant to provide business references or where responses from any of the business references present a basis for concern about the third party.

s. **Unreasonable instructions:** The Group has been asked or directed by someone to use a specific third party, without reasonable or commercial justifications.

t. **Improper practices:** Third party wants to work without a contract or with a vague contract.

u. **Invoice padding:** Total amount for the transaction with third party appears to be unreasonably high or above the customary or arms-length amount.

v. **Indirect or unusual payments or billing procedures** such as:

i. Third party requests for payment to be made to or channeled through a country or geographic location different from where the third party resides or conducts business, or other unusual payment arrangements.
ii. Third party requests for payment in cash or for no records to be made of payments and/or refuses to sign a formal contract or to provide an invoice or receipt for the payment made.
iii. Third party requests for payments of unexpected additional fee or commission or reimbursements of extraordinary or vague expenses, whether or not to 'facilitate' a service, e.g. which involve unknown payees or which are not as described in invoices or receipts.
iv. Third party requests for payments to 'overlook' potential legal or regulatory violations.
v. The Group receives invoices which appear to be non-standard, or the payment request exceeds what is stated in the invoice, or the invoice indicates payment for a fee or commission which appear large given the services stated to have been provided.
vi. Third party requests for payments to anonymous (numbered) bank accounts.
vii. Third party requests for payments to others for goods or services provided by the third party.
viii. Third party requests for payments through shell companies created to receive revenues and facilitate transactions.