

# **ANTI-FRAUD POLICY**

(Version 2.0 – June 2019)

## **1. Introduction**

CLP Group (the “Group”) is committed to prevention, detection, response, and reporting of fraud.

The Anti-Fraud Policy applies to directors, officers and employees of CLP Holdings (CLPH), its wholly owned subsidiaries, and joint ventures or companies in which the Group holds a controlling interest. We encourage all our business partners, including joint venture partners, associated companies, contractors and suppliers to abide by the principles of this Policy.

The Anti-Fraud Policy is an integral part of the Group’s Corporate Governance Framework. The Anti-Fraud Policy and other policies within the Corporate Governance Framework are available for download on the Group’s external web site ([www.clpgroup.com](http://www.clpgroup.com))

It is important to recognise that fraud could result in considerable impact, not only on businesses, but also on individuals and society more broadly. In some situations, fraudulent activities could be resulting in criminal offences.

## **2. Definition of Fraud**

The term ‘fraud’ commonly refers to deceptive conduct with the intention of making some form of financial or personal gain, or making another person suffer a loss. It includes (but is not limited to) activities such as corruption, conspiracy, embezzlement, money laundering, bribery, and extortion, which could all involve an element of fraud.

Examples of the general types of fraudulent activity that may impact the Group include (but not limited to):

- i. claiming personal expenses as business expenses, or other types of false expense claims
- ii. submitting fabricated invoices for payment, or other types of false invoicing
- iii. including non-existent persons on the payroll, or other types of payroll fraud
- iv. deliberately under reporting or failing to report income or overstating deductions, i.e., falsifying financial statements
- v. fabricating or overstating insurance claims, or other types of insurance fraud
- vi. entering into a deceitful agreement in secret with third parties to gain an unfair advantage over others or other types of collusive activities with third parties
- vii. secretly disclosing tendering information to a bidder who could then gain an unfair advantage over other bidders, or other unauthorised disclosure of sensitive information

## **3. General Policy**

- a. Management will maintain a corporate governance framework and control environment that promotes its values including the requirement for all levels of employees to adhere to the Code of Conduct.
- b. Control activities will be designed and adapted to mitigate fraud risks identified internally and by the external auditors.

# **ANTI-FRAUD POLICY**

(Version 2.0 – June 2019)

## **4. Responsibilities for Anti-Fraud**

4.1 Management has the overall responsibility for managing the risk of fraud across the Group including:

- conducting and documenting fraud risk assessments at least once a year to identify the risks and the related mitigating measures;
- developing and maintaining effective internal controls to prevent and detect fraud;
- ensuring that these controls are being complied with;
- monitoring the effectiveness of its controls related to mitigating fraud risk and remediation of any deficiencies identified internally or by the external auditors in a timely manner;
- effectively communicating the Anti-Fraud policy to all levels of employees including the procedures for reporting and responding to fraud to employees and relevant external parties;
- ensuring that the Anti-Fraud Policy requirements have been complied with and compliance is confirmed as part of the annual General Representation Letter process (including the completion of the Fraud Risk Assessment).

4.2 All employees have the responsibility to:

- fully adhere to the principles in the Code of Conduct and to act with the highest standards of honesty, integrity and ethics;
- comply with the Group's policies and procedures and the internal controls requirements;
- report details of suspected fraud to Group Internal Audit in a timely manner.

4.3 Group Internal Audit has the responsibility to:

- undertake periodic fraud risk assessments during the regular internal audits to review the design, performance and overall effectiveness of fraud controls;
- conduct periodic 'tone at the top' surveys to obtain employees' views on their management's ethical commitment and reporting of irregularity cases (average frequency is every 3 years).
- establish and maintain effective reporting channels for staff to report any suspicions of fraud (refer to the Group's Whistleblowing Policy for details);
- investigate suspected fraudulent activities and report to the appropriate parties as necessary;
- maintain and administer Anti-Fraud and related policies, and communicate this Policy and its requirements to all levels of employees as part of the periodic Code of Conduct training.

## **5. Fraud Response and Reporting**

5.1 Suspected cases of fraud should be reported promptly, whether it is known who may be responsible for the fraud or how it may have occurred. They should be reported to one's direct supervisor, team leader or unit manager or directly to the Senior Director-Group Internal Audit.

5.2 As CLP takes this reporting seriously and wants to investigate all potential cases, it is preferred that these reports not be made anonymously. However, it is recognized that for any number of reasons an employee may not feel comfortable reporting potential fraud cases directly. In these cases, anonymous reports should be submitted to the Senior Director-Group Internal Audit. These reports can be made verbally (telephone) or in writing (letters or email).

# **ANTI-FRAUD POLICY**

(Version 2.0 – June 2019)

Everyone in senior management will fully support those who in good faith report potential cases of fraud. For further details on the reporting channels and process, refer to the “Whistleblowing Policy”.

- 5.3 All potential fraud cases should be investigated by Group Internal Audit, except where responsible subject-matter-expert functions are required to conduct the investigations (e.g., cybersecurity incidents investigated by Group Information Technology in accordance with the CLP Group Information Security Policies). These investigations will be handled confidentially. Management will take immediate corrective actions to resolve substantiated cases of fraud. Management will implement internal control improvement measures to prevent similar fraudulent activities from occurring again.
- 5.4 The Senior Director-Group Internal Audit will report fraudulent activity to the Board Audit and Risk Committee at least annually. This report will include the number of cases reported, the nature of important investigations and the results of those investigations. Since the responsibility for monitoring fraud ultimately rests with the Board, the Audit and Risk Committee will submit a summary of fraudulent activity to the Board at least annually.
- 5.5 All material fraud cases and any fraud committed by employees which could impact the Group’s system of internal controls will be reported to the external auditors.
- 5.6 If there is sufficient evidence to suggest that a case of possible criminal offence or corruption exists, the matter will be reported by the Group to the relevant local authorities (for instance, Independent Commission Against Corruption (ICAC) in Hong Kong). In some situations (e.g. in case of possible criminal offence), the Group may have to refer the matter together with the relevant information to the authorities. Please note that once the matter is referred to the authorities, the Group will not be able to take further action on the matter until the investigation by the authorities is complete.
- 5.7 Anyone found committing fraud will be subject to disciplinary action which may include dismissal.