Anti-Fraud Policy

Version	Date	Division
3.0	18 March 2026	Internal Audit & Risk Management

1. Introduction

The Company is committed to the prevention, detection, response, and reporting of fraud.

The Anti-Fraud Policy is to safeguard the Company, customers, and partners against fraudulent activities like scams, identity theft, or misuse of services, fostering a culture of integrity, and complying with Hong Kong laws and regulations. It applies to all employees of the Company, and the Company encourages all business partners, including contractors and suppliers, to abide by the principles of this Policy.

The Anti-Fraud Policy is an integral part of the Company's Corporate Governance Framework. This Policy complements and should be read in conjunction with the Employee Handbook and the Whistle Blowing Policy. The Anti-Fraud Policy and other policies within the Corporate Governance Framework are available on the Company's corporate web site.

2. Scope of the Policy

Management has an overall responsibility to ensure that risk culture and continuous fraud awareness are established with the Company.

The policy applies to all employees, contractors, vendors, partners, and customers interacting with the Company's services, systems, or assets.

"Fraud" commonly refers to deceptive conduct with the intention of making some form of financial or personal gain or causing other person suffering a loss. It covers, but not limited to, deception, bribery, forgery, extortion, theft, conspiracy, embezzlement, misappropriation, false representation, concealment of material facts, collusion and money laundering. Examples of fraudulent behavior include but not limited to:

- Obtaining financial advantage or any other benefit by deception or abuse of authority of official position or duty
- Unauthorized business activities involving conflict of interest and/or gaining of personal interests
- Soliciting, accepting, offering, promising or payment of bribes from or to any individual, company or government official
- Offering or receiving any gift, gratuity or hospitality to influence business decisions
- Entering into deceitful agreements with third parties for unfair advantage or other types of collusive activities with third parties
- Improper use of customer data, commercially sensitive information or Company's information not released to the public
- Theft, unauthorized use and/or disposal of Company's assets or resources

- Claiming personal expenses as business expenses, or other types of false expense claims or false invoicing
- Impropriety in the handling or reporting of money or financial transactions
- Any similar or related irregularity

3. Company's stance on fraud

The Company has zero tolerance for fraud. All stakeholders must report suspicions promptly. Failure to comply may result in disciplinary action, termination, or legal prosecution.

If there is any suspicion that an employee is involved in misconduct, the Company reserves the right to suspend their duties at any time. The Company may also, with or without prior notice to the employee, report the case and relevant information to government or law enforcement agencies for investigation and proceedings. All employees are required to cooperate fully with both internal and external investigations.

4. Fraud Preventive/ Detective Measures

Management has maintained a corporate governance framework and control environment which continuously reviews the control activities to ensure their adequacy to mitigate fraud risks identified internally or by external auditors. Control activities include but not limited to the following:

For Customers:

- Verify identities using official documents (e.g. HKID card or passport)
- Add extra security steps for risky actions (e.g. changing contact information or replacing an SIM card requires SMS/email notification)
- Encrypt sensitive customer information
- Automated alerts for unusual usage patterns (e.g. sudden surge of roaming usage)

For Employees:

- Grant access to sensitive systems on a need-to-know basis
- Automated alerts for potential information leakage
- Regularly check for unusual activity (e.g., bulk orders of SIM cards)

For Partners/Vendors:

- Work only with trusted partners who follow anti-fraud rules

5. Fraud Response and Reporting

Employees should report suspected cases of fraud at the earliest possible stage through the Whistle Blowing Policy, whether it is known who may be responsible for the fraud or how it may have occurred.

Cases will be investigated by the designated Whistle Blowing Officer. Relevant Parties making reports under the Company's Whistle Blowing Policy is assured of protection against unfair dismissal, victimization or unwarranted disciplinary action, even if the reports are subsequently proven to be unsubstantiated.

Employees may be required to assist in the process of evidence collection in any investigation. Employees must co-operate with an investigation, provide requested information and may not interfere with or hinder the course of an investigation.

Employees found committing fraud will be subject to disciplinary action which may include summary dismissal.

If there is sufficient evidence to suggest that a case of possible criminal offence exists, the matter will be reported to the relevant local authorities (e.g. Police, Independent Commission Against Corruption). Once the matter is referred to the authorities, the Company will not be able to take further action on the matter until the investigation by the authorities is complete.

6. Communication and Training

This policy is available on the Company's intranet. The Human Resources Department arranges training for all new employees. Training records are kept by the Human Resources Department.

7. Monitoring and review

Unless prohibited by law, the Whistle Blowing Officer will report to the Audit Committee all confirmed true and genuine concerns received under this policy and actions taken in response to each concern.

Management will review the effectiveness of this policy on a regular basis.