Version 5

Hong Leong Group

Code of Conduct & Ethics for Employees

Table of Contents

OVERVIEW OF THIS CODE

PURPOSE

The Hong Leong Group ("**Group**") expects a high standard of professionalism and ethics from its Employees (hereinafter defined) in the conduct of its business and professional activities as set out in this Code of Conduct and Ethics ("**Code**").

This Code is designed to observe and comply with all applicable laws, regulations and regulatory requirements. Employees at branches and subsidiaries of the Group located outside Malaysia are expected to know and comply with the laws, regulations and Codes of Conduct that apply to them. In cases where local laws and/or regulations prescribe different requirements, the stricter of the requirements shall apply.

This Code may not cover every ethical situation Employees may encounter in their course of work. In any circumstance which is not covered by this Code or in case of any doubt, Employees shall refer to his or her Head of Department or Human Resources Department for clarification or guidance.

SCOPE

This Code applies to:

i. All employees who work in the Group – including, but not limited to, permanent, part-time and temporary employees; and
ii. Any other persons permitted to perform duties or functions within the Group – including, but not limited to, vendors, suppliers, contractors, secondees, interns and industrial attachment students ("collectively, **"third-party service providers**").

POLICY STATEMENT

Employees are responsible for fully understanding and complying with the Code. Employees are required to undergo any training provided in relation to the Code and provide an annual affirmation that they have read, fully understood and will comply with the Code.

If you have any questions about the expected standards, laws, rules, regulations and internal policies that apply to you, talk to your supervisor, Head of Department or Human Resources Department at askhr@hlmg.com.my

The Code also forms part of the terms and conditions of the Employee's employment or engagement with the Group company they are employed/engaged with ("Company"). Any failure to comply with this Code or any of the Group policies relevant to the Employee's role will be treated very seriously by the Group. Such failure shall constitute misconduct and may result in disciplinary action, up to and including termination of employment (for Employees) or termination of engagement or relationship (in relation to contract staff) with the Group and such other consequences as set out in the Code.

There are seven (7) key principles to the Group's Code as set out below:

i. COMPETENCE
ii. COMPLIANCE
iii. INTEGRITY
iv. DEALINGS WITH CUSTOMERS
v. CONFIDENTIALITY
vi. OBJECTIVITY
vii. WORK ENVIRONMENT

PRINCIPLE 1: COMPETENCE

All Employees must help ensure the Group meets its legal, compliance and regulatory obligations, as well as stakeholder and customer expectations, by possessing and maintaining the skills and knowledge needed to perform their roles professionally and proficiently. As such, it is the Employees' duty and responsibility to ensure that they:

Attain Competence

i. Acquire the relevant knowledge, skills and behaviours to attain the competency requirements of the role and the standards of the Group;
ii. Carry out their duties and responsibilities responsibly and competently;
iii. Seek help from their immediate superior to fill in any gaps in skill, knowledge or expertise; and
iv. Understand the steps to be taken to achieve the required competence.

Maintain Competence

i. Keep up-to-date with the job requirements;
ii. Continuously learn and improve their skills, knowledge and expertise for their role and job function; and
iii. Proactively keep abreast with changes in law, regulation and industry best practice that is relevant to their role and function, and to the business of the Company.

PRINCIPLE 2: COMPLIANCE

Personal Declarations on Legal and Regulatory Proceedings, Fitness and Propriety

Employees must promptly declare in writing to the HR Department at askhr@hlmg.com.my any criminal, legal or regulatory proceedings in which they are involved, whether or not the proceedings relate to the Group, including:

i. Any arrest, charge, conviction or legal proceeding relating to a criminal charge including unresolved criminal charges, however minor;
ii. Any inquiry or action by a financial institution regulator, law enforcement agency or similar authority; or
iii. Any legal claims against them relating to fraud, dishonesty, or unfair or unethical conduct committed by them.

Employees do not need to declare minor traffic offenses. If Employees have questions on whether they need to declare a criminal, legal or regulatory proceeding, contact the HR Department.

Employees acknowledge that the Company may make external checks to verify their probity and integrity prior to appointment and thereafter, as and when deemed fit.

Compliance with Laws and Regulations

Employees must comply at all times with all applicable laws, regulations and regulatory requirements, and be open and transparent with regulators. It is important to comply with not just the letter, but also the spirit and intent, of the law.

All Employees must fully cooperate with, and provide accurate information for, any internal or external investigations, subject only to confidentiality requirements or legal privilege.

Additionally, Employees are responsible for fully understanding and ensuring compliance with legal or regulatory requirements which are specific to their role and/or as an Employee.

Violations of the Code or any laws, regulations, or regulatory requirements that apply to the Group will weaken the confidence of regulators, stakeholders or customers and put the Group's reputation at risk. This can result in negative repercussions for the Group including sanctions by regulators, legal action, fines and penalties.

Please take note that Employees may, regardless of whether any such negative repercussion is imminent or threatened, be subjected to the consequences for breaches or violations of the Code.

Misconduct that will result in the consequences for breaches or violations of the Code also includes:

i. Violating, assisting or asking/instigating others to violate the Code;
ii. Failing to raise a known or suspected violation of the Code; and/or
iii. Retaliating against another Employee or third party for raising a concern in good faith or for participating in an investigation.

Competition Laws

Employees must ensure that their interactions with business partners, competitors and governmental authorities at all times are in compliance with the laws and regulations governing competition. Conduct that Employees shall comply with include:

i. To not enter into or cause the Company to enter into any form of agreement or arrangement (whether written or otherwise) with other businesses/enterprises, or to engage in any conduct or cause the Company to engage in any conduct, which has the object or effect of significantly preventing, restricting or distorting competition in any market for goods or services; and
ii. To not engage in any conduct or cause the Company to engage in any conduct which, under the relevant anti-competition laws, amounts to an abuse of a dominant position in any market.
iii. To not engage in or enter into any form of agreement, arrangement or concerted practice with an actual or potential competitor that is or may be deemed to be anti-competitive, such as fixing prices, sales or markets.
iv. To not communicate or share commercially sensitive information with actual or potential competitors, or third parties who may potentially pass such information to competitors.
v. To use commercially sensitive information for legitimate purposes only.

Anti-Money Laundering, Countering the Financing of Terrorism, and Countering Proliferation Financing

i. All persons, including employees, third-party service providers and business partners, must abide by all laws and regulations pertaining to Anti-Money Laundering, Countering the Financing of Terrorism; and Countering Proliferation Financing, which, inter alia, addresses the prevention of disguising illegally obtained funds as legitimate income, halting the flow of funds to terrorist organizations and preventing the funding of the proliferation of weapons of mass destruction. .

ii. Employees and third-party service providers must always ensure that they are conducting business with reputable counterparties, for legitimate business purposes and with legitimate funds. If they suspect money laundering activities, they must report it to their respective Head of Department or the relevant person designated by the Company.

PRINCIPLE 3: INTEGRITY

The Group's Vision, Mission and Values identifies a strong values-based culture to guide decisions, actions and interactions with stakeholders as a key enabler for the success of the Group.

General Conduct

All Employees have a responsibility to uphold the Code and as an Employee of the Group, they have a duty to demonstrate the highest standards of business conduct by doing the right thing.

The Group relies on Employees to practice sound decision-making and take actions that will preserve a strong values-based culture in the workplace. Employees are responsible for their decisions and must not engage in unethical or illegal conduct, even where they are acting on the instructions of another colleague, their manager or superior. If Employees are ~~ever~~ unsure of the proper course of action, they should seek advice from their Head of Department or HR Department, as appropriate.

The Group further relies on the Employees to discharge the Company's or the Group's contractual obligations, covenants and agreements owed to a third party, failing which the Company/Group may face financial liabilities towards such third parties. Employees are responsible for their acts or omissions that may result in any breach of such obligations, covenants and agreements by the Company or the Group.

Anti-Bribery and Corruption

The Group does not condone any form of bribery and corruption and is committed to acting professionally, fairly and with integrity in all our business dealings and relationships.

The Group does not condone or consent to any employee or any person associated with the Group:

(a) Corruptly soliciting, receiving or agreeing to receive any gratification whether for him/herself or for any other person; or
(b) Corruptly giving, agreeing to give, promising or offering to any person any gratification whether for the benefit of him/herself or of another person.

You must at all times comply with local anti-bribery and corruption laws and regulations. In Malaysia, the main legislation is the Malaysian Anti-Corruption Commission Act 2009. Severe penalties, including heavy fines and imprisonment, can be applied to any person found guilty of bribery or corruption.

Integrity of Records and Information

Record-keeping policies and controls are essential to the successful operation of the Group and the Group's ability to meet its legal and business obligations. Employees are responsible for being accurate, complete and honest in the Group's records and for complying with all of the record-keeping policies, controls and procedures that the Group has in place.

Employees must never falsify any book, record or account that relates to the business or activities of the Group, customers, Employees, suppliers or Group assets. This means being honest and accurate in all aspects of their job, including without limitation, entries they make on expense reports, time-keeping records, results they record on sales incentive plans and claims they make under the Group Employee or Employee benefit plans.

Accounting records and reports must be complete and accurate. Employees must never make entries or allow entries to be made for any account, reports, records or documents that are false or would obscure the true nature of the transaction, or to mislead the true authorisation limits or approval by the relevant authority of such transactions.

The Group's Assets

The Group's assets are the resources it uses to conduct its business and includes assets of its counterparties which are provided to the Group under contractual arrangements (collectively "**Assets**"). Employees are to use Assets for legitimate business activities in line with our contractual obligations and appropriately safeguard them including against cyber-related attacks, theft, loss, waste, improper use or abuse.

The Group's assets include, without limitation:

i. Physical assets, such as office furnishings, facilities, cars, equipment and supplies;
ii. Technology assets, such as laptops, tablets, computer hardware, software and information systems and technology applications;
iii. Financial assets, such as cash, equities, bonds etc; and
iv. Information assets, such as Intellectual ~~p~~Property, source codes, computer programmes including information about products, services, systems and other data.

Employees acknowledge that their use of the Group's ~~a~~Assets, including email and internet, may be monitored by the Group, to detect misconduct.

Intellectual Property

i. Any invention, improvement, literary rights, copyrights, trademarks, patents and/or new discoveries ("**Intellectual Property**") which originates from or is conceived by them, whether alone or with any person or persons while in the employment of the Company, which relates either directly or indirectly to the Group, shall belong to and be the absolute property of the Company.
ii. Employees shall promptly disclose to the Company all such Intellectual Property made by them alone or with any person or persons and shall hold such Intellectual Property on trust for the Company.
iii. Employees shall assign and hereby agree to assign to the Company any and all rights to the Intellectual Property, as and when directed by the Company and further agree that the Company and its successors and/or assignees shall have the absolute right to use experimentally or commercially the Intellectual Property or any part thereof.
iv. Employees shall at the request and expense of the Company do all things necessary or desirable to substantiate the rights of the Company as mentioned here.
v. This provision shall not apply to any invention for which no equipment, supplies, facilities, know-how or trade secret information of the Group was used and which was developed entirely on their personal time and which does not relate to the business of the Group, directly or indirectly, or the Group's actual or demonstrated anticipated research and/or development, or which does not result from the work performed by them for the Group.However, the employee is obliged to inform the Company of any such activities they undertake, regardless of the nature or scope.

Unauthorized Dealings with Third Parties

Employees are not authorized to act on behalf of the Company or the Group in entering into or signing any contracts or making any commitments with third parties, unless they have obtained prior written clearance from the appropriate approving authority in the Company and/or the Group. Any such action will be considered a serious breach of conduct. The Company reserves the right to take legal action against the employee for any loss or potential loss incurred as a result. Furthermore, the Company retains the right to terminate the employee's employment immediately and without compensation in such cases.

Personal Finances

As an Employee, any improper handling of personal finances could undermine their credibility and the reputation of the Company/Group. It could also cause others to question their decision-making on the job or task that an Employee is handling.

Therefore, Employees must handle their personal finances responsibly, with integrity and in compliance with all relevant laws and regulations and the contractual terms to which they are bound. In relation to

their borrowings, Employees must not abuse and must be seen not to have abused their position for their personal advantage and the aggregate of their debts shall not cause them serious pecuniary indebtedness.

Employees must not promote or participate in illegal financing schemes, tontine schemes (kootu funds) or otherwise carry on illegal activities for their own personal gain or the gain of others.

PRINCIPLE 4: DEALINGS WITH CUSTOMERS

Employees must, at all times, deal with customers with honour and integrity, and maintain the trust of customers.

PRINCIPLE 5: CONFIDENTIALITY

Protecting Confidential Information

The Group's Employees, business partners and customers trust the Group to protect their confidential information, whether that information relates to financial, personal or business matters.

Confidential information can be written, oral or electronic and includes a wide variety of data – including, but not limited to, technology applications, business strategies, customer lists, credit procedures, customer and personnel information.

In the course of and after cessation of the Employee's employment/engagement, the Employee must not disclose or misuse confidential information of the Group, its Employees, business partners or customers, for any reason whatsoever.

Employees have a duty to protect such confidential information and where disclosure of such confidential information is duly authorised, to take precautions before sharing it with anyone, inside or outside the workplace:

i. Do not share confidential information with friends or family, third parties or with colleagues who are not authorised to receive such information;
ii. Do not discuss confidential information in public or common places where others could hear them (such as corridors, lift, lobby etc.);
iii. Do not access or use confidential information for unauthorised purposes;
iv. Do not widely circulate confidential information, in internal mass postings, or outside the Group (including to their own personal email address), unless permitted to do so under applicable law, regulations, and internal policy or procedures;
v. Do not use audio, video, or other recording equipment to record company meetings, discussions, interviews, disciplinary enquiries or workplace conversations without the express approval of the Chairperson of the meeting or the person being recorded (recordings carried out for official purposes are excluded from this restriction). If recording is permitted, it must be kept confidential, secured, password-protected and destroyed in accordance with information retention period.
vi. Do not upload or transfer any information obtained in the course of work (including confidential information and personal data) onto any third-party platforms on the internet unless prior written permission of the respective Head of Department has been obtained ~~and~~ provided always that applicable laws, regulations, guidelines, and internal policy or procedures are complied with.. This includes web or mobile-based applications and generative artificial intelligence ("AI") tools on company issued devices or personal devices;Collect confidential papers immediately from printers, photocopiers and fax machines;
vii. Be vigilant about whether their computer screen or papers can be read by someone else;

viii. Use passwords and regularly change passwords. Do not share passwords with anyone;

ix. Ensure hard copy confidential information is stored in locked cabinets and soft copies is securely stored; and

x. Shred any documents containing confidential information when they are no longer needed.

Misuse of Information

Employees are prohibited from using material, confidential or non-public information about the Group, its Employees, customers or third parties or other companies that conduct business with the Group for unauthorised purposes or to gain a direct or indirect advantage for themselves or any other person.

Employees must not deal or procure any person to deal in the securities of any company listed or pending listing on a stock exchange at any time when they are in possession of information which they know, or reasonably ought to know, is inside information.

Employees must also keep such inside information confidential and not disclose such information to any person who is not authorised to receive such information. In addition to a breach of the Code, such dealing or disclosure of inside information may also constitute a criminal offence.

'**Inside information**' is information relating to a public listed company which is not generally available to the public and which, if made generally available, would or would tend to have a material effect on the price or value of the securities of such company.

'**Dealing**' includes acting as principal or agent, in acquiring or disposing (or agreeing to acquire or dispose) such securities. Procuring or inducing another person to deal is also prohibited.

Disposal or Return of Confidential Information

Disposal of confidential information must be done in a way that protects the confidentiality of the information. Paper records must be shredded and storage media must be formatted in a way that ensures third parties or unauthorised persons cannot access the information.

Press Releases, Public Statements, Appearances and Appointments

Employees must not make any (oral, written or other) public statement regarding the Group unless with prior written approval from the President/ Group Managing Director ("**GMD**")/ Chief Executive Officer {"**CEO**") (as applicable). This includes without limitation the Group's internal policies, financial

information, internal affairs or corporate affairs or any statement containing or relating to the Group's confidential or proprietary information.

In case of matters concerning the Group, the President/GMD/CEO or other duly authorised person (as applicable) is authorised to make or release any statements on the Group or the relevant Group company to the media or the public, provided that they are statements undertaken in compliance with Group Policy on Public Relations and External Communications.

Employees must promptly inform their President/GMD/CEO (as applicable) if they are approached by a member of the media to comment on any matter pertaining to the Group or a Group company.

Unless with prior written approval from President/GMD/CEO (as applicable) or as allowed under the Group Policy on Public Relations and External Communications, Employees must not:

i. Accept offers for media exposure for the promotion of self or self-interests;
ii. Participate as a speaker in talks, seminars, conferences in their capacity as a Company Employee or on areas of work expertise that are not sanctioned by the Group;
iii. Accept appointments to councils, committees or boards for any associations, governmental or non-governmental organisations, societies etc. in their capacity as a Company Employee. For appointments in their personal capacity, please read carefully the section on **Conflict of Interest;** or
iv. Give reference for any person or entity in the Group's capacity or use the Group's name, save insofar as required in the course of normal business.

When in doubt, you must consult the HR Department and seek approval from your President/GMD/CEO (as applicable).

Social Media Usage

Employees must use good judgment in the use of social media and other online activity.

You must not disclose confidential and/or proprietary information of the Group on social media. Do not post or seek posting of confidential information or information which could cause reputational damage to the Group, its Employees, stakeholders, customers or business partners.

Such restricted postings include referrals, recommendations, materials subject to intellectual property rights, photos, videos, etc. as well as personal data of the Group .Information, regardless of whether is true or accurate, that might damage the reputation of the Company/Group is not to be posted or disseminated and instead, should be reported to the HR Department to facilitate proper handling of the matter, should the Employee become aware of such information.

PRINCIPLE 6: OBJECTIVITY

Employees must not allow any conflict of interest, bias or undue influence of others to override their business and professional judgment. They must not be influenced by friendship, relationships or association in performing their role. Decisions must be made on a strictly arms-length business basis.

Conflict of Interest

Employees must not engage directly or indirectly in any personal or business activity that competes or conflicts with the interest of the Group:

i. Other Business Interests and employment

Conducting any non-Group paid or unpaid employment or business activity (including acquiring another business) is prohibited.

Employees must not undertake paid or unpaid employment or other business activities ~~outside~~ of the Company's working hours unless they have prior written approval from their Head of Department and the HR Department. Approval shall be granted only where the interests of the Group will not be prejudiced.

If an Employee has an interest in a customer, business partner or supplier of the Group or any Group Company – for example as a sole proprietor, partner, shareholder, creditor or debtor, which may result in or causes a conflict or potential conflict of interest, such an interest must be disclosed immediately to the HR Department. The Employee must not be involved in the Group / Company's dealings with the customer, business partner or supplier so long as the interest continues to exist.

ii. Corporate Directorships

Employees must not serve as a director of an ~~legal~~ entity (other than a Group company) without the approval of the HR Department.

If an employee is nominated to serve as a director or as an office bearer or as an advisor/consultant of an industry-related or professional legal entity, body or association in their personal capacity, the prior approval of the company's CEO/GMD/Operating Manager (as applicable) and the President is required before the employee can accept the nomination. In such a case, the HR Department shall be notified after approval is obtained. Subsequently, the respective HR Department must inform GHR after receipt of such notification.

iii. Trusteeships

Employees may only accept an appointment as an executor, administrator or trustee of the estates of a Group customer which may result in or cause a conflict or potential conflict of interest if they have prior written approval from the HR Department. If such an appointment is made without their knowledge, the Employee must notify the HR Department without delay to obtain their approval to retain such appointment once the Employee becomes aware.

iv. Working with Relatives

Employees should not work with their immediate family members (i.e. spouses, parents, siblings or children) as colleagues, or with another colleague with whom they have a romantic relationship, in the same Division/Department/Branch and/or in a position of direct and/or indirect subordination or supervision within the Company/Group.

Employees must promptly declare any such situations to the HR Department. The Company has the right to take all necessary steps to ensure any element of conflict is removed, including requiring the transfer of affected colleagues.

When in doubt about any potential situation of conflict, Employees must consult the HR Department and declare the relationship.

Misuse of Position

Employees must not use their position to influence other Employees, current and potential customers or business partners of the Group to act in their personal interest or in the interest of anyone other than the Group.

For the avoidance of doubt, Employees are prohibited from using or allowing the use of the Group's name or facilities, their position and/or connection with the Group:

i. To gain personal advantage for themselves or for others, including in political, investment or other activities;
ii. To gain preferential treatment for themselves or for others, such as in purchasing goods, securities and in obtaining loans; or
iii. For speculative activities in commodities (gold, silver etc.), foreign exchange or securities, whether acting personally or on behalf of another.

Employees must not enter into prohibited transactions through nominees. Immediate family members (i.e. spouses, parents, siblings or children) are presumed to be nominees.

Gifts and Entertainment

Employees are strictly prohibited from giving or receiving a gift or entertainment which is, or which appears to be inappropriate or excessive, taking into account all relevant facts and circumstances.

Employees must promptly declare any gift or entertainment which they (or others on their behalf) give or receive in accordance with their Company's Gifts and Entertainment Policy and Procedures.

PRINCIPLE 7: WORK ENVIRONMENT

Safe and Healthy Workplace

A safe and healthy workplace is important to the wellbeing of every Employee. All Employees have a duty to help maintain a healthy and safe working environment at the workplace and to comply with applicable health and safety laws (as amended from time to time), including the Penal Code and the Occupational Safety and Health Act 1994, as well as the Group's policies and directives as they relate to the health, safety and security of its workforce, its customers and others who may be present at their place of work.

Employees have a duty to take reasonable care of their safety and health and that of other persons who may be affected by their acts and omissions at work. If an Employee becomes aware that they may pose a health or safety risk to others at their place of work, such as them having or suspecting that they have an infectious disease, the Employee must immediately inform the HR Department and co-operate with the Company to take necessary steps to address such risk.

Harmonious Working Environment

The Group employs/engages people from a variety of backgrounds, ethnicity, origin, experience, culture and religion. It strives to promote diversity and inclusion in the workplace and a harmonious working environment. Employees must not, at any time, engage in or support acts of harassment or inappropriate or abusive conduct by or against the Group's Employees, customers or business partners.

The Group strictly prohibits all forms of bullying and harassment, whether in person, digitally or online (cyberbullying), whether acting with or without intent to bully or harass — such as:

- Use of threatening, abusive, or insulting words, language or behaviour
- Harassment or intimidation of any kind
- Psychological provocation or emotional pressure
- Misuse or publication of identity information of a person with intent to harm, including psychological harm (e.g., doxing)

The Group will take allegations of discrimination, harassment or intimidation seriously. It is the responsibility of every colleague to report to the HR Department of any behaviour or conduct that is unlawful, abusive or otherwise violates this Code.

Drug-free Workplace and Alcohol Consumption

Employees must not grow, manufacture, distribute, possess, sell, use or be under the influence of illegal drugs or substances at all times, whether in the workplace or outside, or whether during working hours or beyond.

Employees must not consume alcohol at any time during the working day, and/or at any official or business event, to such a level that their ability to work is impaired.

Workplace

All Employees are reminded to always be mindful, respectful and sensitive in their actions and words at the office. The Group prohibits all Employees from:

i. Carrying out personal activities such as promoting religious or political beliefs amongst colleagues;
ii. Carrying out political campaigns at the office; and
iii. Performing prayer ritual in the workplace or common areas within the workplace without the prior approval of the HR Department.

SPEAKING UP AND/OR ESCALATING CONCERNS

You must speak up if you witness, become aware of or if you are instructed to carry out or assist with any illegal or unethical act within the Group, including a request from a colleague or third parties (such as customers, regulators, vendors or business partners).

You are required to promptly report any known or suspected violations of the Code, any Group policy or any law, regulation or regulatory requirements applicable to the Group's business. Reporting is required whether or not you are involved in the violation.

You are also encouraged to report grievances or concerns relating to interactions with colleagues or management — including all forms of bullying and harassment.

There are various internal channels that you can use to report potential misconduct or potential ethical concerns. You can raise your concerns to your Head of Department or Human Resource Department at askhr@hlmg.com.my or the Company's whistleblowing channel.

Employees are encouraged to first discuss the matter directly with their immediate supervisor. If the issue remains unresolved, a formal grievance can be submitted to the Human Resource Department at askhr@hlmg.com.my

Just as they will be held responsible for their own actions, an Employee can also be held responsible for failing to report the actions of others if they knew or should reasonably have known that they were in violation of the Code, any applicable policy, law, regulation or regulatory requirements.

The Company prohibits any form of retaliation against any individual who report concerns, violations or suspected wrongdoing in good faith, regardless of who the report involves and against those who assist or cooperate in any investigation. Retaliation means any adverse action taken against a person because they reported or cooperated in such an investigation. Individuals who engage in retaliation are subject to disciplinary action up to and including termination of employment.

Employees' report will be handled discreetly and shared where necessary, for example with persons who are involved in investigating, resolving, or remediating the issue. If Employees have concerns about possible retaliatory action, they may lodge a report with their Head of Department or through the Company's whistleblowing channels.

Critical Incident Reporting

A Critical Incident is an incident that poses a severe financial, legal, reputational or operational risk and/or impact to the Group or Company. This includes but is not limited to, incidents of fraud, corruption, theft, material regulatory non-compliances, any incident that may result in significant

financial loss or reputational damage, employee strikes and workplace safety incidents such as fire, severe injuries, death, acts of violence or other threats.

All Employees have a responsibility to promptly report Critical Incidents that he/she is aware of. To report a Critical Incident, these steps should be followed:

i. **Immediate Action:** If there is an immediate threat to life and safety, prioritise the safety of individuals involved. Call the emergency services such as the police department, fire department or ambulance if necessary.
ii. **Notify:** Promptly notify your superiors, relevant functional reporting heads for prompt communication to the heads of the Group Company involved, namely the Group Managing Director ("**GMD**") or Chief Executive Officer ("CEO"). Depending on the nature of the incident, report to the relevant department, such as HR, IT, Legal or Compliance.
iii. **Escalate:** The heads of the Group Company must then promptly report any major Critical Incidents (as further described below), e.g. incidents include assaults on employees, hostage-takings, the suicide or murder of a co- worker, accidents causing bodily harm or death, natural disasters including floods, fires and tornadoes to the Intermediate Group ("**IG**") level (i.e. President). The President/GMD/CEO (as applicable) should then escalate any major Critical Incidents to the senior management of HL Management Co ("**HLMC**"). This is to enable the Group to manage the situation appropriately in order to mitigate any risk posed or impact to the broader Group or the relevant Group company.
iv. **Maintain Confidentiality:** Employees must ensure that any information relating to the Critical Incident is handled with utmost confidentiality and shared only with the relevant authorised persons.

A Critical Incident may be deemed major if it fulfils one of the following:

1. **Potential for or actual harm**: Incidents with the potential or actual impact of causing serious harm to the safety, health and well-being ~~to~~ of individuals, the organisation or the environment for example serious injuries, fatalities or risk of environmental damage or pollution.
2. **Disruption of operations**: Incidents that disrupt the normal functioning of an organisation's operations or services for example a prolonged electrical outage, major fire incident or flood-related damage.
3. **Public or regulatory interest:** Incidents that attract or have the potential of attracting a high level of public or regulatory scrutiny, for example an employee strike, major breaches in health and safety protocol.
4. **Multiple system failures**: Incidents that involve more than one failure or error in a system or process, for example a targeted cybersecurity attack where core systems are compromised.

Failure to report Critical Incidents shall constitute a serious misconduct and appropriate disciplinary action, including termination of employment, may be taken against the Employee.

CONSEQUENCES OF BREACH BY EMPLOYEES

Where an Employee breaches or violates any part of the Code, the Group reserves the right, at any time, whether or not such breach or violation has since been remedied, to carry out any one or more of the following against the Employee:

i. Remove the Employee from certain positions or roles e.g. position of authority or trust, including without limitation, cash handling;
ii. Take disciplinary action, including without limitation, suspension of employment;
iii. Terminate their employment or terminate their engagement or relationship (in relation to contract staff), with immediate effect upon notice and without compensation;
i. Seek payment or take legal action for any loss or damages suffered by the Company ~~or~~ including to recover any loss in respect of indemnity claims made by third parties
ii. Seek remedies in a civil court including but not limited to monetary damages and/or a court order prohibiting the Employee from violateing the Code or any laws, regulations, or regulatory requirements that apply to the Group;
iii. Report such violation to the police, law enforcement agencies and/or regulators, which may result in criminal liabilities and/or penalties for the violating Employee; or
iv. Report such violation in employment records databases maintained by regulatory authorities and/or industry bodies which may be referred to by future employers during the employment process.

Without prejudice to the foregoing, if an Employee fails to fulfil his/her financial obligations as and when they fall due or has been the subject of a judgement debt which is unsatisfied, either in whole or in part, the Company may take appropriate action, including without limitation, to:

i. Remove the Employee from certain positions or roles e.g. position of authority or trust, including without limitation, to cash handling; or
ii. Terminate employment if the Employee is adjudged bankrupt or is, in the opinion of the Company, no longer suitable to be employed by the Company.

In addition, an Employee's career advancement may also be impacted as a result of his/her poor financial standing, such as his/her promotion being withheld.

.

MISCELLANEOUS

The following capitalised words used in this Code shall have the meanings as shown below:

Term	Definition
CEO	Chief Executive Officer
Code	Code of Conduct and Ethics.
Company	Company that an Employee is employed with or engaged by
Employee	(i) All employees who work in the Group – including, but not limited to, permanent, part-time and temporary employees, secondees, interns and industrial attachment students; and (ii) Any other persons permitted to perform duties or functions within the Group – including, but not limited to, contract and agency staff ("**contract staff**").
Group	Hong Leong Company (Malaysia) Berhad and GuoLine Capital Assets Limited and its direct/indirect subsidiaries (each of them, a "**Group company**").
Head of Department	Head of Department in a Group company.
HR	Human Resource
GHR	Group Human Resources
GMD	Group Managing Director
Intellectual Property	any invention, improvement, literary rights, copyrights, trademarks, patents and/or new discoveries.
President	Intermediate Group President

POLICY DOCUMENT INFORMATION

Policy Owner	Chief Human Resources Officer	
Responsible Person(s)	Heads of Departments	
Version No. and Date Approved	Version 1	August 2020
	Version 2	July 22, 2021
	Version 3	Nov 22, 2022
	Version 4	Nov 24, 2023
	Version 5	Nov 4, 2025
Summary of Revisions	**Principle 3 (Integrity):** **General Conduct** Added point to emphasizes the critical role employees play in ensuring that the company or group meets its contractual obligations to third parties. It reinforces accountability by making employees aware that their actions or inactions can directly impact the organization's legal and financial standing and reputation. **The Group's Assets** Added point to reinforces the importance of responsible asset management and security within the organization. It ensures employees understand their duty to protect both the company's and counterparties' assets entrusted to them under contractual agreements. **Principle 7 (Work Environment):** **Harmonious Working Environment –** added recent Penal Code amendments, which explicitly criminalise various forms of bullying and harassment, including the misuse of personal data and online misconduct. Speaking Up and/or Escalating Concerns - Inserted guideline on how to raise grievances, bullying and harassment.	

	Consequence of Breach by Employees – Inserted a clause ensuring that employees exercise diligence and responsibility in fulfilling their duties to prevent financial and legal consequences for the organization.
Effective Date	Nov 5, 2025
Next Review Date	TBD
Relevant Legislation	• Malaysian Anti-Corruption Commission Act 2009 ("MACC Act"); • Guidelines for Adequate Procedures issued by the Prime Minister's Department pursuant to s17A(5) of the MACC Act; • Occupational Health and Safety Act 1994; • Personal Data Protection Act 2010. • Penal Code (Amendment) Act 2025 • Criminal Procedure Code (Amendment) Act 2025
Related Documents	• Anti-Bribery and Corruption Policy; • Gifts and Entertainment Procedures; • Group Policy on Public Relations and External Communications; • Whistleblowing Policy; • Finance Policy; • Group Gift & Entertainment Policy; • Group Anti-Bribery and Corruption Policy.
Reviewed and Concurred By	Chief Human Resources Officer General Counsel
Approved By	Board