CAHYA MATA SARAWAK

CODE OF ETHICS/CONDUCT

Contents

1 Professional Standards

1.1 An Employee shall not compromise the vision, mission and values of the Company nor his/her own personal moral values for personal gain or unfair competition.

1.2 An Employee's consideration, decision and action, both as a person employed by the Company and as a member of the public, shall be made with due care, professionalism, skill and diligence, and shall not be damaging to the Company' reputation, integrity and credibility.

1.3 Where in doubt, an Employee shall consult his/her immediate superior/supervisor or Head of Department before making any decision or taking any action, in line with the Company' policies and procedures. The immediate superior/supervisor or Head of Department's decision shall be complied with, where it is made in good faith and not damaging to the Company.

1.4 An Employee shall conduct all communications and dealings involving the Company or third parties in a fair, honest and transparent manner and shall at all times ensure that these are done in the best interests of the Company and its stakeholders.

1.5 An Employee shall not discriminate against another on the basis of race, religion, gender or age, as the Company strives to create and maintain an environment where Employees are expected to respect, engage and form work collaborations with one another.

2 Work Commitment, Hours of Work and Attendance Standards

2.1 Work Attendance & Commitment

(i) All Employees are required to diligently perform their official duties during their prescribed working hours of the Company. Increased workloads may occur from time to time, in which case Employees shall be required to work beyond normal working hours but subject to the provisions of the prevailing Sarawak Labour Ordinance/Employment Act and Company rules and regulations, whichever is applicable.

(ii) All Employees are required to be present for work during working hours and shall devote such working hours wholly to the performance of their official duties. Working hours and working week may vary from one Company to another within the Company based on operational requirements, which is to be determined by the Head of Division in consultation with Group Human Resources Department and their respective Company's Board.

2.2 Weekly Working Hours & Rest Days

(i) Employees are required to work a minimum of 40 hours per week but not exceeding 48 hours per week and are accorded a break of no less than 30 minutes for 5 hours of consecutive work. Where Employees are required to

work beyond their normal working hours, such excess work time carried out may be compensated with overtime payment or leave in lieu of overtime in accordance with the Group HR Policies and Procedures Manual.

(ii) For Companies working on a 5 ½-day work week, the first and third Saturdays of the month, where applicable, shall be declared a rest day. However, if the first or third Saturday of the month is a public holiday, the second or fourth Saturday of the month, as the case may be, shall be declared a rest day. For Companies working on a 5-day work week, an additional day shall be credited to the Employee's annual leave entitlement for the year where a public holiday falls on a Saturday.

(iii) The normal rest day is Sunday. For certain categories of Employees including Employees working on shift duty, the rest day may be changed according to operational needs, at the discretion of the Company. The Company observes all gazetted public holidays. If a designated public holiday falls on a Sunday or on a rest day, the working day immediately following thereafter shall be a rest day in substitution thereof for non-shift Employees. As for shift Employees, they shall continue with their normal shift roster but the public holiday shall be credited to their annual leave.

2.3 Working on Rest Days

(i) Employees who are required to work on a rest day or gazetted public holiday shall be compensated with overtime payment or leave-in-lieu of overtime, in accordance with the Group HR Policies and Procedures Manual.

(ii) The Company may, according to operational requirements, introduce shift work as and when necessary. In order to ensure the continuity of operations, all shift workers shall remain on duty until relieved by either the succeeding shift workers or until permitted to leave by their respective immediate superiors/supervisors. Such handing over of duties shall be documented/logged for record keeping.

2.4 Punctuality and Attendance

(i) Employees must commence work on time and are not permitted to leave the work place during work hours (except during lunch hour) without prior permission.

(ii) All Employees working in locations where clocking in/out is practised, must clock in and out daily. Clocking in/out for and on behalf of a colleague is not permitted and shall be regarded as a misconduct warranting disciplinary action.

2.5 Absence & Notification of Superior(s)

(i) If an Employee is unable to commence work on time, his/her immediate superior/supervisor or next higher authority in office must be informed as

soon as is practicable through telephone call or any other form of communication (e.g. email, SMS, etc.).

(ii) If an Employee is absent on a particular day (e.g. on medical leave, emergency leave, etc.), he/she is to notify his/her immediate superior/supervisor or the next higher authority in the absent of the immediate superior/supervisor as soon as possible on the same day.

(iii) If an Employee falls ill and is granted sick leave by the Company's panel doctor or a registered medical practitioner, a medical certificate should be submitted to his/her immediate superior/supervisor on the day that he/she reports back to work.

(iv) An Employee who absents himself/herself from work without prior leave approval or without reasonable excuse shall be liable for disciplinary action.

2.6 Flexible Working Hours

Where really needed and practicable, any Employee who does not work as a member of shift or operation/production crew team, may apply for flexible working hours as provided for under the Work-Life Balance Policy (per the Group HR Policies and Procedures Manual).

3 Dress Code

3.1 Appropriate Attire for Corporate Image/Safety Compliance

(i) Employee dress code covers suitable attire for office and non-office based Employees and is important to promote the good corporate image and to ensure compliance with safety standards.

(ii) All Employees are required to be appropriately dressed and shall be tidy and neat in appearance during working hours to reflect good corporate image especially when performing duties for the Company externally including when dealing with clients and members of the public. All Employees who are not required to wear uniforms whilst on duty are required to dress in proper, neat and tidy office attire to project a professional and business-like image particularly when attending important meetings and corporate functions.

(iii) The following apparels are not suitable for office wear with the exception of proper jeans and corporate polo shirt for casual Friday (1CMS Day), weekend corporate functions or appropriate corporate activities:

(a) Casual attire such as shorts, sweatpants, exercise pants, leggings or other form-fitting pants, denim shirts, sandals, slippers, sneakers, trainers, other collared and casual outfit;

(b) Mini-skirt or short dress that does not allow one to sit comfortably in public, including shorts and/or tight skirt that ride halfway up the thigh;

(c) Spaghetti-strap dresses and blouses, or low-cut dresses; and

(d) Any other attire that is not appropriate for office wear.

(iv) All Employees are expected to maintain good personal hygiene and grooming to reflect a clean and neat overall appearance. Employees are not permitted to have any extreme hair dye, haircut/hairstyle or make up.

3.2 Staff Uniforms & Personal Protective Equipment (PPE)

(i) Employees who have been provided with uniforms and relevant safety gear must wear them during working hours, at a specific time or whenever performing duties for the Company. All Employees working at the Company's construction sites or factories/plants are required to comply to the Company's safety standards on appropriate gear and attire, such as safety helmets, goggles, industrial gloves, ear plugs, safety boots, and other Personal Protective Equipment (PPE) in accordance with the safety requirements and procedures at such construction sites or factories/plants.

(ii) Employees shall only be provided with uniforms upon their confirmation of service with the Company unless otherwise approved by the GMD/Head of Division concerned per the Group Limits of Authority.

(iii) It is the responsibility of each Employee to take care of uniforms and apparels supplied by the Company. Damaged or worn out uniforms and safety gear must be immediately reported to the Company for replacement.

4 Required Knowledge and Compliance

4.1 All Employees are expected to keep abreast and comply with all applicable rules and regulations related to their respective duties and responsibilities, including but not limited to, the regulatory statutory rules and regulations as well as the Company' policies and procedures.

4.2 The Heads of Division/Department/line managers are required to ensure that relevant and applicable rules, regulations, policies, procedures, processes, etc. which have a direct impact on their work areas are disseminated and complied with.

4.3 All Employees are required to understand, seek guidance where necessary and comply with such relevant and applicable rules, regulations, policies, procedures, processes, etc.

4.4 Where specific compliance declarations are mandated, every Employee must strictly comply by completing and duly signing the relevant declaration forms including the Conflict of Interest, Anti-Fraud Management, PDPA, Anti-Bribery and Anti -Corruption, and any other form as required on annual basis or as and when required by the Company, administered by Group HR and supported by divisional functions.

4.5 Where in doubt, an Employee shall not take any action, in his/her own capacity or on behalf of the Company that may violate the law, regulatory rules and regulations or internal policies and procedures. The Employee must consult and seek advice from his/ her line manager/Head of Department/Division.

5 Professionalism in Communication

5.1 An Employee shall ensure professionalism in his/her communication within the Group to Employee, his/her subordinates, immediate superior/supervisor, Head of Department, Senior Management, or external parties. Such communication may be conducted verbally or in writing.

5.2 Use of E-mail, Application Tools and Internet Facilities must comply with the following guidelines:

(i) An Employee's use of e-mail, application tools and internet facilities shall be bound by the Group IT policies and procedures of the Company.

(ii) An Employee shall not send any e-mail, or any form of correspondences that may impair the Company' image or reputation.

(iii) Employees are assigned with a Company email address for work purposes, where applicable. Sending emails from a Company assigned email address must comply with the CMSB Group IT Security Policy on Electronic Mail Security.

(iv) The circulation of e-mail or other forms of communication relating to politics, the Government, rumours, pornographic materials and other sensitive issues are strictly prohibited. This cover messages with inappropriate language, including racist and sexist jokes and offensive materials to his/her internal/external recipients.

(v) Employees must take precautions transmitting confidential information via e-mails or any other communication tools as to minimise security risks which include but not limited to assigning passwords to data files and making sure recipients' e-mail addresses are correct prior to sending such e-mails.

(vi) An Employee should not use the internet facility to download (personal or otherwise) onto the Company's computer or use materials from internet that violates software licenses, copyright, patent and personal data protection laws.

5.3 All Employees are also required to adhere to the Social Media Policy (per the Group HR Policies and Procedures Manual) whenever they communicate using any form of social media so as to reflect himself/herself as a responsible user and not in any way tarnish his/her own image as an Employee and/or of the Company.

6 Fair and Equitable Treatment

6.1 An Employee shall conduct all business dealings for or on behalf of the Company with corporate clients, potential clients, our Employees and/or with any other person in a fair and equitable manner.

6.2 An Employee shall not take unfair advantage of anyone through manipulation, concealment, abuse of material non-public and price sensitive information, misrepresentation of facts or any other unfair dealing practices.

6.3 An Employee shall not accept bribes, kickbacks, make promises or grant preferential extensions of credit and must not conspire or collude in any way in the course of performing his/her duties to the detriment of CMSB.

6.4 An Employee shall not be influenced by friendship or association in the course of meeting client's requirements or in recommending them. Any business transactions/decisions must be made strictly on an arm's length basis.

6.5 An Employee must avoid any preferential transactions within the Company or with related parties/interests. If such transactions occur, they shall be made in full compliance with the regulatory rules and regulations and internal policies and procedures, judged on the basis of normal business criteria and fully documented and duly authorised by the respective Boards or an independent party.

6.6 An Employee shall reasonably anticipate and proactively meet client's/customer's needs, maintain high level of professionalism and provide efficient service.

7 Exclusive Employment Services

While employed on a full time basis with the Company, an Employee shall at all times faithfully and diligently perform his/her duties as may from time to time be assigned to him/her by his/her immediate superior/supervisor and devote the whole of his/her time and attention to the discharge of the duties and functions devolved upon him/her as stipulated in his/her job description. Any form of salaried employment (part-time or otherwise) on top of his/her existing employment with the Company is not allowed unless expressed permission has been obtained and subject to any terms and conditions the Company may impose.

8 Related Party Transactions

All Employees of the Company connected to related parties (including parties related indirectly through immediate family members) are required to declare their interest and shall, where applicable, abstain from deliberating or voting in respect of these related party transactions. A detailed policy on Related Party Transaction is contained in the Group Financial Policies Manual.

9 Conflicts of Interest

9.1 While employed with the Company, an Employee He/she shall not put himself/herself in a position in which there is or might be a conflict between his/her

duties as an Employee and his/her personal or family's interests or, between those duties and any duty he/she owes to any person. An Employee must act in good faith and in the best interests of the Company or entity at all times.

9.2 An Employee shall not, without written consent of the Company engage, whether directly or indirectly, in any business which is similar on in any way connected to or competitive with the business of the Company or which could or might reasonably be considered by others to impair the Employee's ability to act at all times in the best interest of the Company.

9.3 Employees are also required to declare in writing that such policy has not been contravened when they join the Company and subsequently on annual basis.

9.4 Notwithstanding the above Clause 9.3, as and when there is a change in status which may lead to potential breach of the policy, it must be reported/disclosed as soon as practicable after the relevant facts have come to the Employee's knowledge., e.g. when an Employee is being appointed as trustee or director of a family related business entity which is a supplier/service provider to the Company.

10 Offer and Acceptance of Gifts, Entertainment & Corporate Hospitality

10.1 Offer of Gifts, Entertainment & Corporate Hospitality

Offering of gifts, entertainment & corporate hospitality such as the usual corporate gifts or souvenirs (such as hampers, pens, caps, company T-shirts, etc.), traditional festive gifts (such as fruits, gift vouchers, etc.) and modest level of entertainment to clients, business associates or related agencies' representatives as part of business networking and reciprocal deeds are allowed.

10.2 Acceptance of Gifts, Entertainment & Corporate Hospitality

(i) The Company recognises that occasional acceptance of a reasonable gift such as the usual corporate gifts or souvenirs (such as hampers, pens, caps, bags, t-shirts, etc.), traditional festive gifts (fruits, gift vouchers etc.) and modest level of entertainment offered by clients as per the Group Limits of Authority are part of business networking and therefore allowed.

(ii) However, Employees are not allowed to receive any gift(s), entertainment & corporate hospitality as well as entertainment from a third party IF such an act could directly or indirectly compromise the discharge of their duties leading to any personal gain on the part of the Employee and/or third party concerned.

10.3 All Employees are advised to understand clearly and adhere strictly to the Company's Gifts, Entertainment and Corporate Hospitality Policy.

11 Dealing with Third Parties

All dealings with third parties (such as contractors, suppliers, vendors, dealers, agents, transporters, joint venture partners, consultants, intermediaries, clients, etc.) shall be carried out in compliance with all relevant laws and consistent with the Company's values and Code of Ethics as stated in the Employee Handbook. This is to ensure that all business dealings are properly conducted and not be tainted with any form of bribery and corruption which may lead to breach of any relevant laws including the Malaysian Anti-Corruption Commission Act 2009).

Therefore, all Employees (as Company representatives) dealing with third parties in the course of their works are expected to strictly adhere to the above-stated policy and at the same time to inform the third parties concerned to be equally aware of and adhere to the same ethical/legal requirements in order to avoid the business dealings/transactions from being subject to any legal non-compliance which may lead to financial and/or reputational loss to the Company.

12 Compliance to the Malaysian Anti-Corruption Commission Act 2009

12.1 The Company expects all Employees to possess and exercise highest level of accountability, integrity and honesty in performing their duties. Thus any form of corruption/bribery is strictly prohibited.

12.2 All Employees are advised to understand clearly and adhere strictly to the Company's Anti-Bribery and Anti-Corruption Policy.

13 Misuse of Position

An Employee must not use his/her position in the Company or the Company's name or facilities for personal gain or advantage, such as to threaten or gain leverage over his/her subordinates or any other Employees in politics, private businesses or in similar types of activities.

14 Misuse of Information

An Employee shall not remove, copy or make use of any information obtained in the course of their work, in which the Company has proprietary rights, for his/her direct or indirect benefit or of other persons or to cause harm or reputation damage to the Company.

15 Confidentiality/Non-Disclosure

15.1 Unless specifically authorised by the Company or as required in his/her employment with the Company, an Employee shall not, at any time during his/her employment or upon termination thereafter, disclose to any person information as to the practices, business, dealings or affairs of the Company or its subsidiaries, associate companies, business associates, customers or clients, or any other matters which may come to his/her knowledge by reason of his/her employment.

15.2 Violation of this Confidentiality provision is a serious misconduct and may result in immediate dismissal.

15.3 An Employee's right to use confidential information ceases when he/she ceases employment with the Company. He/she must return any confidential information, documents, files, etc. to the Company and act in accordance with instructions from the Company in relation to the confidential information.

15.4 For a period of twelve (12) months from the date of the termination of this employment with the Company, an Employee shall not, without the prior written consent of the Company, whether alone or jointly with or as principal, partner, agent, director, Employee or consultant of any other person, firm or corporation, be engaged in any activity which is in competition with any of the business of the Company and/or its related subsidiary/associated companies where any of such activities would have the effect of infringing the Company's and/or its related/subsidiary/associated companies' trade secret and/or confidential information, such as:

(i) directly or indirectly solicit the services or otherwise deal with any client of the Company or its related subsidiary/associated companies and with whom or which the Employee was personally concerned during his/her employment with the Company where any of such an activity would have the effect of infringing the Company's and/or its related subsidiary/associated companies' trade secret and/or confidential information; and/or

(ii) to directly or indirectly divert or interfere with the Company's or its related/subsidiary/associated companies' business relationships with any of its clients whom the Employee was personally concerned during his/her employment with the Company where any of such activities would have the effect of infringing the Company's/related/subsidiary/associated companies' trade secret and/or confidential information.

15.5 If the Employee is unsure of his/her obligations under this Policy, he/she is to consult his/her immediate superior/supervisor. Failure to comply with this Policy could result in disciplinary action being taken against the Employee, including dismissal.

16 Intellectual Property Rights

All Employees, irrespective of position, role and expertise, are employed by the Company under a contract of service to create value and generate revenue for the Company. Thus all forms of work/value (such as patents, trademarks, copyrights, designs, trade secrets or simply ideas) produced singly or collectively for the Company in the course of the Employee's employment belong to the Company. In other words, the right to the copyright and all other intellectual property in all such work shall be the sole property of the Company. The Employee shall ensure such works produced shall not be in breach of any copyright or intellectual property rights of another person or entity. The Employee shall ensure such works produced shall not be in breach of any copyright or intellectual property rights of another person or entity.

17 Integrity of Records and Transactions

17.1 Employees must ensure that all work information furnished is:

(i) Accurate and up to date, unbiased or not misleading;

(ii) Used only for the purpose for which it is intended;

(iii) Complete and in line with the requirements; and

(iv) Only shared/given to other parties if proper authority and clearance has been given.

17.2 Employees must ensure accurate recording and reporting of all work information to meet financial reporting, regulatory, tax and legal obligations.

17.3 Employees shall retain all business records or documents according to applicable laws, rules, regulations and the Company's policies and procedures.

17.4 Employees must, when disclosing and declaring personal information on themselves and related parties, whether for internal records or to enable the Company to comply with external regulations, ensure that such information is accurate and complete, to the best of their knowledge.

18 Anti-Fraud Management

18.1 Fraud is defined as the intentional perversion of truth in order to induce another to part with something of value or to surrender a legal right. It is also the use of deception by an individual with the intention of obtaining an advantage for direct personal/persons' benefit or for third party or parties, avoiding obligation, or causing loss to another party. Fraud offences are defined as the following but are not limited to:

(i) deception;

(ii) bribery;

(iii) forgery;

(iv) extortion;

(v) corruption;

(vi) conspiracy;

(vii) embezzlement;

(viii) misappropriation;

(ix) false representation;

(x) concealment or omission of material facts;

(xi) collusion; and

(xii) kickback.

18.2 Fraud may occur due to several factors either combined or in part. The following factors can contribute to fraud:

(i) Lack of proper internal control policies and procedures;

(ii) Failure to follow proper control procedures;

(iii) Carelessness/negligent in carrying out proper inspections;

(iv) Inadequate segregation of duties/responsibilities of Employee or Management;

(v) Management override/bypassing of internal controls; and/or

(vi) Collusion between Employees and/or third parties.

18.3 Early detection and prevention of fraud can help to safeguard the Company against the following:

(i) Company's reputation being tarnished;

(ii) Financial/asset loss to the Company; and

(iii) Erosion of Company's corporate and ethical values.

18.4 It is the duty of all Employees to report any suspected incidence of fraud when they see red flags, i.e. warning signals such as anomalies/irregularities/non-compliance of Company policies/procedures.

18.5 All Employees shall be required to sign an acknowledgement form (refer to Appendix-1-B) to state that he/she understands what constitutes fraud and agree to report occurrences of fraud if any, to his/her immediate superior/supervisor and/or the Head of Division/Head of Department/GCOO/GMD who shall determine the next course of action which includes notifying the Group Audit Committee and initiating a Fraud Investigation.

18.6 Failure to report any occurrences suspected of fraud shall result in disciplinary action being taken against relevant Employees.

18.7 In order to mitigate or minimise fraud, the following steps may be taken:

(i) Prior to recruiting a potential candidate, criminal background check (police clearance), qualification verification and reference check should be carried out where practicable and the result recorded in his/her profile;

(ii) An orientation programme shall be conducted for all new Employees and shall include briefing of the code of conduct and whistle-blowing policy;

(iii) Job rotation where practicable, is encouraged in areas where potential fraud may occur (e.g. operations, production line, sales and marketing, tendering process, purchasing, etc.);

(iv) Frequent unscheduled audit checks conducted by Group Internal Audit Department;

(v) Fraud and misconduct awareness training; and/or

(vi) The Company shall monitor any Employees suspected of fraud for lifestyle changes.

18.8 Fraud Response Committee

(i) Appointed representatives from the Group Internal Audit Department, Group Legal Department and Group Human Resources Department shall be members of the Fraud Response Committee.

(ii) The responsibilities of the Fraud Response Committee shall be but not limited to the following:

(a) Investigate the circumstances of the suspected fraud and produce a written report;

(b) Secure records/assets, including restrictions/barring access to offices/systems;

(c) Determine whether the case should be reported to the police;

(d) Decide if the suspected Employee(s) should be suspended from work; and

(e) Provide recommendations on appropriate action (e.g. initiate disciplinary and/or legal process and police action, where applicable).

18.9 Annual Reporting

An annual update on fraud related cases shall be made to the Group Internal Audit Department for submission to the Group Audit Committee based on information provided by Group Human Resources Department.

19 Whistle Blowing

19.1 CMS is committed to high standards of ethical, moral and legal business conduct. Any Employee or external parties (where applicable) can 'blow the whistle' concerning violations to the policy and make a formal confidential disclosure through feedbacks, reports or complaints to a member of the Designated Authority (DA) (defined as Group Managing Director, Group Chief Operating Officer Group Chief Financial Officer or SGM – Group Human Resources who shall refer to the Board of Directors/Group Audit Committee) pertaining to a suspected misconduct such as fraud, misappropriation, abuse of authority, corrupt practices or any other form of contravention or non-compliance with Company policies and procedures, including breach of any terms of the Employee Handbook or any regulatory infringement that may be detrimental to the interest of the Company. Employees are encouraged to raise serious concerns and speak up if any actual, planned or potential behaviour that is illegal or unethical is suspected.

19.2 Where an Employee or external parties (where applicable), acting in good faith, has reasonable grounds to suspect misconduct as stated in the preceding paragraph, he/she may submit a written and duly signed report or verbal report, in strict confidence, to the DA. The DA or his/her representative shall make a preliminary assessment in consultation with the GMD of the allegation in order to establish a case. If the case is worthy to be investigated, the DA shall appoint, in a confidential manner, an Investigating Officer (IO) to initiate a formal investigation per the Group Limits of Authority.

19.3 Investigation will still be carried out in the event any anonymous report is received. However, the effectiveness of the investigation depends on the completeness of the report received.

19.4 Any allegation which cannot be substantiated and which prove to have been made with malicious intent or knowingly to be false shall be viewed as a serious disciplinary offence on the part of the whistleblower.

19.5 For protection of the whistleblower, the DA or his/her representative shall, at all times, keep the confidentiality of the whistleblower's identity (which shall not be revealed without his/her expressed consent) so as to protect him/her from any potential reprisals by the suspect or his/her associates and related parties. The Company shall not tolerate any form of victimisation of an Employee who speaks out and acts in good faith.

19.6 Identity of the person "blowing the whistle" shall be treated with highest confidentiality and privacy. The Company shall take appropriate action including practicable protective measures for the protection of the whistle blower.

19.7 At the sole discretion of the Company, a token of reward may be payable to a deserving whistleblower.

20 Personal Data Protection under PDPA

The Personal Data Protection Act (PDPA) 2010 was enacted by the Malaysian Government to regulate the proper management of personal data in commercial transactions and to protect personal information against misuse. The legislation safeguards the interest of individuals and makes it illegal for any party be it corporate entities or individuals, to sell personal information or allow such use of the data by third parties. In accordance to this Act, the Company is required to notify the Employees on matters relating to their personal data that is being processed, used, disclosed, collected, recorded, transferred, held and/or stored by the Company.

20.1 The Company complies with the Personal Data Protection Act and requires all Employees to know and adhere to the PDPA requirements. Personal data means any information in respect of commercial transactions, which:

(i) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose;

(ii) is recorded with the intention that it should wholly or partly by processed by means of such equipment; or

(iii) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,

that relates directly or indirectly to an individual, who is identified or identifiable from that information or from that and other information in the possession of a data user, including any sensitive personal data and expression of opinion about the data subject; but does not include any information that is processed for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010.

20.2 Scope of PDPA

Three (3) conditions must be met in order for any data to be considered as personal data within the ambit of the PDPA:

(i) Data must be "personal data" and this is defined as information which relates directly or indirectly to an individual who is identified or identifiable from the information;

(ii) The data must be in respect of "commercial transactions". Commercial transactions is defined as transactions of a commercial nature, whether contractual or not and includes any matter relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance; and

(iii) The data must be "processed". Processing is defined as collecting, recording, holding or storing the personal data or carrying out any operation or set of operations on the personal data including:

(a) the organisation, adaption or alteration of personal data;

(b) the retrieval, consultation or use of personal data;

(c) the disclosure of personal data by transmission, transfer, dissemination or otherwise making available; or

(d) the alignment, combination, correction, erasure or destruction of personal data.

20.3 Personal Data Protection Principles

The PDPA stipulates seven (7) Personal Data Protection Principles to be observed by Companies when processing personal data:

(i) (Section 6) General Principles –under this section, the Company is required to seek the consent/explicit consent when processing personal data/sensitive personal data;

(ii) (Section 7) Notice and Choice Principle – under this section, the Company is required to give written notification to the Employees informing them of the nature and information collected, the purpose of processing such information and if such information is disclosed to third parties;

(iii) (Section 8) Disclosure Principle – under this section, the Company is required to obtain the consent of the Employees in disclosing their information to third parties;

(iv) (Section 9) Security Principle – under this section, the Company shall take steps to ensure that their Employees' information are protected from loss, misuse, modification, unauthorised or accidental access;

(v) (Section 10) Retention Principle – under this section, the Company shall not keep its Employees' information longer than required by law (i.e. Up to 6 years);

(vi) (Section 11) Data Integrity Principle – under this section, the Company shall ensure that all information are accurate, complete and kept up to date; and

(vii) (Section 12) Access Principle – Under this section, the Company shall allow its Employees the right of access to their information and the right to correct any inaccurate, incomplete, misleading or outdated information.

20.4 Personal Data Protection Act Compliance

In order to comply with the above mentioned regulatory requirements, the following documents are relevant:

(i) Personal Data Notice

Newly hired Employees will be required to fill in a Personal Data Noticeto give consent to the Company for processing/using/collecting/recording/security/disclosure/retention/holding/ storing/transfer purposes. The Personal Data Notice shall be filled in along with relevant documents provided by the Human Resources Department as stated in the Group HR Policies and Procedures Manual to be inserted into the Employee Dossier;

(ii) Personal Data Access Request Form

An Employee who wishes to access and obtain a copy of his/her personal data shall be required to obtain and fill in the Personal Data Access Request Form from the Human Resources Department. The Employee shall first obtain consent from the Company and shall state his/her purpose for obtaining his/her personal data; and

(iii) Personal Data Correction Request From

Should an Employee have any amendments or wish to update his/her personal information, he/she shall be required to obtain and fill in the Personal Data Correction Request Form from the Human Resources Department. It shall be the responsibility of the Employee to update or amend his/her personal records on a timely basis.

20.5 Failure to comply to the PDPA shall render the Company liable to a fine up to RM 500,000.00 or imprisonment for a term of up to three (3) years or both.

21 Serious Financial Indebtedness

21.1 An Employee shall not in any manner whatsoever cause himself/herself to be in serious financial indebtedness.

21.2 Without prejudice to and without limiting the generality of paragraph 16.1 above, an Employee shall be deemed to be in serious financial indebtedness on the occurrence of any of the following events (which are non-exhaustive):

(i) where an Employee is a judgment debtor and the judgment debt has not been settled within one month of the date of the judgment;

(ii) where an Employee is a bankrupt or an insolvent wage earner, for so long as he/she remains an undischarged bankrupt or the bankruptcy order made against him/her has not been annulled; or

(iii) where the Employee defaults in loan and/or credit card payments.

21.3 If an Employee finds that his/her debts cause, or are likely to cause, serious financial indebtedness, he/she shall forthwith report this fact to his/her Head of Department. An Employee who fails or delays in reporting his/her serious financial indebtedness, or who reports the same but fails to disclose its full extent or gives a

false or misleading account thereof, shall be guilty of serious misconduct rendering him/her liable for disciplinary action.

21.4 For the purposes of this paragraph 16, the term "serious financial indebtedness" means the state of an Employee's indebtedness which, having regard to the amount of debts incurred by him/her, has actually caused serious financial hardship to himself/herself or his/her immediate family and pecuniary embarrassment.

22 Criminal Conviction and/or Imprisonment

Where an Employee has been convicted of a criminal offence or an order of imprisonment, detention, supervision, restricted residence, banishment or deportation shall have been made against him/her, under any law, he/she shall be deemed to have committed an act of serious misconduct rendering him/her liable for dismissal.

23 Sexual Harassment

23.1 Definition

(i) Sexual harassment is defined as any unwanted conduct of a sexual nature, whether verbal, non-verbal/gestural, visual, physical or psychological, directed at a person which is offensive or humiliating or is a threat to his/her well-being, arising out of and in the course of his/her employment.

(ii) A complaint of sexual harassment can be made by the harassed Employee against the harasser who could be his/her peer, superior or subordinate or any person (third party) in the course of his/her employment.

(iii) An Employee is prohibited from sexually harassing another Employee or any other persons both on and off the premises of work and during or outside of working hours.

23.2 An Employee shall not perform any act of sexual harassment, including but not limited to:

(i) making a request of any other Employee or person for sexual intercourse, sexual contact or other forms of sexual activity or person, which contains an implied or overt promise of preferential treatment or an implied or overt threat of detrimental treatment; and

(ii) subjecting any other Employee or person to language (whether written or spoken) of a sexual nature or with sexual connotation, or visual material of a sexual nature or with sexual connotation, where such conduct or behaviour is either repeated on numerous occasions or otherwise, that it is offensive and detrimental to a reasonable person.

(iii) making any unwelcome advances of a sexual nature towards any other Employee or person through non-verbal communication such as any sound or gesture, facial expression, maintaining proximity that is considered uncomfortable to another Employee, and inappropriate eye contact where

such a conduct is deemed offensive, humiliating and detrimental to his/her privacy and well-being.

23.3 In the event where a sexual harassment incident has allegedly happened, the following steps shall take place:

(i) Any Employee who has been subjected to sexual harassment shall:

(a) notify the harasser that his/her conduct is offensive and/or detrimental to him/her (i.e. the Employee concerned) and request immediately that the act be stopped; and

(b) notify his/her immediate superior/supervisor (or in the event the immediate superior/supervisor is the harasser, then the next higher level of authority) or Group Human Resources Department of the sexual harassment, with full particulars of such conduct, including the identity of the harasser and the time(s), date(s) and place(s) of the occurrence thereof and names of witnesses if any.

(ii) Any Employee who is witness or is named witness to the sexual harassment incident shall:

(a) Consider to provide immediate intervention to support the harassed Employee, which may include confronting or distracting the perpetrator, finding a third party to intervene, following up with the harassed Employee and/or documenting details of the sexual harassment incident. If deemed safe and effective, the Employee shall intervene with a view to put an end to the harassment which is taking place.

(b) Give full cooperation to the investigation by Group HR or the Management as and when required.

(iii) Immediate Superiors/Supervisors/Managers/Head of Departments shall:

(a) Take appropriate action expeditiously and impartially to prevent or prohibit such misconduct from recurring when a formal or informal complaint has come to his/her attention.

(b) Report any such incidents to Group Human Resources and the Management immediately so that a prompt investigation can be carried out.

Note: Immediate Superiors/Supervisors/Managers/Head of Departments may be deemed to be in violation of this policy should they fail to report such a misconduct in a timely manner to the appropriate authority of the Company.

(iv) Management of the Company shall:

(a) Conduct a thorough investigation as soon as possible which should be completed within thirty (30) days of receipt of complaint. Investigation

shall be conducted as discreetly as possible taking into consideration the emotional well-being of the complainant as well as other parties involved. Each party shall be interviewed separately and confidentiality is of utmost importance.

(b) Take appropriate disciplinary action if after due process it is satisfied that the sexual harassment is proven, which can include dismissal without notice, downgrading, or imposing any other punishment as deemed just and fit.

(c) Inform the victim (complainant) of the outcome of the investigation. If the victim is dissatisfied with the investigation outcome, he/she may write a formal appeal to the GMD within 14 days from the date he/she is officially notified by the Company.

(d) The Management/Company may also refuse to inquire into any complaint if it is of the opinion that the sexual harassment complaint made is frivolous, vexatious or is not made in good faith. If so, the Management/Company shall within thirty (30) days inform the Complainant of the refusal and reasons for refusal in writing.

(e) If no substantial or insufficient evidence is found from the investigation to prove the accused Employee (perpetrator is guilty of sexual harassment, Group HR Department shall keep a record of the investigation for future reference in the event the victim or other Employees file a complaint of a similar nature.

(f) Any false accusations, fabricated allegations or vexatious complaints of sexual harassment made against another Employee in bad faith are considered as major misconduct and the accuser shall be investigated and liable for disciplinary action.

23.4 Penalty for Breach of Law

Failure to inquire into a formal complaint of sexual harassment, or to inform the complainant of the refusal and reasons for the refusal, as the Employer, the Company commits an offence, and shall on conviction be liable to a fine not exceeding ten thousand ringgit as stipulated under the relevant Labour Law.

24 Discrimination/Harassment

24.1 Harassment and discrimination are defined as any unwanted, unreasonable and offensive verbal, non-verbal, gestural or physical forms of action that is offensive, hostile or intimidating to the recipient (victim). Harassment and discrimination may negatively affect the work performance of the affected Employee, and his/her employment or advancement opportunities.

24.2 There shall be no discrimination against Employees on the ground of religion, race, descent, place of birth, gender or disability in the course of their employment.

24.3 No Employee shall discriminate or harass another Employee in an offensive manner including but not limited to such acts as follows:

(i) Exhibit insulting, harassing and discriminatory behaviour;
(ii) Partake in any form of abuse, threats, assault;
(iii) Make derogatory remarks, slurs or offensive language;
(iv) Make inappropriate inquiries or comments about another Employee;
(v) Display offensive materials in the form of images, videos etc.;
(vi) Isolate or exclude another Employee from work-related social functions; and
(vii) Bully and victimise another Employee on the basis of his/her background/peculiarity as listed under Clause 24.2 above.

24.4 Any Employee who has been subjected to significant harassment and/or discrimination, or has witnessed such significant incident of harassment and/or discrimination shall take the following steps as soon as practicable:

(i) Notify the harasser that his/her conduct is offensive and/or detrimental to him/her (i.e. the Employee concerned); and

(ii) Notify his/her or the victim's immediate superior/supervisor (or in the event the immediate superior/supervisor is the harasser, then the next higher level of authority) or Group Human Resources Department of the harassment and/or discrimination, with full particulars of such misconduct, including the identity of the harasser, the specific action or behaviour of the harasser against the victim, and the frequency of the occurrence thereof.

24.5 Group Human Resources Department shall proceed and complete the investigation within practicable period from the date of receiving the formal complaint.

24.6 Proper investigative measures shall be taken by the Group Human Resources Department, whereby the investigation shall be conducted as discreetly as possible to take into consideration the emotional well-being of the parties involved, and all Employees involved in the investigation process shall be interviewed separately. All Employees shall provide their full cooperation in the investigation process. All parties involved shall practise confidentiality regarding the information collected regarding the incident. The victim shall be informed of the outcome of the investigation.

24.7 An employee found to be guilty of harassment and/or discrimination shall be liable for appropriate disciplinary action which may result in dismissal.

24.8 If no substantial evidence is found from the investigation to prove an Employee guilty of the alleged misconduct, Group Human Resources Department shall keep a record of the investigation for future reference in the event the victim or other Employees file a complaint of a similar nature.

25 Making Public Statements

Unless specifically authorised, an Employee shall not either orally or in writing or in any form, make or circulate any public statement, post on-line, or publish any book, article or other works which contain or make reference to or describe the policies, business dealings or affairs of the Company or any of its subsidiaries, associate companies, business associates, customers or clients, or as to any other matters concerning the Company which may come to his/her knowledge by reason of his/her employment. Public statements include the making of any statement or comment to the press or the public, or in the course of any lecture or speech or broadcasting thereof by sound or vision. The Group Corporate Communications Department shall be consulted on all matters pertaining to the making of public statements.

26 Freedom of Association

Employees are allowed to associate themselves with any legally registered bodies/associations. However, they are not permitted to engage in any political or social activities during office hours nor to do so outside of office hours in any way that could adversely impact the business or reputation of the Company. Employees shall be required to disclose to the Company if they are involved in any political activities.

27 Safeguard and Proper Use of Company's Assets

27.1 Employees must safeguard the Company's assets from theft, waste or loss and ensure efficient use of such assets. The Company's assets include physical and intellectual properties such as the Company's brand, trademarks, copyrights, patents, work tools, machineries, facilities, etc.

27.2 Employees must use the Company's assets for legitimate purposes only.

27.3 Employees must comply with the Company's policies regarding the use of its communication systems, including its computer networks, telephone/faxes, emails and internet.

27.4 Employees must not use the Company's name or facilities for personal advantage to obtain preferential treatment.

27.5 Using Company Telephone and Handphone

Company telephone and handphone facilities are to be used for Company business calls only. Where it is necessary to make or receive personal calls on a Company telephone during working hours, they should be limited in both length and frequency, and be for essential purposes only. All personal calls made on a Company handphone are for the personal account of the Employee.

27.6 Use of Computer Resources

Computing and network facilities (i.e. personal computer, notebook, etc.) and services are provided for official use. Use for other purposes is prohibited; which includes but not limited to game-playing, propagation of chain letters, accessing

pornographic websites, private commercial activities, political advertising or campaigning, setting-up or operating personal blogs, or operating chat sites/forums/social networks or downloading and using pirated or personally downloaded or installed software.

27.7 Employees must immediately surrender company-owned computer assets such as laptops, desktops and mobiles when requested by the Company or a designated representative. All electronic and other data inside such company-owned computer assets must not be tampered with or destroyed during or prior to the surrender.

27.8 Use of Stationery

Employees are required to ensure that office stationery is used sparingly and for Company business only. Using Company's stationery for personal purposes shall be regarded as a misconduct warranting disciplinary action.

27.9 Use of Other Office Equipment and Materials

Office equipment such as franking machine, photo-copier, facsimile, printer, stationery or other materials of the Company should not be used for personal use.

28 Computer Crime

28.1 The Computer Crime Act 1997 (CCA) provides four (4) main offences relating to misuse of computers that also prescribe severe penalties in order to promote confidentiality with computer usage and constructive atmosphere for the development of information technology as follows:

(i) Unauthorised access to Company IT System/Application (e.g. cloud, network, ERP, etc.) and other computer materials, performing any function with intent to secure access to any program or data held therein;

(ii) Unauthorised access with intent to commit or facilitate commission of further offence involving fraud, corruption or dishonesty or those that causes injury;

(iii) Unauthorised modification of the contents of any desktops, notebooks and mobile devices; and

(iv) Wrongful communication by making known directly or indirectly, a number, code, password or other means of access to devices/IT Systems to any person other than a person to whom he/she is duly authorised to communicate.

28.2 An Employee may be guilty of an offence under the CCA for unauthorised modification of the contents and unauthorised communication directly or indirectly of a number, code, password or other means of access of the Company devices/IT systems.

28.3 An Employee convicted under CCA, for example for hacking and unauthorised access to computers under section 3(1) of CCA, may be liable to a maximum fine of RM50,000.00 or imprisonment for a term not exceeding five (5) years or both.

28.4 Notwithstanding the above, an Employee who is found to have committed a computer crime shall be liable for disciplinary action which may result in dismissal.

29 Money Laundering and Terrorism Financing

29.1 All Employees shall ensure understanding and compliance of the Company anti-money laundering policies and procedures.

29.2 The offence of money laundering and terrorism financing in Malaysia are mainly governed under the Anti-Money Laundering and Anti-Terrorism Financing Act 2001 (AMLATFA).

29.3 The offence of money laundering involves the process by which one conceals funds of dubious or illegal origin and then disguises them as legitimate proceeds of lawful activities.

29.4 The offence of terrorism financing could be regarded as an act or threat of action within or beyond Malaysia that endangers a person or public's safety, or damages property or environment. This act or threat of action is carried out for purpose of intimidating the public or compelling Malaysian or other governments or organisations, to act or refrain from doing any act.

29.5 Notwithstanding the above, an Employee who is found to be involved in laundering the Company's money shall be liable for disciplinary action which may result in dismissal.

30 Social Media Policy

The Company recognises the importance of social media to facilitate and enhance communication and dissemination of useful information for business and work-related purposes. This policy is not meant to restrict the sharing of appropriate and useful information but to minimise the degree of risks faced by the Company and its Employees with social media usage. Thus, all Employees shall adhere to the Company social media and related policies and procedures at all times, including outside of working hours and during personal usage.

30.1 Definition

Social media is defined as any form of electronic communication including but not limited to social-networking sites, video or photo-sharing sites, forums or chat rooms, wikis, blogs, text-messaging and others through which online communities are created by users for the sharing of information, ideas, messages and other graphical contents.

30.2 Communications & Multimedia Crime under the CMA 1998

(i) Section 211 (2) of the Communications & Multimedia Act 1998 establishes that it is an offence to utilise a network service to provide offensive content where:

(a) No content applications service provider, or other person using a content applications service, shall provide content which is indecent, obscene, false, menacing, or offensive in character with intent to annoy, abuse, threaten or harass any person.

(ii) Section 233 (1) provides that the improper use of network facilities or network service occurs is an offence when:

(a) A person who by means of any network facilities or network service or applications service knowingly makes, creates or solicits; and initiates the transmission of any comment, request, suggestion or other forms of communication which is obscene, indecent, false, menacing or offensive in nature with an intent to annoy, abuse, threaten or harass another person.

(iii) An Employee may be guilty of an offence under the CMA and if he/she is convicted, for example for posting inappropriate contents and defamatory remarks on social media under section 211 (2) of CMA, he/she may be liable to a maximum fine up to RM50,000.00 or imprisonment for a term not exceeding one (1) year or both.

(iv) Notwithstanding the above, an Employee who is found to have committed an offence involving social media shall be liable for disciplinary action which may result in dismissal.

30.3 Social Media Usage Guidelines

(i) An Employee shall not:

(a) use social media unnecessarily for personal/non-work related communication during working hours;

(b) use company-affiliated email addresses for the registration of social networking sites, forums, blogs or other online web applications intended for personal usage; and

(c) violate the Company's policy on Discrimination/Harassment as per the Group Human Resources Policies and Procedures Manual whilst using any social media platform.

30.4 Online Content Creation

(i) An Employee is solely responsible for his/her postings online and is expected to mind the risks of creating and participating in the dissemination/escalation of online contents. Thus, an Employee shall:

(a) exercise caution and common sense when sharing personal information online or on any social media platforms for their own protection; and

(b) practise common courtesy and tolerance at all times when creating content online and interacting with other users on social media platforms. Any acts of provocation or insinuation online are to be avoided.

(ii) Unless specifically authorised, an Employee shall not either orally, in writing or in any form, create any content online which contains, makes reference to or describes the policies, business dealings/affairs of the Company or any of its associate companies, business associates, customer or clients, or as to any other matters concerning the Company which may have come to his/her knowledge by reason of his/her employment. Any official online content representing or relating to the Company shall only be created by or after consultation with and approval from The Group Corporate Reputation and Communications Department.

(iii) An employee found to be involved in the act of creating content, or contributing to the dissemination/escalation of any content that adversely affects his/her job performance, the performance and reputation of colleagues or associates of the Company; or damages the reputation and brand of the Company and adversely affect its ability to conduct business effectively shall be liable for disciplinary action which may result in dismissal.

30.5 Social Media Behaviour

(i) Employees must practise transparency and use appropriate disclaimers in their communication/postings particularly if they disclose that they are employees of the Company, and that the views expressed are their own and do not necessarily reflect the views, standards and values of the Company during:

(a) usage of personal social media accounts for personal purposes to create content which may directly or indirectly link or implicate the Company in any way; and

(b) usage of personal social media accounts to create any personal content.

(ii) Employees shall not:

(a) engage news media or industry analysts (i.e The Borneo Post, The Edge, Business Insider, etc.) for the discussion of official Company strategy and/or business on behalf of the Company without consultation with and approval from the Group Corporate Reputation and Communications Department; and

(b) use any copyrighted material, trademarks, publicity rights or rights of others without the permission and consent of the rights-holder(s). Any third-party sources utilized by Employees shall be properly credited, and any act of plagiarism will not be tolerated.

(iii) If an Employee sees/witnesses any online activity that may potentially tarnish the image of the Company through unlawful or unethical conduct of another Employee, he/she shall immediately make known this incident to the Group Corporate Reputation and Communications Department.

31 Compliance to Safety and Security Rules and Regulations

All Employees must strictly comply to safety and security rules and regulations at all times. Each work location should have its own set of security and safety rules and regulations. All Employees must comply with such rules and regulations as well as other rules and regulations pertaining to health, safety and security including but not limited to those prescribed in the Occupational Safety and Health Act 1994, Factory and Machinery Act 1967 and CMS Group Safety and Health Policy. All incidents of accidents or near misses involving Employees or third parties must be immediately reported to the Safety and Health Officer at the Divisions, Group Safety Taskforce Chairman (i.e. GMD/GCOO/Group Human Resources and relevant regulatory bodies where appropriate.

32 Right to Conduct Search on Employees

The Management of the Company may, as and when necessary, assign its authorised personnel (such as security/safety staff) to conduct ad hoc search (spot check) on any Employee's personal belongings/bag/vehicle brought into/out of the Company's premises, or subject the Employee to a body search in the event of an investigation into alleged misconduct such as theft/stealing.

33 Right to Conduct Tests for Illegal Substances/Medical Screening

33.1 In line with the Company's commitment for a safer and healthier workplace, the Company reserves the right to conduct test for illegal substances (such as alcohol, illegal drugs or any form of illicit/banned substances) consumed by any suspected Employee which may cause health risk or even safety hazard to other workers.

33.2 Arising from the above, the Management of the Company reserves the right to send any Employee for medical screening, further test or follow up treatment/rehabilitation procedure at its approved medical centres/hospitals. The medical report shall be the basis for further action such as medical and/or disciplinary intervention including termination. For example, an Employee who is suspected of being addicted to alcohol or drug may be required to go for test and medical screening to ascertain the addiction and proper remedial action.

33.3 The Company also reserves the right to send an Employee who is habitually on frequent sick leave or tardiness or malingering (frequent/habitual absence on the pretext of suffering from certain illness) to go for thorough health screening to ascertain the nature and severity of the illness.

34 Disciplinary Control and Supervision

It is the duty of every Employee who is holding a supervisory/superior position to exercise disciplinary control and supervision over his/her subordinates and to take

appropriate action (in accordance with the Group Human Resources Policies and Procedures Manual) in the event of a breach of any provision of this Manual or any other Company practice or policy. An Employee who fails to exercise disciplinary control and supervision over his/her subordinates or knowingly condones or deliberately covers up his/her subordinate's act of misconduct/indiscipline, commits a misconduct and shall be deemed to have been negligent in the discharge of his/her managerial/supervisory duties, thereby rendering him/her liable for disciplinary action.

35 Acts of Misconduct

The acts listed below which are non-exhaustive are regarded as acts of MISCONDUCT, the commission of which shall subject an Employee to appropriate disciplinary actions. Broadly they are summarised/classified as follows:

Acts of Misconduct (in alphabetical order)

(i) Actions/Behaviour Detrimental to Company, Other Employees or Clients and Their Properties
(ii) Alcohol/Illegal Drugs/Controlled Substances Consumption/Possession
(iii) Attendance & Tardiness
(iv) Bullying/Mistreating Colleagues/Others
(v) Dishonesty/Fraud/Theft/Integrity/Conflict of Interest/Bribery/Corruption
(vi) Inappropriate Manner of Performing Work/Inappropriate Behaviour at the Workplace
(vii) Misuse of Company Name/Resources/Assets
(viii) Misuse of Information
(ix) Misuse of Position
(x) Non-Compliance to Safety, Security & Other Company Rules & Regulations
(xi) Racial/Religious/Gender Discrimination/Harassment
(xii) Sexual Harassment/Impropriety

A detailed description of the above list is contained in the Group HR Policies and Procedures Manual.