

PERSONAL DATA PROTECTION POLICY

1. Objectives of Policy

- (1) In Malaysia, the Personal Data Protection Act 2010 (“PDPA”) imposes standards on organisations for the collection, use, disclosure and care of personal data. It also recognises the rights of individuals to the protection of their personal data, including rights of correction and access. The objective of this Personal Data Protection Policy (“Policy”) is to offer information on the Company’s policies and practices in relation to Company Person’s personal data; and correspondingly, provide instructions on how Company Person should comply with the PDPA in the collection, use, disclosure and process of personal data that comes into contact with the Company in the course of business.
- (2) A failure to comply with this Policy could expose the Company to enforcement action by the relevant authorities, including the imposition of financial penalties. There may also be negative publicity from any breach that is made public. Compliance with this Policy will ensure that the Company and the Company Persons avoid such negative consequences.

2. Scope of Policy

- (1) This Policy applies to all Company directors, officers, employees (whether on a part-time, temporary or full-time basis), including interns (each a “Company Person”) working at or attached to the Company.
- (2) “Personal data” refers to information in respect of commercial transactions, which (a) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose; (b) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or (c) 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 the Company, including any sensitive personal data and expression of opinion about the individual. It covers all forms of personal data, whether in electronic or non-electronic form. Some examples of personal data include an individual's:

- i full name, gender, identity card number, passport number, date of birth, place of birth, nationality;
- ii residential address, telephone numbers and email address;
- iii employment and training history, educational qualifications / certifications and employment references;
- iv medical records;
- v details of family members; and
- vi photographs or video image.

3. Collection, Use, Disclosure and Process of Personal Data

(1) The Company collects, uses, discloses and process the personal data of existing Company Persons, former Company Persons and prospective Company Persons for the following purposes:

- i assessing and evaluating your suitability for employment/appointment or continued employment/appointment in any position in the Company and/or any of its affiliates, partners and subsidiaries;
- ii performing obligations under and/or in connection with your contract of employment with the Company (including payment of remuneration and tax);
- iii all administrative and human resources related matters at the Company, including but not limited to – granting access to the Company's premises and computer systems; administering payroll; processing leave applications; providing and administering healthcare benefits and/or insurance for the employee and/or his/her family members; reimbursement of expenses; attendance keeping; auditing Company practices, processes and accounts; investigating or auditing on acts or defaults (or suspected acts/defaults),

developing and/or implementing human resource policies or strategies; management forecasting; planning and negotiations concerning the legitimate business interests of the Company;

- iv managing and terminating the employment relationship (or potential employment relationship) between you and the Company, including monitoring your use of the Company's internet access and intranet email; investigating potential contraventions of the Company's or external compliance regulations; and resolving any employment related grievances;
- v media coverage of Company events;
- vi performing obligations under and/or in connection with the Company's provision of products and/or services to our clients;
- vii facilitating the Company's compliance with any laws, customs and/or regulations which may be applicable to the Company; and
- viii transmission to our parent company and other group entities, any affiliate, partner, subsidiary, agent, consultant, solicitor, auditor, contractor, supplier, network operator and other third party service provider of the Company, any relevant authorities, embassies, statutory bodies, regulatory bodies, financial institutions, and background checking agencies, some of which may be located outside of Malaysia, for the above purposes.

- (2) For the avoidance of doubt, the Company is entitled to continue using (which includes disclosing) personal data collected before enactment of the PDPA for the purposes for which such personal data was collected, unless consent for such use is withdrawn or the individual indicates that he/she does not consent to such use.

4. Withdrawal of Consent

- (1) Company Person's consent will remain valid until such time it is being withdrawn by Company Person in writing. Company Person may withdraw Company Person's consent to the Company's collection, use, disclosure and/or process of Company Person's personal data for any purpose by completing and submitting Annex A to this Policy: Request

Form For Withdrawal Of Consent / Access To Personal Data / Correction Of Personal Data (“Request Form”) to the DPO (defined in Art. 10) via the contact information listed below.

- (2) Once the DPO has determined that the form has been duly filled up with the necessary details, the Company shall endeavour to process Company Person’s request within 21 days from Company Person’s request .

5. Access to and Correction of Personal Data

- (1) Company Person may access and/or make corrections to Company Person’s personal data in the Company’s possession or under the Company’s control by completing and submitting the Request Form to the DPO via the contact information listed below. In particular, Company Person may request for the Company to:

- i provide Company Person with Company Person’s personal data in the Company’s possession or under the Company’s control;
- ii correct inaccurate, incomplete, misleading or not up-to-date Company Person’s personal data which is in the Company’s possession or under the Company’s control.

- (2) The Company may not be obliged or able to grant Company Person access to Company Person’s personal data or part thereof in respect of the situations listed under Annex B, or correct Company Person’s personal data or part thereof if it relates to the situations listed under Annex C. Where the Company refuses to grant access or correct Company Person’s personal data for any situations under Annex B or Annex C, where applicable, the Company shall inform the Company Person of the refusal and the reasons for the refusal within 21 days.

- (3) Once a complete and valid access and/or correction request has been received by the DPO, the Company shall endeavour to process it within 21-days. The DPO will inform Company Person in writing in the event that the Company is unable to do so, stating the reasons why the Company

is unable to do so, and provide Company Person with an estimated time by which Company Person's request will be processed, not later than 14 days from the expiry of the initial 21 day period. If necessary, the DPO may also redirect Company Person's request to the relevant divisions in the Company for processing.

- (4) Corrections to personal data will be made as soon as practicable, unless the Company is satisfied on reasonable grounds, that such a correction should not be made. Company Person's amended personal data may be sent to every organisation to which it has been disclosed to one year before the date of such correction, if that organisation needs the amended personal data for the purpose for which the personal data was disclosed to such organisation.

6. Accuracy of Personal Data

- (1) The Company shall endeavour to ensure the personal data the Company holds is accurate, complete and up-to-date. When Company Person provides the Company its personal data, the Company Person shall ensure it is accurate and complete. Company Person shall also notify the Company promptly and from time to time of any changes and/or updates to such personal data. The Company may also approach Company Person from time to time to have the same updated.
- (2) If Company Person collects personal data on behalf of the Company, Company Person should take steps to verify that the collected personal data is accurate, current and complete, especially if the personal data is collected from a third party source. Company Persons are responsible to report to the DPO for any changes in the following personal particulars in writing within 10 days of the effective date of the change.
 - i Residential address
 - ii Contact numbers
 - iii Citizenship and/or resident status
 - iv Marital status

- v Family composition, person(s) to notify in case of emergency as well as changes in their contact numbers/addresses
- vi Additional academic and/or professional qualifications acquired

7. Protection of Personal Data

The Company has put in place reasonable security measures, both physical and IT security, to safeguard Company Person's personal data against loss, misuse, unauthorised or accidental access or disclosure, unauthorised collection, use, disclosure, copying, modification, alteration disposal or destruction or other similar risks.

8. Retention of Personal Data

(1) The Company will only retain Company Person's personal data if the purposes for which it was collected remains valid, and its retention is still necessary for legal purposes. If Company Person process personal data in the course of Company Person's employment with the Company, Company Person are required to destroy documents containing personal data as soon as it is reasonable to assume that:

- i the purpose for which that personal data was collected is no longer being served by retention of personal data; and
- ii retention is no longer necessary for legal purposes.

9. Transfer of Personal Data Outside of Malaysia

Transfer of personal data to a country or territory outside Malaysia shall be made only if the standard of protection provided to the personal data transferred by the receiving organisation will be comparable to the protection under the PDPA, or consent is obtained from you or for other purpose allowed under the PDPA.

10. Data Protection Officer

HR Assistant Manager is in charge of a Data Protection Officer (“DPO”) to oversee the Company’s compliance with the PDPA.

[Contact Information of DPO]

Contact No: +6018-2346256

Email: norazrin@ihi-ps.com.my

Fax: +603-20262687

[End of Document]