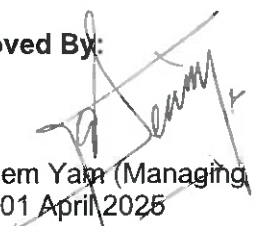




V.S. Personal Data Protection Policy and Procedures

Title: V.S. Personal Data Protection Policy and Procedures		
Reference No.: VS-PP/CORP/004		
Effective Date: 01 April 2025	Version: 2.0	Last Updated: 18 March 2025
Content Owner: Compliance	Contact Email: vscompliance@vs-i.com	

Approved By:


Gan Sem Yam (Managing Director)
Date: 01 April 2025

1.0 Purpose

This Personal Data Protection Policy outlines the Company's commitment to protecting personal data in compliance with the Malaysian Personal Data Protection (Amendment) Act 2024 (“**PDPA 2024**”) and any applicable data protection laws. This Policy will act as guidance for the processing of personal data in commercial transactions as well as for employment and charitable purposes, in compliance with the Act.

2.0 Scope

2.1 Definition

- a) The terms “*personal data*”, “*processing*”, “*commercial transactions*”, “*data subject*” and “*relevant person*” used in this Policy shall have the meaning prescribed in the Act.
- b) The expression “*we*” or “*us*” shall refer to V.S. Industry Berhad and its subsidiaries (“***the company***”)
- c) The expression “*you*” or “*your*” shall refer and include employees, potential employees, former employees, interns, clients, customers, potential customers, vendors, suppliers, contractors, sub-contractors, service providers, distributors, and/or relevant persons such as family members, guardians, parental authorities, dependants, or referees of employee/potential employee/former employee, and authorized representatives receiving, obtaining goods/services from or providing goods/services to the Company.

2.2 Types of Personal Data

Personal Data means any information, whether recorded from any material information from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual. Such information may be collected and processed by us, which may variously include but is not limited to the following:

- a) personal information that you provide when you apply for employment such as your name, identification number (e.g., national registration identity card number or passport number), age, date of birth, place of birth, gender, race, nationality, marital status, contact details including telephone number(s), residential address(es) and email address, current employment details (company name, job position, salary), referee information (such as name of referee, job position, address, contact number and email address), previous examination results, transcripts, academic qualifications, academic records, and bank details (such as name of bank, bank's address and bank account number) and contact particulars of your family, relatives or related parties.
- b) sensitive personal data disclosed by you which are necessary for purposes of performing any obligation in relation to employment, for purposes of protecting vital interests of yourself and other person, for law enforcement purposes, for medical

VS PERSONAL DATA PROTECTION POLICY AND PROCEDURES

purposes which may include but not limited to biometric data such as finger print or face recognition, religious belief, weight, height, health condition, commission or alleged commission of any offence(s) and other necessary sensitive personal data required by law.

- c) personal information that you provide for the facilitation of commercial transactions such as your name, designation, company's and business' name, and contact particulars including telephone number(s), and email address.
- d) your image and photo, by way of video surveillance i.e., closed circuit television ("CCTV") installed in some parts of our premises as part of our security infrastructure.
- e) your network usage data and other information gathered automatically by our computer systems, including your computer IP address, links visited, and other activities conducted online or using our computer systems.
- f) any other personal data required from you for the purposes set out in 2.4.

2.3 Sources of Personal Data

- a) The personal data is voluntarily provided by you, your family members, guardians, parental authorities, recruitment agents, your current or previous employer, or your company, during your course of dealings with us in any way or manner including pursuant to any commercial transactions and/or communications made from/with us such as at events organized or participated by the Company and/or obtained independently by us from other lawful sources such as from public depositories, trade/online directories, credit reporting agencies, public domain and other authorized third parties in our forms, agreements, website, and/or other similar documents.
- b) By voluntarily providing us with your Personal Data, you are giving consent for us to collect, use and process your Personal Data.
- c) By voluntarily providing us with your Sensitive Personal Data, you give us explicit consent for us to collect, use and process your Sensitive Personal Data, and you acknowledge that the collection of Sensitive Personal Data is necessary to protect your vital interest or the vital interest of others.
- d) To the extent that you have provided or will provide Personal Data about your family, spouse and/or other dependents, you confirm that you have explained to them that their Personal Data will be provided to, and processed by us and you represent and warrant that you have obtained their consent to the processing including disclosure and transfer of their Personal Data in accordance with this Policy.

And in respect of minors i.e., individuals under 18 years of age or individuals not legally competent to give consent, you confirm that they have appointed you to act for them, to consent on their behalf to the processing including disclosure and transfer of their Personal Data in accordance with this Policy.

- e) You hereby confirm that the Personal Data given by you or obtained from you, your family members, guardians, parental authorities, referees, recruitment agents, your current or previous employer and your company is sufficient, accurate, complete and not

VS PERSONAL DATA PROTECTION POLICY AND PROCEDURES

misleading and that such Personal Data is necessary for us to facilitate commercial or employment related transaction.

- f) If the Personal Data given by you or obtained from you, your family members, guardians, parental authorities, recruitment agents, your current or previous employer and your company is inaccurate or is out of date, you shall notify the Company promptly.
- g) The facilitation of commercial or employment related transaction may be delayed if such Personal Data is insufficient, inaccurate, incomplete and/or misleading.

2.4 Purposes of Collecting Personal Data

We will process Personal Data in connection with any employment or commercial transactions for any of the following purposes:

- a) to communicate with you;
- b) to facilitate, process, and / or administer commercial or employment related transaction;
- c) for audit, risk management, compliance and security purposes;
- d) to respond to your enquiries or complaints and resolve any issues and disputes which may arise in connection with any dealings with us;
- e) to carry out due diligence or other monitoring or screening activities including background checks and credit reference checks in accordance with legal or regulatory obligations or risk management procedures that may be required by law or that may have been put in place by us;
- f) to process any payments related to your commercial transactions with us;
- g) for any purposes connected with your employment including but not limited to payroll administration, entitlements and benefits, performance monitoring, training and development planning, career development, health and safety administration, succession and contingency planning;
- h) to communicate with family members, guardians and authorized representatives in the event of emergency or accident;
- i) for our storage, hosting back-up whether disaster recovery or otherwise of your Personal Data, whether within and/or outside Malaysia;
- j) to detect, investigate and prevent any fraudulent, prohibited or illegal activity or omission or misconduct;

VS PERSONAL DATA PROTECTION POLICY AND PROCEDURES

- k) to enable us to perform our obligations and enforce or defend our rights and your rights under any agreements or documents that we are a party to, and to comply with, our obligations under the applicable laws, legislation and regulations; and
- l) to comply with or as required by any request or direction of any governmental authority or responding to requests for information from public agencies, ministries, statutory bodies or other similar authorities;

2.5 Disclosure of Personal Data

In order to deliver the services you require, you hereby consent and authorize us to disclose your Personal Data to but not limited to the following parties within and/or outside Malaysia:

- a) our employees;
- b) companies within V.S. Industry Berhad, including the holding company, subsidiaries, associated, related and affiliated companies as well as their subsidiaries, associated and affiliated companies, both local and international), whether present or future (collectively, “**the Group**”);
- c) our Business Partners which include business associates, partners, suppliers, agents, contractors, external consultants, third party intermediaries and any other person associated with the Company;
- d) any third party (and its advisers/representatives) in connection with any proposed or actual re-organization, merger, sale, consolidation, acquisition, joint venture, assignment, transfer, funding exercise or asset sale relating to any portion of the Company;
- e) professional bodies, accreditation bodies or statutory regulatory bodies including but not limited to government agencies, law enforcement agencies, courts, tribunals, regulatory bodies, industry regulators, ministries, and/or statutory agencies or bodies, offices or municipality in any jurisdiction;
- f) foreign embassies and agencies appointed by the foreign embassies;
- g) any party in relation to legal proceedings or prospective legal proceedings;
- h) your immediate family members and/or emergency contact person as may be notified to us from time to time;
- i) payment channels including but not limited to financial institutions for purpose of assessing, verifying, effectuating and facilitating payment of any amount due to us in connection with your purchase of our products and/or services; and
- j) data centers and/or servers for data storage purposes.

3.0 Data Protection Procedures

3.1 Data Collection and Consent

- a) We practice Data minimization i.e., only data necessary for the stated purpose will be collected and excessive data collection is strictly avoided.
- b) Before collecting, using or disclosing Personal Data, we shall ensure that you are fully informed about the nature, purpose, and implications of data collection and your consent will be obtained. There are two types of consent:
 - Actual consent; and
 - Deemed consent under PDPA
- c) We practiced direct collection of Personal Data from the individual where possible. When data is collected from third – party sources, we will notify you of the source and purpose, ensuring compliance with relevant laws. Data may be collected but not limited to the following methods:
 - Electronic Forms: Online forms on websites, apps, and other digital platforms
 - Paper Forms: Printed data collection forms
 - Verbal Collection
- d) A privacy notice will be provided at the point of data collection to inform individuals about:
 - The identity of the Company and contact details
 - The purpose of data collection
 - Data Processing activities
 - Individual rights regarding their data
 - Retention period and data disposal processes
 - Platforms of raising concerns or complaints about data processing
- e) We may collect, use or disclose an individual's Personal Data without your consent in the following circumstances:
 - the collection, use or disclosure is necessary to respond to an emergency that threatens your life, health or safety or any other individual;
 - the Personal Data is publicly available;
 - the collection, use or disclosure is necessary for any purpose which is clearly in your interests, if consent for its collection, use or disclosure cannot be obtained in a timely way;
 - the collection, use or disclosure is necessary for any investigation or proceedings;
 - the collection, use or disclosure is necessary for evaluative purposes; and/or
 - in any other circumstances set out in the PDPA.

3.2 Right to Access, Limiting the Process and/or Correct Personal Data

- a) To the extent that the applicable law allows, you have the right to request for access to, request for a copy of, request to update or correct, your Personal Data held by us and to request us to limit the processing and use of your Personal Data.
- b) In addition, you also have the right, by notice in writing, to inform us on your withdrawal (in full or in part) of your consent given previously to us subject to any applicable legal

VS PERSONAL DATA PROTECTION POLICY AND PROCEDURES

restrictions, contractual conditions and a reasonable duration of time for the withdrawal of consent to be effected.

However, your withdrawal of consent could result in certain legal consequences arising from such withdrawal. In this regard, depending on the extent of your withdrawal of consent for us to process your Personal Data, it may mean that we will not be able to continue with your existing relationship with us or the contract that you have with us will have to be terminated.

- c) Notwithstanding the foregoing, we reserve our rights to rely on any statutory exemptions and/or exceptions to collect, use and disclose your Personal Data.
- d) If you would like to request for access to or correction of your Personal Data or limit the processing of your Personal data, kindly fill in

Data Subject Access Request Form as per Appendix A (for access / limit the access)
Data Subject Correction Request Form as per Appendix B (for correction / update)

And submit the form to

- Human Resource Department for Employment related Data
 - Finance Department for Customer / Vendor related Data
 - General Admin Department for CCTV Footage
- e) If you would like to make any inquiries or complaints, kindly write to

V.S. Industry Berhad

Attention: Data Protection Officer (“DPO”)

No. 88, Jalan I-Park SAC 5, Taman Perindustrian I-Park SAC, 81400 Senai, Johor

DID: +607-552 8901 Gen: +607-552 8888 (*Ext: 8901*)

Email: vscompliance@vs-i.com

- f) You are to put your requests in writing for security reasons and verification purposes.
- g) In the event we refuse to adhere to your request for access and/or correction to your Personal Data such as when the information requested for is of a confidential commercial nature, we will inform you of our reason for the refusal.

3.3 Changes to Personal Data

- a) We are committed in ensuring the confidentiality, protection, security and accuracy of your personal data made available to us. It is your obligation to ensure that all personal data submitted to us and retained by us are accurate, not misleading, updated and complete in all aspects. Therefore, we request that if there are changes to your Personal Data you should notify us directly at the contact details as set out in 3.2 (d).

3.4 Retention of Your Personal Data

- a) Any of your Personal Data provided to us is retained for as long as the purposes for which the Personal Data was collected continues or as required by law.

VS PERSONAL DATA PROTECTION POLICY AND PROCEDURES

- b) Your Personal Data is then destroyed from our records and system in accordance with our retention policy in the event your Personal Data is no longer required for the said purposes unless its further retention is required to meet our operational, legal, regulatory, tax or accounting requirements.

3.5 Security of Your Personal Data

- a) We are committed to ensuring that your Personal Data is stored securely. In order to prevent unauthorized access, disclosure or other similar risks, we endeavour, where practicable, to implement appropriate technical, physical, electronic and procedural security measures in accordance with the applicable laws and regulations and industry standards, and ensure that our employees adhere to the aforementioned security measures, to safeguard against and prevent the unauthorized or unlawful processing of your Personal Data, and the destruction of, or accidental loss, damage to, alteration of, unauthorized disclosure of or access to your Personal Data.
- b) Access to personal data shall be limited to authorised Data processor only.

3.6 Cross Border Data Transfer

- a) Any cross-border transfer of personal data will comply with PDPA 2024 and the data protection regulations of the destination country.

3.7 PDPA Governance Structure

Roles	Governing Body	Roles and Responsibilities
Data Controller	Board of Directors (Board)	Responsible for ensuring that all Personal Data processing complies with the Data Protection Regulations.
	Data Privacy Executive Committee (Executive Directors)	Responsible in determining the purposes for which, and the manner in which, any Personal Data that was hold and are processed.
Data Processors	Business Units and Corporate Functions	Responsible in a) Processing personal data only as instructed by the Data Controller. b) Implementing appropriate technical and organizational measures to safeguard personal data. c) Ensuring that all employees involved in processing understand and respect data confidentiality requirements. d) Notifying Data Controller of any data breach or security incident. e) Obtaining approval from the Data Controller before engaging any sub-processors. f) Maintaining records of processing activities and provide them to the Data Controller upon request. g) Assisting the Data Controller in fulfilling obligations related to data subject requests, DPIAs, and breach responses h) Acting as the primary contact for Data Subject for Data Access / Data Correction Employee Related Data: Human Resource Department Customer / Vendor Related Data: Finance Department CCTV Footage: General Admin Department
Data Protection Officers	Business Units and Corporate Functions (Facility DPO)	Responsible in a) Ensuring the Business Units and/or Corporate Functions complies with PDPA 2024, and other applicable regulations. b) Advising management and employees on data protection obligations and best practices. c) Conducting training sessions to educate employees about data protection requirements. d) Conducting and review Data Protection Impact Assessments (DPIAs) for high-risk processing. e) Managing data breaches, including notification to the Group DPO and affected individuals. f) Acting as the primary contact for the Data Subject on data protection matters. g) Maintain records of processing activities, risk assessments, and compliance measures.
	Risk and Compliance Function (Group DPO)	Responsible in a) Ensuring the Business Units and/or Corporate Functions complies with PDPA 2024, and other applicable regulations. b) Advising Data Controller, Data Processors and Business Units and/or Corporate Functions DPO on data protection obligations and best practices. c) Developing, implementing, and updating data protection policies and procedures. d) Conducting training sessions to educate Data Controllers, Data Processors and Business Units and/or Corporate Functions DPO about data protection requirements. e) Regularly reviewing and auditing data processing activities to ensure compliance. f) Conducting and review Data Protection Impact Assessments (DPIAs) for high-risk processing. g) Managing data breaches, including notification to the Data Controller and affected individuals. h) Acting as the primary contact for the Data Processor and Data Controller, and other stakeholders on data protection matters. i) Maintain records of processing activities, risk assessments, and compliance measures.

3.8 Training and Awareness

- a) Provide regular data protection training for all employees, particularly those handling personal data.
- b) Update employees on new data protection regulations or amendments to existing ones, especially updates introduced by the PDPA 2024.

4.0 Policy Review and Update

This policy will be reviewed periodically to ensure its effectiveness and alignment with the company's goals and objectives. Amendments may be made as necessary to accommodate changing circumstances or company needs and/or any changes in legal or regulatory requirements.