SAMAIDEN GROUP BERHAD

201901037874 (1347204-V)

Data Privacy Policy

1. Purpose

This Policy sets out how Samaiden Group Berhad ("the Company") and its group of companies ("the Group") protects and manages Personal Data belonging to employees, customers, vendors, directors, and other individuals. We are committed to handling all Personal Data responsibly and in compliance with applicable laws, including the Personal Data Protection Act 2010 ("PDPA").

2. Scope

This Policy applies to:

a) All employees, directors, contractors, interns, and third parties who process Personal Data on behalf of the Company and/or the Group; and

b) All Personal Data collected, stored, used, processed, or disclosed in any form, either electronic or physical.

2.1. Definition

"**Personal Data**" means any information in respect of commercial transactions that relates directly or indirectly to a data subject who is identified or identifiable from that information.

3. Principles of Data Privacy

We apply the following privacy principles:

a) Lawful & Purpose-Specific – Personal Data is collected only for legitimate business purposes and used only for those purposes including but not limited to purposes relating to employment administration, project execution, contractual performance, regulatory compliance, corporate governance, information technology operations, and risk management;

b) Data Minimisation – We collect only the data needed to support business, legal, or operational requirements;

c) Transparency – Individuals are informed about why their data is collected and how it will be used;

d) Accuracy & Updates – Reasonable steps are taken to ensure Personal Data is accurate and kept up to date;

e) Security & Confidentiality – Personal Data is protected through physical, technical, and administrative controls;

f) Retention & Disposal – Personal Data is kept only as long as necessary and disposed of securely; and

g) Digital Information & Website Data – The Company's websites and digital platforms may collect limited technical information, including IP addresses, cookies, device identifiers and system logs, for cybersecurity, analytics, system administration and operational purposes in accordance with applicable laws.

3.1. **Categories of Personal Data**

Personal Data processed by the Company and/or the Group may include, without limitation:

a) Identification data (e.g. name, NRIC/passport number);

b) Contact data (e.g. address, email, telephone number);

c) Employment-related data (for employees and contractors);

d) Financial and transactional data;

e) Digital and technical data (e.g. IP address, system logs); and

f) Any other Personal Data provided in the course of business dealings.

3.2. **Directors' Personal Data**

In recognition of the Company's corporate governance obligations, the Company shall take reasonable measures to safeguard the Personal Data of its Directors, including Independent Directors, Executive Directors and Non-Executive Directors, throughout its collection, use, storage, disclosure and disposal.

Directors' Personal Data may include, without limitation:

a) Identification information such as NRIC/passport numbers, residential addresses and dates of birth;

b) Contact details, specimen signatures and emergency contact information;

c) Information required for statutory filings, regulatory submissions, corporate governance disclosures and due diligence exercises;

d) Remuneration, benefits and tax-related information; and

e) Board papers and Board Committee papers containing Directors' Personal Data, declarations of interests, conflict of interest disclosures and other governance-related records containing Personal Data.

Access to such Personal Data shall be limited strictly to authorised personnel on a need-to-know basis and shall only be processed for legitimate corporate governance, legal, regulatory, employment and business purposes in accordance with applicable laws.

4. Protection Measures & Instruments

To safeguard Personal Data, several controls will be used, including:

a) Access controls and secure systems;

b) Confidentiality obligations for employees and contractors;

c) Secure storage and restricted access;

d) Policies and procedures governing data handling; and

e) Non-Disclosure Agreements (NDAs) with employees, vendors, and partners.

The NDA is one of the Company's instruments to protect Personal Data and confidential information. It reinforces confidentiality obligations, restricts improper disclosure, and ensures data shared externally is kept secure and used only for approved purposes.

5. Sharing of Personal Data

Personal Data may be shared only with authorized internal personnel, government/regulatory bodies as required by law, and vendors or service providers who support Company operations including companies within the Group, service providers located within or outside Malaysia, subject always to appropriate safeguards and compliance with applicable data protection laws. Third parties must comply with confidentiality and data protection requirements, including signing NDAs where appropriate.

Without limiting the foregoing, Personal Data relating to Directors shall only be disclosed where necessary for statutory filings, regulatory reporting, corporate secretarial functions, banking and financial transactions, insurance arrangements, due diligence exercises, legal proceedings, or where otherwise required or permitted by law.

Where Personal Data is transferred outside Malaysia, the Company shall take reasonable steps to ensure that such transfer is carried out in accordance with applicable data protection laws and is subject to appropriate contractual, organisational and technical safeguards.

Service providers processing Personal Data on behalf of the Company shall only process such Personal Data in accordance with the Company's documented instructions and applicable contractual obligations.

6. Rights of Individuals

Where applicable, individuals may request access to their Personal Data, request correction of inaccurate data, or withdraw consent for non-essential processing subject to verification of identity and applicable legal or contractual limitations. Requests may be made to the Company's designated Privacy Officer or, where such requests are received by any employee of the Company, such employee shall promptly escalate the request to the designated Privacy Officer for handling.

6.1. Consent

Where required under the applicable law, the Company shall obtain consent from data subjects prior to processing their Personal Data.

Consent may be express or implied depending on the nature of the transaction, and may be withdrawn subject to legal, contractual or regulatory restrictions.

7. Data Breach Management

Any suspected loss, unauthorized access, or disclosure of Personal Data must be reported immediately to

the Company's designated Privacy Officer for investigation, containment and implementation of appropriate remedial measures.

8. Roles and Responsibilities

Management ensures compliance and resources. Employees must follow this Policy and protect Personal Data they handle. Third parties must honour contractual data protection obligations, including NDAs. The Company's designated Privacy Officer oversees privacy compliance and responds to enquiries.

The Company Secretary shall work together with the designated Privacy Officer to ensure that appropriate safeguards are implemented for the handling, storage and disclosure of Directors' Personal Data in connection with Board administration, statutory filings and corporate governance matters.

The Company may conduct periodic reviews, audits or assessments of its personal data management practices to ensure ongoing compliance with this Policy and applicable laws.

9. Review of Policy

This Policy will be reviewed yearly or whenever required due to changes in law or business operations.

Policy authorised by:

Datuk Ir. Chow Pui Hee, Chair of EXCO
Reviewed on: 5th August 2026
Next date of review: 5th August 2027