PERSONAL DATA PROTECTION ACT (PDPA) POLICY

1. OBJECTIVE

The Data Controller (the SLIC Group of Companies) is committed to protecting employee privacy in accordance with PDPA 2010 (PDPA), PDPA Amendment 2024, and PDPA Standard 2015.

2. SCOPE

This Policy applies to all personal data of employees, job applicants, customers, business partners, vendors, event participants, and any other identifiable individuals processed by the Group as a Data Controller and by any third-party service providers acting as Data Processors on behalf of the Group. It ensures compliance with PDPA principles, amendments, and technical standards.

3. DEFINITION AND TYPE OF PERSONAL DATA

Personal data includes any data that can identify an individual and shall include 'personal data' and 'sensitive personal data' as defined under the PDPA. Sensitive personal data includes biometric data such as fingerprints, facial recognition, and iris scans.

i. **Data Controller** - The organization that determines the purpose and means of processing personal data.

ii. **Data Processor** - Any party that processes personal data on behalf of the Data Controller.

iii. **Data Integrity Principle** - Personal data must be accurate, complete, and up to date.

TYPES OF PERSONAL DATA COMPANIES COLLECT

i. Name
ii. NIRC Number / Passport Number
iii. Mobile Contact Number
iv. Personal Email Address
v. Family Members Details
vi. Family Members Contact Number
vii. Residential Address
viii. Photographs
ix. Biometrics Data (e.g fingerprints, face recognition)
x. Any information required by law or as may be required by the Data Controller's internal policies and practices.

4. RESPONSIBILITIES UNDER PDPA 2024

ROLE	RESPONSIBILITIES	PIC
Data Protection Officer (DPO)	Advise on compliance, monitor internal practices, serve as contact point with the Commissioner, oversee breach response, and ensure staff training.	Robert

Data Controller	Ensure compliance with PDPA principles, appoint and notify the Commissioner of a Data Protection Officer (DPO), implement security measures, notify breaches, honor data subject rights, and oversee processors.	HODs
Data Processor	Follow controller instructions, comply with security requirements, assist in breach handling, and maintain confidentiality.	IT Operations, HR, Admin, Finance and external vendors (HR System and Healthcare System)

5. PURPOSE OF COLLECTION, USE, AND/OR DISCLOSURE OF PERSONAL DATA

The table shows some situations where the Data Controller collects, uses, and/or discloses personal data and the purposes of such are set out.

	Collection	Data Collected	Purpose(s)
a.	Job Application	• Information in job applicant's job application forms (e.g. name, NRIC number, personal email, mobile contact number, address, educational history, and background, family members details, referral contact, salary information at current/previous place of employment). • Documents upon job application (e.g. photograph, NRIC copy, certificate, payslip, etc).	• To evaluate the applicant and attend to all administrative work to process the job application. • To conduct background or reference checks for the applicant that are mandated by Data Controller internal policies and practices.
b.	Employees	• Personal Data of its employees (e.g. information in (a) above, bank account details, information relating to their salary, tax etc.	• To use and manage information in HR System and Health Panel System. • For legal, audit, and other compliance purposes, including filings with or disclosure to authorities and bankers. • To facilitate attendance at events/functions/seminars

			organized by Data Controller.
c.	Performance Evaluation	• Performance review forms, Training records, KPI reports	• Appraisal and promotion decisions
d.	Health & Safety	• Medical certificates, Health declaration forms, Emergency contact details	• Medical benefits and emergency contact
e.	Event Participation	• Registration forms, Travel documents, Photographs	• Organize company events, seminars, or training
f.	Regulatory & Legal Compliance	• Statutory filings, Audit reports, Correspondence with authorities	• Respond to government or regulatory requests
G.	IT & Security	• User access forms, System login records, Biometric data	• System access control and cybersecurity monitoring
h.	Cross-Border Data Transfer	• Data transfer agreement, Vendor compliance certification, Consent forms	• Sharing data with overseas branches or vendors

6. PRIMARY DATA PROTECTION RULES

6.1 The Group, as Data Controller, must comply with the following rules when collecting, using, or disclosing the personal data of any individual:

i. Obtain consent from employees or ensure collection, use, or disclosure is permitted under Malaysian law.
ii. Inform employees of the purpose of collection, use, or disclosure.
iii. Collect, use, or disclose personal data only for the stated purpose.
iv. Implement security measures including encryption, access control, and audit logs as per PDPA Standard 2015.
v. Ensure data integrity and retention compliance.

Data Processor Obligations:

i. Comply with the Security Principle when processing data on behalf of the Data Controller.
ii. Process data only under the instructions of the Data Controller.
iii. Assist the Data Controller in breach notifications and data subject requests.
iv. Maintain confidentiality and implement technical and organizational safeguards.

6.2 The Data Controller may collect, use or disclose employee's personal data without his/her consent in the following circumstances: -

i. In response to an emergency case that might threaten the life, health, or safety of the individual or another individual.
ii. For any necessary investigation or proceedings.
iii. In any other circumstances set out in the PDPA.

7. CORRECTION AND ACCESS TO PERSONAL DATA

The Data Controller takes reasonable measures to ensure that the Personal Data we collect from employees is accurate and complete. For this reason, if there is any change or update in Personal Data, the employee shall hold the right to access and correct the personal data held by the Data Controller. Where you wish to have access to your personal data in our procession, or where you discover any inaccurate, incomplete, misleading, or not up-to-date personal data, you may make a request to the HR Department.

8. BREACH NOTIFICATION AND DATA PORTABILITY

Data Breach Notification: The Group must notify the Commissioner immediately upon discovering a personal data breach and inform affected individuals if harm is likely.

Data Portability: Employees have the right to request the transfer of their personal data to another data controller, subject to technical feasibility. Notices and requests may be made email to HR.

9. CROSS-BORDER DATA TRANSFER

Personal data may only be transferred outside Malaysia in compliance with Section 129 of the PDPA amendments.

10. DISCLOSURE, SHARING, OR TRANSFER OF PERSONAL DATA

The Data Controller does not sell or rent personal data that we collect from employees to other third parties except under the following circumstances: -

i. To Data Controller business partners for the purpose of providing products and services to our customers.

ii. To government or non-government authorities, agencies, and/or regulators as required under law or under directions or orders from government and non-government authorities, agencies, and/or regulators for security, regulatory approvals, or permit.

iii. To event organizers and service providers to facilitate the planning of events/ functions/ seminars that the Data Controller is involved in.

iv. To Data Controller service providers for example data storage, electronic mail services, company operations system, and HR system.

v. To professionals, financial agencies and legal advisors, tax advisors, auditors, insurers, and insurance brokers.

11. PROTECTION, RETENTION, AND DISPOSAL OF PERSONAL DATA

Protection of Personal Data

The Data Controller shall take responsibility to protect employee personal data and keep personal data secure. This includes following our security procedures like limiting access to the employee database folder by setting a password to only assigned personnel.

Retention and Disposal of Personal Data

The Data Controller only retains personal data which is required for the purposes as per describe in this policy and for our business and legal purposes. The Data Controller will not retain personal data for resigned/terminated employees for more than seven (7) years after the resignation/termination date for which the personal data collected have ceased to be applicable.

For any unsuccessful job applicants, the Data Controller will retain the personal data for no longer than one (1) year for the purpose of evaluating suitability for a future job opening with the Data Controller, unless informed by the applicant.

The Data Controller must ensure that the personal data is properly disposed of or permanently deleted in accordance with PDPA Standard 2015. Retention may be extended where required by law, litigation, or regulatory investigations.

12. PENALTIES FOR NON-COMPLIANCE

Upon receiving a complaint for non-compliance from Data Controller, the Personal Data Protection Commission ("PDPC") may, or of its own motion, conduct an investigation to determine whether an organization is in compliance with the PDPA.

Failure to comply may result in fines up to RM1,000,000 or imprisonment up to three (3) years for major breaches. Breach notification failures may result in fines up to RM250,000 or imprisonment up to two (2) years.

Internal disciplinary action may be taken against employee for PDPA breaches, in addition to statutory penalties.

13. GENERAL

The Data Controller may revise or amend this policy at its discretion without prior notice to the employee. Employees of the Data Controller are encouraged to review this policy from time to time to ensure that you are aware of any such changes.