PERSONAL DATA PROTECTION POLICY

(In Compliance with PDPA 2010 [Act 709] as Amended 2024)

1) PURPOSE

1.1. The Personal Data Protection Act 2010 of Malaysia ("Act"), which regulates the processing of personal data in respect of commercial transactions and employment, applies to METROD GROUP (hereinafter referred to as "our", "us" or "we") as a data user and requires the Company to inform data subjects about personal data collected from them and how it is processed.

1.2. This Policy serves as guidance for the collection, processing, use, disclosure, and protection of personal data in commercial transactions, employment, and other business activities of the Company, in full compliance with the Act, including the Amendment Act 2024 and related guidelines issued by the Personal Data Protection Commissioner.

1.3. This Policy also outlines the appointment of the Data Protection Officer ("DPO"), management of personal data breaches, and cross-border data transfer practices, ensuring all data subjects' rights are protected and maintained

2) SCOPE & COVERAGE

2.1. Scope of Application

This Policy applies to all personal data collected, processed, or stored by Metrod Group, including:

- Employees & Job Applicants (HR records, payroll, biometrics, training, health data, CCTV)
- Customers & Clients (contact details, billing, delivery, service records)
- Suppliers & Contractors (representative IDs, bank details, site access, contractual documents)
- Visitors & Website Users (registration, CCTV, online forms)

2.2. Coverage

All data subjects associated with Metrod Group, including current and prospective employees, contractors, suppliers, clients, visitors, and other relevant individuals, are covered by this Policy.

3) DEFINITIONS

- Personal Data: Information relating to an identified or identifiable individual.
- Sensitive Personal Data: Includes financial information, health records, biometric data, and other data classified as sensitive under PDPA.
- Data Subject: Any individual whose personal data is processed by Metrod.
- Processing: Any operation performed on personal data, including collection, storage, use, disclosure, or destruction.
- Commercial Transaction: Any transaction, service, or relationship conducted between Metrod and the data subject.

4) TYPES & SOURCES OF PERSONAL DATA

4.1. Types of Personal Data Personal data may include, but is not limited to:

- Name, address, phone numbers, email, identity card or passport numbers, signature, date of birth, gender, nationality, marital status
- Employment and education history, academic records, bank account details
- Images, photographs, audio/video recordings, CCTV footage
- Sensitive personal data: religion, health, medical condition, political opinion, criminal convictions

4.2. Sources of Personal Data

- Provided voluntarily by the data subject or representatives (family, guardians, referees)
- Recruitment agencies or previous employers
- Publicly available sources (directories, credit reporting agencies)

4.3. Accuracy and Notification Data subjects must ensure personal data is accurate, complete, and up-to-date. Any changes should be promptly notified to the Company. Failure to provide accurate data may limit services, benefits, or employment entitlements.

5) COLLECTION, USE, AND DISCLOSURE

5.1. Purposes of Collection & Use Personal data will be collected and processed for legitimate purposes, including:

- Communication and customer service
- Processing applications, employment, or transactions
- Administration of HR, payroll, benefits, training, performance, career planning
- Marketing, promotions, and publicity
- Legal, audit, compliance, and risk management purposes
- Event management, surveys, and contests
- Fraud prevention, security, and safety monitoring

5.2. Disclosure of Personal Data Data may be disclosed, within and/or outside Malaysia, to:

- Employees, consultants, auditors, lawyers, agents, contractors, vendors, suppliers, service providers, distributors, financial institutions
- Metrod Group entities (parent, subsidiaries, affiliates)
- Legal or regulatory authorities, government agencies, courts, or tribunals
- Business partners for product/service development or marketing campaigns
- Emergency contacts or family members (for safety or accident notifications)
- Data centers, servers, storage, and backup service providers
- The general public for promotional purposes (e.g., contest winners)

5.3. Consent for Disclosure By providing personal data, data subjects consent to such collection, use, and disclosure for the purposes described above.

5.4. Use of Personal Data for Marketing Communications

5.4.1. The Company may use personal data of data subjects to send marketing, promotional, or publicity materials, including information about products, services, events, and offers that may be of interest to the data subject.

5.4.2. Opt-Out from Marketing Communications

Data subjects may withdraw their consent or opt out from receiving marketing, promotional, or publicity materials at any time by contacting the Data Protection Officer ("DPO") using the contact details provided in this Policy. Upon receiving such a request, the Company will take reasonable steps to ensure that the data subject is excluded from future marketing communications within a reasonable timeframe.

6) CONSENT & WITHDRAWAL

6.1. Consent is the legal basis for processing personal data. Separate consent may be obtained for employees, customers, vendors, contractors, and minors.

6.2. Withdrawal of consent can be made in writing to the DPO, but may affect services, employment benefits, or contractual relationships.

7) DATA SUBJECT RIGHTS (ACCESS & CORRECTION)

7.1. Data subjects may request:

- Access to personal data
- Correction of inaccurate, incomplete, or outdated data
- Limitation of processing
- Withdrawal of consent (full or partial)

7.2. Requests should be submitted via the Data Subject Access Request Form or Correction Request Form to the DPO.

7.3. The Company may charge a reasonable fee for access requests, reflecting verification, retrieval, and copying costs.

7.4. Requests will be responded to within 21 days, or reasons for refusal provided in accordance with PDPA.

8) RETENTION OF PERSONAL DATA

8.1. Personal data will be retained only as long as necessary to fulfill the stated purposes or comply with legal or regulatory requirements. For illustrative purposes, typical retention periods include:

- HR and employment records: 7 years from the date of termination or last employment.
- CCTV recordings: 30 days from the date of recording.
- Other records: As required by applicable laws or Company policy.

8.2. Data will be securely destroyed or anonymized once no longer required, unless retention is needed for operational, legal, regulatory, or accounting purposes.

9) SECURITY OF PERSONAL DATA

9.1. Metrod implements technical, physical, administrative, and procedural safeguards, including:

- Authorized access on a "need-to-know" basis
- Clean desk and document security policies
- Locking filing cabinets and secure storage
- CCTV monitoring for sensitive areas
- Remote access and wipe for lost devices
- Encryption and cybersecurity for IT systems
- Restriction of removable media/cloud use
- Regular backups with disaster recovery systems

9.2. Internet communications (e.g., e-mails, cookies) are protected, but absolute security cannot be guaranteed.

10) DATA PROTECTION OFFICER (DPO)

10.1. In compliance with the DPO Guideline, Metrod has appointed a DPO to oversee PDPA 2024 compliance.

DPO Details:

Name :	Mr. Jeffery Victor
Position:	Data Protection Officer
Address:	No.3, Lengkuk Keluli 2, Bukit Raja Prime Industrial Park, 41720 Klang, Selangor
Tel :	+603-3361 3422
e-mail :	dpo@metrod.com

10.2. Responsibilities:

- Ensure compliance with PDPA 2024 and related guidelines
- Handle access, correction, and consent withdrawal requests
- Coordinate and report personal data breaches
- Conduct audits and risk assessments
- Report directly to President & CEO

11) DATA BREACH NOTIFICATION

11.1. All suspected or confirmed personal data breaches must be reported immediately to the DPO.

11.2. In the event of a personal data breach, the relevant employee or department shall immediately inform the Data Protection Officer (DPO). The DPO shall assess the nature, scope, and potential impact of the breach and, where necessary, escalate the matter to Senior Management. If the breach is determined to be notifiable, the DPO shall notify the Personal Data Protection Commissioner within 72 hours in accordance with PDPA requirements.

11.2.1. All employees shall have an obligation to promptly report any actual or suspected personal data breach to their respective Head of Department, who shall, without undue delay, notify the Data Protection Officer ("DPO") for further assessment and action in accordance with this Policy

11.3. Affected data subjects will be informed promptly if there is a risk of harm, including details of:

- Nature of the breach
- Personal data affected
- Potential consequences
- Steps taken to mitigate the breach

12) CROSS-BORDER PERSONAL DATA TRANSFER

12.1. Transfers outside Malaysia will comply with the CBPDT Guideline.

12.2. Adequate protection will be ensured through contracts or other safeguards.

12.3. Records of cross-border transfers will be maintained.

13) ENFORCEMENT & REVIEW

- Non-compliance may result in disciplinary or legal action.
- The Policy will be reviewed at least annually or when required by law.
- Updates will be communicated to all stakeholders.

14) ACKNOWLEDGMENT

By providing personal data or maintaining a relationship with Metrod Group, data subjects acknowledge and consent to this Policy.

15) EFFECTIVE DATE

This Policy takes effect from 24th November 2025 and supersedes all prior versions.