1. Scope and Introduction

1.1 This Privacy Policy ("**Policy**") describes how **Entrypass Corporation Sdn Bhd** (Registration No. 200201025775 (593438-M)) ("**Entrypass**", "**we**", "**us**", or "**our**") collects, uses, discloses, and protects Personal Data in connection with the use of **our** products, solutions, software, websites ("**the Site**"), web and/or mobile applications ("**the App**"), platforms, systems, Intelligent Automation Technology Security System products and associated cloud platform and other services provided or made available by Entrypass (collectively, the "**Services**").

1.2 This Policy applies to you where we obtain your Personal Data through:

(a) your interaction with marketing or similar content on our Site;
(b) your evaluation of the Services on behalf of a prospective purchaser;
(c) any communication with our sales team; or
(d) your independent interaction with the Services not at the direction of any Customer.

1.3 Where Entrypass processes Personal Data (including biometric data collected via the Services, such as facial images or fingerprints) on behalf of and at the direction of a business customer that has deployed our Services (a "**Customer**"), Entrypass acts as a data processor, and this Policy does not govern that processing. That processing is governed by (i) the Customer's own privacy notice, and (ii) the data processing agreement between Entrypass and the Customer. If you interacted with the Services through your employer, a business you provided services to, or a company you visited, please contact that organisation directly regarding your data protection rights. Entrypass will support that organisation in responding to your request as required by our data processing agreement with them. Sections 3.2 to 3.4, 4.3 and 6.3 describe how the Access Control System operates and are included for transparency only. Where Entrypass acts as a processor, the Customer determines the purposes of that processing and is responsible for providing notice to, and obtaining any required consent from, individuals.

1.4 The use of our Services is subject to the following terms of use:

(i) The content and information provided in connection with our Services are for your general information and use only. Our Services and the information provided may be subject to change without notice.

(ii) Neither we nor any third parties provide any warranty or guarantee as to the accuracy, timeliness, performance, completeness or suitability of the content, information and materials found or offered in connection with our Services for any particular purpose. You acknowledge that such content, information and materials may contain inaccuracies or errors and we expressly exclude liability for any such inaccuracies or errors to the fullest extent permitted by law.

(iii) Your use of any content, information or materials in connection with our Services is entirely at your own risk, for which we shall not be liable. It shall be your own responsibility to ensure that any products, services, software, applications or information available through our Services meet your specific requirements.

(iv) Our Services contains material which is owned by or licensed to us. This material includes, but is not limited to, the software, source code, design, layout, user interfaces, text, images, content, documentation, features, functionality, graphics, and other materials provided as part of our Services. Reproduction, modification, distribution or use of such material is prohibited other than in accordance with the copyright notice, which forms part of these terms and conditions.

(v) All trademarks reproduced in connection with our Services, which are not the property of, or licensed to us, are acknowledged and remain the property of their respective owners.

(vi) Unauthorised use of our Services may give to a claim for damages and/or be a criminal offence.

(vii) From time to time, our Services may also include links to third-party websites, applications, platforms, or other services. These links are provided for your convenience to provide further information and we do not endorse other third parties' website(s) or services. We have no responsibility for the content of the linked third parties' website(s), platform(s) or service(s) and have no responsibility or liability for their content, availability, security, or practices.

2. Definitions

"**Access Control System**" means the part of the Services that controls entry to a premises or area, comprising (a) controllers; (b) readers and terminals, including facial recognition, fingerprint, RFID card, PIN and Bluetooth or mobile readers; (c) credentials, including cards, tags, biometric templates and mobile credentials; and (d) the software, cloud platform and App used to configure the system and store its records.

"**Customer**" means an entity (not an individual) that signs up to use one or more of our products.

"Personal Data" means any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular person. However, Personal data does not include any deidentified or aggregated information.

"**Sensitive Personal Data**" means Personal Data revealing biometric or health information, or other categories treated as sensitive under applicable law, including the biometric data described in **Section 3** below.

"**Services**" means the Site, the App, our Intelligent Automation Technology Security System hardware, and our cloud platform, collectively.

"**You**" or "**Individual**" means the natural person whose Personal Data is processed under this Policy.

3. Categories of Personal Data We Collect

We collect Personal Data only from individuals who register for or sign up for our services on behalf of their respective companies. Entrypass does not collect personal data through the Access Control System installed at the Customer's premises. Any biometric data collected through the Access Control System, including facial images, video footage, fingerprints and biometric templates, is collected and managed by the Customer within its own systems and infrastructure, which are not accessible by us. Further details regarding biometric data are set out in Section 3.1.

3.1 Biometric Data (Sensitive Personal Data)

We do not collect biometric data through the Access Control System. The Customer independently collects and manages photographs, video footage, and fingerprint data (including biometric templates derived from facial images, palm prints or fingerprints) captured by the Access Control System installed at the Customer's premises for its own access-control and security purposes.

- Storage and Access: Biometric templates are stored in the controllers, software and servers deployed for the Services. All such controllers and servers are installed at the Customer's premises and are not accessible by Entrypass.

- Purpose limitation: the Customer is responsible for ensuring that biometric data collected through the Access Control System is used for its intended access-control and security purposes and in accordance with applicable laws.

- Consent: the Customer is responsible for obtaining any consent required by applicable laws before collecting or processing biometric data through the Access Control System.

- Retention: the Customer is responsible for determining the retention period and ensuring the secure deletion or anonymisation of biometric data stored within its systems, in accordance with applicable laws. Entrypass does not control the retention or deletion of biometric data stored at the Customer's premises.

- AI/model training: Entrypass does not use biometric data to train or improve machine learning or AI models. If it does, Entrypass will make such disclosure and, where required, to obtain a separate consent from Customer.

3.2 Credential Data

We collect identifiers that are read by, issued through or stored in the Access Control System, such as RFID card or tag numbers, PIN codes, and Bluetooth or mobile credentials issued to a user, at the direction of the Customer operating the Services.

3.3 Access Event Data

The Access Control System generates a record each time a credential or biometric is presented to a reader, including the date and time, the reader and door identifiers, the user or credential identifier, whether access was granted or denied, and any alarm or tamper events. These records may be stored on the controller, in the Entrypass software and/or on our cloud platform.

3.4 Device and App Data

Where you use Bluetooth or mobile access through the App, we collect your user ID and location data as necessary to provide the mobile access functionality.. The App may ask for permission to use Bluetooth, location services and notifications. You can change these permissions in your device settings, but some features may then not work.

3.5 Other Personal Data

- **Contact Information:** A name, address, telephone number, and other contact information you or your employer may provide to us.

- **Identifiers:** Identifiers include information like your name, National Registration Identity Card (NRIC) number, passport number, or email address. Entrypass uses Identifiers to provide you with an account to use the Services, to communicate with you regarding your use of the Services, to communicate with you regarding your possible purchase of a subscription to use the Services, to send you marketing communications regarding the Services, or to debug and repair errors with the Services.

- **Your Communications with Us:** When you choose to engage with Entrypass, we collect the content of those exchanges, including emails, live calls, and AI-assisted chat interactions.

- **Internet Activity Information:** Your IP address, session duration, and interactions with the Site/App. Entrypass uses your Internet Activity to debug and repair errors with the Services, to determine how to improve the Services, and to measure marketing effectiveness.

- **Location Information:** General location inferred from data such as your IP address and precise location such as geolocation information collected via our App, where relevant to our Services.
- **Professional Information:** Entrypass sells to businesses and will use the business's Professional Information to determine what business may be purchasing the Services and to send marketing communications to the business.

4. How We Collect Your Data

4.1 Entrypass may collect your information from the following categories of sources:

- Entrypass.net;
- Entrypass mobile applications;
- Entrypass Software;
- Entrypass Access Control System devices (readers, controllers and credentials);
- Direct communications with you;
- Social Media;
- Sales and marketing tools; and
- Entrypass Cloud Server system.

4.2 Entrypass may also collect your data through non-Malaysian Entrypass group of companies. Entrypass has intercompany data sharing agreements with its group of companies that ensure the transfer of personal data into Malaysia complies with data privacy law. See **Section 9** (Cross-Border Data Transfers) for the safeguards that apply to such transfers.

4.3 In a typical deployment of the Access Control System, a reader captures a credential or biometric sample and passes it to a controller, which compares it against stored records and decides whether to unlock the door. The controller communicates with the Entrypass software or cloud platform, to facilitate access management and the processing of user records, access rights and event logs. A user may instead present a Bluetooth or mobile credential through the App. Biometric templates and other records may be stored on the reader, the controller, and/or the Customer's server installed at the Customer's premises, which are not accessible by Entrypass.

5. Legal Basis for Processing

5.1 We process Personal Data on one or more of the following bases, as applicable under law:

- Consent — for marketing communications, non-essential cookies, and any direct collection of biometric data outside a Customer's direction. You may withdraw consent at any time (**Section 10**).
- Performance of a contract — to provide the Services to a Customer or to you directly, including account administration and support.
- Legal obligation — to comply with applicable law, regulation, or a valid order of a competent authority.

- Legitimate interests — for example, to secure and improve the Services, prevent fraud, and communicate with prospective business customers, balanced against your rights and interests.

5.2 Where we act as a processor on behalf of a Customer, the Customer determines the legal basis for that processing.

6. How We Use Your Data

6.1 Marketing and Business Development

- Delivering marketing communications and advertisements about our Services.
- Analysing existing and prospective customers, and our interactions with them, to improve marketing initiatives.

Where consent is legally required, we will use your data for these purposes only with your consent.

6.2 Customer and Business Relationships

If you are a representative of a current or prospective customer, we use your information to:

- Communicate with you during the sales process;
- Provide services and support;
- Create and administer accounts necessary to use the Services;
- Deliver transactional communications about the operation of the Services;
- Communicate with you about payment or other legal obligations;
- To fulfil statutory and other legal functions and duties; and
- To plan, fund, implement monitor, regulate and evaluate Services and function and to improve our products and services.

6.3 Access Control System

Where we act as a processor on behalf of a Customer (see **Section 1.3**), the Customer determines the purposes of processing. The Access Control System uses Personal Data to:

- Verify identity and grant or deny access to premises or areas;
- Maintain access records and audit logs as configured by the Customer;
- Synchronise data between readers, controllers, the software and the cloud platform, and deliver credentials and notifications to the App;
- Diagnose faults, provide technical support and deliver firmware and software updates; and
- Detect and respond to security incidents, tampering and unauthorised access.

7. How We Disclose Your Data

7.1 We do not sell or rent your personal data.

7.2 We may share Personal Data, limited to what is reasonably necessary, with the following categories of recipients:

- Entrypass group companies, for the purposes described in this Policy;
- installation and maintenance contractors, engaged to deploy and service the Services;
- cloud hosting and IT infrastructure providers, who store and process data on our behalf under written data processing agreements;
- marketing service providers, engaged to deliver marketing communications on our behalf;
- mobile platform providers (such as Apple and Google), to deliver push notifications and support Bluetooth or mobile credentials;
- professional advisers (legal, audit, insurance), where necessary for their engagement; and
- regulatory or law enforcement authorities, where required by law, court order, or to protect our legal rights, or those of others.

7.3 All third parties who process Personal Data on our behalf are bound by written contractual obligations to protect that data, use it only for the purposes we specify, and assist us in meeting our obligations under applicable data protection law, including the Security Principle now applicable to data processors under the amended PDPA.

8. Data Retention

8.1 We retain Personal Data only for as long as necessary to fulfil the purposes for which it was collected, including to satisfy any legal, accounting, or reporting requirements. Specifically:

- **Account and Customer-relationship data:** for as long as you are associated with a Customer account, and for **two (2) years** afterward to meet legal and audit obligations.
- **Biometric data:** as set out in **Section 3.1** — limited to the purpose for which it was collected, and in any event no longer than **two (2) years**.
- **Marketing data:** until you withdraw consent or object, or **two (2) years** of inactivity.
- **Support and communications records: two (2) years.**

At the end of the applicable retention period, Personal Data is securely deleted or anonymised such that it can no longer be associated with you.

8.2 We strive to take reasonable technical and organizational measures to safeguard your personal information against loss, misuse, or unauthorized access.

8.3 However, please note that no method of transmission over the internet or method of electronic storage is 100% secure. By using our Site, you hereby agree and acknowledge that no method of transmission over the internet, or method of electronic storage is absolutely secure and reliable, and we cannot guarantee its absolute security. In view hereof, we will take reasonable measures to enhance and improve the security measures on our Site in accordance with the Privacy laws.

9. Cross-Border Data Transfers

9.1 Personal Data may be transferred to, and processed by, Entrypass group companies or service providers located outside Malaysia, including in Singapore, Indonesia, Hong Kong, China, Middle East and other countries that we may expand our Services to in the near future. Where we transfer Personal Data outside Malaysia, we take steps to ensure the recipient country or territory has a level of data protection that is at least equivalent to the protection under the PDPA — for example, through intercompany data transfer agreements incorporating standard data protection clauses, an adequacy finding, or your explicit consent to the transfer, consistent with the Guidelines for Cross-Border Personal Data Transfer issued by the Personal Data Protection Commissioner.

9.2 Entrypass shall take reasonable steps to assess and ensure compliance with applicable requirements for cross-border transfers before transferring or receiving personal data.

10. Data Security

10.1 We implement technical and organisational measures designed to protect Personal Data against loss, misuse, unauthorised access, disclosure, or alteration, including:

- Encryption of Personal Data in transit and, where applicable, at rest;
- Measures designed to protect data in transit, including AES-256 encryption for communications between readers and controllers, and TLS 1.2 encryption for communications between the controller and the software;
- Access controls limiting Personal Data access to personnel who need it to perform their role;
- Relevant certifications;
- Regular review of our security practices; and
- Contractual security obligations imposed on service providers and Customers who process data via the Services.

10.2 No method of transmission over the internet or electronic storage is completely secure, and we cannot guarantee absolute security. We will take reasonable steps to update our security measures in line with applicable law and industry practice.

11. Data Breach Notification

11.1 In the event of a Personal Data breach, Entrypass will notify the Personal Data Protection Commissioner as soon as practicable after becoming aware of the breach, and will notify affected individuals without unnecessary delay where the breach is likely to cause significant harm, in each case consistent with our obligations under the Personal Data Protection Act 2010 (as amended) and the Guideline on Data Breach Notification. Notifications to affected individuals will describe the nature of the breach, the data involved, and the steps we are taking in response.

12. Your Data Protection Rights

12.1 What Are Your Data Protection Rights?

You have rights over your personal information, including the right to:

- Access, correct, or update your personal data;
- Withdraw your consent for marketing communications or any other processing based on consent, at any time; at any time;
- Object to, or request restriction of, certain processing or deletion of your personal information (subject to applicable law and legitimate business needs);
- Request data portability — i.e., request that we transmit your Personal Data directly to another data controller, where technically feasible;
- Lodge a complaint with the Personal Data Protection Commissioner of Malaysia, or another applicable supervisory authority, if you believe your rights have been infringed.

12.2 How can you exercise your rights?

You may choose to restrict the collection or use of your personal information in the following ways:

i) whenever you are asked to fill in a form on the website, look for the box that you can click to indicate that you do not want the information to be used by anybody for direct marketing purposes; or

ii) if you have previously agreed to us using your personal information for direct marketing purposes, you may change your mind at any time by writing to or emailing us at info@entrypass.net.

If you have interacted with our Services through your employer, a business you provided services to, or through a company you visited, please contact that company for more information on the data protection rights available to you. We cannot accept your request directly because, in these circumstances, we do not collect and use your Personal Data on behalf of that company (our Customer).

13. Children and Other Individuals Captured by the Services

The Services may incidentally capture Personal Data (including images) of individuals who are not Customers, App users, or otherwise direct account holders — for example, visitors, household or family members, or employees of a Customer's premises, including children. Where a Customer deploys the Services in a location accessible to such individuals, the Customer is responsible for providing appropriate notice to them (e.g., signage indicating that biometric or video capture is in use) and for obtaining any consent required by applicable law. Entrypass processes such data only as instructed by the Customer and does not knowingly collect Personal Data directly from children without appropriate consent.

14. Automated Decision-Making

Certain Services functions (for example, facial-recognition, fingerprint, RFID card, PIN or Bluetooth/mobile credential-based access control) may make automated decisions that affect you, such as granting or denying physical access. If you wish to contest an automated decision made using the Services, please contact the Customer that operates the Services, or Entrypass if you interacted with the Services directly.

15. Cookies and Other Tracking Technologies

15.1 Our website uses cookies. A cookie is a small file which asks permission to be placed on your computer's hard drive stored by your browser. Upon your acceptance of the cookie, the file is added and the cookie helps analyse web traffic or lets you know when you visit a particular site that enables us to identify you. The web application can tailor its operations to your needs, likes and dislikes by gathering and remembering information about your preferences. This helps us analyse data about web page traffic and improve our website in order to tailor it to customer needs. We only use this information for statistical analysis purposes and then the data is removed from the system. Overall, cookies help us provide you with a better website, by enabling us to monitor which pages you find useful and which you do not. When you visit our website, we may ask for your consent before using any cookies that are not essential. You can adjust your browser or operating system settings to limit certain tracking or to decline cookies. Doing so may affect certain functionality on our website.

15.2 A cookie in no way gives us access to your computer or any information about you, other than the data you choose to share with us. You can choose to accept or decline cookies. Most web browsers automatically accept cookies, but you can usually modify your browser setting to decline cookies if you prefer. This may prevent you from taking full advantage of the website.

16. Third-Party Links

Our Services may contain links to third-party websites. We are not responsible for the privacy practices or content of such websites. We encourage you to review the privacy policies of any third-party sites you visit.

17. Data Protection Officer

In compliance with the Personal Data Protection (Amendment) Act 2024 (Malaysia), Entrypass has appointed a Data Protection Officer responsible for overseeing compliance with this Policy and applicable data protection law. You may contact our Data Protection Officer, Ryan Tan, Executive Director at ryantan@entrypass.net.

18. Notification of Changes to this Policy

We may update our Privacy Policy from time to time to reflect changes to our practices, technology, legal requirements and other factors. When changes are made to this Privacy Policy, they will become immediately effective when published. We will take reasonable steps to alert you to material changes by placing a notice on the www.entrypass.net website. Your continued use of our Services constitutes consent to any changes to this Policy.

19. Contact Us:-

Entrypass Corporation Sdn Bhd

Company Registration No. 200201025775 (593438-M)

No. 40, Jalan TPP 1/10, Taman Industri Puchong,

Batu 12, Jalan Puchong, 47160 Puchong,

Selangor, Malaysia

General Line : +603-80681929

General Email : info@entrypass.net

Data Protection Officer : ryantan@entrypass.net

Inquiry Submission : marketing@entrypass.net

20. Disclaimer

20.1 The information contained in our Services is for general information purposes only. The information is provided by Entrypass and whilst we endeavour to keep the information up-to-date and correct, we make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability or availability with respect to the information, products, services, or related graphics contained in our Services for any purpose. Any reliance you place on such information is therefore strictly at your own risk. In no event will we be liable for any loss or damage including without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever arising from loss of data or profits arising out of or in connection with the use of our Services. Through our Services, you may be able to link to other websites which are not under the control of Entrypass. We have no control over the nature, content and availability of those sites. The inclusion of any links does not necessarily imply a recommendation or endorse the views expressed within them.

20.2 Your use of our Services and any dispute arising out of such use is subject to the laws of Malaysia.