Privacy Policy

Penpower Technology Ltd. (“Penpower Technology”) is committed to protecting the privacy of all customers who purchase our products and users of our website. The privacy policy is to help users of our website understand the policy of the website in terms of personal data collection, processing, and use.

Acquisition of Data

When you choose to join as a member of Penpower Technology, Penpower Technology will collect your personal data according to the agreement in the “Consent for the Provision of Personal Data.” Such data are necessary for the provision of services to you. Meanwhile, we may also require you to provide other relevant data through the website or activities, and the main purpose is hoping to provide more personalized services to you. If you are a minor, you shall obtain the consent of your guardian before choosing to join as a member of Penpower Technology.

Use of Personal Data

According to the agreement in the “Consent for the Provision of Personal Data,” all personal data acquired is only for internal use by Penpower Technology. We collect, process, keep, and use personal data within the reasonable scope to provide other information and services to you, produce statistics of members, or carry out online behavior surveys or research. Penpower Technology will not sell or lend any personal data to any party. Meanwhile, Penpower Technology will also send e-mails or DMs related to product and service nature to you. If you do not wish to receive such e-mails or DMs, simply let us know when providing your personal data.

Data Protection and Termination

Penpower Technology does its best to prevent all member data from being stolen, altered, damaged, lost, or leaked with reasonable technologies and procedures and protects the safety of data transmission. Penpower Technology may terminate your password and account number based on its own consideration due to different reasons, including but not limited to zero usage within a certain period, an order of the court or a governmental agency, your request, the inability to continue the service or the substantial alteration of the service content, unexpected technical or safety factors or issues, fraudulent or illegal behaviors conducted by you, or other matters that Penpower Technology considers that you have violated the specified requirements and spirits of relevant terms. Penpower Technology may also terminate the service or its any part at any time under the circumstances with or without any notification based on its own consideration. You agree that Penpower Technology shall not be held responsible to you or any third party if the service is terminated.

The website or service of Penpower Technology may have website links or service content provided by third parties; such websites and services are not managed by Penpower Technology. Before contacting, clicking, or adopting such websites or services, users shall understand the user terms or privacy policy formulated by the providers of such websites or services. Such websites or services are not within the applicable scope of this Policy, and Penpower will not assume any legal responsibility for the behavior of third-party websites or services in collecting users' personal data. Penpower Technology uses, including but not limited to, the login services and content sharing platforms of the following third parties.
Google Privacy Policy: https://policies.google.com/privacy
Notion Privacy Policy: https://www.notion.so/Privacy-Policy3468d120cf614d4c9014c09f6adc9091

Amendment to the Privacy Protection Policy

Penpower Technology may amend the content of this Policy from time to time. You are recommended to be aware of such changes at all times. If you disagree with the content of this Policy or its subsequent changes or the country or region that you are in excludes the entire or partial content of the privacy protection policy, please feel free to contact our customer service center via e-mail. We will respond and provide descriptions as soon as practicable.

Agreement in the Consent for the Provision of Personal Data

This Consent is established according to laws, regulations, and the regulations for personal data management formulated by Penpower Technology Ltd. (the "Penpower").

I. Collection, update, and preservation of basic data

1. Personal data collected by Penpower is collected, processed, and used under the regulation of the "Personal Data Protection Act" (the "Act") and relevant laws and regulations of the Republic of China according to the personal data management of Penpower.
2. Please provide accurate, the latest, necessary, and comprehensive personal data.
3. Personal data collected by Penpower due to the provision of relevant services, the publication of various information of Penpower, and other reasonable and necessary behaviors include but are not limited to name, date of birth, contact method (contact address, telephone number, and e-mail). Personal data willingly provided by an individual on this Platform due to requirements is deemed legal collection done by Penpower according to this Agreement.
4. **Browser cookies:** Particular data may be collected (i.e., IP addresses, device event information (including but not limited to browser types, crashing or quitting records, system activities, and other service login data)). Penpower may use cookies to improve

personal experience. Personal website browsers will input cookies into the hard drive to record browser records and track the usage information from time to time. An individual may choose to turn off cookies or have the browser set to not notify you when transmitting cookies. However, please be aware that if the setting of the page browser rejects cookies, partial functions may not operate smoothly.

5. If the personal data has any alteration or error, please make an active request to Penpower for corrections or supplements or make corrections through the member login page to allow personal data to remain accurate, updated, and comprehensive.
6. If relevant rights and interests of the party to the Consent or Penpower are harmed due to the provision of false, inaccurate, outdated, incomplete, or misleading data, the individual will be held responsible.
7. An individual may exercise the following rights in terms of personal data according to the "Personal Data Protection Act" of the Republic of China:
   (1) Request to make inquiries or to browse;
   (2) Produce a copy;
   (3) Request to make supplements or corrections;
   (4) Request to suspend the collection, processing, and use;
   (5) Request to delete.

II. Purpose for collecting personal data

1. Penpower is required to collect personal data due to the provision of relevant services, the publication of various information of Penpower, and other relevant operations.
2. If the using method of personal data is different from that of the initial collection purpose of Penpower, Penpower will seek written consent before use. An individual may refuse to provide personal data to Penpower; however, please consider whether there are other unfavorable factors or effects.
3. The period in which Penpower uses personal data is the duration of relevant services. The region of use is Taiwan, the location of the service provision and the server mainframe, or the region agreed upon by individuals for data processing and use.

III. Confidentiality of basic data

Personal data is protected and regulated under the Act, the regulations for personal data management of Penpower, and relevant confidentiality measures. If the personal data collected by Penpower is stolen, leaked, altered, have other infringements due to the violation of the "Personal Data Protection Act" or due to natural disasters, accidents, or other force majeure, Penpower will immediately investigate the cause once being notified and make select appropriate methods for notification via telephone, letters, e-mails, or website announcements and try its best to prevent the occurrence of damages.

IV. Effects of the Consent

Penpower preserves the right to amend the specifications in this Consent according to the Act or the indictments or orders of the court or competent authority at any time. Penpower will announce the fact of the amendment on its intranet or via other appropriate methods

without making individual notifications. If there is no opposing opinion for individual negotiation after the announcement, it is deemed agreeing and accepting the amendments to this Consent or the restriction by the amended content.

V. Governing law and governing court

The interpretation and application of this Consent shall be subject to the laws of the Republic of China. If there is any dispute, the party of the Consent and Penpower agree that the Taiwan Hsinchu District Court is the governing court for the first trial.

Penpower Technology Ltd. Information Security Policy

1. The information security target of the Company is to ensure the confidentiality, integrity, and availability of the important and core systems. The quantitative indicators for information security performance are defined and measured based on different levels and functions to ensure whether the implementation status of the information security management system achieves the information security targets.
2. To achieve the mission target of the Company and the expectations and requirements of the senior management for information security and ensure the security of the Company's information assets, the information security policy is established as follows:
   2.1 Ensure the confidentiality of relevant business information of the Company and prevent the leakage and loss of the Company's confidential information and personal data.
   2.2 Ensure the integrity and availability of relevant business information of the Company to accurately implement the Company's operations and various businesses.
3. To ensure the effective operation of the information security management system, the Company has established its Information Security Committee to coordinate the planning and promotion of the information security management system. Its organizational structure is recorded in the Company's "Information Security Policy" and "Procedures for Information Security Organization and Management Review."
4. Human resources security control: To reduce human factors to affect the information security of the Company, the Company implements appropriate information security education, training, and promotion to improve the awareness of personnel to information security.
5. Asset management: To protect the security of the Company's information assets, the Company established its information asset list according to specifications and established the principles for asset classification, grading, and control measures.
6. Access control:
   6.1 To ensure the authorized access of information processing equipment, user passwords, registration, alteration, deletion, and regular systems are established, and office table and computer screen clearance measures are formulated.
   6.2 To protect network security, a network service system is formulated to segregate the intranet and methods to contact external networks and control remote work and the use of mobile devices.
7. Password control: Establish and effectively use the password policy to protect the confidentiality, authenticity, and integrity of information.
8. Physical and environment security control: To ensure the security of the server room, offices, and relevant equipment, the Company established its principles for server room access and equipment inspection and management for computers and formulated the principles for the general information equipment use, management, and abolishment for offices.
9. Operation and communication security:
   9.1 To ensure the accurate and secure operation of information equipment, specifications for the

accurate use of information are established to prevent the leakage of confidential information, and the system to prevent malicious code and portable code is built.

9.2 To ensure the integrity and availability of information assets, backup operations are established for information processing facilities, and external information processing facility service control principles are adopted.

9.3 To protect network security, the network security control system is established, the use status of the system is monitored, and the track protection principle is adopted.

10. System access, development, and maintenance: To ensure the security of the development management, testing, acceptance, launching, maintenance, and outsourced management of application systems, the Company has established its standard control procedures.
11. Supplier relationship: Supplier relationship and management are formulated to ensure the security of suppliers in accessing, processing, and managing the Company's information and information processing facilities.
12. Information security event management: To reduce damages caused by information security events, the Company has established its information security reporting and processing procedures, which are further recorded.
13. Business continuity management: To ensure the continuous operation of the Company's businesses, the Company has established the information security control principles for business continuity management, built the business continuity management procedures and structure, and prepared and implemented the business continuity operation plan.
14. Compliance: To ensure that the implementation of the information security management system complies with relevant laws and regulations, security policies, and the latest technological trends, the Company has established the compliance confirmation principle.
15. When an employee violates the requirements related to information security, the information security responsibilities he/she shall assume are subject to disciplinary procedures.
16. This policy shall be reviewed by the highest supervisor of the information security organization of the Company at least once a year to comply with relevant laws and regulations, technologies, businesses, and other latest development status to ensure the effectiveness of information security practices.
17. Unaddressed matters in this policy shall be subject to relevant laws and regulations and relevant requirements of the Company.
18. This policy is implemented after being approved by the chief information officer of the Company, and the same shall apply for any amendment.