Tongwei Co., Ltd.

Information Security and Privacy Policy

1. Policy Statement

Tongwei Co., Ltd. (hereinafter referred to as "Tongwei" or " the Company") attaches great importance to information security and privacy protection, and strictly complies with relevant laws, regulations and requirements, including the Network Security Law of the People's Republic of China, the Data Security Law of the People's Republic of China, the Personal Information Protection Law of the People's Republic of China. The Company strictly complies with the requirements of the Network Security Law of the People's Republic of China, the Data Security Law of the People's Republic of China, the Personal Information Protection Law, and other relevant laws, regulations and other related provisions. The Company actively promotes the construction of the information security management system and strictly implements information and data security protection work in conjunction with ISO/IEC 27001 and ISO 37301, for which the Company has already completed implementation of ISO/IEC 27001 and ISO 37301, and with reference to the requirements of information security and compliance standards including GB/T 22239-2019. The Company has formulated this policy to regulate information processing behavior, safeguard information security, and maintain the legitimate rights and interests of relevant parties.

2. Scope of Application

This policy applies to the business and operational activities of Tongwei and its subsidiaries, covering the entire process of information collection, storage, processing, transmission, use, and destruction. At the same time, the Company requires suppliers, contractors, partners, and other relevant stakeholders involved in business dealings with Tongwei to actively comply with this guideline and jointly contribute to a secure and reliable information environment.

3. Responsible Department

The Company specifies that the Information Department is the main department responsible for information security and privacy protection, and is responsible for coordinating the work of information security and privacy protection, including policy formulation, revision, implementation supervision, training and publicity, as well as receiving, investigating and addressing privacy issues. The head of each department is the primary person responsible for information security and privacy within their department and is responsible for ensuring that all departmental personnel strictly comply with the relevant regulations.

Information security and privacy protection are responsibilities that must be shared by all staff members. Based on the current status of the Company's information system, the Informationization and Network Security Leading Group and Working Group have been established to build an information security management organization that consists of both. Under the unified leadership of the Informationization and Network Security Leading Group, each department shall perform its own information security duties and work together to ensure the information security of the Company’s information system.

4. Information Security and Privacy Protection Policy

(1) Risk Management: The Company is committed to continuously improving and upgrading its information security management system. It integrates information security management policies and their implementation into the company-wide risk and compliance management processes. The Company will regularly identify, assess, and analyze information security and privacy protection risks, and formulate corresponding preventive measures, control actions, and contingency plans for potential risk points. In addition, the Information Department of the Company monitors and collects various types of information security threat intelligence through a variety of channels (including but not limited to security vulnerability release platforms, information security professional websites, industry internal information, security company subscription intelligence, etc.), and evaluates and analyzes the collected threat intelligence. For threats assessed and judged to be high-risk and potentially having a tangible impact on the company's information security, the Information Department shall promptly develop and implement internal countermeasures in a timely manner and issue early-warning notifications to relevant internal parties via email and other appropriate means.

(2) Information Security Management System: Under the leadership of the Information Technology and Network Security Leading Group, the Information Department establishes and manages the information security management system in accordance with the Plan-Do-Check-Act (PDCA) cycle. The Company conducts annual information security management system audits, which are designed to determine whether the system's control objectives, control measures, processes and procedures comply with the requirements of relevant standards, laws and regulations, meet the identified information security requirements, are effectively implemented

and maintained, and are carried out in accordance with management expectations. The Company analyzes the results of various monitoring activities and collects internal and external information related to information security management to provide support for the continuous improvement of the system; the Company also identifies the needs for improvement of the management system, the reasons for deviation from the information security objectives or the gaps of the current system in adapting to the environment through the management review, formulates specific measures for improvement and specifies the specific improvement plan; in addition, the Company implements the improvement measures and verifies the results, and retains the implementation process. Verify the results and keep relevant records of the implementation process and results.

(3) Information and Data Security: In order to ensure the confidentiality, integrity and availability of information and data, the Company strengthens the security control of the whole process of information transmission. By deploying encryption technologies, access control mechanisms, and other measures, it prevents information and data from being illegally tampered with, leaked, or destroyed.

(4) Zero Tolerance Policy: The Company has zero tolerance for violations of information security and privacy protection regulations. Upon discovery, the relevant responsible person will be dealt with according to the seriousness of the situation, including but not limited to warning, demotion, dismissal, termination of labor contract, etc.; if the behavior violates laws and regulations, it will be transferred to the judicial organs according to the law to deal with it and pursue its legal responsibility.

(5) Internal and External Audits: In order to ensure the effective implementation of the information security and privacy protection policy, the Company will conduct an internal information security audit once a year to comprehensively check and evaluate the implementation of information security and privacy protection work of each department. Additionally, the Company will regularly invite qualified third-party organizations to carry out external audits, and make timely rectification of problems found in the audits, so as to continuously improve the level of information security and privacy protection.

(6) Partner Management: The Company requires its partners (including suppliers, etc) to actively cooperate with the systems and requirements related to information security and privacy protection. Before establishing cooperation with key suppliers, the Company actively conducts information security-related due diligence to ensure that no significant risks exist. At the same time, partners are required to sign confidentiality agreements to clarify the confidentiality responsibilities and obligations of both parties. In addition, the effectiveness of partners' information security measures is regularly evaluated and monitored to minimize information security risks in the course of cooperation.

(7) Privacy Information Collection and Use Management: The Company respects the customer's right to know and fully informs them of the following privacy protection-related issues.

- Nature of the Information Obtained: including but not limited to the customer's name, attributes, contact details, basic profile, special precautions and other relevant details.

- Purpose of Information Collection: including but not limited to establishing customer profiles, maintaining daily communication, providing personalized products and services, and improving the quality of products and services.
- Information Retention Period: The company undertakes to always store customers' personal information for a reasonably necessary period in accordance with the law. Upon expiration of the retention period, the Company will delete or anonymize the customer's personal information. In the event that the Company ceases operations, the Company will promptly cease all collection of personal information, notify customers individually or by public announcement, and delete or anonymize all retained personal information.
- Right to Information Processing: Customers have the right to access, review, copy, correct, and cancel their user information, except in cases specified by laws and regulations.
- Information Protection Measures: The Company will endeavor to protect customers' personal information by adopting various security measures in line with industry standards to minimize the risk of personal information being destroyed, stolen, leaked, accessed, used, disclosed, or altered without authorization. The Company will actively establish a data classification and grading system, data security management standards, and data security development standards to manage and regulate the storage and use of personal information to ensure that no personal information unrelated to the services provided by is collected.

(8) Supplier Information Security Management: The Company implements full-process information security management for suppliers, and clarifies the security responsibilities and operational specifications of suppliers in the access of information assets. For information assets accessible to suppliers, the Company shall strictly protect them by signing security agreements,

delineating the scope of access rights and establishing an access log auditing mechanism, so as to prevent suppliers from obtaining organizational assets in an unauthorized manner; Additionally, the Company has standardized and controlled the authorization process of suppliers, and avoids leakage of sensitive information due to inappropriate authorization by periodically reviewing the reasonableness of authorization and dynamically adjusting the scope of authorization, and ensures the security and confidentiality of organizational information assets.

(9) Third-Party Disclosure Policy: The Company undertakes to strictly comply with relevant laws and regulations and privacy protection guidelines when sharing, transferring, or providing relevant data to third parties to ensure that data transfer activities comply with the law and respect the rights of the data subjects. The purpose and scope of data transfer cannot exceed the purpose and scope stated at the time of collection. Transfers of high-impact data must be transmitted using a secure transmission channel or encrypted. The data exporter must obtain an explicit commitment from the recipient. If cross-border transfer of data is involved, the requirements of local laws and regulations must be complied with.

(10) Business Continuity Management: The Company focuses on the demand for information security protection, identifies key systems supporting information security based on various factors in business impact analysis and risk analysis, and conducts information system-oriented security risk assessment at least once a year to actually analyze the impacts and possibilities related to security risks; According to the management objectives and strategies for safeguarding information security, the Company formulates emergency drill plans and outputs information security continuity drill plans covering all aspects of information security inspection.

It conducts business continuity information security training on a regular basis to familiarize the relevant personnel with the objectives of information security safeguarding. In addition, the Company carries out an annual comprehensive assessment and audit of its information security risk prevention measures and emergency response procedures for unexpected events. It integrates information security assurance into the overall risk management system and establishes a long-term mechanism to ensure the continuity and effectiveness of information security management.

Tongwei Co.,Ltd.

Date：July 2025

Remarks:

1. The Company encourages and supports suppliers and partners to adopt and implement additional principles and policies under the premise of following this policy, but these additional principles and policies shall not conflict with this policy.

2. The company's business is conducted in strict compliance with the requirements of local laws and regulations. If there are no clear local laws and regulations, this guideline will be implemented.

3. This document is interpreted and revised by Tongwei Company Limited, and the company will update the document in accordance with domestic and international policies, regulatory requirements and industry development in due course. When there is a conflict between the English and Chinese versions of the document, please refer to the Chinese version.