Article 1 Purpose

In order to establish a personal data protection environment, to implement the legality and reasonableness of the personal data collected, processed and utilized by the Company for various businesses, and to properly manage all personal data, we hereby establish this policy in accordance with the Personal Data Protection Act (hereinafter referred to as the "Personal Data Act") and related regulations.

Article 2 The terms used in this policy are defined as follows.

1. Personal Data: The name, date of birth, citizen identity card number, passport number, characteristics, fingerprints, marital status, family members, education, occupation, medical history, medical treatment, genetics, sex life, health examination, criminal history, contact information, financial situation, social activities, and other information that can directly or indirectly identify the individual.
2. Personal Data File: A collection of personal data that can be retrieved and organized by automated machines or other non-automated means in accordance with the system.
3. Collecting: The acquisition of personal data by any means.
4. Processing: The means of recording, inputting, storing, editing, correcting, copying, retrieving, deleting, exporting, linking or internal transmission of data for the purpose of creating or using personal data files.
5. Utilizing: The use of personal data collected for purposes other than processing.
6. Transmitting Internationally: The processing or use of personal data in a foreign country.
7. Governmental organization: This refers to the central or local authorities or administrative legal entities that exercise public power in accordance with the law.
8. Client: The person to whom the personal data is provided.

Article 3 Applicable Target and Scope of Protection

1. This policy applies to all employees of the Company, including directors, consultants, and customers or outsourced companies with whom the Company has business dealings.
2. The scope of protection of this policy is the personal data protected by the Personal Data Protection Act, and the relevant regulations are set for the personal data collected, processed, utilized and transmitted internationally by the Company for various businesses to ensure the security of personal data.

Article 4 Rights and Responsibilities

1. All employees of the Company shall understand and comply with this policy and shall fully participate in the implementation of this policy.
2. Each unit shall assume the responsibility of managing personal data to ensure compliance with the Personal Data Protection Act and this policy, and the rights and responsibilities for its maintenance are as follows:
   - （a） Personal data of all employees and job seekers: Human Resources Department
   - （b） Personal data of shareholders, directors, independent directors and functional committees: Finance Department
   - （c） Internal personnel information and related party information: Finance

Department

（d） Personal data of vendors or suppliers: Administration Department General Affairs Unit, Procurement Unit

（e） Personal data of business clients: Sales Department, Operation Support Department

（f） Personal data of whistleblowers or complainants: Human Resources Department, Legal Affairs Office

（g） Auditing the personal data of the company's internal control operators, suppliers and customers: Auditing Office

3. The Information Department is responsible for the information security network of personal data to prevent the risk of personal data being stolen, tampered, damaged, destroyed or leaked by hackers and to strengthen the control of security measures.。

Article 5 Principles and Procedures of Personal Data Collection, Processing and Use

1. The collection, processing, or use of personal data shall respect the rights and interests of the parties involved, be done in an honest and trustworthy manner, shall not exceed the scope necessary for the specific purpose, and shall be properly and reasonably related to the purpose of collection. The purpose may be exceeded only when there are legal exceptions; the implementation requirements are as follows:

   （a） To confirm that the specific purpose of the collection, processing or use of personal data is in accordance with the regulations, and to keep an appropriate audit trail.

   （b） Personal data shall be handled in accordance with the Company's information security regulations.

   （c） Fulfillment of the obligation to inform: Except for those who are exempt from informing according to the law, appropriate methods of informing shall be adopted according to the situation of collection, and the content of informing shall include:

      1. the name of the company/unit;
      2. the purpose of collecting;
      3. the type of personal data;
      4. the period, place, subject and manner of use of the personal data;
      5. the subject may request access to, make copies of, supplement or correct, stop collecting, process, use or delete his or her personal data;
      6. The parties may freely choose to provide their personal data and the impact of not providing it on their rights and interests.

   （d） To confirm that the use of personal data is in accordance with the specific purpose and whether the use of personal data for purposes other than the specific purpose is allowed, and to keep an audit trail as appropriate.

   （e） To comply with the restrictions on the collection, processing, or use of personal data in accordance with Article 6 of the Personal Data Protection Act.。

2. The specific purposes include: contractual or similar contractual or other legal relationship matters, personnel management, customer management and services, procurement and supply management, investment management, commercial marketing, internal management of shareholders, directors and supervisors, or other members of the register, website maintenance and communication, necessary to assist public authorities in carrying out their legal duties, protection or exercise of the Company's

legal rights, and other measures necessary to carry out the Company's operations.

Article 6 Rights and Interests of Parties

1. Based on their personal data autonomy, the parties may exercise the following rights to the Company in accordance with the law:
   （a） To make inquiries or requests for access
   （b） To request for a copy
   （c） Request for supplement or correction
   （d） To stop collecting, processing or using the information
   （e） Request for deletion
2. When exercising the rights of the parties, they should fill out the "Personal Data Application Form". If the application is submitted by a non-employee, the application will be filled out by the application processing unit of the Company.

Article 7 Personal Data Security Management and Maintenance

1. The Company adopts appropriate security maintenance measures for personal data to ensure complete control over access, processing, transmission, retention, reading privileges, and information security of related transmission and storage devices to prevent damage, loss, theft, leakage, or unauthorized reading, copying, use, and alteration of personal data. The relevant appropriate security maintenance measures are as follows:
   （a） Use appropriate secure data transmission and storage devices to protect personal data, such as secure encryption (SSL, HTTPS, etc.) for personal data transmission.
   （b） Establishing firewalls to protect personal data from unauthorized access.
2. In the event that personal data is stolen, leaked, tampered with, destroyed, or otherwise illegally infringed upon by hacker attacks, each unit shall notify the subject of the data security incident and emergency response in an appropriate manner as soon as possible.

Article 8 Data Security Auditing Mechanism

1. At least once a year, the Company shall conduct a personal data security audit to check whether the Company has implemented the provisions of this policy, and shall plan improvement measures and ensure the implementation of relevant measures for non-compliance and potential non-compliance risks. When implementing improvement and preventive measures, the following items shall be followed:
   （a） Confirm the content of the nonconformity and the reasons for its occurrence.
   （b） Propose improvement and preventive measures.
   （c） Record the inspection situation and results.
2. The previous audit situation and results shall be included in the audit report and signed by the responsible person of the Company.

Article 9 Awareness Promotion and Education Training

The Company shall regularly or irregularly conduct awareness and education training on the Personal Data Protection Act to enhance employees' understanding of the importance of personal data protection.

Article 10 Continuous Improvement of Personal Data Security Maintenance

1. The Company will review the appropriateness of this policy and make necessary amendments at any time based on the implementation status and pay attention to relevant technological development and legal amendments.
2. To plan improvement and preventive measures for those personal data security audit results that do not comply with the law.

Article 11 Retention and Destruction of Personal Data

1. Personal data shall be deleted, cease to be collected, and cease to be processed or used when the specific purpose for which the personal data was collected disappears or the time limit expires. Personal data may be retained unless expressly provided for in applicable laws and regulations, necessary for the performance of duties or business, or with the consent of the individual concerned.
2. When personal data is destroyed in writing, the destruction record shall be kept by filling out the [Personal Data Disposal Form], which shall include: the content and scope of destruction, the date of destruction, the method of destruction, the unit of destruction, the person who destroyed it, and the review by the supervisor of the unit of destruction. ◦

Article 12 Other Matters

1. All employees of the Company shall follow this policy. If there is any violation of this policy or the relevant provisions of the Personal Data Protection Act, the Company shall be punished in accordance with the relevant regulations.
2. In case of civil compensation, criminal liability, or administrative penalty, the Company may terminate the employment relationship and pursue the legal responsibility as appropriate.
3. The personal data protection obligation of the employee to the Company shall continue to be effective after the termination of the employment relationship between the two parties.

Article 13 Related Forms

1. Form – Personal Data Application
2. Form - Personal Data Disposal

Article 14 Implementation and Amendment

Any matters not covered by these Regulations shall be handled in accordance with the relevant management regulations of the Company and the laws and regulations of the relevant competent authorities.

This policy shall be implemented after approved by the Board of Directors, and vice-versa for amendments.