

Personal Data Protection Policy and Implementation Status

The Company places great importance on the protection of personal data and has established the Personal Data Protection Act as the basis and standard operating procedures for the collection, processing, and use of personal data.

I. Policies and Management Mechanisms

The Company's Personal Data Protection Management Regulations cover the collection, processing, and use of personal data; handling of data subjects' rights; security maintenance of personal data files; emergency response measures and procedures for abnormal incidents. All relevant regulations have been submitted to and approved by the Board of Directors.

II. Protection of Employee Privacy

The Company enters into a "Notice on the Collection of Personal Data and Consent to the Provision of Personal Data" with employees, clearly specifying the purpose, scope, methods of use, and the rights of data subjects, and obtains written consent in accordance with applicable laws.

III. Protection of Customer Privacy

During the reporting period, the Company experienced no major violations involving customer personal data. To safeguard customer privacy, the Company has implemented a series of security measures, including document encryption technologies, multi-layer firewall systems, and regular system data backup and redundancy mechanisms to ensure data security. In addition, the Company has established internal system access authorization procedures and external document circulation review mechanisms.

IV. Personal Data Management Responsibilities

Personal data protection measures are implemented by the Human Resources Department and the Information Technology Department in accordance with their respective responsibilities, as outlined below:

- Human Resources Department: Responsible for the storage and confidentiality of personal data of employees and job applicants.
- Information Technology Department: Responsible for access control of files

(including document encryption technologies and multi-layer firewall systems), system risk assessments, and information security settings.

•

V. Implementation Results in 2025

1. Education and Training

1.1 Information security officers and personnel completed at least six hours of information security training.

1.2 Through annual training programs, the Company continuously enhances employees' awareness and professional capabilities in personal data protection. In 2025, personal data protection-related training totaled 246.5 hours, with 331 participants completing the training.

2. Number of personal data-related complaints in 2025: 0 cases.

3. Administrative penalties and litigation compensation arising from violations of personal data protection laws in 2025: 0.

4. All data processing activities and access to or use of files require approval from the responsible supervisor. Access permissions are granted by IT personnel based on approved application forms to prevent data damage or theft. In 2025, internal auditors conducted effectiveness testing of data access using individual employee access rights, and no non-compliance issues were identified.