RiSiN LLC (hereinafter referred to as "the Company") is committed to the proper protection and use of customers' important personal information, individual numbers, and specific personal information (hereinafter referred to collectively as "Specific Personal Information, etc.").

1. Compliance with Laws and Regulations Related to Personal Information

The Company complies with the Act on the Protection of Personal Information, the Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures, relevant guidelines issued by authorities, and other norms to ensure the proper protection and use of personal and specific personal information.

2. Proper Acquisition and Use

The Company will acquire and use customers' personal and specific personal information in a lawful and appropriate manner within the scope necessary for business operations.

3. Restrictions on Use Purpose

Unless otherwise agreed upon by the customer or permitted by law, the Company will use personal information only within the scope necessary to achieve the purposes explicitly stated or disclosed. Specific personal information is used only within the scope prescribed by law.

4. Management of Personal Information

The Company strives to keep the personal information it holds accurate and up to date. Measures are taken to prevent unauthorized access, destruction, falsification, or leakage, and necessary supervision of employees is conducted to ensure a secure management system.

(1) Formulation of Basic Policy

In order to ensure the proper handling of personal data, we have established this Privacy Policy as our basic policy. It covers the name of the business operator, compliance with relevant laws and guidelines, matters related to security control measures, and contact information for inquiries and complaints.

(2) Establishment of Rules for the Handling of Personal Data

To appropriately manage and record the acquisition, use, storage, provision, deletion, and disposal of personal data, we maintain a “Personal Data Ledger.” We also define roles and responsibilities of managers and personnel, and have established internal regulations on information management, including handling personal data, and appropriate procedures for each stage.

(3) Organizational Security Control Measures

We appoint a person responsible for handling personal data, clearly define the personnel who handle personal data and the scope of data they are responsible for, and establish a reporting system to the relevant management department in the event of a data breach, legal violation, or signs thereof.

We conduct regular self-inspections to ensure the proper handling of personal data, as well as audits by other departments.

(4) Human Security Control Measures

We provide regular training to all personnel on compliance with laws and internal regulations related to the proper handling of personal data.

Confidentiality obligations and disciplinary actions in case of violation are stipulated in the employment rules, and we periodically obtain written pledges from all employees to ensure strict handling of personal data.

(5) Physical Security Control Measures

In areas where personal data is handled, we manage access by employees and restrict devices that can be brought in, while also implementing measures to prevent unauthorized access to personal data.

We also implement measures to prevent theft or loss of devices, electronic media, or documents containing personal data. When carrying such items, including moving them within the office, we ensure that personal data cannot be easily identified.

(6) Technical Security Control Measures

We implement appropriate access control by limiting the scope of personnel and databases that handle personal data.

We have also introduced systems to protect information systems handling personal data from unauthorized access or malware and ensure their proper operation.

(7) Understanding of External Environments

When handling personal data overseas, we assess the legal systems in the relevant foreign country regarding personal information protection and implement necessary and appropriate measures to ensure the security of the data before proceeding.

5. Management of Subcontractors

If the Company outsources processing of personal or specific personal information to a third party within the scope of its intended use, it will ensure the subcontractor meets adequate security standards and exercise necessary and appropriate supervision through contracts and other means.

6. Response to Customer Requests for Disclosure

When customers request disclosure, correction, suspension of use, or records of third-party provision regarding their retained personal data, the Company will confirm the identity of the requester and respond appropriately and promptly in accordance with laws and regulations.

7. Handling of Inquiries

The Company will respond promptly and accurately to inquiries regarding the handling of personal and specific personal information.

8. Provision to Third Parties

The Company does not provide personal information to third parties without the customer's consent, except in cases permitted by law, such as when outsourcing operations, business succession, or joint use with specified parties. Specific personal information will not be provided to third parties unless permitted under relevant laws.

9. Continuous Review of Privacy Measures

The Company will continuously review and improve its efforts to protect personal information and this policy.