Information Security Basic Policy

1. Basic policy

Alps Alpine Co., Ltd. and its subsidiaries in electronic components segment and automotive infotainment segment (hereinafter referred to as "the Company") develop, manufacture, and sell electrical and precision equipment such as electronic components and automotive infotainment systems, and build software and provide services that accompany these products. We consider it our duty to protect our information assets and the information assets entrusted to us by our customers and business partners. We will manage information security in accordance with this basic policy.

2. Active organization

The Company has established an information management structure headed by an information management supervisor and will establish an information management committee to promote and operate our information management activities. Through risk assessment, the information management committee understands information security risks at the company, implements countermeasures, and promotes dissemination and continuous improvement to the organization.

3. Attendance in security education

To bring awareness to appropriate information management, we will provide education and training on information security to all (executives, employees, contract employees, partner company employees, etc.) who can access our information assets.

4. Protection of information assets

Based on the international standard ISO 27001/2 and industry management standards such as VDA-ISA, the Company has established the following standards and regulations regarding ISMS (Information Security Management System). By requiring all parties involved in our business to comply, we will endeavor to handle information assets appropriately. In addition, when sharing information assets with a third party, we will thoroughly examine and judge on whether sharing information is necessary, and will appropriately manage and supervise the assets when shared.

-Management and organization of Information Security – Governance of Information Security

-Asset management – What needs to be protected

-Human resources – Who will be using the assets

-Physical and environment – How assets will be physically protected
-Communications and operations management – How information systems will be managed securely
-Access control – How access to information will be managed effectively
-System acquisition, development and maintenance – How new and existing information processing systems will be managed in a secure fashion
-Information security incident management – How information security breaches are to be communicated, managed and resolved
-Business continuity management – How the continuity of critical business processes are to be maintained
-Compliance – How the implementation of the policy requirements and effectiveness of the information security system are validated

5. Security monitoring and audit

In order to continuously maintain and better the information security, we will appropriately carry out second- and third-party evaluations and commit to rapidly improving the identified issues.

6. Compliance with laws, regulations, contracts, etc.

When formulating information management standards and regulations and using information assets, we will understand and comply with various laws, rules and contracts applicable to our business activities.

Alps Alpine Co., Ltd.
March 26, 2024

Vice President / CXO

Junji KOBAYASHI