Information Security Basic Policy

Purpose and Basic Approach

PRESS KOGYO CO., LTD. (hereinafter referred to as "the Company") *upholds the principle that* "With pride and self-belief, we will continue to grow together with our stakeholders as a positive presence in our society"

To this end, we recognize that the protection of information assets is the foundation of our business activities, and under the leadership of top management, we position information security as a critical management issue, and hereby declare that we will secure the necessary management resources (human resources, budgets, technology, etc.) and make company-wide efforts.

1. Protection of Information Assets

・The Company will protect information assets from unauthorized access, leaks, damage, loss, and tampering through the establishment of appropriate safety management measures.

2. Scope of Application

・This policy shall apply to all officers and employees, dispatched employees, and outsourcing partners at all business sites of the Company, and be disseminated as a standard to be observed by all relevant parties.

・This policy applies to all information assets handled in the Company's business activities and all information systems that process, store, and transmit them.

3. Promotion Organization and System

・The Company shall clarify the responsibility structure for information security, establish a promotion system centered on the Chief Information Security Officer (CISO), and realize effective operations throughout the entire organization.

4. Legal and Regulatory Compliance

・The Company shall comply with relevant laws and regulations, and contractual obligations concerning information security, and shall respond to information security requirements in the automobile industry in particular, in compliance with industry standards, regulatory requirements, industry conventions, and agreements of contracting parties.

5. Education and Training

・The Company shall provide continuous education and awareness activities to all employees and dispatched employees, and promote a heightened awareness of information security.

6. Risk Management

・The Company shall continually evaluate risks to information assets, implement appropriate countermeasures, and seek to reduce risks.

7. Supplier Chain Management

・The Company shall manage suppliers appropriately and seek the maintenance and improvement of information security throughout the supply chain.

8. Continuous Improvement

・The Company shall engage in regular monitoring and reviews, implementation of improvements, and continuous improvement of this policy and related regulations.

May 1, 2026

Representative Director and Senior Managing Director, Chief Information Security Officer

Masahiko Sato