

Information Security

KOITO has identified “information security” as one of our materiality, and ensuring the protection of personal information and confidential information based on the Information Security Policy while implementing proper information security measures to materialize safe and thorough management.

We have established a cyber security system that can detect the latest viruses and abnormal conditions at all sites, including domestic and overseas affiliates. At the same time, we have established CSIRT (specialized team that deals with information security issues) at each site to ensure an immediate response in the event of an emergency.

Information Security Policy

KOITO MANUFACTURING CO., LTD. (“KOITO”) recognizes that the appropriate management of information is a critical management issue, and has formulated an “Information Security Policy” to gain the trust of customers and society at all times.

KOITO intends, from now on, to comply with this Information Security Policy, maintaining and improving information security by protecting information assets from various threats and handling information appropriately.

1. Establishment of information security management system

KOITO has appointed a Chief Information Security Officer (CISO) and established an information security management system that enables prompt implementation of security information measures, to gain the trust from the society at all times. This management system shall be reviewed and improved regularly. With this CISO and management system, KOITO makes every possible effort to protect all information assets held by us and comply with laws, regulations, and other rules related to information security.

2. Development of internal information security-related rules

KOITO develops internal rules based on our Information Security Policy to have a clear policy for the handling of not only personal information but also all other information assets, and makes all employees and business partners fully aware of KOITO’s strict measures against information leaks etc.

3. Implementation of appropriate information security measures

KOITO implements organizational, physical, technological, and personal security management measures so that information assets of KOITO are not subjected to unauthorized access, destruction, leakage, or alteration. These measures shall be adjusted and adapted to changes when technological and social needs arise.

4. Implementation of internal information security audits

KOITO regularly conducts internal information security audits to verify that security measures are functioning effectively in the course of business operations, in accordance with relevant laws and internal regulations and rules.

5. Enhancement of information security literacy

KOITO provides thorough security education/training to employees etc. so that all people dealing with our information assets perform their duties with information security literacy. KOITO also continues to provide its employees with education/training to respond to ever-changing circumstances.

Organization for Information Security Activities

The KOITO Group monitors computers and networks of the Group as a whole, including its domestic and overseas affiliates, and is building CSIRT (Computer Security Incident Response Team), capable of responding immediately to any cyber-attacks or abnormal conditions on a global basis.

KOITO’s information security is managed by the Information System Department, along with General Affairs Department and Compliance Promotion Office. Furthermore, each department periodically checks for information security risks and implements a PDCA cycle to continuously improve security.

Information Security Management System

In order to protect information assets from the risk of leaks, theft, alternation, etc., the KOITO Group operates information security management based on management standards for the confidentiality, integrity, and availability of information. In particular, major functional divisions are assuring information security and promoting the improvement of security reliability. Divisions for design, development, sales, purchasing and quality management of automotive lighting equipment and others have acquired ISO 27001, an international standard for information security.

The KOITO Group will continue to strive to further maintain and improve information security by improving our information security management system through continuous PDCA cycle and by expanding the scope of certification within the Group.

Information Security Measures

To strengthen information security measures against cyberattacks, KOITO has established internal regulations based on its Information Security Policy and is implementing various cyber security measures, including the establishment of a Group-wide monitoring system and an incident response system. We are seeking to build a strategic information management system that not only appropriately manages confidential and personal information, but also manages and utilizes intellectual property and other intangible assets.

In addition, KOITO periodically conducts internal and external intrusion tests by external specialist agencies to thoroughly inspect and confirm security vulnerabilities and strive to improve information security.

Fostering Awareness of Information Security

To prevent information security incidents, KOITO strives to foster awareness within the company by holding annual information security training sessions for all employees.

In addition, targeted email drills are conducted once a year for all employees. The results are reported to Managing Committee and IT Meetings, and necessary measures are taken.

Moreover, KOITO periodically provides information on information security to all employees via email, introducing examples of information security, precautions for teleworkers and alert anticipated targeted email attacks.

To our suppliers, we are asking them to implement information security-related measures, and conducting necessary assessments and improvements using checklists and other means.

Intellectual Property Management

The KOITO Group places intellectual properties as the source of international competitiveness and develops business strategies by integrating R&D and intellectual property strategies. KOITO will continue to encourage activities to create intellectual properties and work to protect and utilize the intellectual property rights appropriately. At the same time, we will respect the intellectual property rights of others and strive to prevent infringements.

■ R&D expenditures and number of patents

	FY 2018	FY 2019	FY 2020	FY 2021	FY 2022
R&D expenditures (billion yen)	36.1	34.0	36.1	32.6	34.0
Number of patents applied	800	1,230	1,130	938	867
Number of patents held	2,630	2,890	2,830	2,813	2,900

Organization for Intellectual Property Management

The KOITO Group makes effort to reinforce the intellectual property management system of the entire Group to acquire intellectual property rights, conclude licensing contracts, and respond to the violation of rights globally by developing a management system with KOITO MANUFACTURING at the center to establish and execute intellectual property strategy integrated with business strategies.

Measures to Prevent Violation of Intellectual Property

Given the importance of intellectual properties, the KOITO Group provides training on intellectual property rights through the job-rank based education to increase the awareness of every employee.

In addition, KOITO has introduced a patent research system available to all researchers and designers to avoid violating intellectual property rights of others and preventing future conflicts.