04 Sustainability
Information Security

The use of digital technology is expanding across an increasingly wide range of fields. At the same time, the volume of information and data is also increasing dramatically with the forms in which it is held and used continuing to diversify. Against the backdrop of this business environment, in addition to the risks associated with the improper handling of information, there are growing concerns surrounding information leaks and the adverse effects on the supply chain due to increasingly sophisticated cyberattacks. Positioning information security management as one of its important management tasks, NSK is working to reduce a variety of risks while strengthening its response to relevant laws and regulations. Moreover, we are promoting initiatives for more robust mechanisms and organizational structures, such as network countermeasures, against increasingly sophisticated cyberattacks.

Information Security System

The NSK Group is enhancing its managerial resources and transforming its business through the power of digital technology. We established the Information Security Enhancement Office under the Digital Transformation Division HQ to enable the safe use of digital technology and to globally deploy information security enhancement measures that take into account the relationship between digital technology and cybersecurity. Moreover, information security–related risks are supervised under the Corporate Risk Management System. Information security is also discussed by the Board of Directors as an issue that concerns the Group as a whole. The Information Security Enhancement Office regularly holds global meetings, working in cooperation with information security management committees in Japan, the Americas, Europe, China, ASEAN and Oceania, India, and South Korea. NSK is working to improve the information security management level of the entire NSK Group, and to plan and implement information security measures.

Management and Operation of Rules and Regulations

NSK has established a basic information security policy and put in place subordinate rules and regulations. We review and expand this policy, as well as rules and regulations, in line with the enforcement and revision of statutory and regulatory requirements and changes in our operating environment. Moreover, we are working to ensure that information security rules and risk countermeasures are implemented throughout the organization via increased awareness, development, and education, as well as periodic checks on the status of their penetration.

Major Information Security-Related Regulations

NSK Group Basic Policy on Information Security	This policy sets out the objectives for the NSK Group's information security (information security initiatives, handling of information assets, compliance with laws, regulations, and contracts, as well as education and continuous improvement).
NSK Group Information Security Management Standards	As the top information security directives in the NSK Group, these standards outline the principles for bringing the levels of information security management across the Group up to the same high standard.
NSK Group Information Security Procedural Standards	These rules stipulate measures to protect information assets, such as proper methods for handling information assets that need to be adopted across the NSK Group.

Information Security Initiatives

NSK has established a PDCA cycle for its information security management system, which includes periodic inventory and risk assessment of information assets and the formulation of plans for addressing and improving risk issues. As a result, we have acquired and maintain ISO/IEC 27001 certification, an international standard. In addition, based on demands from customers, we acquired TISAX certification, a security certification broadly adopted in Germany's automobile industry, at nine locations in Europe, China, and Japan.

As part of our efforts against cyberattacks, we have put in place a security incident response system to reduce risk and minimize the impact of damage through swift action based on preparatory steps and detection. In addition, we have defined incident levels and set out response procedures. We have also conducted drills on the assumption that an incident has occurred as well as targeted threat e-mail training to all NSK Group employees using PCs in cooperation with the Systems Management departments of each region. Furthermore, security assessments are conducted by an external expert contractor for Internet public systems and internal critical systems. Given the growing risk of attacks against the supply chain in recent years, we are enhancing security systems at our plants and conducting information security inspections at business partners.

As far as the Company's training and education endeavors are concerned, NSK is working to maintain and raise employee awareness toward information security through periodic e-Learning courses for employees in Japan and overseas. We are also conducting training by employee category, including officers and Systems Management Department members, as well as for employees entering the Company or personnel posted overseas.

Please see our website for more information. ▶