# Information Security Management

## NSK's Approach

Recent advances in information and communications technology (ICT) have dramatically enhanced the convenience of information handling. However, in addition to the risk of mishandling information, there is a greater risk of information being stolen or leaked through sophisticated cyberattacks or due to the growing number of people working from home. Positioning information security management as one of its important management tasks, NSK is working to reduce risk and strengthen its response to relevant laws and regulations. Having started efforts to acquire ISO 27001 certification in fiscal 2019, we succeeded in gaining certification in the Information System Department in fiscal 2020. To respond to customer requests, we are also working to revise and further strengthen our security regulations.

Moreover, we are promoting initiatives for more robust mechanisms and organizational structures, such as network countermeasures, against increasingly sophisticated cyberattacks.

■6th Mid-Term Management Plan Targets (FY2019–2021) and the FY2020 Targets and Performance

| 6th Mid-Term Management Plan Targets | FY2020 Targets | FY2020 Performance |
|---|---|---|
| Enhance information security infrastructure | Continue PDCA cycles for the Information Security Management System (ISMS) | Implemented ongoing ISMS activities |
| Obtain ISO 27001 certification | Obtain certification in the Information System Department | Obtained certification in November 2020 |
| Strengthen incident response capability (including the C-SIRT system) | Establish C-SIRT organization and commence activities | Appointed person to C-SIRT and conducted incident response training |
| Enhance ID and access management | Complete preparations for building an ID and access management system | Continued work to build the system and implemented preparations for switching production |

Note: SIRT is the abbreviation for Security Incident Response Team. For example, C-SIRT is an organization that responds when an event occurs that poses a security threat to computer systems.

## Examples of Fiscal 2020 Initiatives

In contrast to conventional information security management activities that focus on preventing information leaks, we are working to build and enhance a management system to respond to the sophistication of cyberattacks and the expansion of attack targets. Not only computer systems but also factory production equipment control devices and the controllers fitted to products are the targets of attacks, so management systems are required in each field. Specifically, we are putting in place an organizational structure as measures for computers (C-SIRT), factory production equipment control devices (F-SIRT), and product security (P-SIRT). In addition to preventing security incidents, these organizations are working on early detection and early recovery with the support of tools and external vendors.

The positioning of in-house training and the raising of awareness as important security activities have not changed, and we are continuing to carry out e-learning for employees and activities to raise awareness through our in-house intranet and digital signage. In fiscal 2020, e-learning was conducted by preparing training content geared toward directors and executive officers, security administrators, and employees. Including domestic Group companies, 96.7% of the target participants completed the course.

In our external certification acquisition activities, we acquired ISO 27001 in the Information System Department. In Europe, we gained registration in a security assessment mechanism called TISAX, which has been widely adopted in the German automobile industry, in our German subsidiary. We will continue our efforts to expand the number of departments that have acquired these official certifications.

### For diverse work styles

**Promotion of web-based remote work, meetings, training, etc.**

The COVID-19 pandemic has significantly changed employee work styles. Even before the COVID-19 outbreak, NSK had in place remote connections and a virtual PC usage system for remote work, and the rules and mechanisms had been established. Due to COVID-19, a much larger number of employees have moved to work from home, and we have, for example, expanded our network in response to the rapid increase in users and are now arranging for environments in which they can carry out their duties without any major difficulties.

As employee work styles continue to diversify, we are aiming to maximize the power of ICT to realize more efficient and convenient work styles. Therefore, we are organizing issues from the perspectives of urgency and impact, drawing up a response road map, and proceeding with initiatives. In addition, diverse work styles can be achieved not only by introducing new ICT technology but also by having that very technology mastered by employees. We will promote the necessary training and activities to raise awareness for employees and respond quickly to changes in the environment surrounding ICT.

▸ Please see our website for more information. https://www.nsk.com/sustainability/infoSecurity/index.html