Initiatives Related to Information Security

Information Security Policy

The spread of the Internet and the broad use of devices such as smartphones have ushered in a convenient era in which anyone can connect with the online community easily at all times. On the other hand, with cyberattacks, email spoofing, and other crimes against information security growing rampant and ever more advanced, the risks are increasing of everyone becoming either a victim or perpetrator of information leakage.

Information handled by the Nissha Group regarding our customers and suppliers, and our employees, is of vital importance. In particular, it is unforgivable to allow information on new products, state-of-the-art technologies, personal information and other highly confidential information assets to leak outside the company or beyond related parties. To ensure this does not happen, we aim to build a highly reliable and safe information security management system (ISMS). To that end, in 2005 we drew up our Information Security Policy, which all employees are required to be familiar with.

Information Security Policy

Nissha and its subsidiaries committed to establish, maintain, and improve highly reliable and secure an information security management system to protect our own business information and the information assets, which we acquire from customers, suppliers and employees, etc., through our business activities performed, from any kinds of threat. And we take internal and external information security requirements into consideration and reduce all risks below the acceptable levels.

1. We continually improve an Information security management system by establishing, implementing, and reviewing the information security objectives, so that the confidentiality, integrity, and availability of information can be maintained and improved.
2. We comply with legal and regulatory requirements for information security and with contractual security obligation.
3. We establish and improve the criteria for reasonably evaluating risks concerning information security as well as the risk assessment methods, to mitigate risks and to maintain the information security levels which contributes to the corporate developments.
4. We make Information Security Policy known to all employees working in the premises of Nissha Group and its subsidiaries to raise their awareness of the issues related to information security.

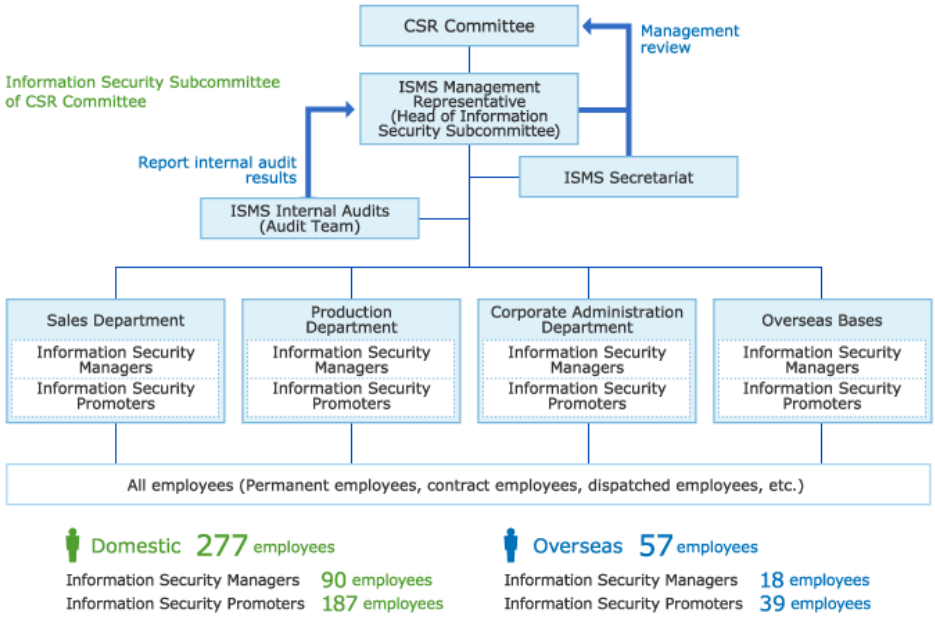
July 1, 2013

Junya Suzuki
President and CEO
Chairman of the Board
Nissha Co., Ltd.

Information Security Management Structure

We have in place an Information Security Subcommittee of the CSR Committee to serve as a center for the promotion of information security in Nissha Group. The subcommittee is run by an ISMS management representative (the Chief Information Officer, or CIO) and comprises information security managers and promoters selected from each department. An ISMS secretariat set up within the IT Department functions as the subcommittee secretariat.The subcommittee plays an important role in the promotion of our ISMS by addressing issues that have become evident as well as reporting and sharing the results and challenges of initiatives related to information security.

Management Structure



Initiatives in Information Security Management

Rapid advances in information technology and the diversification and spread of IT devices pose not only conventional security risks such as information leakage and tampering caused by virus infection and cyberattacks, but also the risks of casual posts, tweets, rumors, and reviews on social media harming a company's image and its brand value. Companies today are required to address such risks to their trust from society. Moreover, with the swift global popularization of bring-your-own-device (BYOD), companies are required to manage a broader range of information appliances, beyond company-issued computers to personally owned devices used at work. Dealing with these risks appropriately and promptly is considered a corporate social responsibility. (Nissha supports BYOD since December 16, 2013.) At the Nissha Group, we work to maintain and improve our ISMS by naming the Chief Information Officer (CIO) as ISMS management representative of an ISMS secretariat established within the IT Department.

We select information security managers and promoters from each department to promote thorough operation of our ISMS. And we organize regular reviews by top management, ISMS internal audits, and ISO 27001 screenings by an outside examination institute, recognizing these as good opportunities for improving our ISMS.

Information Security Education

Preventing the occurrence of information security incidents and accidents requires the formulation of policies and regulations, and more importantly, that all employees take disciplined action with sufficient awareness of information security.

We provide education to the Nissha Group based on the Information Security Compliance Manual, a teaching material that reflects the information security policies and other matters

established within Nissha, working to deepen the understanding of all Nissha People regarding information security. In the fiscal year ended December 2018, we used e-learning to ensure all employees follow our policies.

ISO27001 Certification

The Nissha Group has obtained ISO27001 certification, a global standard for ISMS, and is working to expand its scope of application to all bases and divisions. In the fiscal year ended December 2018, Nitec Precision and Technologies' (NPT) Tsu Factory obtained certification for the first time. In addition, our current focus is a global expansion of compliance with ISO27001 requirements.