Information security

Background of setting the issue of materiality

The risk of information leaks caused by internal fraud targeting information retained by companies and by disruptions to business activities caused by cyberattacks have been increasing in recent years.

In order to provide reassurance to all stakeholders, we believe that it is important to protect the various types of information we retain, including technical, management, and personal. This includes both information handled by the company and information provided by clients, customers, and partners. For this reason, Murata has set this key issue.

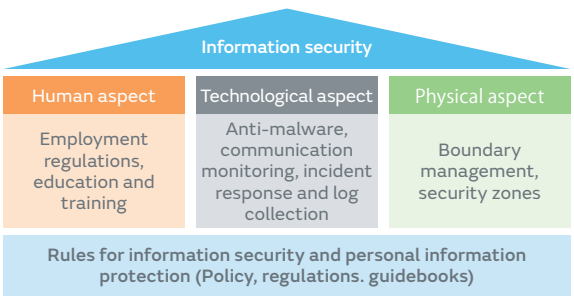
Our goal

We aim to minimize risk by running through the information security risk management PDCA cycle routinely in order to prevent potentially serious incidents from happening.

In FY 2007, Murata established an information security subcommittee as a lower branch of the Risk Management Committee, which incorporates recent risk trends and related guidelines from Japan and overseas based on international standards (ISO27001) to implement information security management. Specifically, Information security basic policy, Information security management regulations, Privacy policy and other rules are enacted to develop and operate information security measures in terms of human, technical, and physical aspects. The information security subcommittee periodically meets to examine new and persistent risks, and to propose and implement measures. The subcommittee also strives to increase the adoption and improvement of such measures through internal and external audits and diagnostics.

Due to an incident where an individual subcontracted to a Murata outsourcing partner had inappropriately handled personal information and other data*, we now confirm how data is being managed when we provide such data to any outsourcing partner in order to prevent a similar incident from occurring.

* News release: https://corporate.murata.com/en-global/newsroom/news/company/general/2021/0805



Human aspect

Information security-related rules are described in the employee handbook and the pledge with employees. In addition, the Information Security Guidebook, which explains the rules in an easy-to-understand manner, is written and distributed in Japanese, English, and Chinese so that all officers and employees in Japan and overseas can understand information security and handle information in the proper way.

The company also implements annual training, phishing e-mail exercises, new employee and in-house training by level, information security training for telecommuting employees, and other forms of education targeting all employees to increase their awareness on information security. (Global training ratio* = 96% [*Training ratio = (Number of sites that have conducted training) / (Total number of sites)])

Technological aspect

In order to deter leaks of Murata's company secrets and personal information as well as interruptions of business activities due to cyber attacks, we continue to strengthen anti-malware measures, hardware asset management, firewall construction, Internet communication checks, ID management, system access controls, and diagnosis and countermeasures for vulnerabilities in current information systems.

Moreover, we are globally collecting and monitoring various logs to construct a system for responding to incidents which may become a security accident. In particular, we continue to strengthen security at the plant sites that form the basis of our business activities and promote responses and countermeasures to constantly changing cyberattacks and risks in order to maintain a stable and safe production system.

Physical aspect

To prevent unauthorized intrusions into premises at offices, sites and affiliated companies in Japan and overseas, access control of people and vehicles is carried out at all times. Security zones are established within business sites according to the level of security control, and various measures including access controls using ID cards, etc. are implemented in highly secure zones to prevent unauthorized internal and external intrusions. Moreover, in order to continuously improve the physical security level, we periodically diagnose and audit the operating conditions from the perspectives of early detection and evidence accumulation measures in addition to restricting people's movements and preventive measures, and we are promoting the construction of a system to horizontally deploy responses to accidents and incidents which may become accidents with other offices, sites and affiliated companies.