Information Security

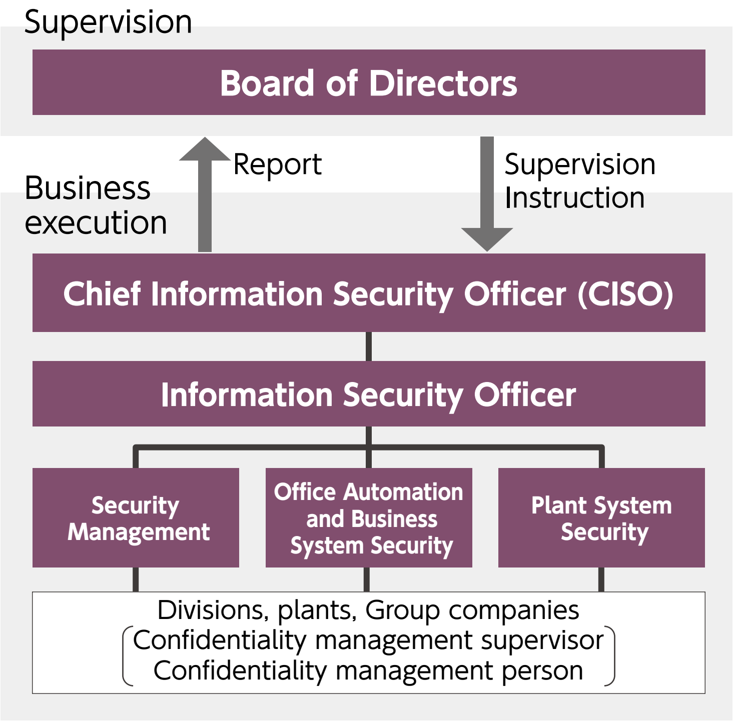
Basic approach

In addition to holding important information assets, including entrusted customer and supplier information and proprietary trade secrets, Aichi Steel has been adopting remote operations and networking plant equipment over recent years. We are implementing information security measures in recognition that stability of product supply is a company responsibility and an important management issue. We are doing this by protecting information assets from cyberattacks and other threats, data leaks, and other issues that have been increasing on a yearly basis, and by maintaining continuity of normal business activities.

Promotion structures

We have established Groupwide structures, based on the All Toyota Security Guidelines (ATSG) shared within the Toyota Group and led by the Chief Information Security Officer (CISO), for maintaining and improving information security on a systematic and ongoing basis. We are also working to ensure the same level of security can be maintained on a global level.

The CISO oversees all information security and information asset protection for the Group as a whole, while the Security Management, Office Automation and Business System Security, and Plant System Security organizations are in charge of planning, promotion, auditing, and support. Twice a year, the Board of Directors receives progress, issue, and other reports from the CISO as part of its supervisory function.


Supervision
Board of Directors
Report
Supervision
Instruction
Business execution
Chief Information Security Officer (CISO)
Information Security Officer
Security Management
Office Automation and Business System Security
Plant System Security
Divisions, plants, Group companies
(Confidentiality management supervisor
Confidentiality management person)

Examples of specific initiatives

Security inspections and audits based on the ATSG

We continually inspect the status of information security measures across the Group, and continually maintain and improve our information security.

This fiscal year, we are working with Group companies to strengthen measures to comply with version 8.1 of the ATSG.

Email-based cyberattacks

Cyberattacks are becoming increasingly complex and sophisticated these days, and with many of them coming via email viruses, there is an urgent need to strengthen countermeasures. We are also working to prevent such cyber incidents through technical measures, including adoption of defense systems against suspicious emails from outside, and through people-centered measures, including employee training and education on targeted email attacks.

Security incident training

We conduct security incident training to minimize damage and impacts on our operations in the event of a security incident occurring. We start by formulating specific risk scenarios so that participants can experience an actual incident in chronological order. We can then verify and improve the effectiveness of handling in the event of a cyberattack, procedures for early recovery of systems, and a division of roles that enables our operations to continue even without the usual systems. In this way, we are improving our systematic incident response capabilities and our ability to handle unexpected events.