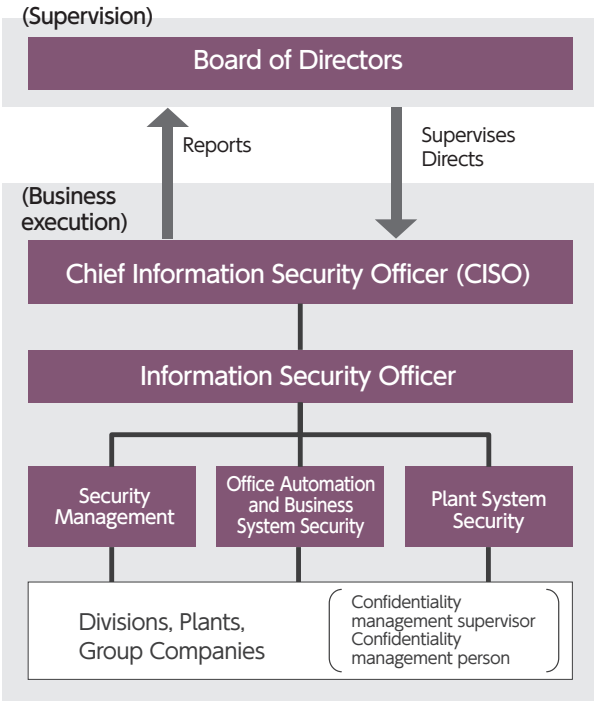
Corporate Governance

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 factory 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 framework

We have established a groupwide system, 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.

Security management

To prevent leakages of trade secrets and personal information, we have established rules regarding the procedures for handling documents and data, sending and receipt of email, and management standards and procedures for computers and peripheral devices.

Examples of rules:
- Document control rules
- Information security control rules
- Information disclosure rules
- Private information protection rules, etc.

Cybersecurity

We have adopted a range of security systems and use the monitoring services of specialized security organizations to enable detection, defense, rapid response to incidents and accidents, and other measures against cyberattacks on our networks, infection by computer viruses, and other problems. With a recent increase in the threat of cyberattacks on factory equipment, we are taking a number of measures such as establishing dedicated security policies for our plants and strengthening physical measures.

Auditing and education

To maintain and improve security, each of our worksites does a self-assessment once a year using a confidentiality management audit sheet to ascertain the state of their confidentiality management. Depending on the result of that assessment, the confidential information management department carries out an onsite inspection to audit the site and provide guidance. We also conduct local inspections of group companies and provide ongoing support for ATSG-based measures.

To improve the IT literacy of employees and raise their awareness, we regularly provide and share the latest information at the Workplace Representative Liaison Meeting, and provide training about suspicious emails, e-learning opportunities and other education to all employees.