Information Security

Basic stance

As companies are accelerating their DX strategies, more and more things and types of information are being connected to each other, bringing new value to society. Unfortunately, threats such as cyber attacks are being carried out more skillfully each day, and there is an ever-present threat that company information, customer details, and other private information will be leaked. It is critical that these risks are managed for the sustainable growth of companies.

Policy

We have established the AISIN Group Information Security Basic Policy, under which we carry out systematic and continual information security measures.

AISIN Group Information Security Basic Policy

(1) Legal compliance
(2) Maintenance of stable financial and managerial base
(3) Provision of safe products and services
(4) Contribution to building secure cyberspace
(5) Information security management

WEB AISIN Group Information Security Basic Policy

Vision

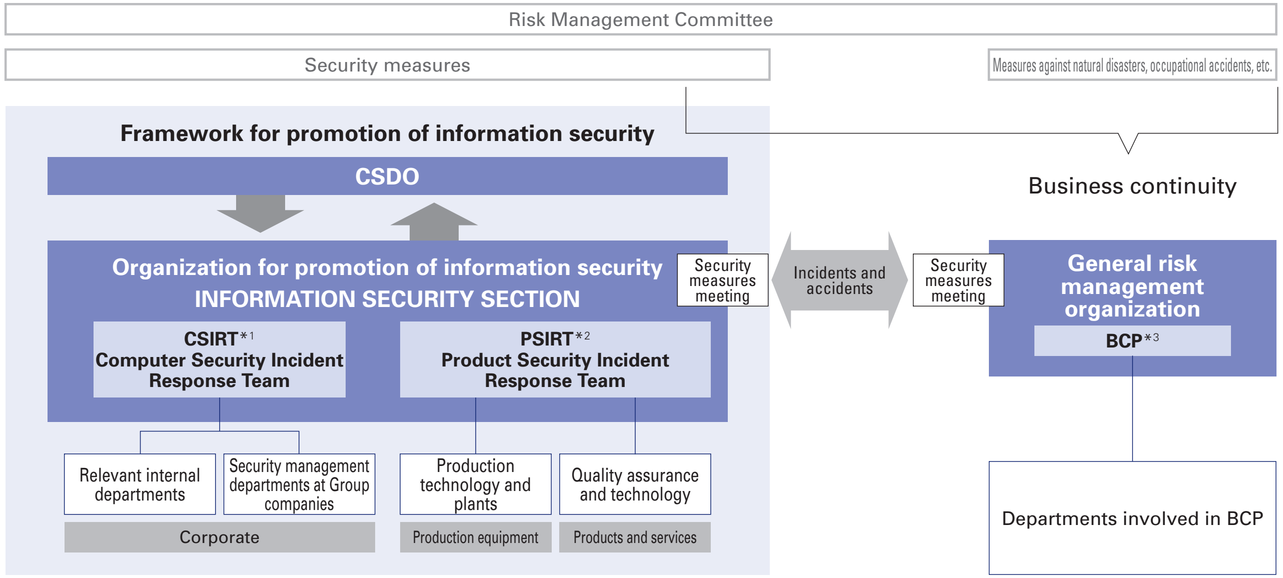
Based on the belief that information assets related to our business activities that are entrusted to us by customers and business partners, or are held by the AISIN Group, are important assets, we will appropriately identify changing threats to corporate management activities and keep track of technological advances, and implement comprehensive countermeasures across the entire Group.

Implementation frameworks

Aisin CSDO* is responsible for establishing structures such as information strategies and IT investment plans based on our business strategies, and holds responsibility and authority for execution and operations related to information security and privacy throughout the AISIN Group. Under our CSDO, we have established the INFORMATION SECURITY SECTION as a specialist security organization to protect the company from risks, such as cyber attacks and unauthorized actions by employees, and are carrying out security activities throughout the AISIN Group. Information security policies and measures are proposed by the Risk Management Committee and are shared across the Group for common understanding, to improve the level of security and ensure that measures are in place.

* CSDO: Chief Software & Digital Officer

Framework for promotion of information security



Risk Management Committee
Security measures
Measures against natural disasters, occupational accidents, etc.
Framework for promotion of information security
CSDO
Business continuity
Organization for promotion of information security
INFORMATION SECURITY SECTION
Security measures meeting
Incidents and accidents
Security measures meeting
General risk management organization
BCP*3
CSIRT*1 Computer Security Incident Response Team
PSIRT*2 Product Security Incident Response Team
Relevant internal departments
Security management departments at Group companies
Production technology and plants
Quality assurance and technology
Departments involved in BCP
Corporate
Production equipment
Products and services

*1 CSIRT: Computer Security Incident Response Team
*2 PSIRT: Product Security Incident Response Team
*3 BCP: Business Continuity Planning

Information security initiatives

The AISIN Group centralizes the whole Group's security measures at its head office, works to ensure security against the increasingly agile and advanced cyber attacks and methods of leaking internal information that are occurring, and to comply with the laws and regulations of the respective countries. Major security incidents that could cause issues such as stopping production are immediately reported to our CSDO and departments involved in risk management, and investigations, analysis, and countermeasures are carried out.

Information security measures

We have formulated security guidelines that comply with the international standards ISO 27001/27002 (certified in April 2022) and the JAMA/JAPIA Cybersecurity Guidelines, prepare to respond to customers' requests for security measures, and utilize these guidelines to mutually improve the level of the entire supply chain.

Security guidelines

Management item	Details of measures
Organization	Implementation frameworks, rules, and procedures
Education	Implementing education, awareness-raising, and training
Technical measures	Asset management, access control, networks, etc.
Physical management	Facilities and area control
Incident and accident framework	Reporting framework and rules

Product security measures

In anticipation of the regulation of more vehicles, we are working on vehicle security measures centered on PSIRT. Also, we are members of AUTO-ISAC*1 in Japan and the U.S. We collect information on risks that have occurred in the industry and use this to implement activities in our in-house development, and carry out initiatives according to ISO21434.

*1 AUTO-ISAC: Automobile Information Sharing and Analysis Center (an automotive cybersecurity organization in North America)

Personal information protection measures

When it comes to personal information protection measures, ensuring compliance with the laws of the respective countries, including GDPR,*2 is important. As we accelerate our DX strategy, transference of personal information between countries will be required. Therefore, the AISIN Group has concluded a comprehensive Group SCC agreement*3 between Group companies that enables the transfer of personal information across the Group.

We will continue to strive to handle personal information securely by training and communicating with all of our employees with a focus on the laws of the respective countries.

*2 GDPR: General Data Protection Regulation (EU)
*3 SCC contract: Standard Contractual Clause

Fostering security awareness

To improve security, it is essential for all employees to perceive improving security as a personal matter, and to be constantly mindful of security and act accordingly as something that is close to their hearts. Our Group-wide efforts include rank-specific training for new employees and promotions, training for events such as overseas assignments, training on responding to suspicious emails, and activities to raise awareness during Information Security Month.

For example, we create educational video content in-house, conduct comprehension tests after training, and publish in our "Cyber Security News" information security slogans solicited from employees in Japan and overseas, in order to encourage each employee to participate and to foster security awareness.

Examples of training and awareness-raising activities

(1) Rank-based training for new employees and promotions (FY2023: 3,000 people across the Group)

2) Onboarding training for events such as overseas posts and business travel

(3) Training for all employees on handling suspicious emails (once a year)

(4) Awareness-raising activities throughout Information Security Month (once a year) and distribution of Group newsletters (once a month)