Information Security

Basic Policy

In order to respond to the threat of cyberattacks, which are rapidly becoming more sophisticated and diverse, the Mitsubishi Electric Group is continually working to strengthen its cyber security and governance of information management and operations.

Our goal is to achieve Level 2 or higher on Cybersecurity Maturity Model Certification (CMMC)[*1] Version 2.

We manage the information entrusted to us by customers and stakeholders of Mitsubishi Electric as well as confidential corporate information, including sales, engineering, and intellectual property information, based on the Declaration of Confidential Corporate Information Security Management.

Framework and Guidelines

In April 2020, we established the Corporate Information Security Division directly under the president and integrated three functions—confidential corporate information management and personal information protection, information systems security, and product security—to oversee all information security management activities. We have been continually enhancing the functions of the division and increasing the number of staff.

We will invest over 50 billion yen to strengthen cyber security measures and improve our information security management system to achieve Level 2 or higher on CMMC Version 2.

The Executive Officer in charge of Information Security supervises information security management. Under the Executive Officer's instructions, the Corporate Information Security Division plans and implements countermeasures for the Mitsubishi Electric Group's information security management system and rules, cybersecurity, and compliance with the laws and regulations related to personal information protection.

Meanwhile, Corporate CSIRT[*2] in the division cooperates with CSIRTs in business groups and business sites to ensure information security.

In addition, in response to the cyberattack targeting a factory of a manufacturer, which caused production to shut down, Mitsubishi Electric has established a group in the division in charge of OT security.

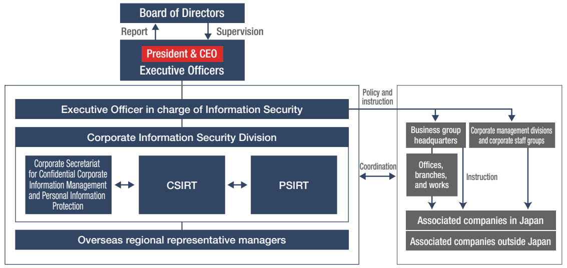
The PSIRT[*3] in the division, which is in charge of enhancing product security, was certified as a CNA[*4] in November 2020. It has begun allocating CVE IDs[*5] to vulnerabilities that affect Mitsubishi Electric products, and it announces these vulnerabilities to the public.

By doing so, the PSIRT strengthens vulnerability handling processes in cooperation with outside stakeholders.

The PSIRT reports identified vulnerabilities according to the processes and issues instructions to respond properly and prevent secondary damage.

Business groups and business sites (offices, branches, and production plants [works]) provide instructions and guidance on information security to domestic and overseas associated companies.

As for cybersecurity issues at overseas associated companies, the Corporate Information Security Division cooperates with overseas regional representative managers in America, Europe, and Asian countries, while considering each region's unique circumstances .


Board of Directors
Report
Supervision
President & CEO
Executive Officers
Executive Officer in charge of Information Security
Policy and instruction
Corporate Information Security Division
Corporate Secretariat for Confidential Corporate Information Management and Personal Information Protection
CSIRT
PSIRT
Coordination
Overseas regional representative managers
Business group headquarters
Corporate management divisions and corporate staff groups
Offices, branches, and works
Instruction
Associated companies in Japan
Associated companies outside Japan
Control and planning
Units responsible for promoting information security

Information Security Organization Structure
(Mitsubishi Electric Group)

Personal Information Protection

Mitsubishi Electric formulated company rules on personal information protection in October 2001. Since then, it has ensured that all employees and relevant individuals understand the rules and has worked on protecting personal information.

In 2004, the company formulated the Personal Information Protection Policy and improved it as a set of personal information protection activities that meet the requirements of JIS Q 15001: 2006 Personal Information Protection Management Systems.

In January 2008, we were granted the right to use the PrivacyMark, which certifies the establishment of management systems that ensure proper measures for personal information protection. We have been renewing the PrivacyMark certification since then.

In January 2024, we completed the eighth PrivacyMark renewal process.

Cyberattack Countermeasures

Cyberattacks are becoming more sophisticated and diverse every year, posing major threats to companies.

To combat cyberattacks, the Mitsubishi Electric Group has introduced the centralized management of networks, computer terminals, and servers (cloud) and adopted defense-in-depth.

The defense-in-depth provides protection against cyberattacks and enables the detection of suspicious activities and intrusions. The immediate response system we have established also helps to prevent and minimize damage.

In order to support work at the office as well as work requiring access from home or on a business trip, strong multifactor authentication has been introduced and authentications are centrally managed.

Internet websites are constantly exposed to many external threats, and so we only launch websites that are approved in order to maintain a high security level.

*1 The Cybersecurity Maturity Model Certification framework by the U.S. Department of Defense. Certification Level 2 or higher means excellent security measures and management structure.

*2 CSIRT stands for Computer Security Incident Response Team.

*3 PSIRT stands for Product Security Incident Response Team. This team works on improving the security quality of products and services.

*4 CNA stands for CVE Numbering Authority, and CVE stands for Common Vulnerabilities and Exposures.

*5 Globally used vulnerability identifiers.