MITSUBISHI ELECTRIC
Changes for the Better

Mitsubishi Electric Group

Information Security Report 2025

Contents

Editorial Policy

The purpose of this report is to apprise customers and stakeholders of the information security initiatives that the Mitsubishi Electric Group engages in on a daily basis in order to enhance the quality of life in our society.

Period Covered by the Report

April 1, 2024 to March 31, 2025

This report partially mentions policies, targets, and plans for April 2025 and beyond.

Scope of the Report

Information security initiatives at the Mitsubishi Electric Group

Publication Date of the Report

December 2025

Inquiries

IT & Security Corporate Governance Dept.,
Mitsubishi Electric Corporation

Tokyo Building, 2-7-3, Marunouchi,
Chiyoda-ku, Tokyo 100-8310

Inquiries about the Information Security Report

Executive Message

We safeguard cyberspace, promote digital innovation, and contribute to our customers' growth while addressing increasingly diverse social challenges.

Satoshi Takeda

Senior Vice President
CIO (In charge of Information Security and IT)
Mitsubishi Electric Corporation

As advancements in AI, data science, and digital transformation (DX) continue to accelerate, cyberattack methods have become increasingly sophisticated, and pose a growing threat to the global community. The Mitsubishi Electric Group recognizes cybersecurity as a critical management issue and is addressing it while expanding its diverse operations both domestically and internationally.

Our goal is to become a "Circular Digital-Engineering Company" that aggregates and analyzes data obtained from our customers in the digital space, fostering strong connections and sharing our ideas within the group to create new value and solve societal challenges. In order to accelerate this transformation, we have restructured the organizations related to DX, IT, and information, and established the Digital Innovation Group and Mitsubishi Electric Digital Innovation Corporation on April 1, 2025.

Our advanced integration capabilities are developed through extensive experience in large-scale projects and global operations across various fields. These capabilities, along with expertise gained from our information security strengthening measures, allow us to offer optimal solution services, integrated with the latest digital technologies, and a full range of services, including comprehensive security measures from information technology (IT) to operational technology (OT) and operation and maintenance (O&M) service, to address diversifying security risks.

The Mitsubishi Electric Group is continuously working to maintain and improve the current level of security under the leadership of the Corporate Information Security Division. In recent years, cyberattacks have become more sophisticated, and OT security in manufacturing and other fields is becoming increasingly important, along with security measures for customers. In response, we established a FSIRT (Factory Security Incident Response Team) structure in October 2024, which includes the business divisions (Business groups and Sites). This initiative supports our stakeholders, including customers, shareholders, investors, and employees, through four pillars: information security (CSIRT*1), product security (PSIRT*2), factory security (FSIRT*3), and confidential corporate information management and personal information protection.

Security laws and regulations, including the European NIS2 Directive and the Cyber Resilience Act (CRA), are being strengthened in countries all over the world. Therefore, we will investigate and analyze legal trends in every country and implement necessary measures. Furthermore, we will enhance collaboration between the Corporate Information Security Division and business divisions. In particular, we will collaborate with overseas associated companies, to ensure compliance with all the applicable laws and regulations throughout the entire Mitsubishi Electric Group.

This report introduces the information security initiatives of the Mitsubishi Electric Group. We hope that you will find it useful.

*1 Computer Security Incident Response Team
*2 Product Security Incident Response Team
*3 Factory Security Incident Response Team

Mitsubishi Electric Group Vision and Strategy

Cyberattacks have become increasingly advanced and sophisticated in recent years, and they are posing invisible threats to the global community. In this regard, the Mitsubishi Electric Group is committed to addressing these threats through collaborative efforts across borders, safeguarding a secure cyberspace environment, promoting digital innovation, and attaining a vibrant and sustainable society. In order to transform into a “Circular Digital-Engineering Company”, we are implementing security measures through the entire lifecycle of our products and systems to safeguard our customers' critical data and systems, as well as ensure their safety and security. This contributes to the realization of a sustainable society. Given the ongoing evolution of cyberattacks, we are continuously developing and implementing our cybersecurity measures. We constantly monitor the latest attack trends and changes in the laws and regulations to implement further security measures.

One-stop security solution

In our commitment to strengthen security within the Mitsubishi Electric Group, we have a corporate division that is dedicated to group security initiatives, and security business divisions that leads the initiatives to ensure safe and secure products and services for customers. Along with organizational restructuring in April 2025, we are enhancing collaboration between these two divisions. By integrating the strengths of each department—information security, factory security, product security, security governance, monitoring and operation, and consulting—we will provide a one-stop security solution.

Global human resource development

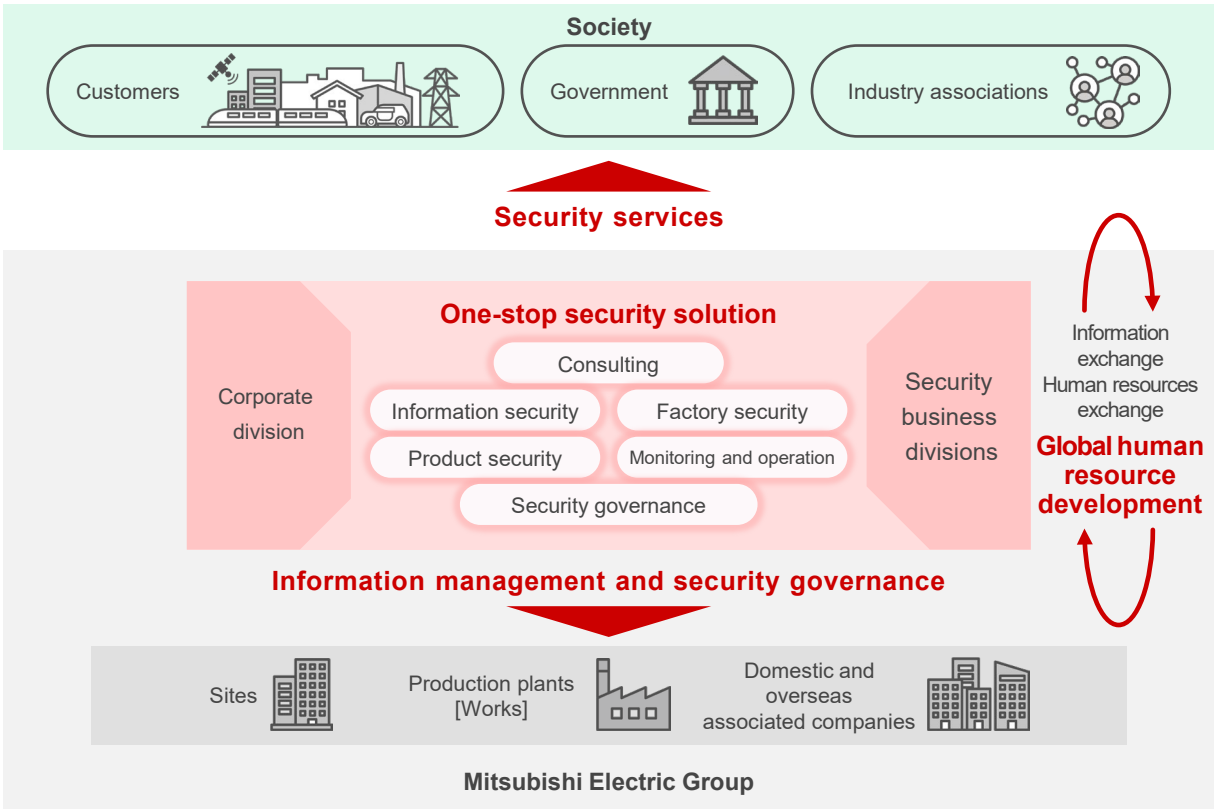
We believe that the development of human resources capable of promoting security measures is essential to safely advance our global business operations. We have developed human-resource education programs for information management and security tailored to different positions and roles, and we encourage participation in these programs. We are also rolling out international intra-company transfers to enhance the skills of our employees worldwide, and are facilitating human resource exchanges between industry, academia, and government.

Information management and security governance

In order to advance the measures throughout the entire Mitsubishi Electric Group, we are clarifying our organizational structure and roles. We are also advocating for and supporting measures to counter increasingly sophisticated and rapidly evolving cyberattacks, while leveraging data, effectively and efficiently. To this end, we will implement flexible and highly effective security measures based on the latest threat intelligence, depending on the degree and priority of risk.

Security services

We will contribute to the safety and security of the supply chain through our one-stop security solution for IT, OT, and products, which leverages the results of the Mitsubishi Electric Group's information security strengthening measures. With comprehensive integrated security measures and planning and advanced security capabilities, we are committed to be a partner that fully resolves any of our customers' concerns or dissatisfaction.



Information Security Management

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 cybersecurity and governance of information management and operations.

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.

Declaration of Confidential Corporate Information Security Management

With respect to the information assets that constitute its core business activities, Mitsubishi Electric Group shall disclose information that should be released externally in a timely and appropriate manner, while ensuring strict and appropriate management of confidential corporate information.

In the unlikely event that confidential corporate information including valuable information entrusted to us by others were to leak, this would not only cost the trust and confidence invested in the Company Group; the improper use of this information could also threaten national, societal and individual security.

Recognizing that appropriate management of confidential corporate information is a key corporate social responsibility, the Company Group hereby declares that all employees shall comply with the following confidential corporate information management policies.

Additionally, “Confidential corporate information” means valuable technical or business information held by the Company Group, and information (such as personal information, information obtained from outside the Company and insider information), which, if disclosed or used in an unauthorized way, could be disadvantageous to the Company Group and/or its stakeholders. Physical objects that constitute confidential corporate information are also subject to control.

1) Appropriate Management of Confidential Corporate Information through Compliance with Laws, Ordinances and Regulations
   The Company Group shall manage all confidential corporate information concerning business activities appropriately in accordance with laws, ordinances and Company Group regulations.

2) Enforcement of Security Management Measures
   The Company Group shall implement appropriate security management measures for the protection and proper control of confidential corporate information.
   “Security management measures” means organizational, human, technological and physical measures that are strictly enforced according to the confidentiality level of the applicable corporate information.

3) Enhancement of Information System Security Measures
   The Company Group shall enhance its information system security measures to prevent unauthorized access, intrusion and wrongful use of confidential corporate information, and implement comprehensive countermeasures with IT.

4) Education
   Recognizing that the awareness of individual employees who are involved in handling confidential corporate information is fundamental to management, the Company Group shall provide regular education for all employees concerning the importance of confidential corporate information management and efforts to enhance it.

5) Continual improvement of Management through the PDCA Cycle
   The Company Group shall establish a confidential corporate information management system and improve it proactively and continually through the PDCA (Plan-Do-Check-Act) cycle.

6) Timely and Appropriate Information Disclosure
   In addition to rigorously managing confidential corporate information in an appropriate manner in line with items 1 through 5 above, the Company shall disclose information that should be externally released in a timely and appropriate manner.

May 26, 2025
Kei Uruma, President & CEO
Mitsubishi Electric Corporation

Information Security Organization Structure

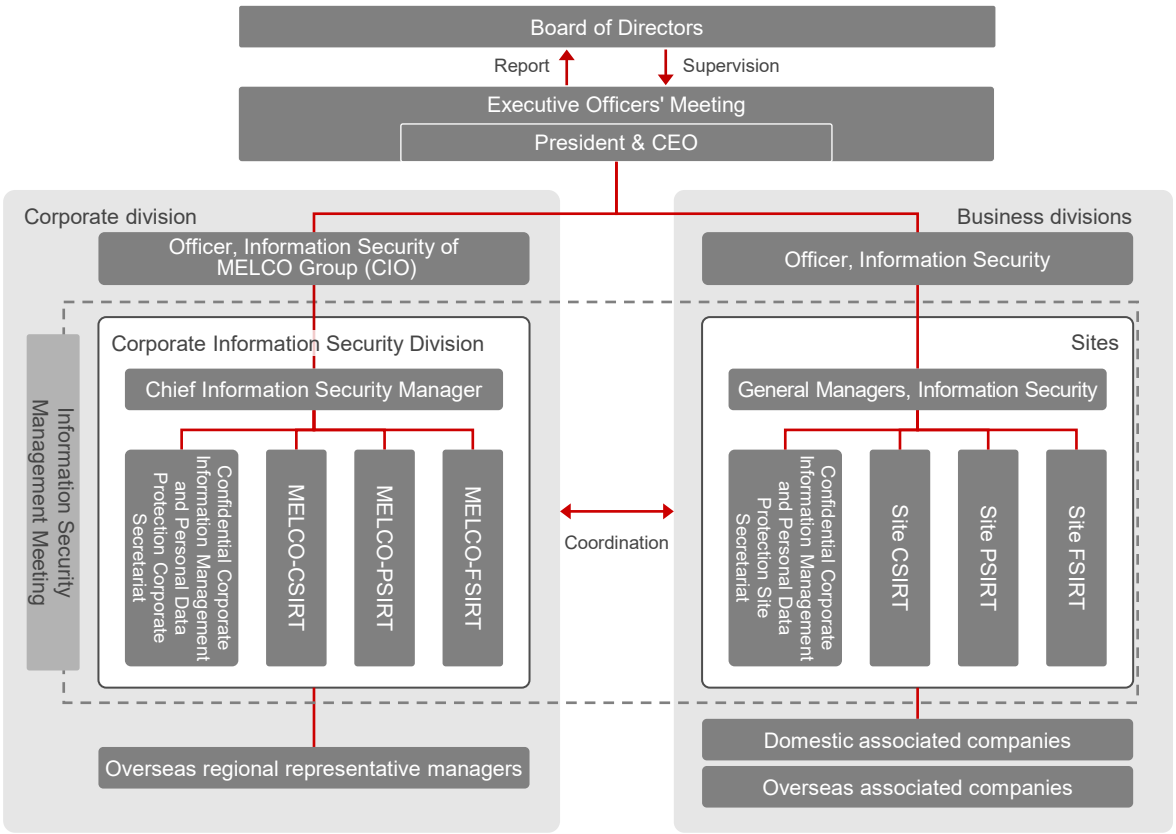
The Mitsubishi Electric Group's information security framework designates the President & CEO as the Chief Officer responsible for information security management. It consists of a corporate division that manages information security across the organization and business divisions that bear responsibility for information security risks within their business activities. Within the corporate division, an Executive Officer in charge of Information Security appointed as the Officer, Information Security of MELCO*1 Group oversees all aspects of information security management. Under the direction, the Chief Information Security Manager ensures compliance with customer supply chain requirements, international standards, and industry best practices, while regularly reporting on the division's activities. In each business division, General Managers, Information Security operate under the supervision of their respective Officer, Information Security to manage information security of their own divisions, including oversight of associated companies. In business divisions, information security general managers operate under the supervision of their respective information security officer to manage information security for their own divisions and associated companies.

The Officer, Information Security of MELCO Group convenes regular Information Security Management Meetings with General Managers, Information Security to communicate and coordinate the formulation of group-wide information security policies and the planning of related initiatives.

Each division is equipped with functions for information management: CSIRT, PSIRT, and FSIRT. The Corporate Information Security Division is responsible for planning and promoting the Group's information security mechanisms, rules, IT system security, and compliance with personal data protection laws and regulations. In the event of a security incident, this division collaborates with the relevant business divisions to make prompt and informed decisions based on operational circumstances, ensuring swift incident response.

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

*1 Mitsubishi Electric Corporation



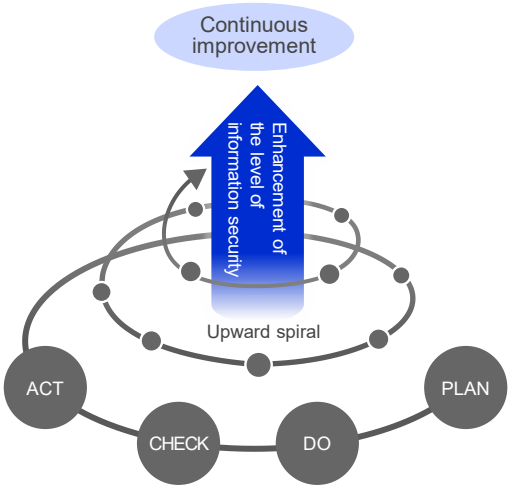
Information Security Organization Structure (Mitsubishi Electric Group)

Management Principles

The Mitsubishi Electric Group oversees confidential corporate information management and protects personal information as its continuous improvement activity using the Plan, Do, Check, Act (PDCA) cycle and implements four security measures, which are organizational, human, technological, and physical security measures, to safeguard confidential corporate information and personal information while taking into consideration external factors such as handling of personal data overseas.

PDCA cycle

We strive to continually raise the level of our information security in an upward spiral. First, plans are formulated at the beginning of the fiscal year based on an annual policy (Plan). Then, various information security measures are rolled out and employees are trained (Do). Afterward, the status of information security management is checked (Check). Finally, the measures are revised accordingly based on the results (Act).



PDCA cycle to ensure information security

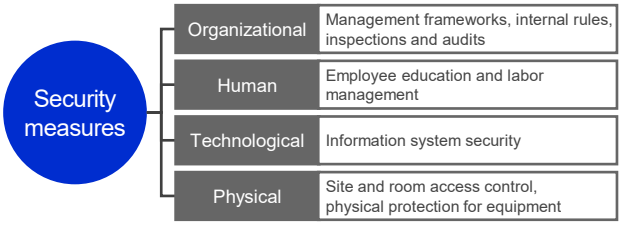
Four security measures

Organizational security measures consist of systems such as management frameworks, internal rules, inspections and audits to safeguard confidential corporate information and personal information. They are revised as needed to ensure that there is no loss of effectiveness due to changes in the operating environments.

Human security measures consist of education for employees and personnel management to ensure employees carry out information security measures.

Technological security measures consist of information system security efforts such as cyberattack countermeasures.

Physical security measures consist of site and room access control as well as physical protection for equipment to prevent unauthorized third parties from entering a business site and potentially accessing confidential corporate information and personal information.



Four security measures

Global activities

To maintain and improve the information security level of the Mitsubishi Electric Group including overseas associated companies, various inspections are conducted according to information management system prescribed in the Guidelines to Information Security Management Rules for associated companies. In addition, we regularly monitor ever-changin global cybersecurity laws and regulations, including the NIS2 Directive and Cyber Resilience Act. We are collectively improving our responses as the Mitsubishi Electric Group.

Information Security Regulations and Guidelines

In accordance with Declaration of Confidential Corporate Information Security Management and Personal Information Protection Policy, Mitsubishi Electric Corporation has established information security regulations and guidelines from the perspective of the four security measures, and reviews them as necessary to comply with current laws.

To protect personal information, the Mitsubishi Electric Group handles the personal information appropriately and takes a global approach complying with the laws and regulations of Japan and applicable third countries and regions. Our common guidelines are also applied to associated companies.

Item		Basic regulations
Security measures	Organizational security measures	Regulations on confidential corporate information security management / Personal data protection guidelines
	Human security measures	Regulations on the work of employees
	Technological security measures	Regulations on information security management
	Physical security guidelines	Physical security guidelines

Responding to changes in the operating environment

In addition to the basic regulations given above, we have established regulations concerning the release of information on public-facing websites, regulations concerning the use of smartphones, management standards to strengthen information security in the supply chain, and other regulations to address today's changing business operation environment.

Information Security Inspections

The Mitsubishi Electric Group performs the following inspections as part of the C (Check) stage of the PDCA cycle at head office management departments, business groups and offices, and associated companies. These inspections focus on checking whether confidential corporate information management and personal information protection activities are being implemented properly by the Mitsubishi Electric Group as a whole, and on confirming the status of those activities.

The group reviews measures based on the results, and this leads to the A (Act) stage of the PDCA cycle.

These inspections are set down in the Confidential Corporate Information Management Regulations, which cover Mitsubishi Electric Corporation, and in the Guidelines for Information Security Management Regulations, which cover domestic and overseas associated companies.

Name Content	Name	Content
Content	Self-check program for confidential corporate information management and personal information protection	Using a checklist, each Mitsubishi Electric Group company performs a self-inspection of its activities for information security.
Third-party check	Third-party check program for confidential corporate information management and personal information protection	Mitsubishi Electric's business sites mutually check each other's status of information security management. Mitsubishi Electric checks the status of information security at associated companies.
	Personal information protection audits (Personal information protection management system audits)	At Mitsubishi Electric, the status of personal information protection is audited company-wide under the instructions of the Audit Manager for Personal Information Protection appointed by the President & CEO of Mitsubishi Electric. At domestic associated companies that have been granted the right to use the PrivacyMark, the same audit is carried out by the audit manager of each company.

Information Security Education

Mitsubishi Electric is working on fostering a corporate culture that ensures the appropriate handling of confidential corporate information and personal information. We provide the educational programs described below to train employees on how to fully implement concrete security measures, including storing files on servers or encrypting them in accordance with their confidentiality level.

Education for all employees

An e-learning program on information security is provided once a year to all employees and other staff members (about 50,000 in total) to ensure their full understanding of the Mitsubishi Electric policies, status of data breach incidents, laws and regulations related to the protection of personal information, Unfair Competition Prevention Act, and security measures (organizational, human, technological, and physical measures) that each employee must be aware of. In addition, due to the rapid increase in teleworking and the shift in business type and environment due to the use of cloud services, educational materials for employees are released as needed.

Education corresponding to each career stage

We teach confidential corporate information management and personal information protection through training programs for new employees, newly appointed section managers, the personal information asset manager, the Corporate Secretariat involved in operation and the like, so that our employees can fulfill the roles expected at each career stage in the duties for which they are responsible.

Exercises to practice handling spoofed e-mails

As a measure against cyberattacks, Mitsubishi Electric regularly conduct exercises that allow all employees, including officers, to verify that they know how to handle spoofed e-mails. Employees of domestic associated companies can participate in this exercise. At overseas associated companies in America, Europe, and other Asian countries practice exercises are conducted according to local circumstances under the direction of regional representative managers.

Other individual training

Employees posted overseas are provided with a preliminary education program which covers risks in confidential corporate information management and personal information protection outside Japan and examples of data breach incidents that have occurred overseas.

Personal Information Protection Activities by Mitsubishi Electric Group

The Mitsubishi Electric Group's core philosophy regarding personal data protection

The Mitsubishi Electric Group has established a corporate purpose: “We, the Mitsubishi Electric Group, will contribute to the realization of a vibrant and sustainable society through continuous technological innovation and ceaseless creativity.” We are engaged in a variety of businesses and receive a variety of information from all stakeholders—including customers, shareholders, investors, business partners and employees—through our business activities while recognizing that personal data is an important asset.

As such, it is our social responsibility to ensure accurate and safe processing of personal data.

We handle personal data in accordance with eight principles based on laws and regulations of various countries and regions, and strive to improve and maintain these principles by establishing systems and implementing appropriate measures.

The Mitsubishi Electric Group's principles for processing of personal data

The Mitsubishi Electric Group processes your important personal data in accordance with the following principles.

(1) Lawfulness: We acquire and process personal data appropriately in accordance with relevant laws and regulations.

(2) Fairness and transparency: When processing personal data, we provide you with clear and easily understandable information about our procedures for handling personal data, using simple and accessible methods, at the appropriate time and from your perspective.

(3) Purpose limitation: We process personal data only if it is sufficient, relevant and necessary in relation to the purpose.

(3) Data minimization: We limit our processing of personal data to what is necessary in relation to the purpose.

(4) Accuracy: We keep personal data accurate and up to date where necessary.

(5) Storage limitation: We determine the period for which storing personal data is necessary for its purpose. When the storage period ends, we delete personal data by an appropriate method.

(6) Integrity and confidentiality: We take appropriate technical and organizational measures to protect personal data from breaches, including unauthorized access, accidental loss, destruction, alteration, or leakage.

(7) Privacy by design: We consider protective measures necessary to comply with the above principles at the planning stage, or in other words, prior to conducting the processing of personal data.

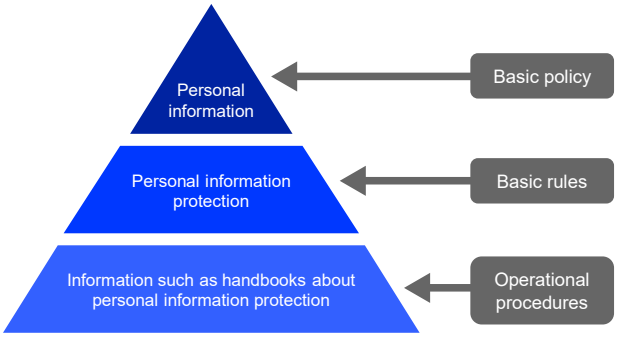
Personal Information Protection Activities at Mitsubishi Electric

Establishment of personal information protection management system

Mitsubishi Electric has established a Personal Information Protection Policy and Company Rules on Personal Information Protection, developing a framework in accordance with the Japanese Industrial Standards JIS Q 15001: Personal Information Protection Management System – Requirements.

Through this framework, the Company ensures thorough awareness of personal information protection among its employees and actively promotes initiatives to safeguard personal information.

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 renewal process.



Structure of personal information protection rules

Personal information collected from customers through questionnaires, registration of purchased products, after-sales service, and so on is managed in accordance with the “Personal Information Protection Policy”. Furthermore, Mitsubishi Electric has been granted the right to use the PrivacyMark and is making ongoing efforts to ensure the proper handling of personal information.

Personal Information Protection Policy

Mitsubishi Electric (“the Company”) will continually improve its technologies and services by applying creativity to all aspects of its business, thus enhancing the quality of life in society. Through these activities, the Company collects various types of information from its customers and affiliated persons. Since personal information is an important asset of individuals, it is the company’s social responsibility to protect the personal information appropriately and use it correctly and safely in compliance with laws. The Company has established the personal information protection management system as a part of corporate management. With this system, the Company will ensure that the Company’s employees (including corporate officers, employees, short-term/long-term part-timers, and temporary staff) and affiliated persons fully understand personal information protection, implement the actions listed below, and improve and maintain personal information protection.

1. Objective of Personal Information Protection
   The objective of personal information protection is to appropriately and effectively use personal information and protect the rights and interests of individuals with due consideration given to the usefulness of personal information.
2. Purpose of Use of Personal Information
   The Company uses personal information within the extent of the purpose of use clearly described to the information owner and uses such information only when required for business reasons.
3. Acquisition of Personal Information
   The Company acquires personal information through legal and fair means. When acquiring information directly from the information owner, the Company will clearly explain the requirements, including the purpose of use, and obtain consent.
4. Disclosure and Submission of Personal Information
   The Company will obtain the consent of the information owner before disclosing or submitting his/her personal information to a third party for the purpose of outsourcing or collaboration.
5. Handling of Personal Information
   (1) Compliance with laws and regulations on the protection of personal information
   The Company fully complies with laws, regulations, national policies, and other rules concerning the protection of personal information.
   (2) Prevention of data breach, losses, and damage to personal information (e.g., security measures), and corrective measures
   The Company takes reasonable safety actions and necessary security measures to prevent unauthorized access, losses, corruption, falsification, or leakage of personal information. It also audits all departments to check the handling of personal information and implements corrective measures. Through this audit, all divisions review the latest data breach risks or issues and make improvements to avoid similar incidents in the future.
   (3) Creation and operation of the personal information protection management system
   The Company has created and is operating the personal information protection management system in line with the requirements of JIS Q 15001: 2006 Personal Information Protection Management Systems. It has also been reviewed by JIPDEC and as a result, obtained the right to use PrivacyMark, which is given to businesses that handle personal information properly. It will continue to protect personal information while continually improving the personal information protection management system.
6. Handling of Information Related to Individuals
   When the Company handles information related to an individual such as location data, IP address, and cookies on the Company website or in other places, it may notify the information owner of the purpose of use and obtain his/her consent.
7. Responses to Inquiries from Information Owners
   When the information owner requests the disclosure, correction, removal, or suspension of use of his/her personal information, or when the Company receives inquiries, including complaints or consultation, from the information owner, it will respond without delay.
   The Company also strives to keep personal information accurate and up to date.

PrivacyMark

Date of formulation: April 16, 2004
Date of revision: April 1, 2022
Kei Uruma, President & CEO
Mitsubishi Electric Corporation

Proper handling of personal information

We handle personal information appropriately; we acquire it by specifying the purpose of use, use it only within the intended scope, and provide it to a third party only with the consent of information owners. At the same time, we will further strengthen security measures, including storing data on servers and using data encryption, to address the risk of data breach caused by cyberattacks.

PrivacyMark

Mitsubishi Electric and some domestic associated companies have been granted the right to use the PrivacyMark.

Response to Japan's "My Number" system

Personal identity numbers are managed strictly and handled appropriately in accordance with internal regulations adapted to Japan's "My Number" system. Employees who handle personal identity numbers are trained individually.

Compliance with the EU General Data Protection Regulation (GDPR) and China's Personal Information Protection Law

When Mitsubishi Electric transfers or handles personal information as defined by national and regional laws, such as the EU General Data Protection Regulation (GDPR*1: Effective May 2018) and China's Personal Information Protection Law (Effective November 1, 2021), Mitsubishi Electric shall appropriately protect personal information in accordance with the requirements of the relevant national and regional laws.

*1 GDPR stands for General Data Protection Regulation.

Other Measures

Contractor management

Confidential corporate information and personal information are entrusted to a contractor only after a proper non-disclosure agreement is concluded between Mitsubishi Electric and the contractor. The agreement stipulates all the security and personal information protection matters that we require.

To ensure that confidential corporate information and personal information entrusted to a contractor will be handled with appropriate control, before entrusting the information to the contractor, we confirm that the contractor will maintain the proper level of protection. After submitting the information, we supervise the contractor by regularly examining a status report on the use and management of the information that we have submitted.

Data Breach Prevention Measures through AI Predictive Detection

Given the increasing importance of protecting critical information from the perspectives of economic security and maintaining corporate competitiveness, there is a growing need to strengthen measures against "Human-mediated data breaches".

In order to ensure safe and secure working environments for our employees and to strengthen the protection of our technical information and assets, we have implemented predictive data breach prevention measures, such as AI-assisted email monitoring.

Cybersecurity Initiatives

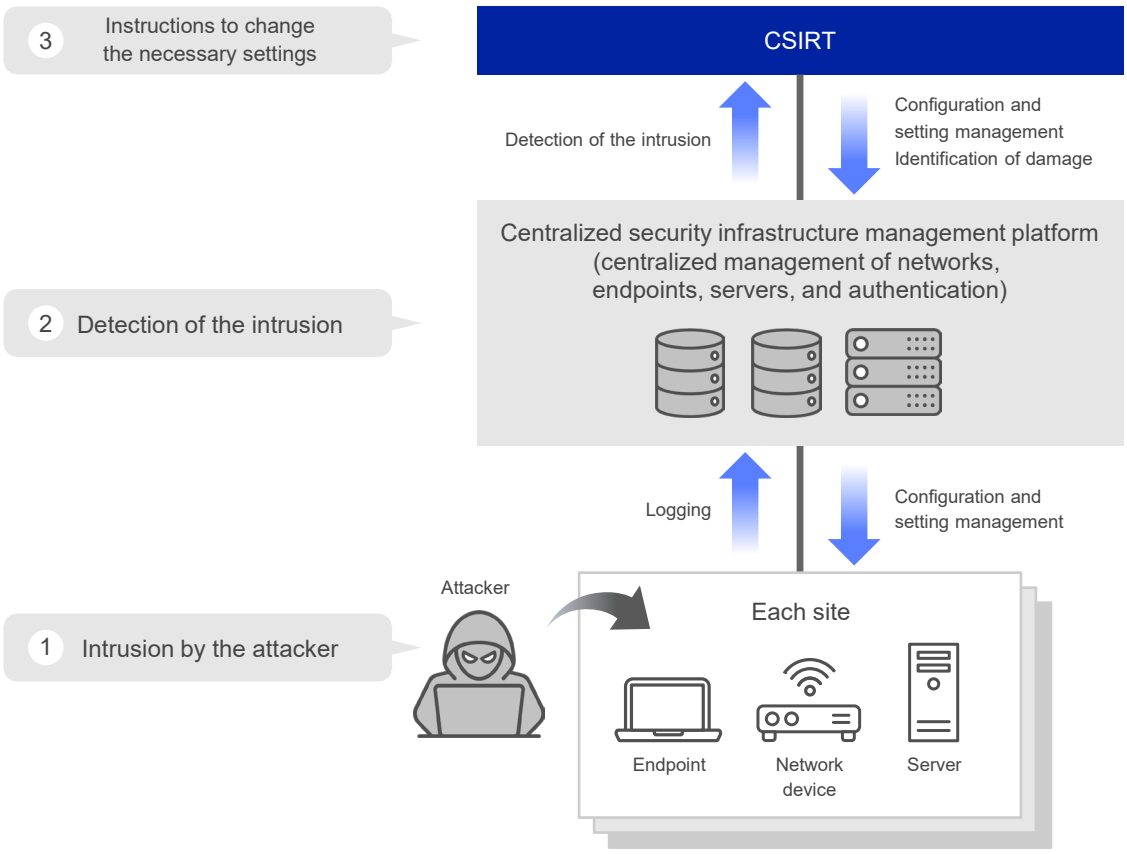
The information security initiatives of the Mitsubishi Electric Group include cyberattack countermeasures and physical security measures for the IT infrastructure.

Cyberattack Countermeasures

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

To counter cyberattacks against companies, the Mitsubishi Electric Group is implementing centralized management of networks, endpoints, and servers (cloud) and adopting defense-in-depth. 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.



Centralized security management

Defense in depth

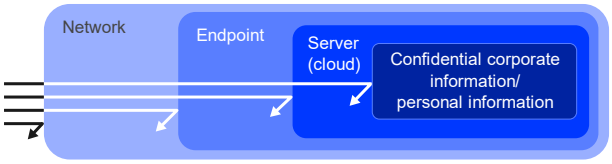
The Mitsubishi Electric Group has adopted defense in depth, consisting of three layers of technological security measures, which are network, endpoint, and server (cloud) security measures.

In the network security measures, various security devices are installed at perimeter to control and monitor email and web communications, among others. This will block unauthorized access or malware from outside or prevent information from being leaked. Furthermore, within our internal network, we strictly control and manage communications between endpoints and servers, as well as between different production plants [Works], to localize potential damage. The Mitsubishi Electric Group will continue to strengthen these measures in the future.

Regarding endpoint security measures, endpoints are centrally managed, malware is detected and removed using anti-malware software, and security patches for software vulnerabilities are applied to prevent the infection of malware. The anomaly behavior detection (EDR*1) tool is installed in all endpoints to strengthen endpoint security. In addition, we have deployed multifactor authentication (device authentication) that combines two or more authentication factors to access information systems for enhanced security.

Servers that are becoming cloud-based are periodically checked to find vulnerabilities, and communications and operations are monitored. This will make servers (cloud) robust, which have critical information.

To confidential corporate information and personal information stored in servers or in the cloud, access control and encryption is applied based on the principle of least privilege. For the management of these types of information, the Mitsubishi Electric Group also develops and fully implements rules, educates employees, and carries out inspections.



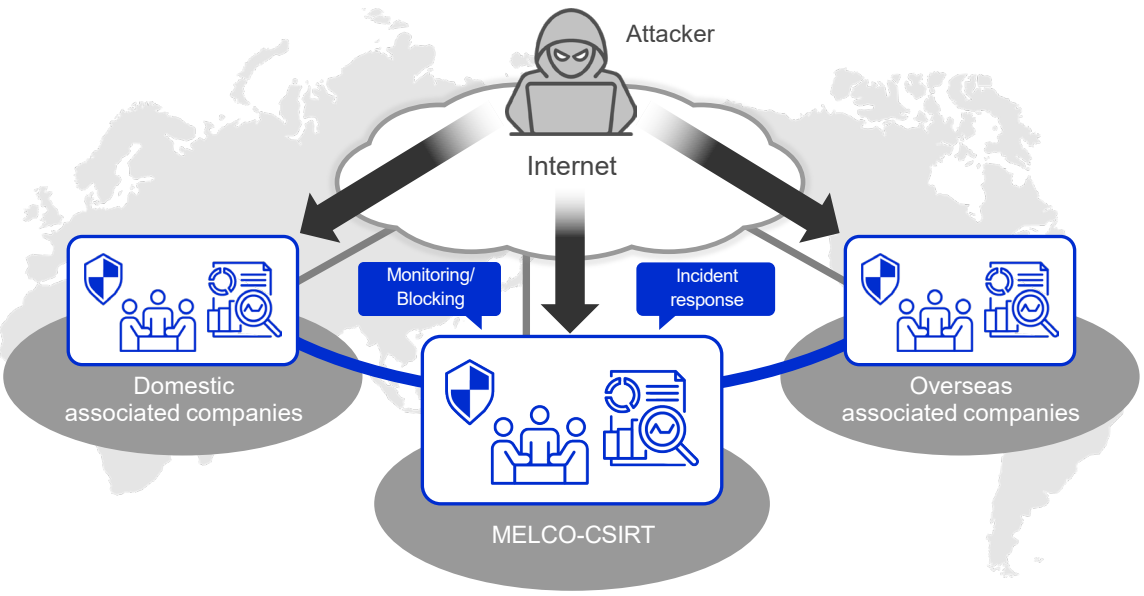
Multilayered defense

Computer Security Incident Response Team

The Mitsubishi Electric Group has established the Mitsubishi Electric Corporation Computer Security Incident Response Team (MELCO-CSIRT) to monitor cyberattacks and respond immediately to any incidents.

In order to prevent cyberattacks, we have also developed a process to monitor our domestic and overseas associated companies, which has been insufficient in the past. The above-mentioned communication monitoring identifies suspicious behavior, allowing you to quickly detect and block cyberattacks. On the endpoint side, information on malware infections and the current soundness of endpoints are gathered and identified. In the event of an incident, the MELCO-CSIRT will utilize these security measures to immediately assess the damage, make prompt and appropriate responses, restore operations, and minimize damage as much as possible. After that, it will analyze the incident in detail and support the implementation of permanent measures by the department where the incident occurred.

*1 EDR stands for Endpoint Detection and Response.



MELCO-CSIRT

Security measures for teleworking

Teleworking is becoming more common as work styles diversify to include working from home or at a satellite office, in addition to mobile work during a business trip.

Meanwhile, the use of a network and the cloud contributes to the diversification of business operation, and traditional security measures at the perimeter becomes insufficient due to an increase in normal access from outside. For this reason, we are implementing more powerful security measures, including the encryption of communications using a virtual private network (VPN) for security and the use of multifactor authentication.

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.

Management of Internet websites

As a lesson learned from past incidents that occurred due to unauthorized access, the Mitsubishi Electric Group now ensures that only websites that have been approved by Mitsubishi Electric are launched in order to maintain the security level of websites.

Websites may go live only after they have passed a security test and problems have been resolved. We also regularly inspect our public websites on the Internet to assess their management status. By doing so, we remove unnecessary websites and strengthen security measures for websites where they are insufficient.

Initiatives Regarding the Security Quality of Products and Services

Roles of the Mitsubishi Electric PSIRT

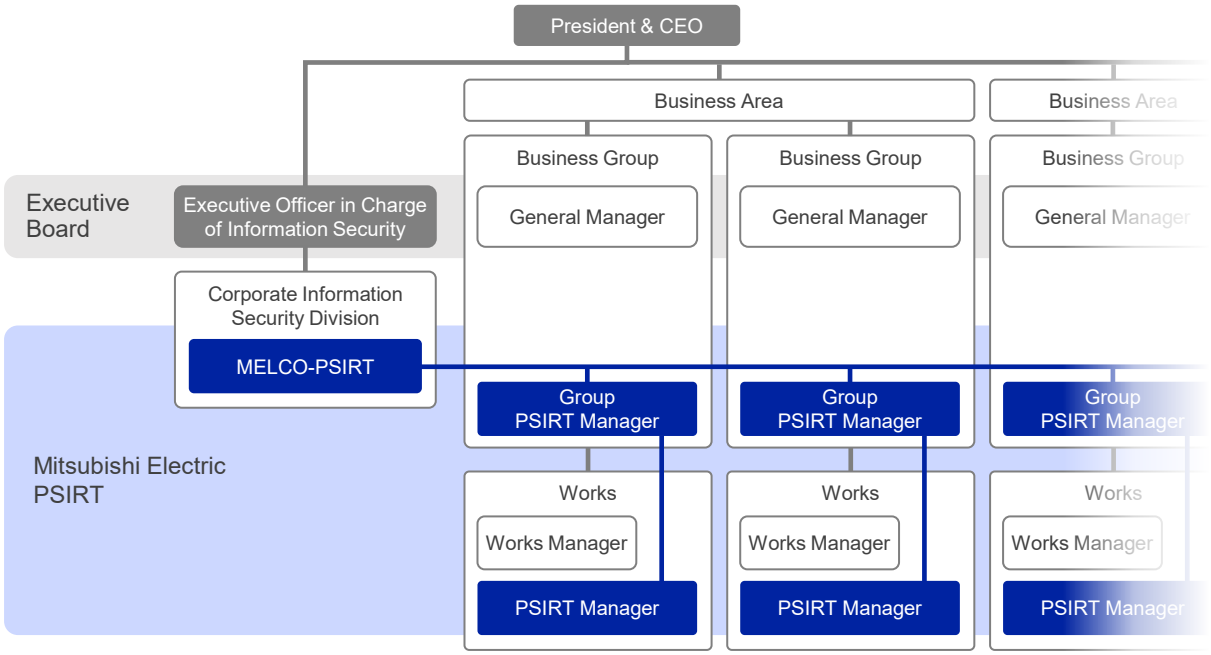
Mitsubishi Electric has formed the Mitsubishi Electric Product Security Incident Response Team (PSIRT), an internal unit for handling issues related to the security quality of products and services, and is making company-wide efforts to ensure the information security of our products and services.

The roles of the Mitsubishi Electric PSIRT are listed on the right:

- Gather information on vulnerabilities in products and services provided to customers
- Respond swiftly to vulnerabilities discovered in cooperation with product design and production departments and service management departments
- Strengthen and promote technical initiatives to preclude vulnerabilities from the stage of product and service development
- Provide necessary security training to all officers and employees concerned with product and service development
- Disclose vulnerability information and measures to customers

The Mitsubishi Electric PSIRT Organization Structure

Mitsubishi Electric has established the MELCO-PSIRT (Mitsubishi Electric Corporation Product Security Incident Response Team) at the head office to serve as an external contact point, and has appointed Group PSIRT Manager to each business group and PSIRT Managers to the production plants [Works]. This ensures the security quality of products and services throughout the company.



The Mitsubishi Electric PSIRT Organizational Structure

Compliance with Laws and Regulations Related to Product Security

With the advancement of digitalization in recent years, the impact of cyberattacks on society has been increasing. Countries around the world have strengthened their legal regulations on products by introducing cyber security acts such as the EU Cyber Resilience Act. In addition to measures that ensure the security quality of products and services, Mitsubishi Electric is constantly working with all our businesses to comply with the legal requirements of each country.

Factory (OT Security) Initiatives

Promotion of OT Security Measures

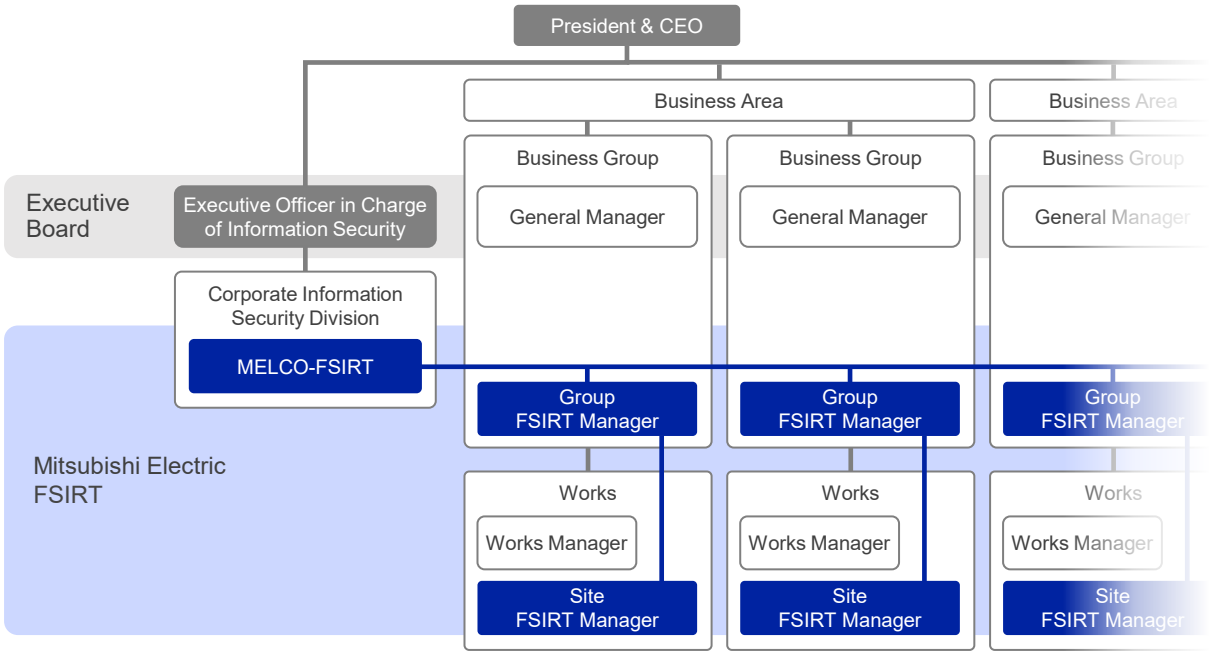
Various new technologies and environmental changes, such as IoT, DX (Digital Transformation), and teleworking, are flowing into factories that have been operating in closed environments with no external connections such as the Internet. As a result, factories are now starting to operate in more open environments.

Consequently, the threat of cyberattacks, which had previously been unheard of in the factory environment, has reached factories, leading to numerous incidents that cause significant damage, such as factory shutdowns, in recent years.

At Mitsubishi Electric, we have established the Mitsubishi Electric FSIRT (Factory Security Incident Response Team) and are working to strengthen cybersecurity measures for Mitsubishi Electric Group's factories. The Mitsubishi Electric FSIRT is comprised of MELCO-FSIRT (Mitsubishi Electric Corporation Factory Security Incident Response Team) which has been established in the Corporate Information Security Division, Group FSIRT Managers who have been appointed to the business groups, and Site FSIRT Managers who have been appointed to the production plant [Works].

In the Mitsubishi Electric FSIRT, the MELCO-FSIRT oversees overall management and assists with the resolution of any issues that may arise within the company. They also systematically accumulate knowledge and expertise gained through their activities to enhance company-wide initiatives. The Site FSIRT Managers work closely with MELCO-FSIRT to coordinate and manage the respective divisions/departments within their production plants [Works]. During standard operations, they are responsible for considering and promoting measures tailored to their organization's specific circumstances. In the event of an incident, they lead any necessary corrective actions. The Group FSIRT Managers cooperate with MELCO-FSIRT to support production plants [Works] in the event of an incident. They are also responsible for coordinating and managing OT security operations for the associated companies within the jurisdiction of their business groups.

Each organization is structured to facilitate inter-organizational collaboration during standard operations and in the event of an incident, ensure that OT security measures can be properly and smoothly promoted throughout the company.



The Mitsubishi Electric FSIRT Organizational Structure

Collaboration with OT Security Solutions

During our OT security measures promotion activities, we implemented technical measures at the Mitsubishi Electric Group's production plants [Works]. We have also addressed various issues that arose during the implementation and operation of these measures in collaboration with the relevant on-site departments. The expertise gained in promoting these activities is now being applied to the OT security solutions for our customers.

MITSUBISHI ELECTRIC CORPORATION

https://www.mitsubishielectric.com