Kawasaki
Powering your potential

Kawasaki Group

Information Security Report

2023

Kawasaki Heavy Industries, Ltd.

The story behind the publication

This report is published with the purpose to disclose the Kawasaki Group's initiatives on information security for our stakeholder's understanding. It is based on "Cybersecurity Management guidelines Ver.3.0" made by the Ministry of Economy, Trade and Industry, Japan.

INDEX

○Ministry of Economy, Trade and Industry "Cybersecurity Management Guidelines Ver. 3.0"

[Ten important items of cybersecurity management]

- Direction 1 Recognize cybersecurity risks and develop an organization-wide policy
- Direction 2 Build a management system for cybersecurity risk
- Direction 3 Secure resources (budget, workforce, etc.) for cybersecurity measures
- Direction 4 Identify cybersecurity risks and develop plans to address them
- Direction 5 Establish systems to effectively address cybersecurity risks
- Direction 6 Continuously improve cybersecurity measures through a PDCA cycle
- Direction 7 Develop a cybersecurity incident response team and relevant procedures
- Direction 8 Develop a business continuity and recovery team and relevant procedures in preparation for damage due to cyber incidents
- Direction 9 Understand the status of and implement measures considering the entire supply chain, including business partners and outsourcing organizations
- Direction 10 Facilitate the gathering, sharing and disclosure of information on cybersecurity

○Subject Period

This report covers activities up to December 31, 2023.

Message from the CISO

The advent of the digital age is bringing rapid changes to people's lives. By connecting everything through networks, we can access vast amounts of information regardless of our location and receive a variety of services that utilize the strong computing power of the cloud. While such evolution is increasing the convenience of society, cyberattacks that threaten the stability of social infrastructure and the privacy of individuals have become a major social issue. Additionally, the world is becoming more geopolitically unstable, and cybersecurity is mentioned often as a challenge in security. I feel that confronting with cyber threats is a new challenge that requires the nation and society to work together as one.

For more than 120 years, the Kawasaki Heavy Industries Group (Kawasaki Group) has honed its technology and expertise through manufacturing in a wide range of fields, including land, sea, and air transportation equipment, energy, plants, and industrial machinery, and has continued to provide products and services that meet the diverse needs of customers around the world in line with the changing times. Furthermore, we have established "Group Vision 2030" as our goal to be achieved by 2030, which declares that we will contribute to the global community by providing innovative solutions that solves future social issues. To this end, we are currently promoting Kawasaki DX (Digital Transformation), an activity to significantly transform our business style and the processes that support it.

On the other hand, the digitalization of operational processes through DX and the introduction of new work styles, such as remote work, have led to a rapid increase in risks from cyberattacks. It has become more important than ever to conduct activities to prevent events, such as the leakage of personal information, corporate information, and the suspension of business systems.
In light of such circumstances, the Kawasaki Group has built a mechanism to strengthen the information security framework of the entire group, with reference to the "Cybersecurity Management Guidelines Ver. 3.0," issued by the Ministry of Economy, Trade and Industry, Japan. We have established a specialized organization to oversee information security activities and monitor cyberattacks 24/7. This structure will allow us to respond quickly to minimize the impact even if an attack occurs. Furthermore, we will provide information security education and training to all employees to improve their knowledge and awareness of information security.

Regarding the product where digitization is progressing, we are also beginning to put our efforts into establishing a product security system. By analyzing and preventing cyber security risks from planning and design phase, we are establishing a system to achieve safe, high-quality product development that continues to address its vulnerabilities throughout its operation.
In addition to creating new solutions to solve social issues, the Kawasaki Group will actively promote to enhance information security as part of our initiatives for a safe and secure society.

Hiroshi Nakatani
Representative Director;
Senior Corporate Executive Officer;
Assistant to the President;
in charge of Technology, Production, Procurement, TQM, General Administration, Digital Transformation (DX) Strategy, and the North America Project Management Task Force;
and General Manager, Corporate Technology Division

Information security policy

Basic information security policy

Direction 1

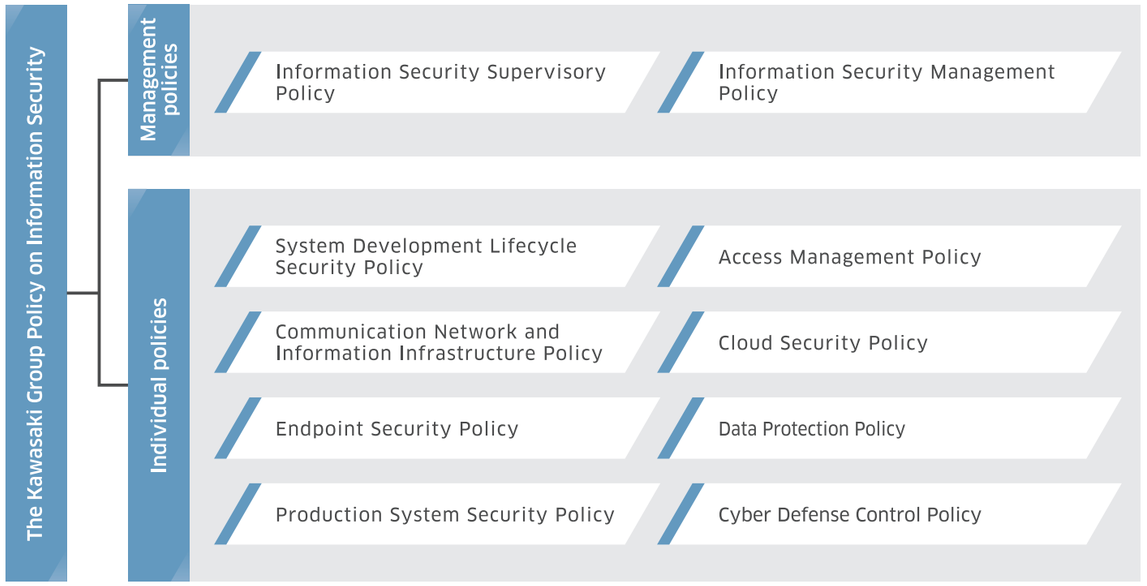
The Kawasaki Group provides products and services for a diverse range of customers, from social infrastructure businesses to general consumers, and any information leakage could affect our credibility and brand value and thereby undermine the foundations of our management. This is why ensuring information security is an important management issue that needs to be consider. In order to protect our business from such management risks, we are working to appropriately manage and protect important information assets, such as information concerning customers, business partners, and company's business. It is our social responsibility to ensure, maintain and improve information security.

The following four principals are the basic idea for our approach to information security. "The Kawasaki Group Policy on Information Security" is established based on these principals, as well as various information security policies and rules which follow world standard such as NIST CSF*.

(1) Build a system to strengthen collaboration across the Kawasaki Group
(2) Identify and manage important information assets
(3) Plan and deploy appropriate measures to identify, defend, detect, respond, and recover from cyberattacks
(4) Ensure all officers and employees improve their knowledge and awareness of information security

* NIST CSF (Cybersecurity Framework): A framework for improving the cybersecurity of a critical infrastructure published by the National Institute of Standards and Technology

The Kawasaki Group information security policy structure



Based on the these policies, Kawasaki Heavy Industries and related companies have established company rules according to each business activity.

The Kawasaki Group Policy on Information Security

○ Compliance with laws and regulations and fulfillment of contractual obligations

The Kawasaki Group will observe laws, ordinances, regulations, and other norms relating to information security, as well as contracts with business partners.

○ Information security management structure

The Kawasaki Group will strive to establish a management system which can be operated continuously as one organization to ensure information security for the purpose of protecting not only the trust, safety, and peace of mind of our customer but also the whole society by implementing appropriate security measures throughout our complex business activities.

○ Implementation of education and training

The Kawasaki Group will continuously conduct education and training on information security required according to the one's duties and promote the entrenchment of policies and awareness raising on information security. In addition, we will implement drills simulating attacks from outside the company, thereby endeavoring to enhance our detection, response, and recovery capabilities against the latest cyber threats.

○ Ongoing improvement of information security management

The Kawasaki Group will formulate an information security strategy and deploy its measures as planned, while conducting internal audits at the same time to inspect and assess the state of management and operation regularly for continuous improvements. In addition, we will endeavor to maintain information security management by collecting, evaluating, and analyzing information on threats to our business and constantly implementing optimum countermeasures. Also, in collaboration with the legal affairs and compliance departments, we will respond firmly to each country's laws and regulations relating to information management and build a system that contributes to the expansion of global business.

○ Incident response

In the event of an information security incident, the Kawasaki Group will respond swiftly to minimize damage, investigate the cause, and take steps to prevent any recurrence. We will endeavor to strengthen our system by setting up a dedicated department in charge of detecting, responding, and recovering from cyberattacks. In the event of a serious information security incident, we will share information with the officer in charge immediately. At the same time, we will promptly report to business partners, related government ministries, and related organizations.

Information security policy

Information security management structure

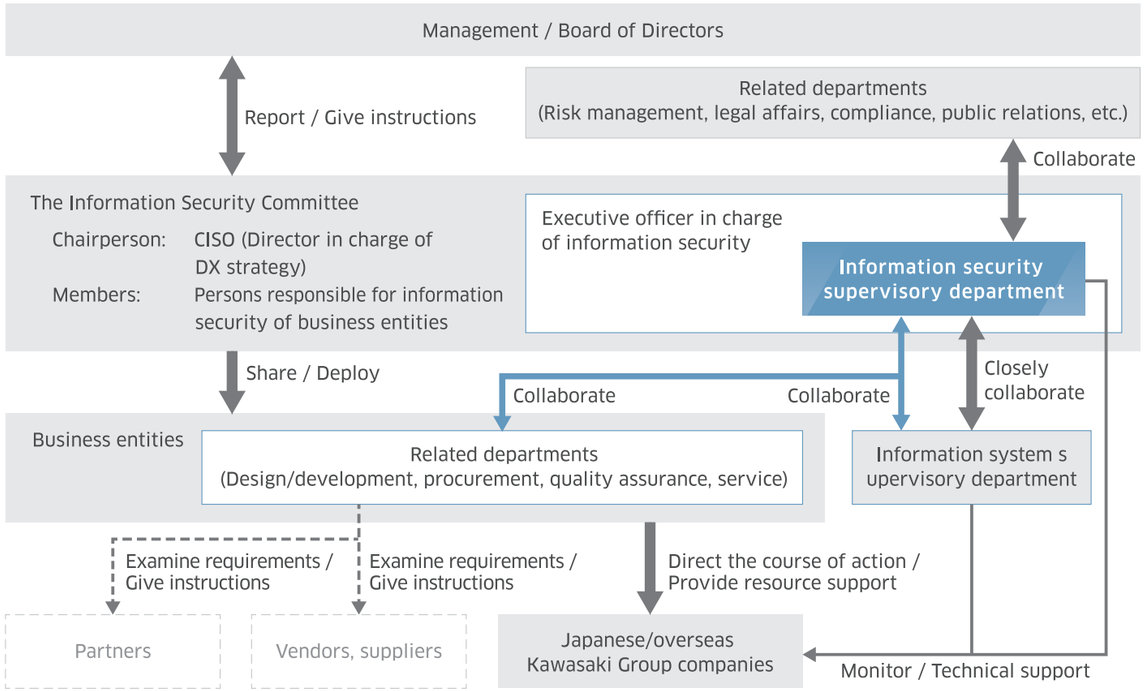
Direction 2 Direction 6

As for our information security management system, the Director in charge of DX strategy takes on the role of CISO. The information security committee is organized as the CISO being the chairperson and the person in charge of information security in each business entities as members. The committee share and deploy policies and plans related to information security and various measures against information security risks to business units, the Kawasaki Group companies, and related organizations.

Also an information security supervisory department is established under the executive officer in charge of information security within the head office. The department will develop information security strategies, identify information security risks, plan and implement measures, conduct audits, and handle information security incidents (detect, address, and recover).

Based on instructions from the Information Security Committee, the information security supervisory department will lead each business entities, the Kawasaki Group companies, and related departments to collaborate with each other and systematically prepare and promote ways to ensure, maintain, and improve information security from the three perspectives of "technical measures," "education / training," and "rules" to address ever-changing information security risks.

Information security management system



Management of Information security risk

Awareness of information security risks

Direction 4

The information on customers and business partners, as well as the Kawasaki Group's confidential information, intellectual property, personal information, and information and production systems that support our business are treated as important information assets throughout the Kawasaki Group's business activities. These information assets are exposed to all kinds of threats, including cyberattacks. For this reason, we consider risks related to information security to be one of the important issues in the foundation that supports our business activities. Cyber threats are evolving day by day, and to minimize the impact on our business activities, we believe it is important that activities to reduce information security risks are commonize within the Kawasaki Group.

Initiatives against information security risks

Direction 3 Direction 4 Direction 10

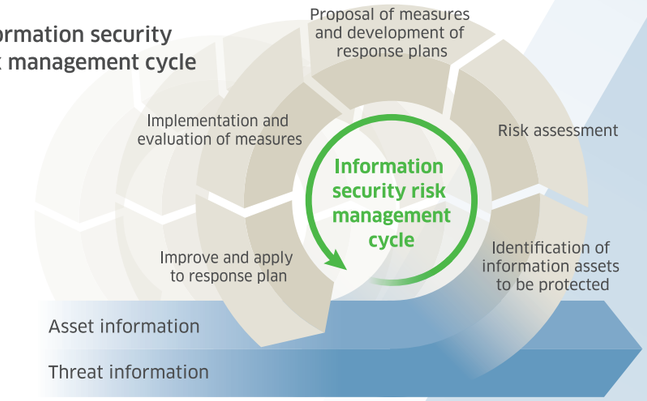
As part of our initiatives to reduce information security risks, we identify the information assets to be protected by the Kawasaki Group and collect threat information on a daily basis from the Information-technology Promotion Agency, Japan (IPA), Japan Computer Emergency Response Team Coordination Center (JPCERT/CC), and other specialized organizations, as well as security vendors, security analysts and other sources, in order to accurately capture increasingly sophisticated cyber threats. Based on the collected threat information, we analyze possible attackers, attack methods, and attack scenarios and identify vulnerabilities. We then conduct periodic assessments to determine whether information assets are protected accordingly from the analyzed or identified threats and vulnerabilities to evaluate risks. Based on the results of the evaluation, we propose the necessary information security measures and develop and implement the risk response plan that includes securing the human resources, budget, and other resources needed to implement the measures. Regarding the effectiveness of information security measures, we evaluate the degree to which initiatives and operational management have taken root by measuring the maturity level of information security management, etc. with reference to various frameworks, such as the NIST CSF.

Continuously improve information security measures

Direction 6

Based on the results of the evaluation, we conduct improvement activities to proactively contain risks before they become apparent by continuously running the PDCA cycle, such as strengthening monitoring of cyber threats, taking countermeasures against vulnerabilities, improving management and operation rules, and incorporating training and education into the risk response plan.

Information security risk management cycle



Implement risk management with reference to the National Institute of Standards and Technology (NIST) Cybersecurity Framework

System and mechanism for responding to information security incidents

System for responding to information security incidents

Direction 7

In order to protect the information of our customers and business partners and the information assets of the Kawasaki Group from cyber threats which is becoming more enhanced and dangerous, we have put in place a system necessary to detect cyber threats and promptly respond to cybersecurity incidents.

We have established a Cyber Defense Center (CSIRT*), which consists of the following three functions, within the information security supervisory department.

Intelligence function

Investigate and analyze cyber threats and support response to cybersecurity incidents

Detection/analysis function

Constantly monitor cyberattacks, and detect and analyze anomalies

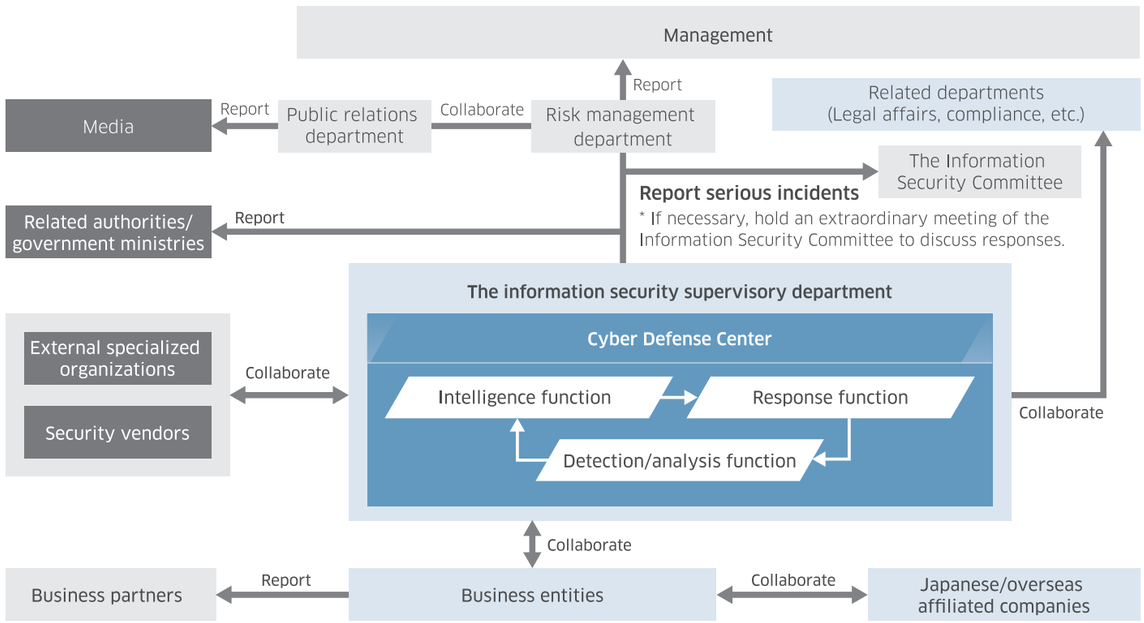
Response function

After detecting an attack, immediately collaborate with parties concerned and take prompt countermeasures to minimize damage

When an incident occurs, a prompt response is essential. To this end, we prepare for the occurrence of incidents by developing a process for responding to incidents and conducting periodic training in cooperation with parties concerned, such as management, the risk management department, and the public relations department.

* CSIRT (Computer Security Incident Response Team): If a security threat incident, such as virus infection, unauthorized access, or denial-of-service attack (DoS attack), occurs in a company's information system or communication network, this team is already aware of the incident and acts as a point of contact within the organization to prevent the spread of damage, collect and notify related information, and develop measures to prevent recurrence.

System for responding to cybersecurity incidents



Mechanism for responding to information security incidents

Direction 5 Direction 7 Direction 8

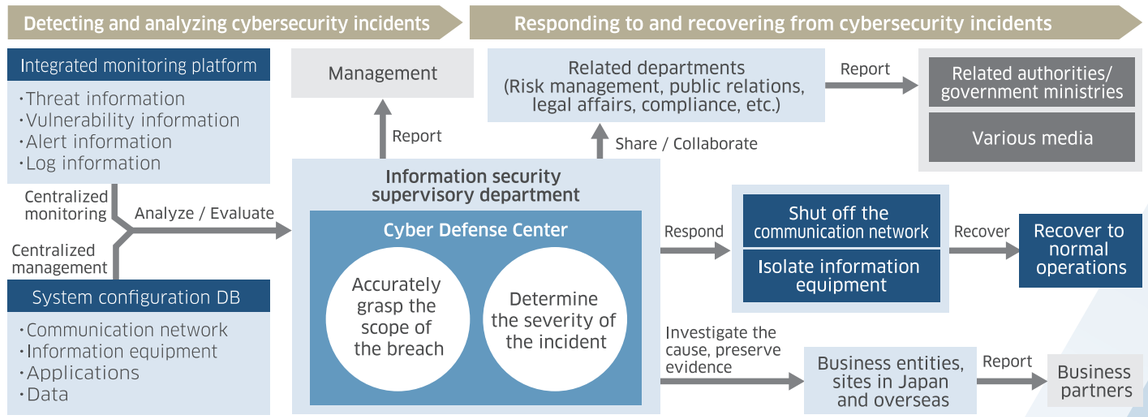
Incident detection and analysis

We will establish a platform that monitors security alerts and various logging data. Managing the configuration data of the information assets in every location as a whole would enables us to understand the scope of the breach. With this management system, we monitor communication networks, information equipment, applications, data, etc. for unauthorized access or abnormal activities on a 24/7 basis. If any incident is detected, we conduct a detailed investigation, identify breached systems or data, and assess the impact on our business activities immediately. Then the information is processed through the defined report route for the purpose of sharing and coordinating with the concerned parties.

Insident response and recovery

If the incident is determined to be a breach after the analysis, further action would be taken to prevent damages to spread, such as shutting off the communication network or isolating information equipment. Then based on the business impact, the area damaged, and so forth, we cooperate with the concerned parties to investigate the cause, preserve evidence, and restore business to normal operations. In the event of a serious incident, we immediately report to management according to the defined route and coordinate with the related departments to give out immediate report to our business partners, related government ministries, and related organizations.

Overview of the process for responding to cybersecurity incidents



Plan preventive measures

To prevent the same incident from happening, necessary reinforcement measures, such as reviewing rules related to information security, improving procedures for responding to incidents, reconfirming the method of collaboration among parties concerned, and changing the settings of information systems and communication networks are taken. These activities become lesson & learn among the concerned parties and leads to the improvement of information security.

Drills for insident response

In preparation for all types of cyberattacks and unauthorized access, we conduct drills regularly involving persons in charge from related departments to confirm the roles, response process, and information sharing method. Specifically, the drills include desk-based confirmation of response procedures and penetration testing (red team testing) that simulates an actual attack on actual equipment to ensure a prompt response and better collaboration. In addition, the know-how accumulated through drills is reflected into the incident response procedures as a feedback to the whole incident process (detect, analyze, response, and recover).

Education and collaboration on information security

Awareness-raising campaign and education/training on information security

Direction 3

Awareness-raising campaign and education/training

We regularly provide all employees with education on information security based on laws, company rules, incident cases, etc., tailored to their respective positions. We also conduct a drill by simulating targeted attack emails to ensure that we do not fall victim to cyberattacks or Internet crimes in our daily work. In FY2022, education on information security was provided to 9,803 employees, and a drill using simulated targeted attack emails was provided to 2,308 employees.
Additionally, we post content related to information security in the Kawaaski Group's newsletter in an effort to raise security awareness throughout the Kawasaki Group.

Duty-specific awareness-raising campaign

Target personnel	Goals	Details
Management	Being able to foster an appropriate crisis awareness among all employees and promote thorough management	Executive education for management
Executives	Being able to accurately identify security risk of the company and take leadership in making improvements	Education for managers based on the latest security trends, etc.
General employees	Being able to take appropriate actions and responses to risks and threats encountered in daily work	Education on information security for general employees based on points to be noted in daily operations, etc. Drill exercises using targeted attack emails
Employees joining the company	Acquiring basic knowledge of information security management	Training for new employees, including new graduates, mid-career employees, and temporary employees

Contents published in the Kawasaki Group's newsletter "Kawasaki"

Cultivating human resources for information security

We provide training since it is essential to have personnel with a high level of expertise in information security to protect the Kawasaki Group's business from cyber threats and ensure the continuity of business activities. We dispatch our personnel to the Information-technology Promotion Agency, Japan (IPA) or external security specialist companies to enable them to gain experience at the forefront of the industry and learn about the latest trends and technologies through interaction with experts from such companies. Moreover, regular training is provided by external security specialist companies in an effort to improve the ability of our personnel to deal with security risks.

In addition to cultivating human resources for security, we also develop medium- to long-term human resource recruitment plans, based on which we implement personnel transfers and recruit new graduates and mid-career workers. In recruiting new graduates, we actively work to secure talents, for example, by offering opportunities to experience actual work through internships.

Initiatives with the Kawasaki Group companies and business partners

Direction 9

Information security measures at the Kawasaki Group companies

The Kawasaki Group companies in Japan have put in place a system to constantly monitor and detect cyberattacks by installing the tools used within the Kawasaki Group for centralized management. They are also working to appropriately encrypt confidential information and important information such as customer information and strictly restrict its access. In addition, our Kawasaki Group companies overseas have been deploying security measures in consideration of the unique characteristics of each region.
As cyber threats become more sophisticated, we have been implementing measures throughout the Kawasaki Group to maintain information security.

Information security measures taken by business partners

Information security measures in the supply chain is also important.
We have prepared guidelines for our business partners to encourage them to work on information security measures and help them tailored to their respective characteristics.

Certification and new initiatives

Acquisition of certification

The Kawasaki Group promotes the acquisition of third-party evaluations and certification relating to information security. The organizations that have acquired certification relating to information security are as follows.

ISMS (ISO/IEC 27001)*-certified organizations

- Kawasaki Heavy Industries, Ltd. (Project Management Department,Presidential Project Management Division)
- BENIC SOLUTION CORPORATION (Infrastructure Design Department/Operation Service Department, Digital Infrastructure Solution Service Division)

CSMS (IEC 62443-2-1)*-certified organization

Kawasaki Heavy Industries, Ltd. (Plant Engineering Business Division, Energy Solution & Marine Engineering Company)

Privacy Mark-certified companies

BENIC SOLUTION CORPORATION

K Career Partners Corporation

*ISMS (ISO 27001) (Information Security Management System): A system to ensure a certain level of confidentiality, integrity, and availability regarding the handling of information within an organization. It refers to overall efforts to define the level of security that should be ensured based on the type of information handled, etc., develop plans and regulations, and reflect them in the operation of information systems as part of the organization's management.

*CSMS (IEC 62443-2-1) (Control Systems Security Management Systems): A cybersecurity management system for industrial automation and control systems

Initiatives for product security and plant security

Initiatives for product security

The Kawasaki Group's products continue to evolve to provide more advanced functions and services by connecting to networks and clouds. On the other hand, the advancement of digitalization has increased the risk of exposure to cyber threats such as cyberattacks. To protect our customer and their business, we prioritize product security as one of the aspects and continue to maintain and improve the quality of the product.

Our initiatives for product security include complying with Japanese and international laws and regulations, standards, and agreements with our customers, as well as establishing the Kawasaki Group Product Security Policy to provide safe and secure products and services by preventing breaches from cyberattacks. In addition, we have developed guidelines to ensure appropriate security in activities throughout the entire product life cycle, from planning, design, and manufacturing to operation of products and services.

We have established a specialized organization (PSIRT*) to oversee activities based on the product security policy, which continuously collects and analyzes information related to product security and strives to improve the quality of our products and services to ensure that there will be no security weaknesses, known as vulnerabilities, in the products and services, thereby enabling the processes related to product security to function properly.

*PSIRT (Product Security Incident Response Team): This team is responsible for such activities as finding vulnerabilities in products, analyzing problems, investigating their severity and impact, providing upgraded or modified versions, notifying or disseminating information to customers and the general public, providing information, responding to inquiries, accepting reports from outside parties, and liaising and coordinating with collaboration partners and related organizations.

The Kawasaki Group Product Security Policy

○Compliance with Laws, Regulations and contracts

In ensuring the cybersecurity of products and services, the Kawasaki Group will thoroughly comply with relevant laws, regulations and rules, other norms, and agreements with customers.

○Product Security Management System

The Kawasaki Group will develop a management system to realize systematic and continuous operations to ensure product security throughout the life cycle of products and services.

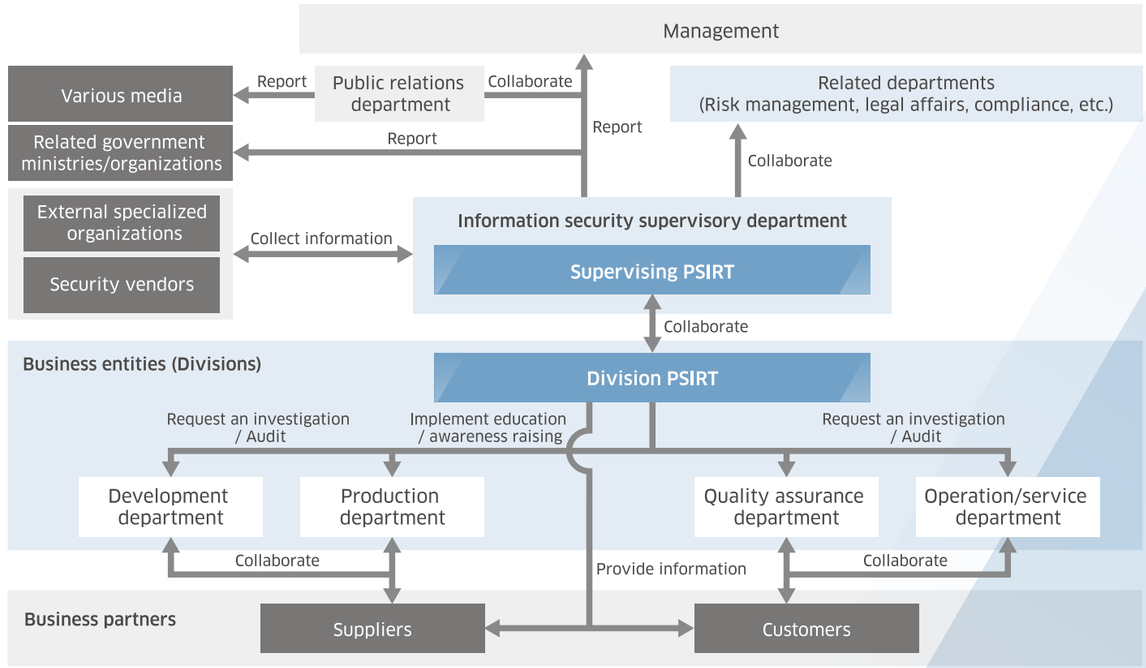
○Promotion of Product Development with Attention to Product Security

At the planning and development stages, the Kawasaki Group will take into account the assets to be protected, such as the safety of products and services, as well as the possibility of cyberattacks against them so that there will be no vulnerabilities in the products and services.

○Promotion of Operations with Attention to Product Security

The Kawasaki Group will continuously collect and analyze information on product security. If any product security issue is found in our products or services, related departments will work together to respond promptly to minimize damage, investigate the cause, and take measures to prevent recurrence so that our customers can use our products and service with confidence. If necessary, the Kawasaki Group will promptly report it to the related government ministries and organizations.

Product security promotion system



Certification and new initiatives

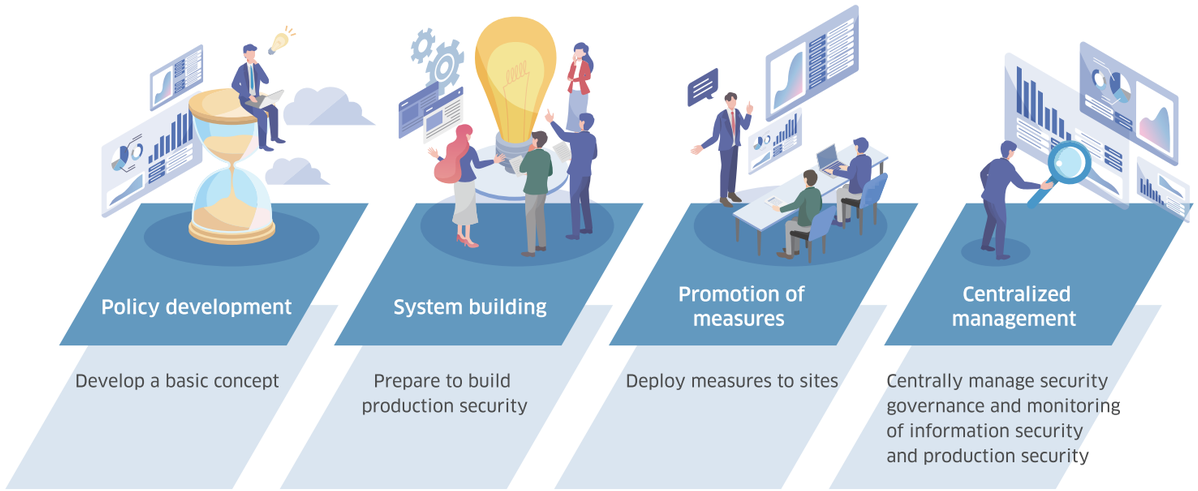
Initiatives for plant security

In recent years, efforts have been made to connect various business systems with production systems/manufacturing equipment through communication networks to accumulate or utilize data for the purpose of improving productivity. As a result, cyber threats to plant production systems have become a major social issue; for example, there have been many cases where the impact of a breach from a cyberattack against a single company in the supply chain has spread in a chain reaction, resulting in a forced production halt.

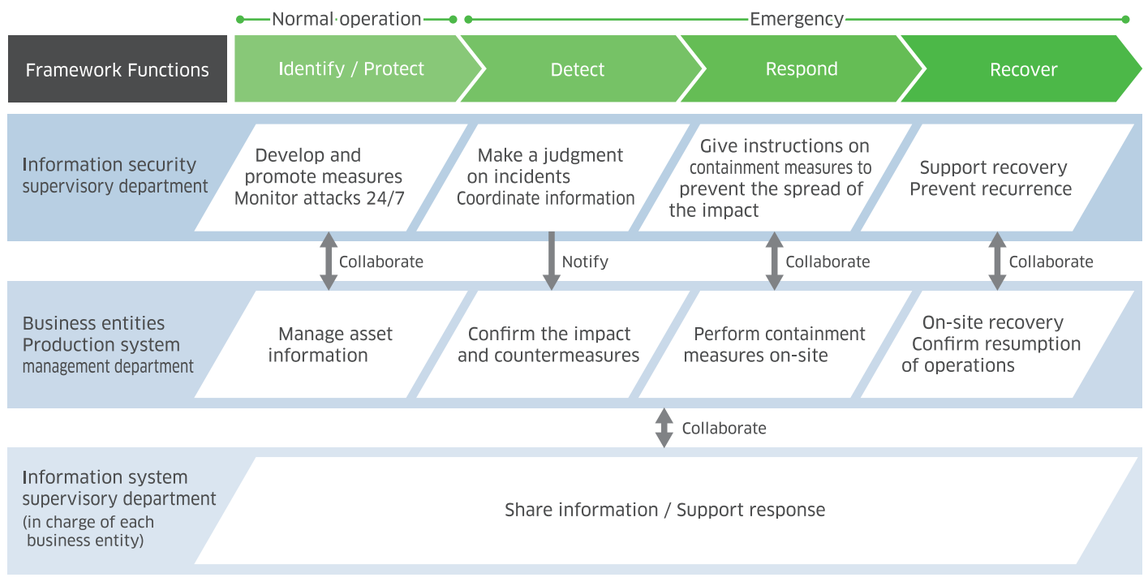
Under these circumstances, the Kawasaki Group has taken measures in line with the international standard CSMS (IEC 62443-2-1) to protect the safety of control systems by strengthening the security of plant production systems and the infrastructure that supports plant operations, with the aim of ensuring the safety of production sites and equipment as well as minimizing the impact on the environment and stabilizing production activities, including the supply chain.

We have developed a management system by developing basic policies for the security of production systems and strengthening collaboration between the production management department and the information security supervisory department. Also we are identifying cyber threats through risk evaluation that are held regularly and taking necessary measures towards those risk, such as minimizing the access to production systems, communication networks within plants, communication networks with external parties, etc. to the minimum necessary. Furthermore, we have been developing a system for responding to cybersecurity incidents immediately and effectively in the event of an emergency.

Status of initiatives for plant production security



Roles and management process in plant production security



Initiatives for industry-academia collaboration

Ensuring information security is an essential element in business activities and is indispensable for forming corporate infrastructure, especially in the industrial world, which handles important information such as corporate secrets related to products and information on customers and business partners. On the other hand, however, it is difficult to secure personnel particularly in the cybersecurity field, among other information security fields.

As part of our efforts to address this issue, the Kawasaki Group cultivates human resources by promoting exchanges through joint research and on-site lectures in the form of industry-academia collaboration to help our personnel learn the latest technologies and knowledge due to the fact that the activities and achievements of academic and research institutions in the cybersecurity field are highly regarded both in Japan and abroad.

In addition, by providing students and researchers with opportunities to experience the Kawasaki Group's actual work related to cyber security in the field, we also contribute to the cultivation of future cybersecurity experts.

Through such mutually beneficial industry-academia collaboration, the Kawasaki Group works to ensure a higher level of information security and cultivate human resources in the cybersecurity field for the future.

Kawasaki Heavy Industries, Ltd.
https://global.kawasaki.com/en/

This report can be accessed using the 2D barcode above

March 2024