

FUJIFILM Holdings Corporation

# Information Security Report



Top Message .....	3	Security Suggestions to Customers .....	11
Information Security Structure .....	4	Information Security of the Fujifilm Group .....	12
Information Security of Products and Services .....	8	Third-party Assessment and Certification/ Overview of the Fujifilm Group .....	18

## Fujifilm Group's Purpose

### Giving our world more smiles

We bring diverse ideas, unique capabilities, and extraordinary people together to change the world.

## DX Vision

The Fujifilm Group has actively taken on DX by utilizing AI and IoT. In 2021, the company has drawn up the "DX Vision" to further promote DX to provide products and services of even greater quality than ever before, thereby dramatically enhance value the Group provides to customers as the company continues to work toward solving social issues.

### Fujifilm Group's "DX Vision"

Fujifilm's relentless pursuit of a better world is entrenched in the Company's commitment to a more sustainable, healthier, and safer future. We are well prepared for taking on the greatest challenges of our time through the use of advanced and digital technology, valuable and innovative products and services, and from the connected contributions of every business, every team, and every individual at Fujifilm.

## Information Security Policy

The Fujifilm Group establishes the Information Security Policy towards the maintenance and improvement of Information Security as one of critical issues in business activities in order to continue to be a reliable corporation under our open, fair and clear corporate culture, and to fulfill our social responsibility.

### 1. Preparation and observance of information security rules

We prepare documents such as regulations and guidelines and ensure that they are fully complied with to follow this Policy, as well as to comply with all applicable laws, and regulations enforced in the regions in which we conduct business.

### 2. Establishment of information security management organization

We clearly define the organization structure and responsibilities to implement information security measures appropriately and reliably. Under our information security management organization, we, as a member of society, appropriately provide information and actively collect information from external information security organizations.

### 3. Information security education

We endeavor to raise awareness through enlightenment, education and training to implement information security measures appropriately and reliably.

### 4. Continuous improvement of information security measures

We review various measures as necessary for continuous improvement based on risk assessments to respond to changes in legal or regulatory requirements and new information security risks such as cyberattacks. We also maintain and improve supply chain security of business partners and other parties.

### 5. Maintenance and protection of information assets

We protect critical information including customer information, information of business partners, and company technical information from threats of leak, falsification, and loss by observing our code of conduct. We endeavor to ensure information security of our products and services to protect customer information. In case of a security incident, we will minimize the impact by a prompt initial response such as the prevention of damage propagation, and taking recurrence prevention measures.

### 6. Compliance with laws and regulations

We comply with information-security-related laws and regulations enforced in the regions in which we conduct business, as well as contracts with customers and business partners.

## Enhancing Information Security, the Very Foundation of Our Efforts to Solve Social Issues

On January 20, 2024, the Fujifilm Group celebrated its 90th anniversary by establishing a new Group's Purpose intent upon "Giving our world more smiles." We will bring more smiles to so many around the world by contributing to the solution of social issues and create innovation by utilizing our diverse resources of "people, knowledge, and technology."

In 2021, the Group formulated and announced its Digital Transformation (DX) Vision, outlining our commitment to continue challenging the task of solving social issues by promoting determined DX and providing better products and services than ever before. However, we have witnessed heightened geopolitical risks around the world in recent years as well as more advanced digital transformations of societies and industries, which have altered the background fabric and increased the risk of information leaks due to cyberattacks. The importance of information security has increased rapidly as a result. Today, ensuring robust information security across the Fujifilm Group is essential to the proper advancement of DX.

In view of these developments, we have positioned information security as an extremely important management issue that directly impacts corporate value, and the topic of information security is discussed at length in Board of Directors' meetings and our ESG Committee. We are also focusing on groupwide information security measures including additional enhancements to our information security governance and the development of products and services that offer customers additional safety and peace of mind.

For instance, to protect against cyberattacks, we are fortifying our FUJIFILM Security Operation Center (FUJIFILM SOC) on a global scale, which detects any signs of an attack at an early stage, as well as our FUJIFILM Cybersecurity Emergency Response/Readiness Team (FUJIFILM CERT) framework, which is designed to minimize the impact and damage caused if an incident does occur. We also utilize security solutions and attentively train employees as part of our tireless effort to strengthen measures against cyberattacks that grow more sophisticated and more ingenious by the day. Meanwhile, we are striving to strengthen comprehensive security by addressing human error, internal fraud, and the various laws and regulations pertaining to information security. On a wider scale, rather than limit our initiatives to the Fujifilm Group, we are also working with our business partners to encourage the adoption of specific security measures across our supply chain. These efforts have been duly recognized, with the Company being awarded the Cyber Index Awards 2023 Grand Prize\* in December 2023.

The Fujifilm Group remains committed to the quest of solving social issues. This report introduces the Group's information security measures that serve as the very foundation upon which this challenge is built. I hope that this report will prove useful to you all.

\*Please see the Topics section on P.19 for more details.



**Teiichi Goto**

President and Chief Executive Officer,  
FUJIFILM Holdings Corporation

# 1

## Information Security Structure

### Information security governance

The Fujifilm Group conducts group business under the leadership of the holding company, FUJIFILM Holdings Corporation, and consists of FUJIFILM Corporation and FUJIFILM Business Innovation Corporation, which are operating companies, as well as other companies, including affiliated companies. (For details, see "Overview of the Fujifilm Group" on page 19.)

The Fujifilm Group implements various information security activities to allow our customers to rest assured when using our products and services. This section describes the Fujifilm Group's policy regarding information security and the governance structure.

#### Fujifilm Group's policy of information security

The Fujifilm Group considers ESG (Environment, Society, and Governance) an important agenda in business, and we conduct information security activities as an important element of ESG.

Since its establishment, the Fujifilm Group has been creating innovations that meet the changes of the times and the needs of society and making reforms to its business portfolio. These business reforms increased our opportunities for handling not only the Group's technological information, but also being entrusted with important information of the customers in the domain of healthcare, such as medical systems and biologics contract development and manufacturing organization, and in the domain of business innovation, which focuses on IT-enabled solution services. Accordingly, the importance of information security is becoming even greater.

Also, the strengthening of global information security governance is required due to the globalization of our businesses and expansion of sales around the world.

#### Structure for promoting information security

The Fujifilm Group has a dedicated corporate information security governance structure, led by the officer responsible for the ESG Division of FUJIFILM Holdings Corporation (hereafter, the ESG Division), who is appointed Corporate Information Security Governance Officer, and Corporate ICT Security Control Organization, led by the officer responsible for the ICT Strategy Division of FUJIFILM Holdings Corporation (hereafter, the ICT Division), who is appointed Corporate ICT Security Officer. The organization that governs information security for all companies has qualified professionals, such as Registered Information Security Specialists, to implement measures to reduce risks that may arise from external threats such as cybersecurity and internal threats such as errors and misconduct, as well as from responding to the Personal Information Protection Law and other information security laws.

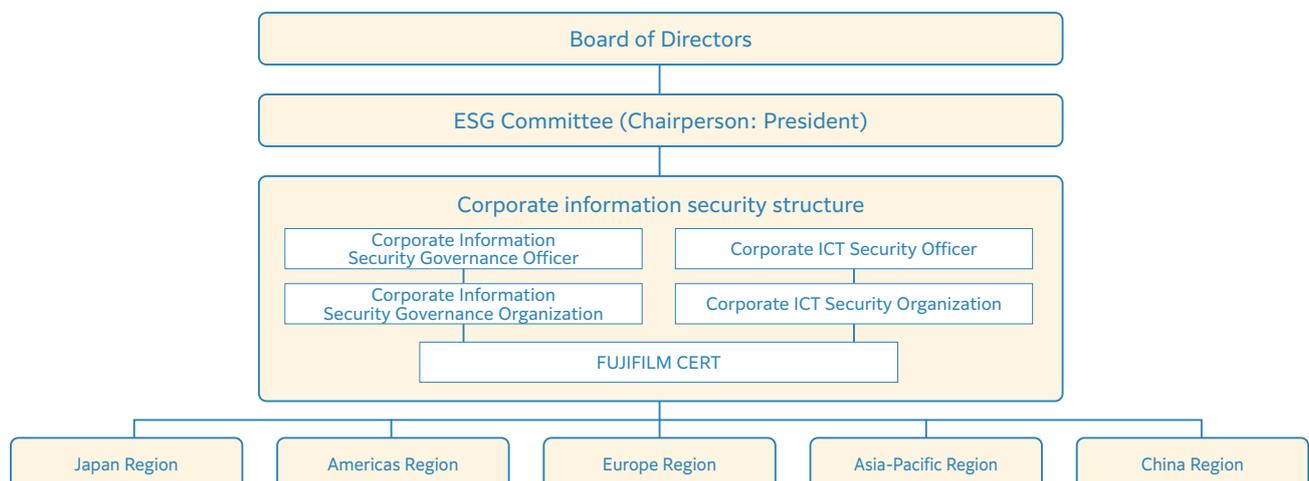
To carry out information security governance, we engage in efforts to strengthen our abilities to deal with management measures for the Identify, Protect, Detect, Respond, and Recover phases by referencing global standards, such as NIST Cybersecurity Framework and NIST SP800-171, in order to heighten our response to the threat of cyberattacks, in addition to conducting information security management based on ISO/IEC 27001 (ISMS).

As part of our cybersecurity measures, our Computer Security Incident Response Team (CSIRT\*<sup>1</sup>), named FUJIFILM CERT\*<sup>2</sup>, has been set up to be prepared for possible attacks on company IT infrastructures, products, services, and factory information systems.

\*1 Computer Security Incident Response Team

\*2 FUJIFILM Cybersecurity Incident Response/Readiness Team

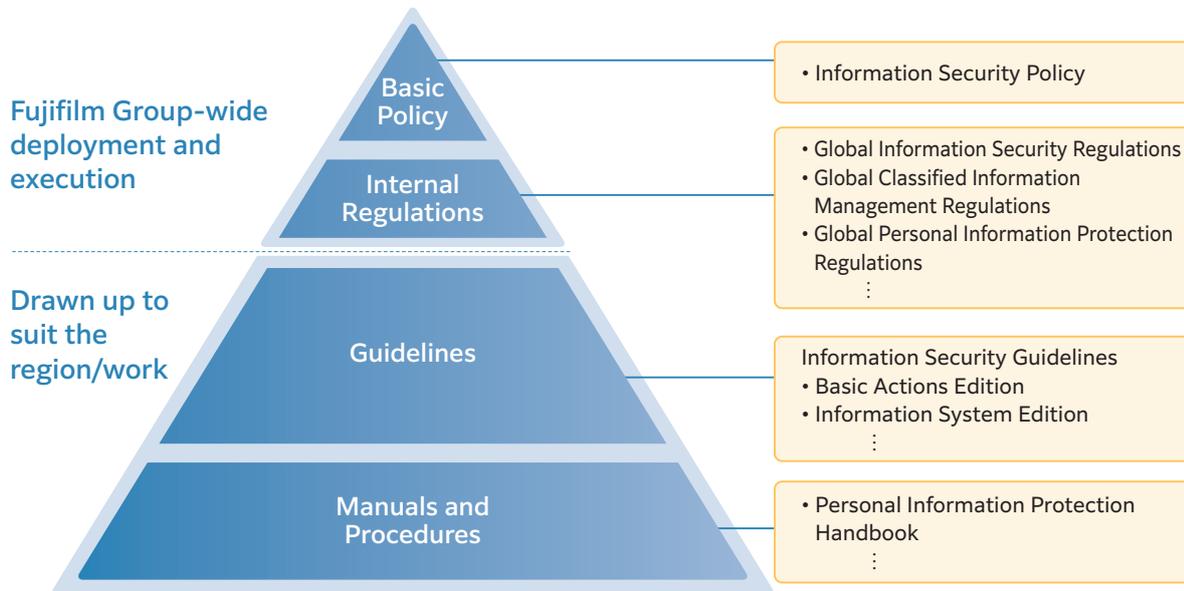
#### FUJIFILM Holdings information security structure



## System of information security rules

The Fujifilm Group has established rules related to information security from various viewpoints, including the categorization of information confidentiality, compliance, and information ethics. These rules are made up of "Basic Policy" (sets forth the Fujifilm Group's stance on information security and is made known inside as well as outside the Group) "Regulations" (stipulates the basic rules), "Guidelines" (lays out specific management

measures), and "Manuals and explanatory document." A common set of "Basic policy" and "Regulations" are deployed throughout the Group, including all overseas regions, while the "Guidelines" and other rules that are deployed are individualized to suit each region's environment and business. Furthermore, all of the information security rules are reviewed and updated to adapt to the circumstances.



## Response to information security incidents and preventive measures

The Fujifilm Group endeavors to prevent incidents through the exhaustive implementation of information security rules and various management measures. However, even if the best preventive measures are implemented, we cannot assume that information security incidents will not occur.

For this purpose, we set up a central contact point for accepting information security incident reports of cyberattacks and other incidents. When information security incidents are detected in any of the divisions of the Group, this information is grasped by the person in charge in the division where the incident occurred and collected by the organization overseeing security. The organization overseeing security shares the information with relevant organizations according to its content and promptly initiates the response to minimize the impact while considering and implementing preventive measures for recurrence.

Should the information security incident that occurred be an urgent and important matter, it is immediately reported to the President, the Corporate Information Security Governance Officer, and the Corporate ICT Security Officer. After that, if a company-wide response is required, the Total Risk Management Committee chaired by the President is set up as a subcommittee of the ESG Committee, to take measures aimed at minimizing damage.

Incident information requiring such responses is periodically reported to the ESG Committee and the Board of Directors. Moreover, once every year, each organization carries out activities to extract risks. In these activities, risks related to information security are also extracted based on the occurrence of the security incidents. The ESG Division collects and evaluates the results and determines important risk themes to be addressed by the entire Group, implement countermeasures to prevent the occurrence as well as the recurrence of information security incidents.



## Cybersecurity

### Fujifilm Group activities to respond to cyberattacks

With products and services provided in Japan and other countries around the world, the Fujifilm Group considers cyberattack response as important global business agenda. In order to provide products and services to customers safely and continue business stability, the Fujifilm Group organizes and operates a FUJIFILM CERT that functions as the Computer Security Incident Response Team (CSIRT). The CERT, which is a dedicated cybersecurity organization responsible for the early detection of cyberattacks and the minimization of damage in case of cyberattacks.

### Structure of FUJIFILM CERT

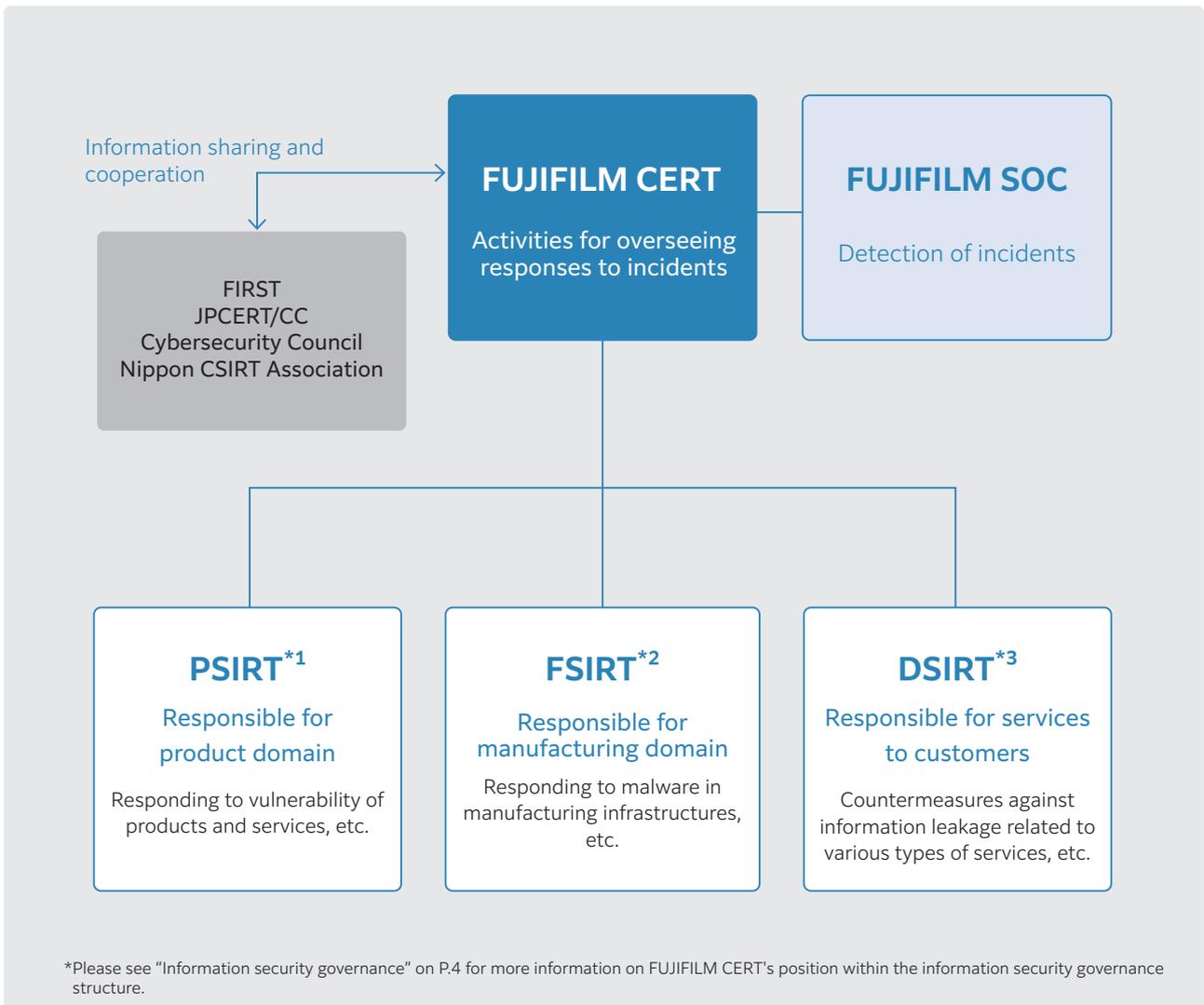
FUJIFILM CERT operates as a cross-organizational body that encompasses affiliate companies and organizations of the Fujifilm Group. FUJIFILM CERT has its secretariat in the Corporate Information Security Organization of FUJIFILM Holdings Corporation, and oversees the cooperated

activities of PSIRT (Product SIRT), which is responsible for the domain of products of various companies, including overseas sites of the Fujifilm Group; FSIRT (Factory SIRT), which is responsible for the domain of manufacturing; and DSIRT (Digital service SIRT), which is responsible for the domain of services for customers. FUJIFILM CERT also cooperates with FUJIFILM SOC (Security Operation Center), which monitors IT infrastructures of the entire Fujifilm Group for cyberattacks and internal suspicious behaviors, 24 hours a day, 365 days a year, to detect and respond to incidents at an early stage.

Furthermore, in addition to establishing in-house points of contact for reporting incidents, FUJIFILM CERT has set up a point of contact for outside sources (indicated below) to receive reporting of vulnerability, threats, and other information from external security institutions and good faith whistleblowers.

Contact point: [fujifilm-cert@fujifilm.com](mailto:fujifilm-cert@fujifilm.com) (FUJIFILM CERT)

### Organization of FUJIFILM CERT



\*1 Product Security Incident Response Team \*2 Factory Security Incident Response Team \*3 Digital service Security Incident Response Team

## Activities of FUJIFILM CERT

FUJIFILM CERT provides activities listed below to all affiliate companies of the Fujifilm Group. Furthermore, in line with the organization and division of roles, as defined in CSIRT documents, FUJIFILM CERT responds to incidents and makes continuous improvements daily while sharing information with members at regular meetings.

Type of activity	Activity overview
Threat intelligence	<ul style="list-style-type: none"> <li>● Cybersecurity assessment (threat and risk analysis based on the investigation of the company network configuration, websites for public access, and the usage condition of external cloud platforms) of the entire Fujifilm Group</li> <li>● Collection and analysis of threat information from external sources (Cybersecurity Council, JPCERT/CC, FIRST, etc.) and FUJIFILM SOC</li> </ul>
Incident handling	<ul style="list-style-type: none"> <li>● Preparation of escalation structure and incident response support in anticipation of the occurrence of cybersecurity incidents</li> <li>● Prevention of suspicious activities such as taking information outside without permission in cooperation with FUJIFILM SOC monitoring</li> </ul>
Vulnerability handling	<ul style="list-style-type: none"> <li>● Response to information security vulnerabilities in products and services provided by the Fujifilm Group (registration of product developers to JPCERT/CC, and response based on the information security early-warning partnership led by PSIRT)</li> <li>● Investigation of impact on the business IT infrastructure based on threat and vulnerability information, and taking actions</li> </ul>
Preventive actions	<ul style="list-style-type: none"> <li>● Strengthening of the security of the manufacturing site network (FSIRT)</li> <li>● Vulnerability assessment of public access websites (PSIRT and DSIRT)</li> <li>● Operation of secure design and development processes (PSIRT)</li> <li>● Security measures for all cloud services (DSIRT)</li> <li>● Prevention activities for internal misconduct, such as removal of information, in cooperation with monitoring activities by FUJIFILM SOC</li> </ul>
Enlightenment, education, and training	<ul style="list-style-type: none"> <li>● Periodically issue activity reports within FUJIFILM CERT</li> <li>● Training for all employees on handling suspicious email</li> <li>● Initial response training for members, including top management, anticipating the occurrence of incidents</li> <li>● Cyber exercises for CSIRT and administrators of public access websites</li> </ul>

## Collaboration with external security institutions

FUJIFILM CERT is conducting its activities as a member of the following external security institutions.

### FIRST

Forum of Incident Response and Security Teams (FIRST) is the international community of CSIRT, with companies and organizations from countries all over the world as members. FUJIFILM CERT joined FIRST in 2015 to build a relationship of trust internationally with different CSIRTs and facilitate smooth information sharing and collaboration.

### JPCERT/CC

JPCERT Coordination Center is an organization that accepts reports related to computer security incidents, such as occurrences of intrusion or interference with service via the internet, supports responses, grasps the situation around occurrences, analyzes methods, and investigates and offers advice on recurrence prevention measures from a technological standpoint. FUJIFILM CERT, too, makes use of the early warning system provided by this organization in dealing with cybersecurity.

### Cybersecurity Council

The Cybersecurity Council was established in response to The Basic Act on Cybersecurity, and is run by the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) and the JPCERT Coordination Center (JPCERT/CC). The objective of the Council is the prompt sharing of information that is necessary to ensure cybersecurity against information security threats and attacks at the earliest possible stage. The company has taken part in the Council since 2019.

### Nippon CSIRT Association

Nippon CSIRT Association is a CSIRT community with over 400 members of domestic companies and organizations. Today, as an administrative member of the association, FUJIFILM CERT contributes through its active participation in association activities (such as the working group for cyber exercises).

# 2

## Information Security of Products and Services

### Security of medical products

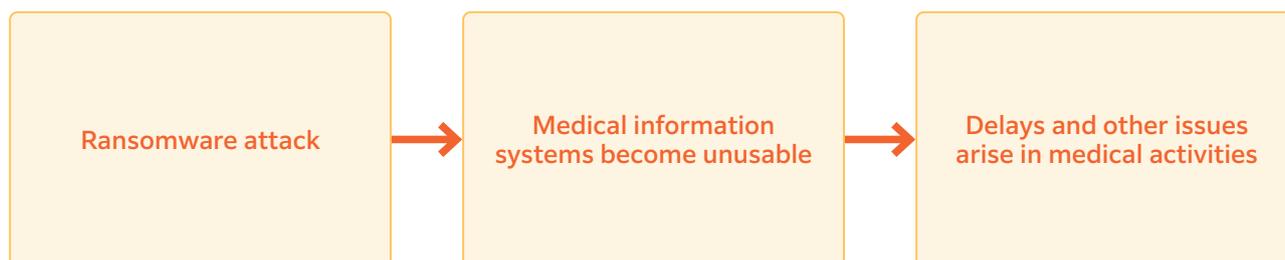
#### Cyber risks of medical information systems

Ransomware attacks, which illegally encode data and demand ransom as a condition for decoding, have been increasing significantly since 2020, and attacks on medical institutions associated with it have also been increasing. Medical institutions infected by ransomware are exposed to the risks of their medical information systems (including medical equipment) being unavailable, causing delays in medical treatment and testing, and resulting in even more serious consequences, such as being forced to transport patients to other facilities. System recovery may take months in some cases.

The reasons that medical institutions are prone to be targeted for ransomware attacks are: (1) they maintain vast volumes of sensitive information, such as patients' personal information and medical records, making them vulnerable to demands for ransom money; (2) medical information systems tend to be used for a long period of time, often exceeding the support period for OS used by the system, which are making these systems vulnerable.

In Japan, in particular, it has been reported that more than 70 percent of ransomware intrusions are caused by VPN devices\*1.

#### Risks that ransomware poses to medical institutions



#### Trends in medical devices cybersecurity regulations

With regard to cybersecurity for medical devices, the Food and Drug Administration (FDA) of the United States has been actively involved from early on, issuing guidance, and demanding comprehensive security measures from product design to after-sales management. At the end of 2022, the FD&C Law\*2 was revised, making the securing of cybersecurity for medical devices a regulatory requirement.

In Europe, cybersecurity requirements have been incorporated in the Medical Device Regulation (MDR) and In Vitro Diagnostic Medical Device Regulation (IVDR), and in 2019, Europe's Medical Device Coordination Group (MDCG) issued the Medical Device Cybersecurity Guidance to supplement regulatory requirements.

In March 2020, the International Medical Device Regulators Forum (IMDRF), which is engaged in activities aimed at coordinating the medical device regulations of various countries, released the Principles and Practices for Medical Device Cybersecurity. This guidance notes the importance of the timely sharing of information related to product security among stakeholders, including the government,

medical device manufacturers and vendors, medical institutions, and healthcare workers. It also mentions points to consider as best practices before and after sales. Regulatory authorities around the world, including Japan, have issued guidance for introducing the guidance put forth by IMDRF in their own countries.

In December 2021, IEC 81001-5-1, an international standard regarding cybersecurity for healthcare software including medical devices, was issued. This standard regulates activities that manufacturers should carry out throughout the product life cycle, from design to post-marketing and disposal, and includes many points that align with the regulatory requirements of the United States and Europe. In Japan, cybersecurity requirements have been added to the basic requirement standards for medical devices under the Pharmaceutical and Medical Devices Act, mandating a response in accordance with JIS T 81001-5-1 to ensure conformance with these requirements.

\*1 Reference: Publicity release issued by National Police Agency "State of Threat Involving Cyberspace in the First Half of 2023"

\*2 Federal Food, Drug, and Cosmetic Act

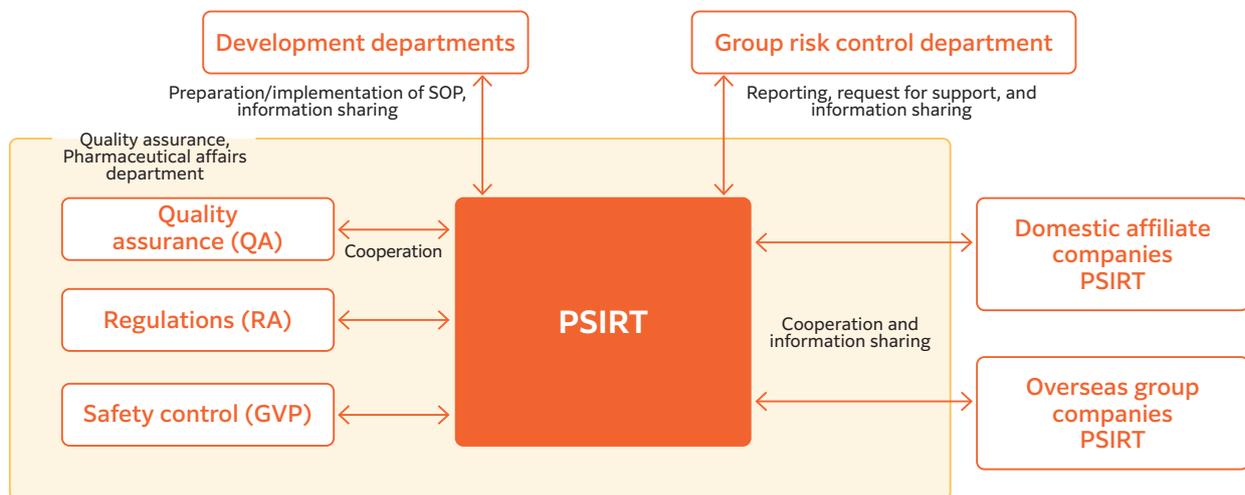
## ■ FUJIFILM efforts for product security for medical devices

FUJIFILM launched Product Security Incident Response Teams (PSIRT) in April 2019 to appropriately respond to requirements to strengthen security regulations by regulating authorities of various countries and ensure the security of medical products and services provided to customers. PSIRT primarily has five roles as described below.

- (1) Promotion of responses to laws, regulations, and standards of various countries
- (2) Promotion of response to product vulnerabilities
- (3) Promotion of responses to product information security incidents
- (4) Information disclosure to external parties
- (5) Promotion of maintenance and expansion of acquisition of ISO/IEC 27001 certification

Since it was established, PSIRT has been expanding its operations in stages, including dealing with product vulnerabilities and disclosing information to the outside, and has been engaging in efforts to prepare and implement standard operating procedures (SOP) for development and management processes necessary to meet the requirements of standards and laws and regulations of each country. Today, PSIRT continues to engage in efforts to prepare responses and improve processes that are mindful of the latest trends. Furthermore, in June 2021, FUJIFILM acquired ISO/IEC 27001 certification, the international standard related to information security management systems, and is continuing its efforts to expand subject fields.

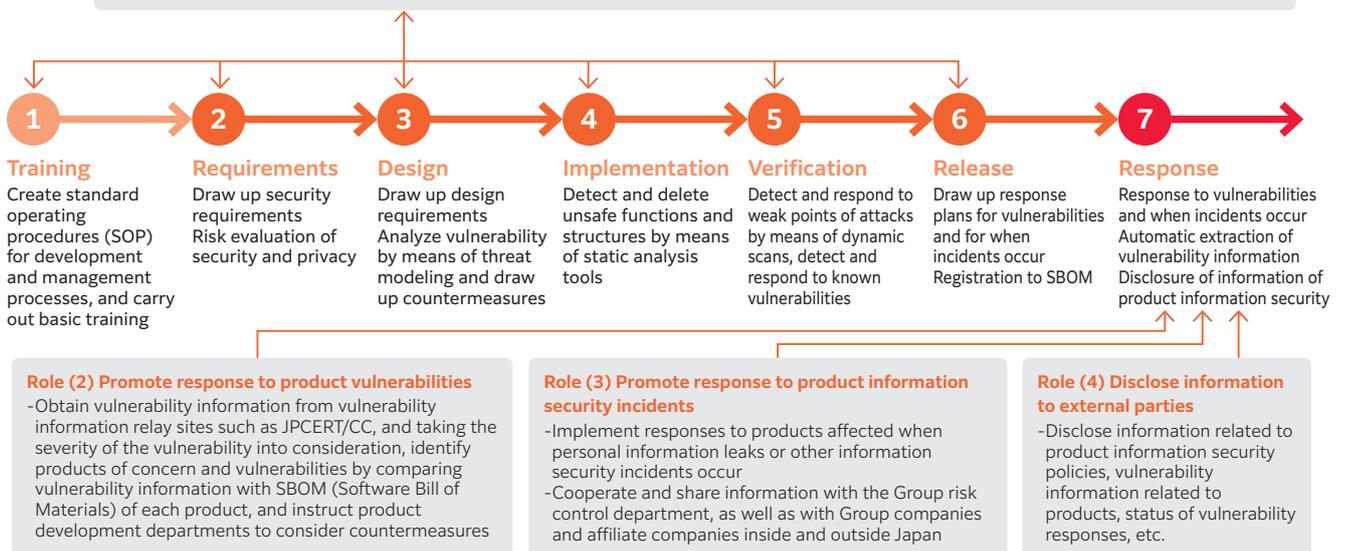
### ■ Diagram of organizational cooperation led by PSIRT



### ■ Main tasks of PSIRT and security management processes of FUJIFILM's medical devices

#### Role (1) Promote response to laws and regulations, as well as standards of various countries

- Monitor trends in technologies for product information security measures, as well as in related standards and laws inside and outside Japan, and disseminate information to planning and development departments.
- Prepare and provide training for development and management processes (SOP) in order to cope with standards as well as laws and regulations.
- Examine risk assessment methods, analyze vulnerabilities, and evaluate, select, and implement security test tools.



Product security information is disclosed at the official site. <https://www.fujifilm.com/jp/ja/healthcare/security-information> (JAPANESE ONLY)

## Security of multifunction machines

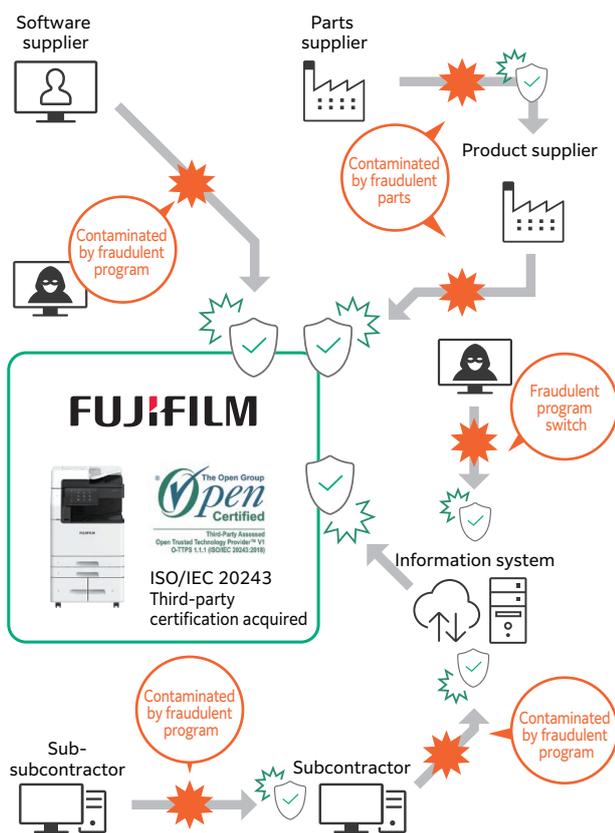
As multifunction machines are information devices that handle data, which are important information assets of customers using multifunction machines in various environments, protecting the customers' data is an important issue. Moreover, with cyberattacks becoming more advanced and sophisticated day by day, we believe that the speed at which unauthorized access to data and intrusion into multifunction machines are detected and addressed for later recovery is crucial for ensuring the continuity of the customer's business.

In order to solve the customer's security issues, FUJIFILM Business Innovation not only provides various types of security functions, but also strives to reduce security risks over the entire supply chain. The acquisition of security certification enables us to provide customers all over the world with products they can use with peace of mind.

### Efforts for supply chain security and acquisition of ISO/IEC 20243 certification

In recent years, there has been an increase in "supply chain attacks," in which the information systems of targeted companies are attacked by fraudulent parts or programs contaminated with malware or the like being planted in the development or manufacturing process of products. FUJIFILM Business Innovation is undertaking activities to ensure the transparency of the supply chain and raise the trustworthiness and safety of its products, and is striving to prevent contamination by counterfeit items in the overall development and manufacturing processes.

In July 2024, the company acquired the international standard ISO/IEC 20243 third-party certification. This certification is a standard for the handling of risks of switching or contamination by fraudulent parts or programs, or infiltration of counterfeit products in the supply chain



(development, procurement, manufacturing, sales, distribution, maintenance, and disposal of products by suppliers, subcontractors, and the company itself). Certification of this standard confirms that measures against security risks of the overall product supply chain have been taken. Through these efforts, we are able to ensure that our products can be used safely and with peace of mind throughout their life cycle.

### Policies for security measures for multifunction machines

In the United States, SP800-171 and SP800-172, set forth by the National Institute of Standards and Technology (NIST), are applied as security guidelines for defense and government procurement, and the scope of the application of these guidelines is expanding into industries, including the automobile industry. The Japanese government is also considering the introduction of the abovementioned guidelines for procurement in defense and other fields.

FUJIFILM Business Innovation has been working to conform to NIST SP800-171 and SP800-172 by implementing security measures for multifunction machines from the five perspectives of "Identify," "Protect," "Detect," "Respond," and "Recovery," resulting in the company being given an "AAAs," the highest possible ranking, from an information security rating institution for its conformity to the guidelines.

### Antivirus measures for multifunction machines

We have set up countermeasures against the threat of the legitimate software of a multifunction machine being tampered with by means of intrusion of a multifunction machine by a virus or unauthorized access by exploitation of a vulnerability. The countermeasures include "a tampering at startup detection function," which checks for unauthorized access when the multifunction machine is starting up and restores the software if any tampering is detected; and "a tampering prevention during operation function," which prevents the execution of fraudulent applications by means of white-list monitoring.

### Early detection of security threats

Events such as security settings of a multifunction machine, change of the certificate, log-in or log-out of the user, and job runs can be sent to an external server on a real-time basis as an audit log. Connecting multifunction machines with a SIEM\* product enables the central control and analysis of multifunction machine audit logs, making possible early detection of incidents that can pose a security threat.

\*Security Information and Event Management (SIEM) is a security software product or service that accumulates and manages operation logs of devices and software at a central location for early detection and analysis of security threat incidents.

### Security certification of multifunction machines

To ensure the validity and reliability of the security functions of multifunction machines, FUJIFILM Business Innovation has acquired the certification of international security standard ISO/IEC 15408 (Common Criteria Certification), which satisfies the security requirement of digital multifunction machines: Protection Profile for Hardcopy Devices V1.0 (HCD PP v1.0). Furthermore, multifunction machines of FUJIFILM Business Innovation have passed the BLI Security Validation Testing (Device Penetration Assessment) of Keypoint Intelligence based in the United States.

# 3

## Security Suggestions to Customers

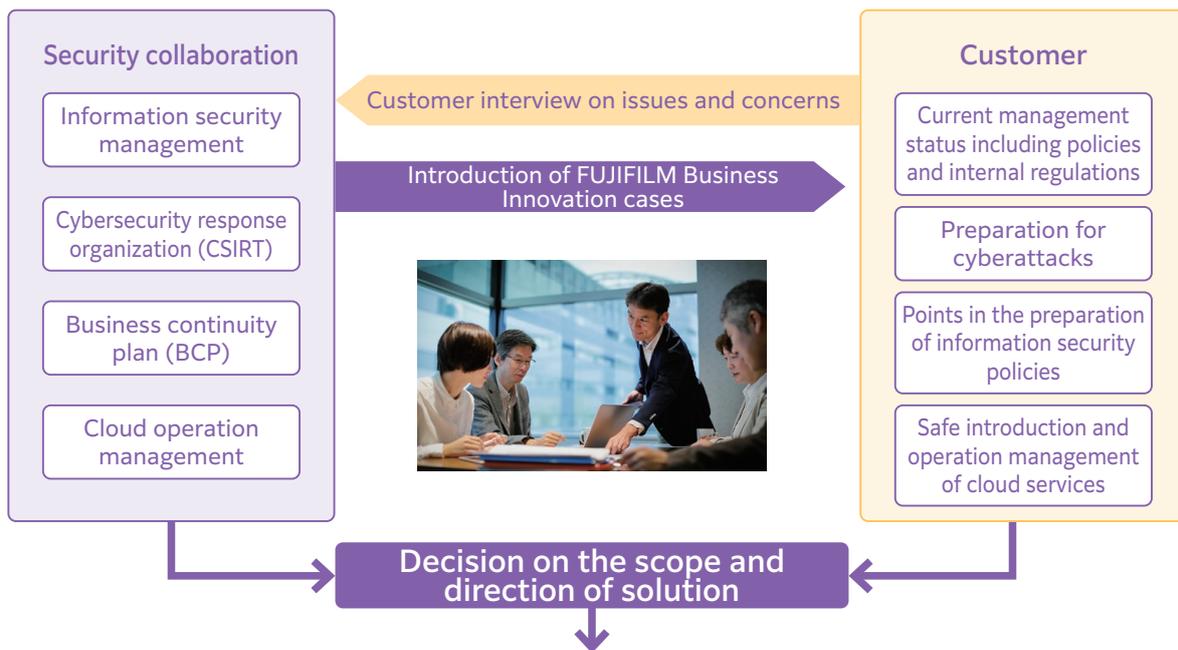
### Solution of information security issues by FUJIFILM Business Innovation Cases for Customer Collaboration

FUJIFILM Business Innovation has acquired ISO/IEC 27001 certification, the international standard of information security management systems. In carrying out its information security activities, the company not only conforms with ISO/IEC 27001, but also references NIST SP800-171. FUJIFILM Business Innovation has been accumulating substantial technical knowledge regarding issues that are faced when carrying out such activities and methods for rectifying such issues. This knowledge is used not only within the company but also in the FUJIFILM Business Innovation Cases for Customer Collaboration, where concrete directions for solving the respective issues of customers are introduced. For the collaboration sessions, major issues faced by companies when implementing measures for information security are compiled into a menu. With

this menu of key issues, FUJIFILM Business Innovation collaborates with individual customers to investigate and analyze the actual state of their issues, which differ in scale and depth depending on the company, to find the direction for solving the issue. The contents of the collaboration sessions are ideal, especially for members of top management, who are responsible for information security.

Moreover, the information security booth that has been permanently set up in the Toyosu showroom in Koto-ku, Tokyo, is equipped with functions that offer a hands-on experience of the risks and the latest solutions for dealing with malware and other problems, based on the ever-changing threats to information security, providing visitors with concrete images of how issues are resolved.

#### Overview of FUJIFILM Business Innovation Cases for Customer Collaboration



#### Hands-on experience of the information security risks and the latest solutions

##### Toyosu showroom

##### Bridge for Innovation

Live Security Tokyo (information security of new era)

##### Main features

- (1) Introduce information concerning latest security
- (2) Propose hints for solutions according to customer issues
- (3) Contents of exhibit are hands-on and visually easy to understand



Ransomware infection experiencing corner, password cracking experiencing corner, etc.

\*Exhibition contents may change

# 4

## Information Security of the Fujifilm Group

### Information security measures of the Fujifilm Group

Based on the idea of information security basic policies, the Fujifilm Group properly protects and controls information assets through various information security measures from the standpoint of human and organizational measures, physical measures, and technical measures.

#### Three aspects of information security measures

\*Photos are for illustrative purposes only. This is not an actual scene.  
Please note that some measures are only implemented in Japan.

##### Human and organizational measures

- Preparation/maintenance of internal regulations and guidelines related to information security
- Delivery of a handbook explaining rules and educational material on incident cases
- Information security governance by information security officers/risk managers selected from each companies and departments
- Periodic training courses on information security and personal data protection
- Information security training courses for different layers of the organizational hierarchy, such as new employee training and manager training
- Report promptly and without fail when information security incidents are discovered
- Cybersecurity training for top management and FUJIFILM CERT
- Training for employees on handling suspicious email
- Information security investigation of suppliers/subcontractors
- Prepare an initial response manual in anticipation of emergency



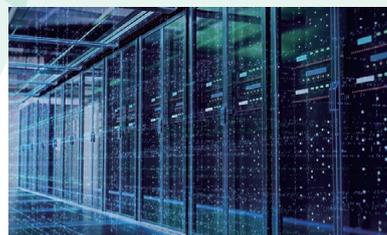
##### Technical measures

- Individual user account access control to servers and systems
- Acquisition and management of logs of computer operations of employees
- Control and log management of data export to unregistered devices such as personal devices
- Monitoring for unauthorized data being taken outside
- Remote deletion of files in PCs in case of loss or theft
- Smartphone usage management
- Monitoring of communication over the Internet (web access and exchange of emails)
- Encryption of the entire hard disk of PC
- Web content filtering to prevent access to malicious sites and sites of prohibited categories
- IC card authentication when printing out documents
- Embedding a copy prohibition code when printing confidential documents
- Monitoring and disconnection of unauthorized communication
- Information management regarding network vulnerabilities
- Encryption of document files
- Detection, monitoring and eradication measures based on anticipation of intrusion



##### Physical measures

- Entry/exit control using employee ID badges (IC cards) at major business locations
- Securing computers with wire locks or locked storage
- Attaching straps to USB flash drives
- Measures for high-security areas (setting up zoning, monitoring with cameras, prohibition of personal devices carried in)
- Locking control and key management of cabinets that store confidential documents
- Sanitization (safe disposal) of information devices at the end of their use



## Supply chain security

As cyberattacks in recent years have become more advanced and sophisticated, the scope of their impact has spread throughout the supply chain. The information security carried out by companies has gone beyond the phase of "focusing solely on strengthening the security of the company itself." What is needed now is the building and strengthening of an information security system that takes into consideration the entire supply chain.

The Fujifilm Group carries out its business activities with the support of many partner companies, including suppliers that supply and deliver parts and raw materials necessary for manufacturing our products, as well as subcontractors to which we outsource various work, such as product development and company administrative work. Should a partner company that is a part of the supply chain be breached by a cyberattack, it could lead to manufacturing and supply risks of our company, as well as risk of leakage of confidential or personal information that has been entrusted to the partner company. For this reason, we maintain a close collaboration with our partner companies and endeavor to provide our customers with a sense of safety and security regarding information security as a part of the quality we provide. Moreover, when consigning work, we regard not only the subcontractor but also the companies that are involved further down the line to be within the scope of management by the respective companies of the Fujifilm Group, in order to ensure and strengthen the information security of the entire supply chain.

### Initiatives to strengthen the information security of suppliers

The Fujifilm Group has drawn up information security requirements for suppliers, and carries out information security investigations based on designated processes to verify the status of suppliers' basic handling of information security.

The information security investigation of suppliers is carried out by using web system etc., and the results of the investigation are fed back to each supplier in the form of a report, enabling suppliers to confirm their own handling status as well as that of other suppliers.

Furthermore, if the results of the information security investigation show a security issue for which countermeasures are found to be insufficient, the report provides an explanation on the risks arising from continuing operations without implementing countermeasures, as well as methods for counteracting the issue. Moreover, activities to raise awareness are being carried forward to increase the level of awareness for security over the entire supply chain through communications with suppliers, such as holding study sessions and other activities regarding cybersecurity countermeasures.

### Strengthening of subcontractor audit

Triggered by an incident of a large-scale leakage of personal information that occurred in another company's subcontractor, FUJIFILM Business Innovation has been conducting security investigations of partner company to which important information is entrusted outside the Fujifilm Group. The company prepared and has been putting into practice a guideline for cases where important information of the company or a customer is commissioned to a partner company. The information security control organization and the quality assurance department, which are responsible for security, and the procurement department worked together to revise the guidelines for the reinforcement of the governance and streamlining of the process of selecting partners appropriate for

individual projects, as well as for the correct execution of processes of investigation and requests for making improvement. The survey forms are divided into three types depending on the content of the outsourced work, and FUJIFILM Business Innovation requests the partner company to respond to one of three kinds of survey forms. Each survey form contains questions on security conditions from the perspective of organizational measures, human measures, physical measures, and technical measures. The results of the replies to these questions are gathered at the procurement department for centralized management. When the information entrusted includes personal information, FUJIFILM Business Innovation and the partner company exchange an agreement about information handling requirements, including control measures so that the partner company properly handles the information, observes laws and regulations, and satisfies the personal information policies of Fujifilm Group.

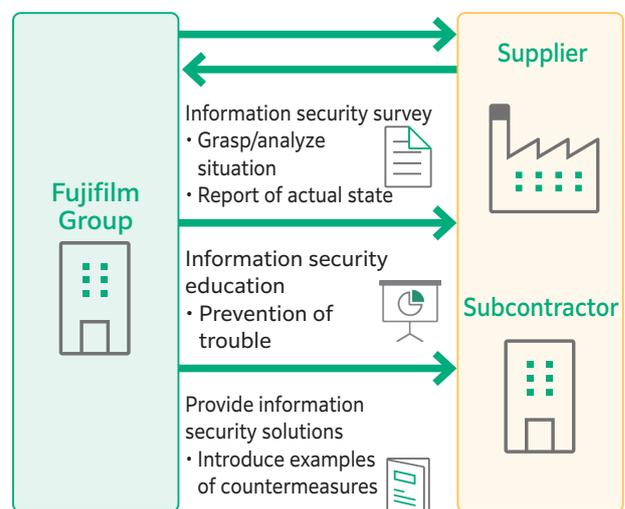
FUJIFILM Business Innovation has been expanding their efforts within the Group as well.

### Examples of security efforts Submission of a letter of commitment by the partner company employees of subcontractor

FUJIFILM Business Innovation receives a letter of commitment on the proper use of information, equipment, and other assets from nonpermanent employees, dispatched employees, and employees of partner companies of subcontractor, who works in the office. This letter of commitment aims to ensure thorough and Group-wide adherence to security requirements, and consists of the following items:

1. Prevention of information leakage or theft in accordance with the confidentiality agreement
2. Proper use of the facilities and equipment of FUJIFILM Business Innovation and its affiliated companies
3. Proper protection of the Group assets including information assets
4. Thorough observance of the entry/exit control rules at the sites of FUJIFILM Business Innovation and its affiliated companies
5. Proper use of the company network and company information system
6. Proper use of electronic access card entry/exit permission

### Initiatives to strengthen the information security of partner companies

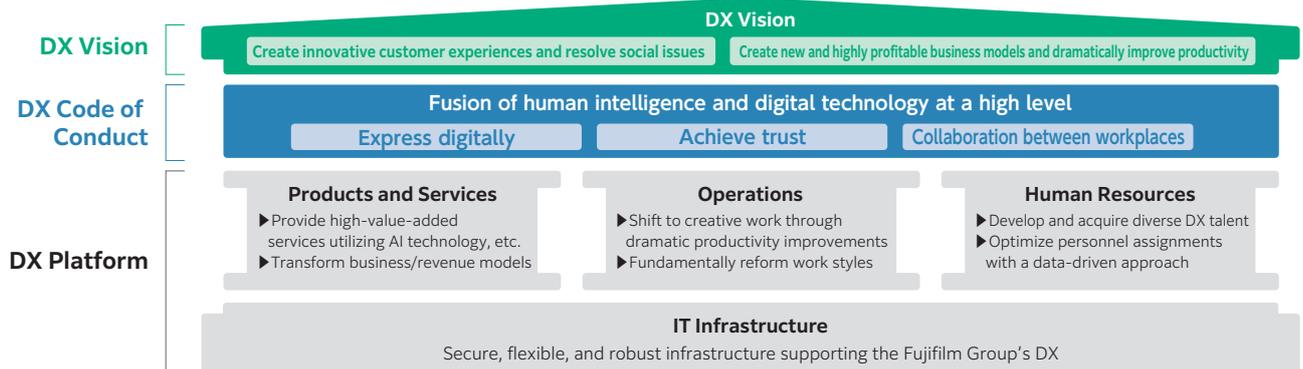


## Promotion of DX and handling risk

### DX and use of AI that Fujifilm Group is aiming for

Efforts are currently being made in Product DX by putting robotics and AI technology to use in our products and services to support the acceleration of DX of customers; in Work DX by making use of software and other tools to fundamentally reform work processes and significantly increase productivity; and in Human Resources DX, which develops DX-capable human resources and promotes optimization of human resources deployment based on data. Furthermore, a flexible and robust IT infrastructure is being built under solid information security as a foundation for supporting these efforts.

Pursue the fusion of human intelligence and digital technology at a high level to accelerate the realization of Fujifilm Group's DX vision

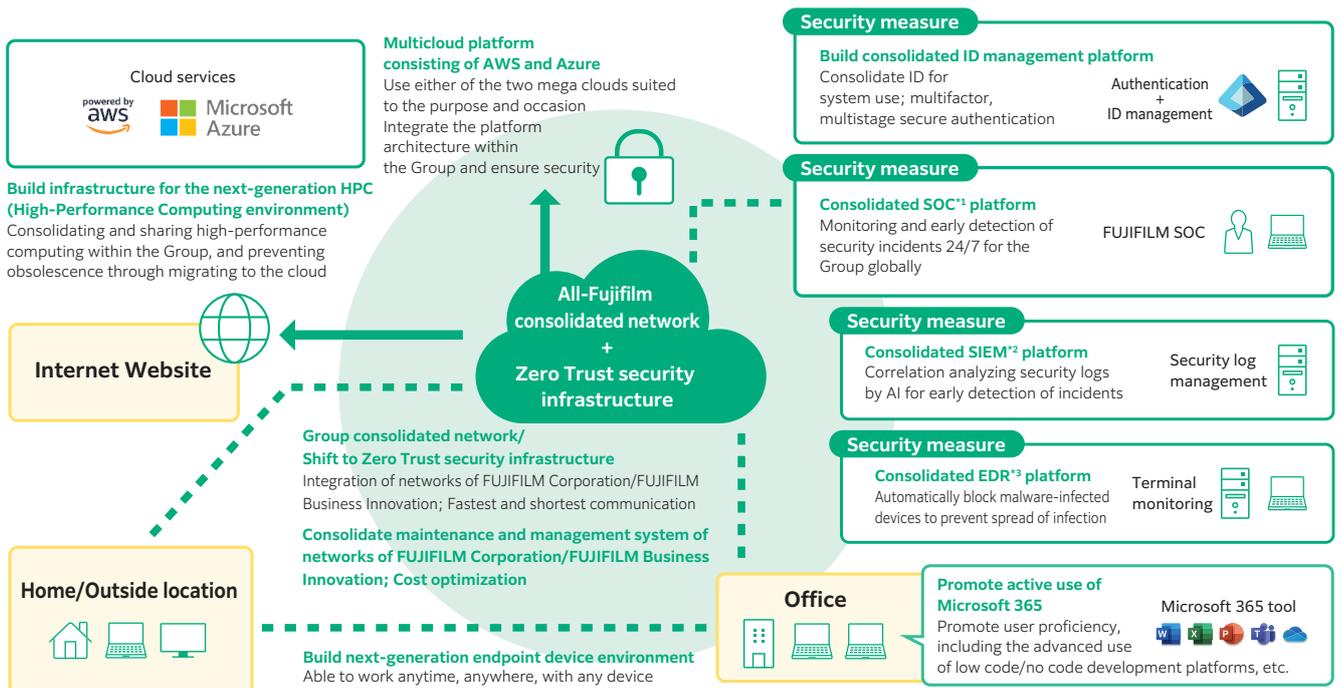


Responding to risk in the use of AI is another important factor in order to further accelerate the strengthening of products and services, improving productivity of work, and realizing active participation by diverse human resources, by proactively using AI at all the workplaces that are promoting DX inside and outside Japan.

At the Fujifilm Group, the relevant organization of each company handles risk not only in the aspect of cybersecurity but also in the aspects of coping with laws and new regulations of various countries related to such matters as copyright and privacy rights, in order to ensure appropriate use of AI.

### Key measures for infrastructure and security

High productivity and safe working environments are achieved through the use of cutting-edge technology and services, and the implementation of measures that are shared by all the Group companies in Japan and abroad.



\*1 SOC: Security Operation Center. An organization dedicated to conducting monitoring, detection and analysis of cyberattacks

\*2 SIEM: Security Information and Event Management. A system for detecting such incidents as cyberattacks and malware infection through centralized collection of logs and data from firewalls, etc., and conducting correlation analysis of the aggregated data

\*3 EDR: Endpoint Detection and Response. Security software that monitors computers and servers connected to a network to detect suspicious behavior

Having drawn up a roadmap for promoting DX, it is our aim to get products and services to become established as “a foundation to support a sustainable society” and to continue to contribute to solving social issues through the formation of a new ecosystem by collaborating with various stakeholders. To accomplish this, it is absolutely essential that we provide all stakeholders with a safe and secure environment, for which we regard cybersecurity to be an indispensable factor.

## Strengthening of cybersecurity measures

Using the global standard cybersecurity framework put forth by the National Institute of Standards and Technology (NIST), FUJIFILM is carrying forward the following robust measures from both aspects of technologies and operations.

Phase	Action item	Examples of measures
Identify	Identification of assets and important information	<ul style="list-style-type: none"> <li>● Investigations have been conducted at the Group companies globally of devices that corporate divisions normally manage, as well as devices managed at individual workplaces, regarding security measures and locations of important information</li> <li>● Network equipment management that is common to all the Group companies globally has been started, in order to grasp information of the network equipment configuration and strengthen vulnerability countermeasures</li> </ul>
Protect	Prevention of information leakage	<ul style="list-style-type: none"> <li>● SASE<sup>*4</sup> has been started to restrict access to external services, in order to strengthen the prevention of removal of company information using private external storage or other means</li> <li>● In order to ensure safe storage of important information, shared storage for the group companies in and out of Japan is being deployed</li> <li>● Encryption settings with IRM<sup>*5</sup> are being used in order to prevent viewing by a device that is not a terminal device provided by the company, even if removal of important information has occurred</li> </ul>
	Platform measures	<ul style="list-style-type: none"> <li>● Use of multicloud platform environment based on common security settings has started, in order to ensure the security of the cloud environment of Group companies inside and outside Japan as a whole</li> <li>● Strengthening of data center network security through microsegmentation<sup>*6</sup> has been carried out, in order to minimize damage that would otherwise spread to others after intrusion by an attacker</li> </ul>
Detection	Early detection	<ul style="list-style-type: none"> <li>● A framework utilizing EDR and SOC for monitoring/responding to abnormalities around the clock, 365 days a year, is being implemented throughout Group companies inside and outside Japan as a whole, for the early detection of and response to signs of cyberattack</li> <li>● Detection and response capabilities continue to be strengthened by making improvements to facilitate the identification of issues using Red Team tests<sup>*7</sup> and other tools, with the aim of increasing the accuracy of monitoring and improving the operation quality of FUJIFILM SOC</li> </ul>
	Whistle-blowing	<ul style="list-style-type: none"> <li>● A framework for reporting emergencies has been set up and is in operation, enabling employees to immediately report emergencies at any time, including nighttime and holidays</li> </ul>
Respond	Instructions and responses for emergencies	<ul style="list-style-type: none"> <li>● Action rules have been put in place to use the disaster emergency report system that can be accessed from personal terminal devices, the public address system, and bulletin boards to enable emergency instructions to be sent to employees without using terminal devices provided by the company</li> </ul>
	Action meeting	<ul style="list-style-type: none"> <li>● A process is in place that enables the ESG Committee to discuss countermeasures in the event of a serious cyberattack, so that prompt, appropriate decision-making can be carried out by top management</li> </ul>
	Investigation of impact and cause	<ul style="list-style-type: none"> <li>● In anticipation of an emergency, preparations have been made, including deciding in advance on possible external vendors to be requested to conduct an investigation into the cause so that the investigation can be promptly carried out through digital forensics of terminal devices<sup>*8</sup></li> </ul>
	Report to relevant institutions	<ul style="list-style-type: none"> <li>● In order to comply with the Act on the Protection of Personal Information, reporting procedures have been prepared and are being put into effect for reporting to Personal Information Protection Commission and other possible institutions</li> </ul>
Recover	Business continuity	<ul style="list-style-type: none"> <li>● In preparation for an emergency, alternative measures (BCP: Business Continuity Plan) for work that is anticipated to be seriously affected by a system outage have been prepared and are being put into effect so that such work is replaced with work that can be done without requiring the use of PCs</li> </ul>
	Recovery	<ul style="list-style-type: none"> <li>● Determination is made of priority for recovering systems, and activities are periodically carried out to spread awareness of the necessity to back up important information in preparation for when systems become inoperable.</li> </ul>

\*4 SASE: Secure Access Service Edge. A network security model for achieving a zero-trust network. This model is a concept for realizing a safe environment, even in a cloud-centric environment, by having all communication go through a virtual security platform on the internet.

\*5 IRM: Information Rights Management. Software that encrypts document files, making it possible to manage and control the viewing and editing of files.

\*6 Microsegmentation: A design technology for subdividing the network segments and carrying out detailed visualization and control of traffic in order to heighten security.

\*7 Red Team Test: This is an assessment that calls for a security specialist to launch various realistic attacks on a customer company in order to test the effectiveness of the security measures of the company.

\*8 Forensics: A process that calls for meticulously retrieving information from data and management information, even if the data has been deleted, in order to reveal what operations have actually been carried out.

# Efforts for personal data protection

## Basic Policy

The Fujifilm Group's code of conduct, which defines how domestic and overseas employees should behave, stipulates the protection of personal information as a part of respecting human rights. Each group company defines a privacy policy that contains the common content of the Fujifilm Group to handle personal data with the Group's common idea.

This policy is applied to the entire supply chain of the Fujifilm Group including suppliers and subcontractors.

## Organization structure for promotion

The Fujifilm Group is building and maintaining an organization structure for promoting the protection of personal information, with the officer responsible for the ESG Division as the general manager of this organization.

Decisions on policies related to personal information for the Group as a whole are made by the ESG Committee, which is chaired by the President of FUJIFILM Holdings Corporation, with the decisions being regularly reported from the ESG Committee to the Board of Directors. The Board of Directors is responsible for the supervision of the Group compliance and risk management, with responsibility for the protection of personal information being understood to be an important issue, ensuring the effectiveness of this process in protecting personal information. After policies are decided by the ESG Committee, the policies and goals are disseminated throughout the Group by the ESG Division, which is responsible for controlling the protection of personal information. The ESG Division also strives to grasp the status of the implementation of the policies and progress towards the goals, provide instruction and advice to the head of each organization that handles personal information, and keep the employees thoroughly informed about the contents of regulations. Furthermore, with the rise in society's awareness of personal information protection, the ESG Division understands that the protection of personal information is a critically important risk issue for the company, formulates action plans when carrying out risk identification every year, and checks activities taking place within the risk management structure of the entire Group.

In addition, each Group company and organization designates a Personal Information Protection Manager who works to protect personal information. Furthermore, in some of the business organizations, the quality assurance division is assigned a role of promoting personal information protection so that appropriate responses to laws and regulations can be ensured across the entire business, rather than for each product. The Group companies that have acquired an ISMS/PrivacyMark undergo periodic external audits in conjunction with their ISMS activities, and implement improvement activities based on the results of these audits.

## Employee training

The Fujifilm Group believes that in order to prevent the occurrence of accidents or infractions related to handling personal information, it is important for each and every employee to have the necessary knowledge and a high level of awareness. For this reason, the Group conducts an e-learning program regarding personal information protection for all employees every year. For Group companies that have opportunities to handle particularly large volumes of personal information, the Personal Information Protection Handbook

has been distributed to employees to educate them.

Within our domestic operations, our employment rules establish measures that include disciplinary action for unauthorized removal of personal information. We are also implementing similar measures for situations abroad. Furthermore, we are actively conducting activities to protect personal information such as raising awareness through the sharing of near-miss cases including examples from other companies, and implementing activities to detect the unauthorized removal of information.

## Proper handling of personal information

The Fujifilm Group has implemented appropriate safety management measures to protect the personal information held by the Group, establishing internal rules (the Global Personal Information Protection Regulations, the Personal Information Management Regulations, various guidelines, etc.) for the handling of personal information, as well as privacy policies. Changes made to the privacy policies are disclosed on the company's website, and if it is required by law to obtain consent from the data subject, appropriate actions will be taken.

When asked by the government agencies to disclose personal information, we decide properly after reviewing the content of the request and applied laws.

## Response to global compliance

Recently, as preparations and revisions of personal information protection laws and regulations of various countries around the world are processing rapidly, including the EU's General Data Protection Regulation (GDPR), it is necessary for us to catch up with the updates and make sure we are in compliance with them.

While major administrative responses for compliance are carried out by the regional head quarters and local subsidiaries in each country, the ESG Division also confirms the status of preparations and revisions of laws and regulations of countries around the world, and checks how the regional headquarters and local subsidiaries in the countries are responding.

In 2023, we have introduced a common personal information inventory system for some Group companies in Europe, the United States, Asia-Pacific regions enabling us to centrally manage the handling of personal information in these regions. Inventory is taken once a year to check and make corrections to safety management measures, or delete personal information that no longer needs to be kept. The ESG Division undertakes audits of the relevant organizations regarding the status of the inventory being carried out.

## Incidents and violations in handling of personal information

In FY2023, the Fujifilm Group did not experience any serious incidents related to personal data, such as information leakage and use in unintended purposes, that we decided should be disclosed due to directives by third parties or regulating authorities. Furthermore, even minor incidents are all handled as information security incidents and depending on the contents of the incident, information is disclosed to the relevant individuals, and detailed analysis of the cause is conducted, and recurrence prevention measures are drawn up and deployed.

\*For details regarding collaboration with suppliers and subcontractors, please refer to page 13 of Supply Chain Security.

## Management of important information

In response to information security risks that have been increasing in recent years, we have also been simultaneously carrying forward the strengthening of the management of confidential information of the company, information entrusted to us by customers and business partners, and personal information, in addition to the cybersecurity measures and security monitoring mentioned earlier.

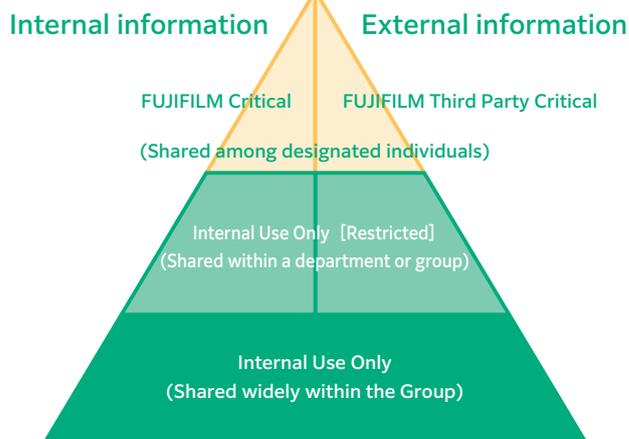
As shown in the illustration on the right, the Fujifilm Group classifies information into four classifications, based on the degree of importance. Company rules have been established so that each document that is used internally is marked to clearly indicate which classification it belongs to, and taking a document outside of the company, making copies, or using it in external communications is handled in accordance with its classification.

Information Rights Management (IRM) is used for simultaneously carrying out encryption and access control of documents containing information that is highly important to the company (inside the yellow outline of the illustration on the right), so that even if the document is leaked outside the company, a third party would not be able to view it.

Thus, IRM protects important information, that should be protected by the organization, from unauthorized access. Furthermore, by promoting ledger management, organizations in Japan and overseas are identifying information assets (important information including personal information) which needs to be protected, and are taking appropriate measures.

In carrying forward these measures, a "classification support tool," which was developed internally, has been introduced to Group companies in Japan, to show the employees an easy-to-understand standard for determining the degree of importance of the documents they are creating, and easily configure the encryption settings.

### Document information classifications in the Fujifilm Group



### Classification support tool

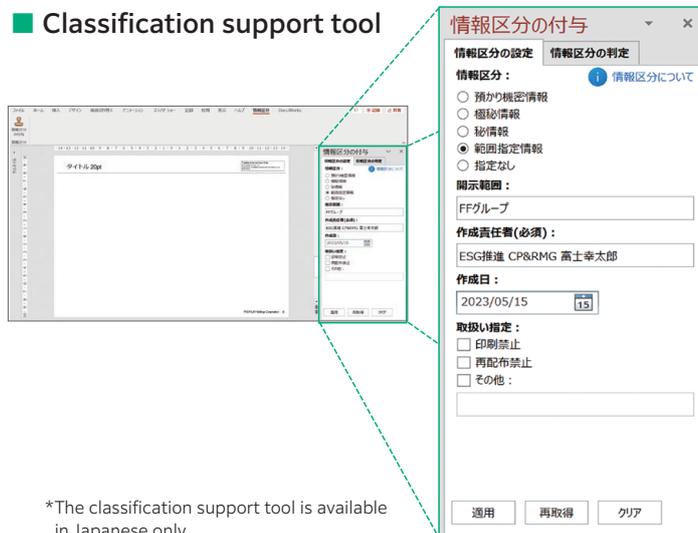
The classification support tool (shown at right) is an Office application add-in that allows the display of data classification in Office documents (PowerPoint/Word) that are being created, and at the same time, enables encryption settings to be made. The classification support tool has two functions: "data classification determination" and "data classification setting." "Data classification determination" is a function that provides support when the author is in doubt about which of the four categories indicated in the above illustration the document fits into, by enabling the author to make a selection from the indicated choices based on the type of information contained in the document. The "data classification setting" function creates the data classifications and the classification labels of "disclosure range, creator, date of creation, handling specifications."

Furthermore, encryption settings are set so that only users who are employees of the Group can open the documents..

Overseas, Microsoft's sensitivity label is used, with encryption of and control over access to important information being carried out in the same way.

Thus, we are carrying out management so that even if there is unauthorized access resulting in damage, the damage is kept to a minimum. In addition to this, corresponding to the importance of the information that was compromised, we have also established a system and procedures that enable us to promptly carry out the necessary response, such as making a public announcement and submitting report to the supervisory authorities.

### Classification support tool



\*The classification support tool is available in Japanese only.

### Protection of technological information and other important information of the company

We are implementing activities to strengthen measures against information leaks by identifying important information such as technical information that could have a significant impact if leaked. The purpose of these activities is to respond to external threats such as cyber attacks and internal threats such as the unauthorized removal of information by insiders.

Principle measures to strengthen the information security include: (1) building robust IT infrastructure and information management systems against cyberattacks and unauthorized removal of information by authorized persons; (2) technical measures to prevent the removal of information; and (3) measures to monitor the removal of information. In order to carry out these measures, we identify important information assets through inventory, and carry out risk assessments to find where potential risks are.

# 5

## Third-party Assessment and Certification/ Overview of the Fujifilm Group

### Acquisition status of the PrivacyMark and ISMS in the Fujifilm Group (as of April 2024)

#### PrivacyMark\*1

Companies that have acquired JIS Q 15001 certification for their Personal Information Protection Management System (PMS) and have been accredited by the Japan Institute for Promotion of Digital Economy and Community (JIPDEC) to use the PrivacyMark are listed below.

FUJIFILM Imaging Systems	FUJIFILM Techno Service	FUJIFILM Media Crest
FUJIFILM Imaging Protec	FUJIFILM Healthcare Systems	FUJIFILM Medical
FUJIFILM Medical Solutions	FUJIFILM Healthcare Laboratory	FUJIFILM System Services

#### ISMS (Information Security Management System)\*2

The companies with organizations that have acquired the international standard ISMS-PIMS (ISO/IEC 27001) certification are shown below.

FUJIFILM*3	FUJIFILM Service Creative	FUJIFILM Business Innovation Korea
FUJIFILM Imaging Systems*3	FUJIFILM Service Link	FUJIFILM Business Innovation Malaysia
FUJIFILM Imaging Protec*3	FUJIFILM Digital Solutions	FUJIFILM Business Innovation New Zealand
FUJIFILM Software*3	FUJIFILM RIPCORDER	FUJIFILM Business Innovation Philippines
FUJIFILM Medical*3	FUJIFILM Eco-Manufacturing (Suzhou)	FUJIFILM Business Innovation Singapore
FUJIFILM Wako Pure Chemical*3	FUJIFILM Manufacturing Hai Phong	FUJIFILM Business Innovation Taiwan
FUJIFILM Business Innovation	FUJIFILM Manufacturing Shenzhen	FUJIFILM Business Innovation Thailand
FUJIFILM Business Innovation Japan	FUJIFILM Business Innovation Asia Pacific	FUJIFILM Business Innovation Vietnam
FUJIFILM System Services	FUJIFILM Business Innovation Australia	FUJIFILM Business Innovation Malaysia Sdn Bhd
FUJIFILM Printing Systems	FUJIFILM Business Innovation China	FUJIFILM Data Management Solutions
FUJIFILM Manufacturing	FUJIFILM Business Innovation Hong Kong	

#### ISMS-PIMS (Privacy Information Security Management System)

The companies with organizations that have acquired ISMS-PIMS (ISO/IEC 27701) certification\*4 are shown below.

FUJIFILM System Services*3	FUJIFILM Business Innovation Korea	FUJIFILM Business Innovation Taiwan
----------------------------	------------------------------------	-------------------------------------

\*1 Mark given by JIPDEC to companies that properly handle personal information.

\*2 Certification based on international standard that specifies the building and operation method of a system for managing information security risks.

\*3 The scope of certification in Japan and the names of the organizations/divisions can be viewed by clicking on "Certified Org." at the "Information Security Management System Accreditation Center (ISMS-AC)" website.

\*4 Certification related to privacy protection for which the acquisition of an ISMS certification is a prerequisite. Please see also Topics on page 19.

### State of acquisition of ISO/IEC 15408\*5 certification

Multifunction machines, printers, and other products of FUJIFILM Business Innovation and its affiliate companies have acquired ISO/IEC 15408 certification since 2007. The products that have newly acquired certification between April 2022 and March 2024 are listed below.

Product name	Date of certification
FUJIFILM Apeos C3060 / C2560 / C2360 / C2060 / C3060 GK / C2560 GK / C2060 GK Models with copying, printing, fax, scanning, and storage overwriting erasure functions	May 9, 2022
FUJIFILM Apeos 5570 / 4570 / 3570 / 5570 GK / 4570 GK Models with copying, printing, fax, scanning, and storage overwriting erasure functions	May 9, 2022
FUJIFILM Apeos 3560 / 3060 / 2560 / 3560 GK / 3060 GK / 2560 GK Model with copying, printing, fax, scanning, and storage overwriting erasure functions	May 9, 2022
FUJIFILM Apeos C5240 Model with copying, printing, fax, scanning, and storage overwriting erasure functions	June 2, 2022
FUJIFILM Apeos 6340 Model with copying, printing, fax, scanning, and storage overwriting erasure functions	June 2, 2022
FUJIFILM Revoria Press E1136 / E1125 / E1110 / E1100 Models with copying, printing, scanning, storage overwriting erasure, and PostScript functions	July 8, 2022
FUJIFILM Apeos 7580 / 6580 / 5580 Models with copying, printing, fax, scanning, and storage overwriting erasure functions	March 5, 2023
FUJIFILM Apeos 5330 / 4830 Models with copying, printing, fax, scanning, and storage overwriting erasure functions	March 20, 2023
FUJIFILM Apeos C4030 / C3530 Models with copying, printing, fax, scanning, and storage overwriting erasure functions	March 20, 2023

\*5 International security standard for evaluating whether information technology-related products and systems are properly designed from the standpoint of information security, and whether the design has been correctly implemented.

## Topics

### FUJIFILM System Services obtains the first ISMS-PIMS certification for the Fujifilm Group

On October 27, 2023, "Family Registry Comprehensive Service Bookless cloud service" provided by FUJIFILM System Services was approved for initial registration of the ISMS-PIMS certification (ISO/IEC 27701), which is an international standard for privacy protection. ISMS-PIMS certification is an add-on standard to ISO/IEC 27001 (ISMS), which is widely recognized as an information security management platform and ISO/IEC 27701, which is the standard for its implementation. FUJIFILM System Services is the first company to obtain this certification in the Fujifilm Group.

### FUJIFILM Holdings Corporation wins Grand Prix of Cyber Index Awards 2023

On December 8, 2023, FUJIFILM Holdings Corporation was awarded the Grand Prize, which is the highest award at the Cyber Index Awards 2023 hosted by Nikkei Inc. The Cyber Index Awards is given in recognition of companies and initiatives that have achieved outstanding results in cybersecurity, and key for significant progress in the digital transformation (DX) of the economy and society.

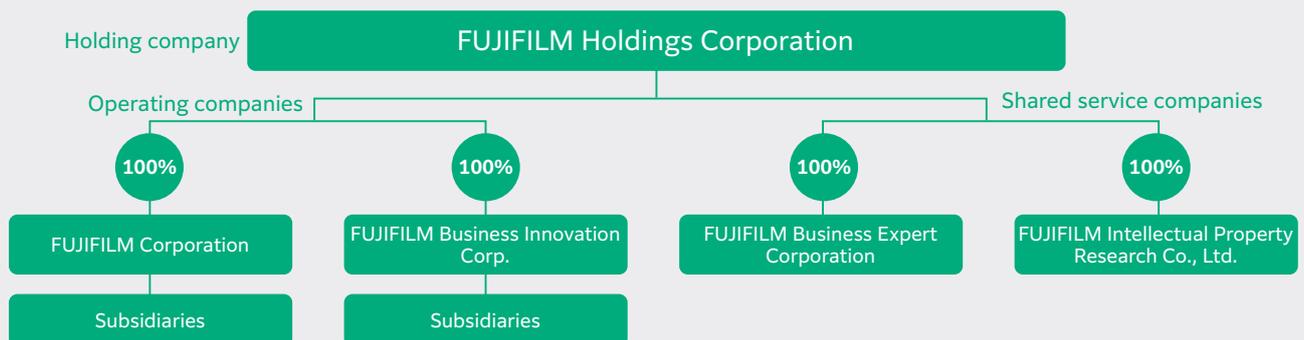


- The following initiatives were particularly highly evaluated in the award-winning DX Vision; The company has established "DX Vision," under which the Fujifilm Group continues to create innovative customer experiences and contribute to solving social issues through the utilization of digital technology to realize dramatic improvements in the productivity of each employee, resulting in the creation of outstanding products and services, and the CEO himself is taking a leading role in promoting DX of the entire Group.
- The company positions DX and cybersecurity as indispensable factors for the sustainable growth of the Fujifilm Group and for continuously contributing to the development of society.
- From the perspective of sustainability for all of the Group companies, taking into consideration the society, economy, environment, human rights, etc., the company has built a governance structure for the entire Group, including rules for reporting cyber-related incidents and a comprehensive response system. The company also publishes these initiatives inside and outside the Group through integrated reports, sustainability reports, etc.
- The company is promoting DX and striving to strengthen cybersecurity in the medical field, where such activities have great social significance.

## Overview of the Fujifilm Group

**Company name:** FUJIFILM Holdings Corporation  
**Head office:** Akasaka 9-7-3, Minato-ku Tokyo (Tokyo Midtown)  
**Establishment:** January 20, 1934

### Organization



### Business fields

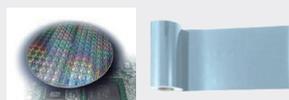
#### Healthcare

Providing a wide range of businesses in the 3 areas of prevention, diagnosis and treatment as a total healthcare company



#### Electronics

Providing advanced materials for products that support the digital age, such as semiconductors and next-generation displays, as well as recording media for data storage



#### Business innovation

Providing products, solution services and graphic communications that bring about new work styles, improving productivity and inspiring creativity



#### Imaging

Providing various products and services related to photographs from shooting to printing





Contact

---

## **FUJIFILM Holdings Corporation**

ESG Division

Postal code: 107-0052 Akasaka 9-7-3, Minato-ku, Tokyo

Tel: +81-3-6271-1111

Issued in September 2024