

## Management information

### Relevance to our business

The Fuji Oil Group recognizes information security as a category of risk directly tied to our business, and is working to strengthen our information security management.

As information technology and digital data become increasingly vital to our operations, we have a responsibility to our employees, business partners, suppliers, and other stakeholders to ensure our business continuity by countering external threats and protecting information. We seek to meet this social responsibility and achieve sustained improvements in our corporate value.

### Basic approach

The Fuji Oil Group works to improve our security level in order to safeguard our information systems against surrounding threats, and to protect and maintain the confidentiality, integrity and availability of our information assets. We formulated the Information Management and Information Security Regulations. Employees are trained on a continual basis to ensure that they understand and follow these regulations. On a technical level we are taking multilayered measures to prevent unauthorized access from outside the Group's information systems and to protect against computer viruses. We will further raise our information security level through a process of review, verification and improvement.

### Management system

The Chief Financial Officer (CFO) oversees initiatives in this area. An Information Officer and a Computer Security Incident Response Team (CSIRT) were established under the CFO at each Group company. The CSIRT also appointed an Information Management Director and an Information Security Manager for each Group company. We aim to systematically raise the information security level of all Group companies, with the advice of external experts.

The Sustainability Committee,\*1 an advisory body to the Board of Directors, monitors the progress and results of initiatives as a material ESG issue.\*2

\*1 Follow the link below to learn more about the Sustainability Committee.  
 > [https://www.fujioilholdings.com/en/sustainability/sustainability\\_management/](https://www.fujioilholdings.com/en/sustainability/sustainability_management/)

\*2 Follow the link below to learn more about material ESG issues.  
 > <https://www.fujioilholdings.com/en/sustainability/materiality/>

### Goals / Results

○ At least 90% complete △ At least 60% complete ✕ Less than 60% complete

FY2021 Goals	FY2021 Results	Self-assessment
Continue to conduct internal security audits that reflect risk trends and expand the scope of audits to cover systems that are not controlled by the IT Division	<ul style="list-style-type: none"> <li>Added audit items to address new threats, such as supply chain security risks and threats arising from increased telework. Conducted internal audits at 13 Group companies worldwide as scheduled.</li> <li>No serious security incidents occurred, thanks to the increased internal awareness of security risks.</li> </ul>	○

### Analysis

COBIT Level 4 requires the ability to demonstrate implementation of activities that guarantee IT security, to measure the status of information asset protection and IT security assurance compliance, and to be ready to implement improvements when necessary. We adopted an internal security audit to meet these requirements.

In FY2020, we expanded the scope of the audit to include more systems. In FY2021, eight Group companies carried out a self-assessment to follow up on improvements made after audits conducted in FY2020, and additional 13 Group companies were audited. This shows that the PDCA process for information security management is reliable.

When the audits identify areas requiring improvement, each Group company devises measures with assistance from the CSIRT and implements them after approval from the Information Management Director at each company.

## Next step

---

Cyber threats are constantly evolving. To follow the latest trends in security risk across the Group, we set the following goal for FY2022.

- Review and update the Group's Information Security Regulations to reflect the latest risk trends

## Specific initiatives

### Education

---

Since FY2018, we have been conducting IT security awareness training for Group company employees mainly by e-learning. The completion rate in FY2021 was 93.5%.\* We will work to develop the content of the training and encourage participation with the aim of achieving 100% participation in the future.

\* Targeted at employees who have a company email address and use a computer in their day-to-day operations.

### Internal security audit

---

Since FY2020, we have been conducting internal security audits at Group companies in order to assess the state of compliance with security requirements together with explicit evidence, and to set up a PDCA cycle for correction. In FY2022, we plan to continue conducting internal audits and self-assessments following on an audit program that incorporates the updated Group policies and additional items focused on manufacturing facility security and supply chain security.