Information security

Kao's approach

The Kao Group has an Information Security Committee, the purpose of which is to protect information assets including confidential information (trade secrets) and personal information, as well as IT hardware, software and data, in accordance with Kao's Information Security Policy. Based on the committee's discussions, Kao has established an administrative system that aims to set internal rules and to see that internal controls are thoroughly implemented and rules are observed. Kao also carries out related awareness-raising activities for employees.

Kao's creating value to address social issues

By making active use of confidential information and personal information, companies are able to implement their business operations in such a way as to maximize their unique strengths. At the same time, information technology is used extensively across a wide range of business activities, from order processing and placement to sales booking, budget processes, R&D and production. It is therefore very important for companies to adopt measures to counter the threat of information leaks or cyber-attacks on their IT systems.

To prevent the unauthorized disclosure of information through criminal activity of company personnel, we strive to implement the Kao Way, our corporate philosophy, and endeavor to ensure that all employees are familiar with the Kao Business Conduct Guidelines (BCG), which constitute our code of conduct. This is supported by the dissemination of messages from senior management, effective monitoring, and awareness-raising activities (including strengthening awareness of the penalties for violating the Unfair Competition Prevention Act).

With regard to external criminal activity, we have been implementing technical and human-focused measures to guard against cyber-attacks, which have caused serious problems for society in recent years.

Contributions to the SDGs

Policies

We have formulated our Information Security Policy, Guidelines on Handling Trade Secrets, Guidelines on Handling Personal Information and IT Security Guidelines to ensure that business activities are carried out in accordance with the relevant laws and with the guidelines promulgated by government ministries, agencies and committees.

With regard to the protection of confidential information, to ensure that confidential information is able to receive full legal protection as trade secrets, we have drawn up relevant rules in accordance with the guidelines and handbooks, etc. issued by the Japanese Ministry of Economy, Trade and Industry (METI). We also implement management in accordance with these rules, and perform self-checks on a regular basis.

Personal information is also managed carefully in accordance with the guidelines formulated under the jurisdiction of the Personal Information Protection Committee, etc. When operations that involve the handling of personal information are outsourced, we implement careful management by requiring the companies in question to sign appropriate contracts or memorandums of understanding, and by implementing rigorous auditing procedures, etc. We also implement proper management of employees' personal information, in accordance with the guidelines formulated by the competent ministries, agencies and committees.

Framework

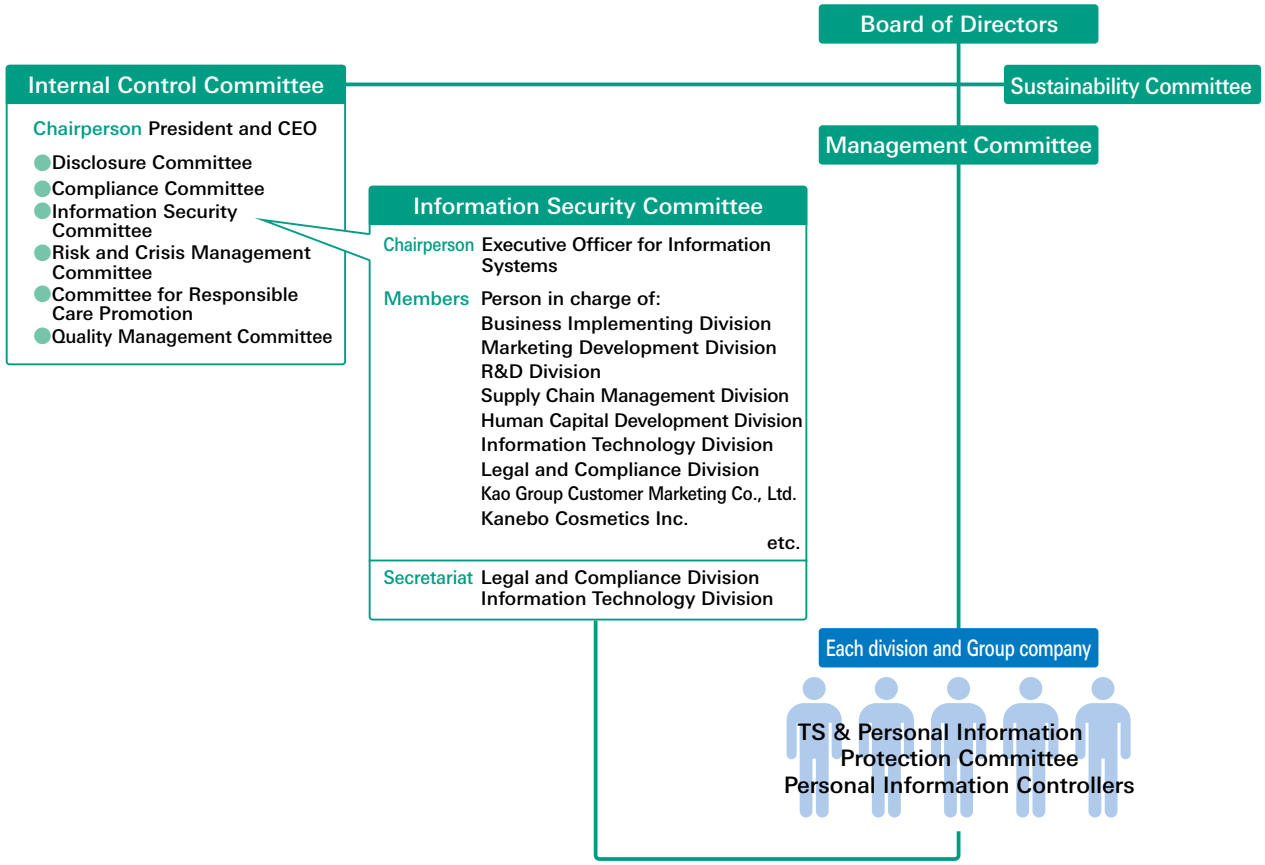
The "Protection of Confidential Information Handbook" published by METI in February 2016 specifies that management should take the lead in participating in internal system establishment, and that measures should be formulated from a variety of different perspectives, including those of intellectual property management, human resources and labor affairs, information security and compliance with laws and regulations. The handbook also emphasizes that confidential information exists in all departments within any given company.

We have appointed executive officers to serve as Chair and Vice-Chair of the Information Security Committee, and both the committee members and the staff of the committee's secretariat are drawn from many different divisions, including Human Capital Development, Information Technology, Marketing, Intellectual Property Management, Production and Engineering and Legal and Compliance. In this way, we benefit from a wide range of different perspectives when formulating internal rules, putting management systems in place, and implementing awareness-raising activities.

In addition, staff members from each division are selected to serve as members of the Trade Secret (TS) & Personal Information Protection Committee and as Personal Information Controllers. We continue to implement confidential information and personal information protection activities using the PDCA (plan–do–check–act) cycle, focusing in particular on awareness-raising activities and self-checks.

Information security

Information security management framework



*As of December 2017.

Education and promotion

Our basic approach to internal education involves having it conducted at the level of each individual division. In accordance with this approach, to ensure thorough promotion of the protection of confidential information and personal information, we arrange lectures given by external instructors for the members of the TS & Personal Information Protection Committee and for Personal Information Controllers, and awareness-raising activities are held to familiarize our staff with the latest trends. In addition, awareness-raising materials for education at the level of the individual divisions are provided to the members of the TS & Personal Information Protection Committee and Personal Information Controllers. Company-wide warnings and awareness-raising messages for all staff are sent via the company intranet portal site.

To evaluate the effectiveness of in-house education, checking is performed using self-checks. On the basis of the results obtained from these self-checks, any problems that may exist are identified, and improvement targets are set and improvement activities implemented.

Information security

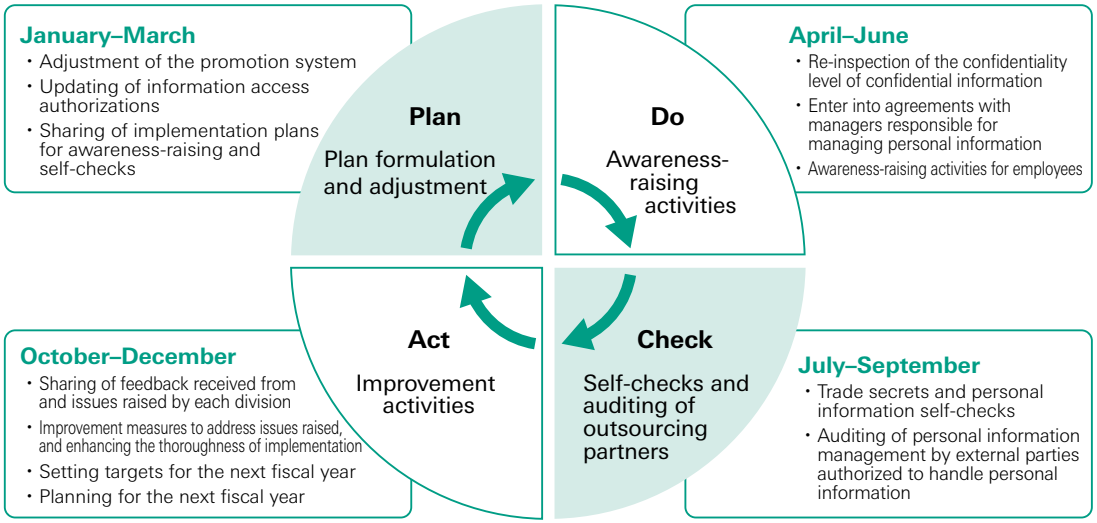
Mid- to long-term targets and performance

Within Japan, we are working to standardize the management cycle in relation to cyber-attack prevention measures, protection of confidential information and personal information, and information security with respect to the appropriate use of PCs, smartphones, networks, etc. The quarterly cycle is as follows:
First Quarter: Plan formulation and adjustment, Second Quarter: Awareness-raising activities, Third Quarter: Self-checks and auditing of outsourcing partners, Fourth Quarter: Improvement activities.

By implementing activities in accordance with this PDCA cycle, we are promoting a fundamental transformation aimed at preventing cyber-attacks and other incidents relating to confidential information or personal information. We are also putting in place an incident response framework and response processes that will enable us to respond appropriately if an incident does occur.

At the same time, we are providing support for the putting in place of rules and systems that comply with the requirements of local laws and regulations in other countries (including countries in Asia, the Americas, and Europe). Regarding our cyber-attack prevention strategy, we are aiming to realize a global improvement in our overall level of information security by implementing information security assessments, clarifying the current situation, identifying problems, and implementing improvements.

PDCA cycle for information security activities



Information security

Performance in 2017

The following activities were implemented in 2017 in relation to the information security management cycle.

First Quarter: Plan formulation and adjustment

- Revision of the Guidelines on Handling Personal Information (revised to take into account the revisions to the Personal Information Protection Act coming into effect on May 30, 2017)
- Updating of systems and information access authorizations
  To ensure that activities can proceed smoothly under the new systems, in line with the changes in roles due to organizational restructuring and personnel changes, information access authorizations were set for 40 members of the TS & Personal Information Protection Committee, 47 Personal Information Controllers, and two Information Security Committee members.

Second Quarter: Awareness-raising activities

- Holding of presentations to introduce the revisions made to the Guidelines on Handling Personal Information (653 participants in total)
- Issuing of information security awareness-raising materials

Third Quarter: Self-checks and auditing of outsourcing partners

- Implementing self-checks using confidential information "self-patrols"
- Implementing self-checks using personal information "self-patrols"
- Implementation of paper audits of outsourcing partners undertaking work that relates to personal information

Fourth Quarter: Improvement activities

- Holding of the 24th TS & Personal Information Protection Promotion Meeting
  Provision of feedback and setting of improvement targets in relation to confidential information and personal information incident reporting and "self-patrols" in 2017.
- Re-launching of "Security Assessments Outside Japan"

Collaboration with stakeholders

We contribute to the enhancement of information security in the chemical industry through our participation in the Security Information Management Subcommittee established by the Japan Chemical Industry Association (JCIA), an industry body whose members include chemical product manufacturers.

We also participate in two information-sharing networks that work to combat cyber-attacks: the Initiative for Cyber Security Information sharing Partnership of Japan (J-CSIP), which is directed by the Information technology Promotion Agency, Japan (IPA), and the National Police Agency's Cyber Intelligence Information Sharing Network. Starting in 2017, we are also participating in the JPCERT Coordination Center's "Early Warning Information" program. Through our participation in these information-sharing networks, besides obtaining information about software vulnerabilities and cyber-attacks, we are also able to disclose and share information about cyber-attacks that we have experienced, thereby contributing to the enhancement of cyber-attack prevention measures in Japan.

Information security

Our initiatives

First Quarter: Plan formulation and adjustment

Revision of the Guidelines on Handling Personal Information

Following the adoption of the "My Number" system in Japan in 2016, full-scale implementation of the revised Personal Information Protection Act began on May 30, 2017. In response to the revisions made to the Act, Kao announced revisions to our Guidelines on Handling Personal Information on March 14, 2017.

The main revisions included changes relating to the definition of personal information (which has been expanded to include not only name, gender, date of birth etc. but also other information that can be used to identify individuals, such as DNA, fingerprints, finger vein images, etc.), personal information that requires special care (including information relating to race, ethnic background, ideology, religious beliefs, medical history, criminal record, etc.), provision of information to third parties (record-keeping), and handling of anonymized information.

Handling of personal information leaks

Within Japan, starting in 2016 the handling of personal information leaks has been positioned as corporate risk. With the secretariat of the Information Security Committee playing a key role, we have established response systems and formulated response flow to be followed when an incident occurs. In this way, we have put in place a comprehensive response flow for handling personal information leaks that includes reports to the chairperson of the Information Security Committee. We have also implemented training using desktop simulations based on case studies of serious personal information leaks that occurred in the past.

In 2017, we performed training using desktop simulations with scenarios based on incidents that occurred within the Kao Group.

Second Quarter: Awareness-raising activities

Presentations regarding the revision of the Guidelines on Handling Personal Information

Following the approval of the revisions to Kao's Guidelines on Handling Personal Information internal rules on March 14, 2017, "Presentations Regarding the Revision of the Guidelines on Handling Personal Information" were held at those workplaces in Japan that have units involved in the handling of personal information.

A total of seven presentations were held: three at the Kayabacho office, two at the Sumida office, and one each at the Tochigi Plant and the Odawara Plant. Including those employees who participated via web-conferencing, a total of 653 employees attended these presentations. The presentations explained how the key revisions related to specific business situations. A large number of questions were raised during the presentations, making it possible to provide extensive explanations based on individual cases. Through the holding of these presentations, we were able to implement the preparations needed to comply with the revised Personal Information Protection Act.

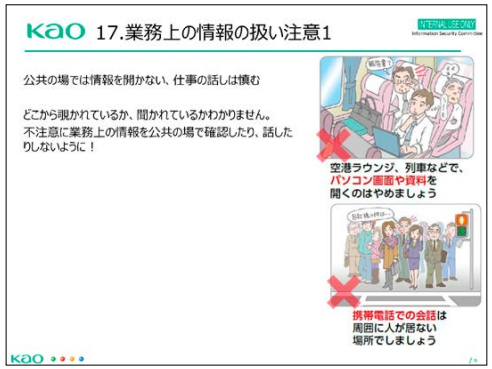
Information security

Second Quarter: Awareness-raising activities

Issuing of information security awareness-raising materials

In May 2017, we issued information security awareness-raising materials for use by Kao Group employees in Japan. The aim was to explain the points covered by Kao's information security-related rules – the Guidelines on Handling Trade Secrets, Guidelines on Handling Personal Information, and IT Security Guidelines – in an easy-to-understand way, so as to deepen employees' understanding of these rules. The materials include simple explanations on the left side, with easy-to-understand graphics etc. on the right side.

The materials have been made available on our intranet portal site, and members of the Trade Secret (TS) & Personal Information Protection Committee and Personal Information Controllers have been notified by e-mail of their availability, to facilitate the utilization of these materials in awareness-raising activities by each division.



Information security awareness-raising materials for employees

Third Quarter: Self-checks and auditing of outsourcing partners

Implementing self-checks using confidential information and personal information "self-patrols"

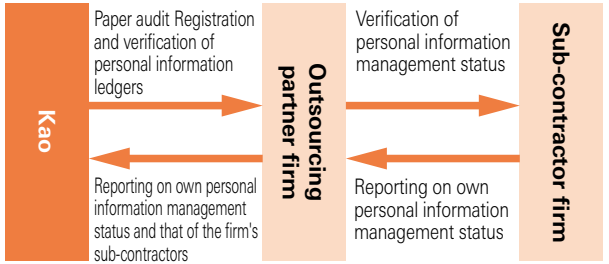
Accompanying the issuance of the information security awareness-raising materials, substantial revisions have been made to the suggested questions for confidential information and personal information "self-patrols." The questions relating to verification of awareness-raising materials content have been revised to reflect how important it is that employees understand the materials and are able to put them into practice.

Implementation of paper audits of outsourcing partners whose work involves handling of personal information

When operations that involve the handling of personal information are outsourced, there is a responsibility to ensure effective management and oversight of the companies in question. The Kao Group in Japan implements management and oversight of outsourcing partners using annual paper audits, in accordance with the requirements of the Personal Information Protection Act. In 2017, we verified the status of personal information management by conducting paper audits of 162 outsourcing partners. Starting from 2017, we have also begun asking outsourcing partners to provide details of their own sub-contractors and the work performed by these firms, so as to get a clearer picture of sub-contracting operations.

We are also strengthening management by continuing to register and verify the personal information ledgers that our outsourcing partners are required to maintain, as we have been doing since 2016.

Auditing of external parties authorized to handle personal information



Information security

Fourth Quarter: Improvement activities

Holding of the 24th TS & Personal Information Protection Promotion Meeting

The 24th TS & Personal Information Protection Promotion Meeting was held on November 14, 2017. The purpose of the Meeting was to use lectures by external experts to enable members of the Trade Secret (TS) & Personal Information Protection Committee and Personal Information Controllers to acquire new knowledge, to confirm the status of incidents occurring in 2017, to receive feedback on and identify issues relating to "self-patrols," and to set improvement targets in relation to these issues.

Project launched in response to the EU's General Data Protection Regulation (GDPR)

Implementation of the European Union's General Data Protection Regulation (GDPR) is scheduled to begin on May 25, 2018. The GDPR regulates the handling and transfer of personal data, and is characterized by strict rules and penalties.

The Kao Group is responding to the introduction of the GDPR by promoting the formulation of project frameworks by various divisions in relation to legal affairs, human capital development, information systems etc., with Kao Group companies in Europe playing a central role.

In principle, the GDPR restricts the transferring of personal data outside the European Economic Area (EEA). The Kao Group is responding to these requirements through the use of standard contractual clauses.

Response to China's Cyber Security Law (CSL)

China's new Cyber Security Law (CSL), which came into effect on June 1, 2017, requires that all personal data collected in China be stored within China, regardless of whether the data in question needs to be transferred across national boundaries. As the Kao Group preserves customer data – particularly in relation to our cosmetics business – we need to implement measures in response to the CSL. Since Kao's customer databases are located in Japan, we are establishing new databases in China. All customer data collected in China will be stored in these new databases. As the grace period for these measures extends only until December 31, 2018, we will need to complete these operations before the end of 2018.

Relaunching of "Security Assessments Outside Japan"

Up until the 2000s, the Kao Group implemented IT security assessments. As cyber-attacks have become increasingly rampant throughout the world in recent years, we have relaunched our security assessments outside Japan, as part of our efforts to strengthen the security measures of the Kao Group as a whole. We have compiled a checklist of 158 items to serve as a reference for external IT security assessments.