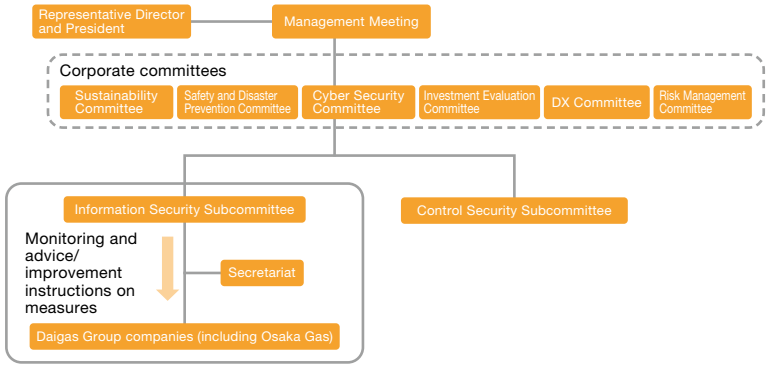
Information Security

Principle and Outline

The evolution of the Internet has led to sharp rises in leaks of confidential information, infections by computer viruses and other serious social issues, and the harm suffered by companies from such incidents increasingly extends beyond direct damage, even resulting in the loss of public trust.

As a business operator responsible for social infrastructure, the Daigas Group recognizes the importance of managing customer information and other data and has established the Cyber Security Committee in August 2019 as a corporate comittee. The Cyber Security Committee is chaired by the Head of Technology (Representative Director and Executive Vice-President), who oversees the Group's information security and other technology-related activities, and consists of the heads of related organizations and other members. The Cyber Security Committee meets twice a year to formulate medium- to long-term security strategies, coordinate and promote cross-organizational measures to address security risks across the Group, and gives instructions on improvements as necessary. The Committee submits to the Management Meeting deliberation proposals and reports on important agenda items. Under the leadership of its subcommittee called the Information Security Subcommittee, the Committee strives to step up information security measures.

Information Security Promotion System (April 2025)



Efforts to Strengthen Information Security

Under the leadership of the Information Security Subcommittee, the Daigas Group has established a system to enhance its overall information security by deploying managers in charge of promoting information security at core companies of the Daigas Group and organizations in charge of supporting the management of Osaka Gas and by deploying staff in charge of promoting information security at other organizations and affiliated companies.

In FY2022.3, we worked to strengthen information security measures through the establishment or revision of the internal rules for the Daigas Group, including the Information Security Guidelines. In addition to the existing content, we added and revised the Information Security Measures Standards based on recent security incidents that occurred inside and outside the company. We have been operating the telework guidelines, guidelines related to smart devices to respond to the expansion of the use of smart devices, and guidelines which compile the requirements that must be observed when using the cloud services, all of which were created in FY2021.3 and have been updated in light of the spread of telework.

Also, we conducted on-site surveys and checkups regarding information security at group companies, formulated improvement plans for each of these companies, and had them implement suitable measures. Education on security was also provided to all Daigas Group employees and employees in charge of IT at each affiliate and organization to improve the information security awareness and skills of each and every employee. To enhance employees' information security awareness and enable them to respond appropriately to security incidents, we conducted simulation training on targeted email attacks, based on actual cases (for about 20,000 employees).

In preparation for Osaka/Kansai Expo, we are re-inspecting the information security management status of major systems and strengthening monitoring during the event.

In addition to the above measures, we have conducted vulnerability assessments and introduced mechanisms to detect and prevent unauthorized access. We are reviewing various countermeasures from time to time to strengthen information security measures.

Major information security measures undertaken in FY2025.3

- Maintained and operated the Information Security Guidelines, etc.
- Implemented voluntary information security inspections of affiliated companies
- Implemented training on targeted email attacks (for approx. 20,000 employees)
- Implemented e-learning for employees (for approx. 8,000 employees)