Compliance / Information Security

Compliance

Policy and Management Framework

The Asahi Kasei Group positions compliance as a priority issue of materiality from the perspective of value creation. We seek to act with sincerity in accordance with our Group Values through strict compliance with internal rules as well as laws and regulations that relate to our businesses and operations. We apply the Asahi Kasei Group Code of Conduct to all executives and employees and thoroughly familiarize them with the code while continuously revising it in light of changing societal demands and circumstances.

To strengthen management of compliance, we established the Risk Management & Compliance Committee, which is chaired by the President and has Presidents of SBUs and core operating companies as members. Matters to be reported include plans and results of compliance promotion activities, serious compliance violations, and the operational status of the Compliance Hotline.

Awareness of the Code of Conduct

Group companies in Japan maintain an understanding of the status of compliance through questionnaires on the issue and regular exchanges of opinions in small groups—such as sections and subsections—using examples of compliance violations, which help promote awareness and understanding of compliance. In fiscal 2021, the compliance questionnaire response rate came to 93.5%, with 97% of respondents answering that they had read the Asahi Kasei Group Code of Conduct and approximately 80% that they understood it. Going forward, we will also expand and strengthen compliance activities globally.

Compliance Hotline

The Asahi Kasei Group operates a Compliance Hotline in order to promptly collect information on compliance violations and take measures in response. A wide variety of reports and consultations are received, including from suppliers and their employees, with the designated office or an investigation and response team carrying out investigations depending on the nature of the reports or consultations. The Executive Officer for Risk Management & Compliance reports on the operational status of the hotline to the Risk Management & Compliance Committee and to the Audit & Supervisory Board.

The system was revised in June 2022 in accordance with an amendment to Japan's Whistleblower Protection Act.

Number of reports and operational status (fiscal 2021): 66 reports
(4 of which were in relation to human rights issues, such as discrimination and harassment)

Prevention of Bribery

The Asahi Kasei Group has endorsed the United Nations Global Compact and declared that it will work to prevent all forms of corruption, including coercion and bribery. In particular, we consider bribery to be a serious risk factor that could considerably jeopardize our corporate reputation. Accordingly, we have established the Asahi Kasei Group Basic Policies for Prevention of Bribery and operate bribery prevention measures in accordance with regulations.

Information Security

Policy and Management Framework

The Asahi Kasei Group considers information security to be a serious issue for management in promoting digital transformation (DX). Accordingly, we formulated the Asahi Kasei Group Information Security Policy with the aim of ensuring and further enhancing information security. Regarding the information security framework, we have established a specialized internal organization (the Security Center) for the implementation of information security measures at all Group companies in Japan and overseas from the perspectives of both corporate governance and technology.

Cybersecurity

Cybersecurity measures have become increasingly important due to the sharp rise and growing sophistication of cyberattacks. The Asahi Kasei Group began operating a security operation center (SOC)[1] utilizing advanced security systems, such as endpoint detection and response (EDR),[2] to prevent such cyberattacks. In addition, we devote efforts to employee awareness activities, including carrying out targeted email attack drills several times a year, as most cyberattacks originate from suspicious emails, and implementing regular information security training.

[1] A SOC is an organization that monitors security. It receives alerts and other intelligence from security tools and investigates the impact scope and severity of attacks.
[2] EDR is a system for detecting advanced cyberattacks. The system can also respond to incidents in a variety of ways, such as by collecting logs required for analysis and isolating breached computers.