Raising Employee Awareness

Compliance Book

We have opened the "Compliance Room," a new webpage accessible from the intranet information portal. This page features compliance violation case studies as well as four-frame comics and blog posts aimed at raising employee awareness of compliance. Moreover, we provide employees with web-based compliance learning programs to aid in their acquisition of compliance literacy and identification of compliance issues specific to their workplaces. In addition, we implement compliance training specially designed for new hires and individuals appointed to managerial positions. At the end of January 2020, we issued our *Compliance Book* in the Japanese, English and Chinese languages, with the aim of offering specific compliance standards. In these ways, we are striving to help employees deepen their understanding of compliance and assist them in its proper practice.

Bribery and Corruption Prevention

Whether it takes place in Japan or overseas, our Compliance Code of Conduct stipulates that all forms of corruption must be prevented. Furthermore, we have established basic rules and systems to be observed in the prevention of bribery. In FY2019, these rules were upgraded into the "Rules for the Prevention of Bribery" with the aim of preventing violations of the OECD convention and the Foreign Corrupt Practices Act (FCPA) as well as laws and regulations, enforced in countries where we operate, to prohibit unfair competition and bribery. In addition to strictly adhering to these rules, we have included articles on such topics as the prohibition of bribery, such as bribery to public officials and limitations on excessive gifts and entertainment, in our Compliance Book to raise employee awareness.

Tax Compliance Initiatives

Due to the globalization of our business, we are more likely to confront a more diverse range of increasingly complex tax-related issues in the course of operations. Accordingly, we recognize that coordinated handling of tax compliance is a matter of increasing importance. With this in mind, we established the "Group Tax Regulations," "Group Tax Practices Guide" and other relevant rules aimed at stipulating the Group's policies on tax compliance and the detailed treatment of tax-related issues. We are thus striving to fulfill our corporate social responsibility by paying taxes in a proper manner and complying with all applicable tax laws enforced in countries where we operate in line with the Group Basic Tax Policy.

■ **Group Basic Tax Policy**

(1) Compliance with Tax Compliance

The Group employees must adhere with a basic policy of properly filing taxes, making payments, and otherwise handling transactions involving the Group in conformity with tax laws and regulations, and are prohibited from engaging in tax evasion or other illegal actions.

(2) Proper Management of Tax Expenses

The Group employees must give due consideration to various tax systems to prevent the emergence of tax-related risks. At the same time, they are expected to fully utilize legally permitted measures to optimize the Group's tax-related operations.

Risk Management

Policy of Risk Management

Idemitsu Group strives to stabilize its management by proactively recognizing and evaluating various risks associated with its business activities and taking appropriate measures in accordance with those risks. At our group, we classify risks associated with our business activities into two categories: "Operational Risk" and "Business Strategy Risk" and promote countermeasures against them. "Operational Risk" is the risk of impeding business execution that causes losses and yields no profit. Risks under this category are typified by accidents, disasters, non-compliance, business errors, product defects, customer complaints, environmental pollution, system failures, terrorism, and labor problems. The term "Business Strategy Risk" refers to risks associated with business activities that exclude "Operational Risk" and significantly affect profit or loss. In addition to risks associated with current business strategies such as investments and finance, this category includes risks associated with the future business environment.

Risk Management Promotion Structure

Enterprise Risk Management Committee

The Enterprise Risk Management Committee, which is supervised by the Board of Directors, handles "Business Strategy Risk" and is tasked with the determination of risk management policies associated with Group operations and monitoring the status of risk management. In principle, this committee meets once every six months and requests reporting from other committees with regard to major risks categorized under "Operational Risk" or "Business Strategy Risk." Also, the committee provides the Board of Directors with updates on the status of its activities once a year in principle.

Risk Management Committee

We have established the "Risk Management Committee" tasked with handling "Operational Risk" and is promoting company-wide risk management by taking necessary measures in a timely and prompt manner. The committee holds periodic meetings on a quarterly basis to specify and select the prioritized risks for the entire Group, formulate countermeasures, and identify signs of their emergence while assessing newly emerging risks. In addition to deliberating on these and other matters related to the management of Operational Risk, including measures for risk prevention and managing the progress of such measures, the committee is responsible for submitting its conclusions to the Enterprise Risk Management Committee.

Other Risk Management Initiatives

Further Enhancement of Crisis Readiness Capabilities

We formulated the "Crisis Response Rules" as the highest rules for crisis response. These rules stipulate our policy on crisis response, crisis level definitions, reporting lines, and methods for establishing emergency task forces, among other matters related to crisis response.

Should an incident occur at any facility run by a group entity, the business unit responsible for the incident site will swiftly relay the ascertained risk-related information will be swiftly reported to the business unit responsible for the incident site and the General Affairs Department's Risk Management Section in accordance with these rules. This risk-related information will also be communicated to the Risk Management Committee as necessary. Furthermore, corporate and other relevant departments will work to assist or spearhead risk countermeasures undertaken at the incident site to minimize the social impact and potential damage.

Initiatives to Upgrade our Business Continuity Plans (BCPs)

In FY2006, we formulated BCPs assuming the occurrence of an earthquake with an epicenter in the Tokyo metropolitan area, a megathrust earthquake involving the Nankai trough, and the outbreak of avian influenza, respectively. Based on said BCPs, we have held annual comprehensive disaster drills and clarified problems regarding actual execution and coordination among all business bases in order to strengthen our practical response capabilities and have reflected appropriate revisions to the BCPs. In September 2020, we held the 14th round of the comprehensive disaster drill. To prevent the spread of COVID-19, this round was tried to implement fully online based, with approximately 200 individuals, including those from Head Office's task force, participating through their PCs. Also, each refinery, complex and plant carries out periodic disaster prevention drills encompassing their entire site in accordance with applicable crisis response regulations.

In FY2015, we were appointed as a designated public institution by the Cabinet Office and we accordingly announced the Disaster Prevention Action Plan. This plan was updated in conjunction with the business integration, with the latest edition being submitted to the relevant authorities in December 2019. As a designated public institution, we worked to ensure that the tanker trucks we operate in each prefecture have been registered for emergency use.

Online based comprehensive disaster drill

Countermeasures against the COVID-19 Pandemic

Based on our BCP assuming the outbreak of avian influenza, in February 2020 we established the task force headed by the President and Representative Director. Aiming to ensure the stable supply of petroleum products and materials, which are essential to supporting economic and social activities, we have constantly updated our relevant policies and measures in light of changes in social conditions. At the same time, we rallied the Group's overall strengths to protect the safety of employees and implemented thoroughgoing countermeasures to prevent the spread of infection.

■ **Outline of our initiatives**

January 2020	Distributed the first alert regarding the prevention of infection, urging the families of expatriates in China to temporarily return to Japan
February 2020	Established the task force chaired by the President and Representative Director
April 2020	In response to the declaration of a state of emergency, thoroughgoing and highly effective measures to prevent the spread of infection were immediately enforced. These measures included a general prohibition of commuting to company facilities and taking business trips.
May 2020	In conjunction with the lifting of the state of emergency, the aforementioned measures were partially relaxed. Discussion regarding the incorporation of new working styles was launched, with an eye to adapting to the new normal in the post-pandemic period.
July 2020	In response to a resurgence in the outbreak, preventive countermeasures were once again strengthened, with the target of decreasing the ratio of employees who commute to company facilities to less than 30%. (These restrictions on commuting were still place as of September 2020.)

Information Management

Information Management System

In line with the Information Security Basic Policies, the Idemitsu Group is endeavoring to ensure the confidentiality of its information assets and to simultaneously secure the accessibility and security of its information systems and networks. Utilizing information technologies, we are thus striving to maintain and enhance the level of customer services. In addition, Idemitsu has established the Customer Information Management Standards to appropriately collect and use customer information, keeping it up to date while safeguarding it. The standards also mandate the proper disposal of such information.

As part of our thoroughgoing information management measures, we mandate that all IT system users (including permanent and temporary employees as well as subcontractors) undergo annual information security education focused on Security Standards for the Use of IT Systems via e-learning. At the same time, each division carries out an autonomous inspection of information management every year and data security audits are implemented as part of periodic internal audits.

Should information leakage occur, the incident will be handled in accordance with the "Crisis Response Rules," and the Information Control Guidelines.

Employee education

● Information security education via e-learning

We provide annual e-learning programs (in Japanese, English and Chinese) to instill information security rules that must be observed by all IT system users. Targeting all Group employees at home and abroad, the 2020 round of these programs was implemented during the March – April 2020 period and completed by a total of 14,545 people, or 100% of targeted individuals.

● Specialized e-learning program

In FY2019, we also launched e-learning programs for employees tasked with handling or administering control systems. The 2020 round of this program was implemented during the February – March 2020 period and completed by a total of 4,516 people, or 100% of targeted individuals.

● Training on the handling of suspicious e-mails

On a quarterly basis, we implement training focused on handling targeted e-mail attacks, with the aim of mitigating the risk of contracting computer virus infections borne by suspicious e-mails and raising cybersecurity awareness among employees.

● In-house newsletters designed to raise employee awareness

We distribute the monthly cybersecurity newsletter via e-mail, calling employees' attention to relevant cybersecurity-related topics and thereby raising their awareness.