Corrective process against negative impacts | Risk management

GRI 2-12,16,25/403-2,4

Promotion of the Business Continuity Plan (BCP*)

NOF has formulated a BCP, to enable its core business to be continued or, if damaged, to be restored quickly while minimizing the loss of business assets in the event of a natural disaster such as an earthquake or tsunami, or an emergency situation such as the COVID-19 pandemic. The activities of the BCP Task Force to promote the BCP primarily focus on the formulation of the BCP manual which sets forth the responses to be implemented in normal times and in emergencies, in addition to the preparation and yearly renewal of information on the estimated damages to the plant and various government-, infrastructure- and supply chain-related information, which will be required when resuming operations. Additionally, the BCP Task Force performs annual internal audits and training in an effort to firmly establish the BCP and to enhance its effectiveness.

Information security management

(1) Management of trade secrets and protection of personal information

Recognizing the importance of information as one of our vital management resources to business activities and the indispensability of active strengthening of corporate competitiveness by active utilization of information and firm establishment of information security to steady business management, NOF has set forth the Information Security Policy as a basic principle for promoting effective utilization and protection of information. At the same time, recognizing protection of personal information as its obvious social responsibility, NOF has formulated and announced the Privacy Policy.

Under such policies, NOF has set forth specific measures for enhancing the levels of confidentiality, completeness, and utility of information and specific ways of handling personal information in its internal rules, including information security management rules, personal information protection rules, and information system-related sets of provisions, a confidential information handling manual, and an information equipment handling manual, and is ensuring their thorough understanding by the staff.

(2) Management setup

In the organizational aspect, the Information Security Management Subcommittee is set up, and under its chairperson, who has overall supervising responsibility for information security management, persons responsible for document information security management, electronic information and information system security management, and addressing complaints regarding personal information, as well as a person responsible for management at each level of organizational unit, are appointed to administer the implementation of specific measures. Against illicit access from outside and other risk factors including loss, destruction, and alteration, safety measures are taken at appropriate and rational levels. In addition, NOF continually reviews through internal auditing setups and measures pertaining to information security management and protection of personal information to improve them wherever necessary.

* The BCP (acronym for Business Continuity Plan) illustrates policies, systems, and procedures designed to prevent important operations from being interrupted even in the face of unforeseen events, such as a major earthquake or other natural disaster, the spread of infectious disease, a terrorist incident, a major accident, a disrupted supply chain (supply network), or a sudden change in our business environment, and, if business is interrupted, that it is restored within the shortest possible timeframe.