Corrective Process Against Negative Impacts | Risk Management

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

Information security management

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

NOF considers information assets as an important management resources in corporate activities, and the establishment of secure information assets are essential for achieving stable management, thus, we have established the Information Security Policy as a basic principle for promoting effective utilization and protection of information assets. At the same time, based on the recognition that protecting personal information is a fundamental social responsibility, NOF has established and published the Privacy Policy.

Under such policies, NOF has set forth specific measures for enhancing the levels of confidentiality, completeness, and availability of information and specific ways of handling personal information in its internal rules and manuals and is ensuring thorough dissemination and understanding within the company.

Such internal rules and manuals include: ‘Information Security Management Rules’, ‘Personal Information Protection Rules’, ‘Provisions Related to Information Systems’, ‘Information Equipment Handling Manual’, and ‘Confidential Information Handling Manual’.

Information assets: Information obtained from customers and business partners, trade secrets of NOF Group and personal information, and systems for utilizing such information

(2) Management structure

In the organizational aspect, the Information Security Management Subcommittee is set up to deliberate and make decisions on important matters related to information security. Under ‘Information Security General Manager’, who is the chairperson of the Subcommittee, ‘Document Information Security Manager’, ‘Electronic Information and Information System Security Manager’, ‘Personal Information Complaint Handling Manager’, as well as a person responsible for management at each division, production base and department are appointed to administer the implementation of specific measures.

Against threats such as unauthorized access from outside, information leakage, tampering, and destruction, appropriate and reasonable security measures are implemented. In addition, NOF continually reviews and strives to improve the information security management and personal information protection systems and measures through internal audits.

NOF Group Information Security Policy

The NOF group considers information assets as an important management resources in corporate activities, and the establishment of secure information assets are essential for achieving stable management, thus, our group shall establish and comply following policies.

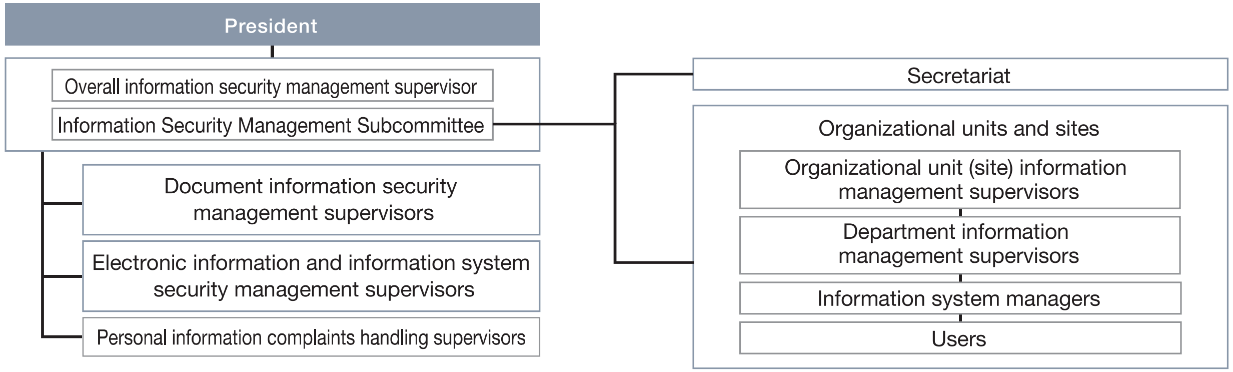
Information assets: Information obtained from customers and business partners, trade secrets of NOF Group and personal information, and systems for utilizing such information

1. **The NOF Group shall develop the information security system to further strengthen the management function of information assets.**
2. **In order to protect the information assets from leakage, falsification, and destruction, the NOF Group shall provide information security education for employees, develop regulations, and implement technical measures for information systems.**
3. **The NOF Group shall comply with laws, regulations, codes and contractual obligations related to information security.**
4. **In the event of an information security incident, the NOF Group shall respond promptly and appropriately to each incident and prevent a recurrence.**
5. **The NOF Group shall maintain and continually improve these efforts in this Policy.**

Corrective Process Against Negative Impacts | Risk Management

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

Diagram of NOF's information security management system


President
Overall information security management supervisor
Information Security Management Subcommittee
Document information security management supervisors
Electronic information and information system security management supervisors
Personal information complaints handling supervisors
Secretariat
Organizational units and sites
Organizational unit (site) information management supervisors
Department information management supervisors
Information system managers
Users

Risks and opportunities in information security and measures against risks

Risks and opportunities	Details	Measures
Risks	● Long-term stoppage of production, sales, and R&D activities and loss of corporate credibility due to cyberattacks (illicit access, malware infection) ● Loss of corporate trust and technological competitiveness due to leakage of confidential and personal information	● Conduct self-inspections, develop improvement plans, and implement improvement plans ● Information sharing through meetings of IT managers of domestic Group companies (once a year) ● Conduct training on handling suspicious emails (once a year) ● HDD encryption for computers taken outside the company, and restrictions on the use of private storage media ● Conduct information security-related training for employees (once a year)
Opportunities	● Improvement of company competitiveness through cybersecurity measures ● Earning of customer trust and enhancement of corporate brand value by strengthening information asset management ● Increased employee awareness through strengthened information security	-

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.

In fiscal 2023, as a response to information security risks, we conducted BCP training based on the assumption of a cyberattack, and confirmed the initial response procedures in the event of an incident and the roles of each department and site for business continuity. The training was designed to minimize damage in the event of a cyberattack and to improve response capabilities, including speediness.

* Abbreviation for Business Continuity Plan. The BCP 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.