Information Security and Personal Information Protection

Seven & i Holdings positions the appropriate protection and security of information assets handled by the Group as an important priority and social responsibility of its management and operations and as mandatory for all executives and employees. We strictly manage personal information received from customers in particular and take special care to prevent information leaks and other such incidents. Seven & i Holdings and Group companies protect customer information and other information assets possessed by the Group from various threats, including illegal access and cyberattacks. The Group as a whole recognizes that ensuring information security is an important issue in terms of both management and business. Seven & i Group has built information security management and personal information protection systems so that all executives and employees and all parties, including contractors, involved in our operations handle information assets appropriately and use them properly. These systems are disseminated to all executives and employees through education and training. In addition, we have established a management system that responds to changes in the environment related to social demands, compliance, and information security. We endeavor to appropriately manage and protect personal information and corporate information and are making continuous improvements.

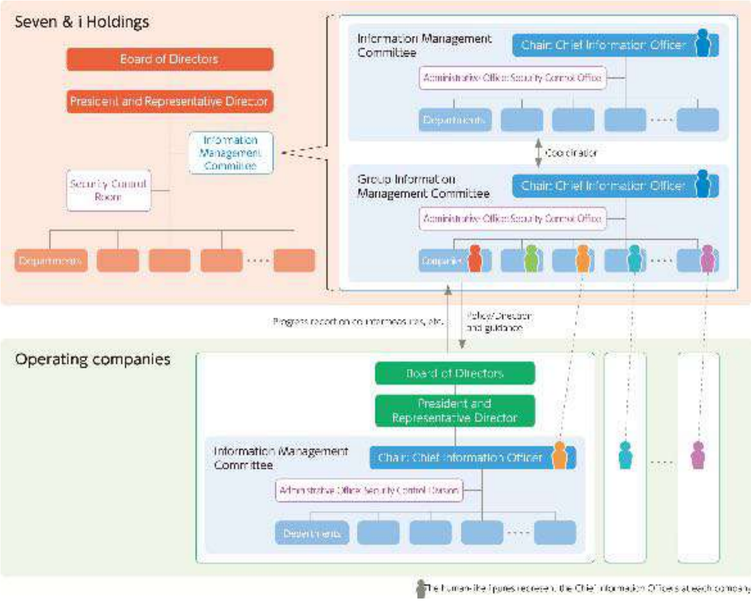
Development of Information Security Management System

Seven & i Holdings has established the Security Management Office under the direct control of the representative director as an organization that oversees information security for the entire group. The office prepares and disseminates to all group companies policies, attached rules, guidelines, and other documents related to information security and personal information protection. The office also supports Group companies in establishing information security management systems (ISMS), training security personnel, and developing monitoring systems, thereby strengthening overall information management.

The Group Information Management Committee of Seven & i Holdings, which oversees the Group, works with the information management committees of each company to establish and continuously improve management systems that respond to changes in the environment, including the planning, promotion, and management of information security-related measures. In addition, we promote thorough implementation of technical security measures through specialized subcommittees under our control to further ensure safety. Risks related to information security and the status of these activities are regularly reported to the Board of Directors for advice and instructions.

> More details about our Basic Policy on Information Security can be found here

> More details about our Personal Information Protection Policy can be found here


Seven & i Holdings
Board of Directors
President and Representative Director
Information Management Committee
Security Control Room
Departments
Information Management Committee
Chair: Chief Information Officer
Administrative Office: Security Control Office
Departments
Coordination
Group Information Management Committee
Chair: Chief Information Officer
Administrative Office: Security Control Office
Companies
Progress report on countermeasures, etc.
Policy/Direction and guidance
Operating companies
Board of Directors
President and Representative Director
Information Management Committee
Chair: Chief Information Officer
Administrative Office: Security Control Person
Departments
The human-like figures represent the Chief Information Officers at each company

Information security management system

Accident and Emergency Response Related to Information Security

Seven & i Holdings has established a reporting line among Group companies through the "Material Fact Reporting Guidelines," and has built a system to ensure the reliable communication of information and minimize damage and impact. In the unlikely event of an incident or suspicious event related to information security, we will strive to report it appropriately and without delay to the victim and all related parties in accordance with our reporting obligations under laws and regulations.

In the event of a serious incident, we promptly report it to the President and Chief Executive Officer and the Chief Information Management Officer.

Compliance with International Standards

Seven & i Holdings has established information security rules and regulations with reference to ISO 27001, an international certification standard related to information security, National Institute of Standards and Technology (NIST) Cyber Security Framework, Center for Internet Security (CIS) Controls, Ministry of Economy, Trade and Industry (METI) Cyber Security Management Guidelines, and so on. Seven & i Holdings and its group companies have established and are operating an information security management system (ISMS) based on these rules to control information security risks such as leakage, falsification, and service suspension of information assets. Through continuous improvement of this management system, we strive to maintain the confidentiality, integrity, and availability of our information assets.

In addition, major locations and related departments of our operating companies that deal with customers' personal information have been assessed and certified by a third-party organization for their ISMS organizational structure, and we are in the process of expanding the scope of certification.

> A list of ISMS certified locations can be found here (in Japanese)

Employee Training to Raise Awareness of Information Security and Cyber Security

Seven & i Holdings believes that to ensure the appropriate handling of personal information and confidential information in daily work, it is necessary for every executive and employee to understand the importance of information security, to raise their awareness of information security, and, on top of that, to have the knowledge required for accurate judgement and conduct.

Seven & i Holdings provides education several times a year about the latest trends in information security and personal information protection, management systems, and general information security measures through e-learning and online training programs for directors, managers, and general employees. The aims of education are responding appropriately to information security and cyber security threats, as well as laws and regulations concerning personal information and other matters. These educational materials are also being rolled out to all Group companies so that all executives and employees of the Seven & i Group can acquire the same level of knowledge.

In addition, we have opened an educational portal site with materials that can be quoted in manuals, meetings, etc. on information security, personal information protection, and so on, as well as a security video that can be borrowed. We are endeavoring to provide enlightenment so that all executives and employees can think and act for themselves.

Targeted Email Attack Training

The threat of cyberattacks by means of targeted email attacks is increasing day by day. Regular training is essential for all executives and employees to be able to respond properly if they come under attack. Seven & i Holdings sends multiple patterns of mock email to all executives and employees of the Group and strengthen their ability to respond through actual experience of how to discern suspicious email and how to respond should such email be received.

Strengthening of Cybersecurity Countermeasures

Seven & i Holdings has positioned cyberattacks, which are becoming more advanced and more sophisticated by the day, as a serious risk in management and is endeavoring to strengthen cybersecurity countermeasures, including the building of a multitiered defense network to guard against illegal hacking into networks, conduct proper access control, etc.; the establishment of a setup capable of responding to threats; the education and training of human resources; and collaboration with outside professional bodies.

(1) Establishment of special organization
As a special organization to handle cybersecurity, we have set up the 7&i Computer Security Incident Response Team (7&i CSIRT) to undertake security reviews of the information system and its operation and to promote cybersecurity countermeasures for the prevention of security incidents, such as vulnerability diagnosis by a third-party body, monitoring of illegal access, and vulnerability response.

(2) Education and training
At least twice a year, we implement education and training supposing a cybersecurity incident or accident so that if a cyberattack or the like does occur, we can respond swiftly and appropriately and minimize the damage. By thus improving the response capability of the special organization and all executives and employees, we ensure that our response setup and response measures against incidents and accidents function effectively.

(3) Outside collaboration
In order to be able to respond speedily to cyberattacks and so on, we collaborate with such outside organizations as the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) and the Nippon CSIRT Association, sharing information with them on cyberattacks, countermeasure trends, etc.