Information Security and Personal Information Protection

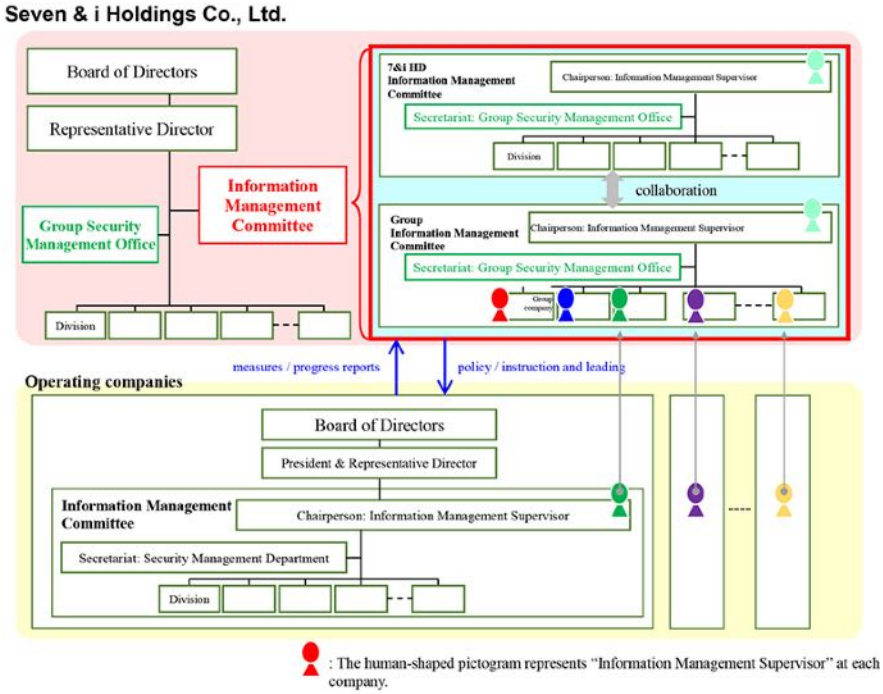
Seven & i Holdings and the Group companies recognize that it is an important management and business issue to protect customer information and other information assets held by the Group from various threats, including unauthorized access and cyber-attacks, and to ensure the information security of the entire Group.
Seven & i Group has established policies to ensure that all stakeholders involved in business operations, including executives, all employees, and contractors, handle and use information assets appropriately and correctly. The Group has built an information security management system and a personal information protection system, and aim to instill these practices through education and training for all executives and employees. Additionally, we have established a management system that responds to social demands, compliance, and changes in the information security environment, striving for the proper management and protection of personal and corporate information, and are committed to continuous improvement.

› 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

Development of Information Security Management System

Seven & i Holdings has established the Group Security Management Office directly under the President and Representative Director as an organization overseeing information security for the entire Group. This office develops policies, related regulations, and guidelines concerning information security and personal information protection, and disseminates them to Group companies. Additionally, it supports Group companies in building an Information Security Management System (ISMS), training security personnel, and establishing monitoring systems, thereby striving to strengthen overall information management.
The Group Information Management Committee of Seven & i Holdings, which oversees the Group, collaborates with the information management committees of each company to plan, promote, and manage information security measures. We establish a management system that responds to environmental changes and are committed to continuous improvement. Furthermore, we ensure thorough technical security measures through specialized subcommittees under our jurisdiction, promoting enhanced safety.
Risks related to information security and the status of these activities are regularly reported to the Board of Directors, where we receive advice and instructions.



Information security management system

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, NIST (National Institute of Standards and Technology) Cyber Security Framework, CIS (Center for Internet Security) Controls, 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.

【ISO27001 Certified Major Companies】
・Seven & i Holdings Co., Ltd.
・Seven-Eleven Japan Co., Ltd.
・Ito-Yokado Co., Ltd.
・Seven Financial Service Co., Ltd.
・Akachan Honpo Co., Ltd.
・THE LOFT CO., LTD
・Seven & i Food Systems Co., Ltd.
・Seven & i Netmedia Co., Ltd.
・Seven Culture Network Co., Ltd.

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.

Training to Raise Awareness of All Executives and Employees

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 for directors, managers, and general employees. These educational materials are also being rolled out to all Group companies as part of our efforts to ensure that all executives and employees of the Seven & i Group can acquire the same level of knowledge, and so that they are equipped with the ability to think and act on their own initiative.
In particular, the threat of cyberattacks by means of targeted email attacks is increasing day by day, meaning that regular training simulating responses to actual attacks is essential. 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.

Initiatives to Ensure Security for IT Services

IT services without appropriate security measures are at an increased risk of cyberattacks. In particular, a service that holds large amounts of personal data has the potential to lead to increased damage in the case that information leaks occur.
At Seven & i Holdings, the Group Security Management Office conducts security reviews prior to system releases to ensure prescribed levels of security quality are maintained for the information system.
In addition, vulnerability assessments are conducted while making use of external expertise before system releases or to coincide with modifications. These are performed under a mechanism to check for the presence of serious vulnerabilities with the potential to become the source of cyberattacks, with corrections implemented in advance of the release if vulnerabilities are found.

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.

Establishment of Special Organization and Outside Collaboration

As a special organization responsible for cybersecurity, we have set up the 7&i Computer Security Incident Response Team (7&i CSIRT), and have put systems in place designed to minimize impacts from security incidents by analyzing their causes and formulating responses in cooperation with the incident response contact points at Group companies.
We also 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, and related topics in order to be able to respond speedily to issues such as cyberattacks.
We implement education and training for incident response contact points at Group companies premised on a cybersecurity incident or accident at least twice per year, and are endeavoring to improve the capacity to respond to accidents for all Group companies, which includes reflecting the areas for improvement identified in accident response manuals.
We additionally aim to have in-house organizational mechanisms in place for the detection of issues such as cyberattacks and unauthorized logins and are creating systems to ensure efficient cybersecurity countermeasures are implemented at the Group.