

Cybersecurity & personal information management

Approach

GRI418-DMA

▶ Group Shared Policy on Information Security

Framework

GRI418-DMA

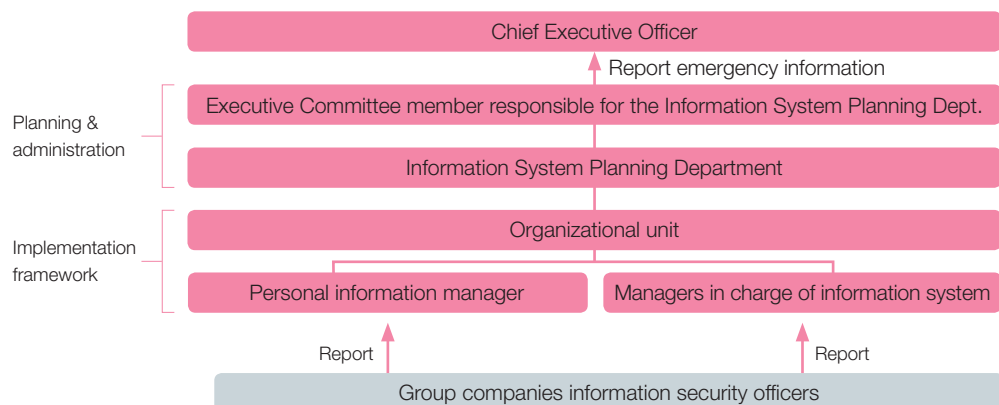
Basic Cybersecurity Policy

The Ajinomoto Group defines cybersecurity as a significant risk. As such, the Group is extremely attentive to the handling of customer and confidential corporate information and has formulated the Group Shared Policy on Information Security and related Group-wide regulations, standards and guidelines.

In 2019, the Group plans to create and adopt Group-wide guidelines on local area networks (LANs) to address the risks of information leakage from IoT devices and external hacking.

Information Security Management System

Each organization of Ajinomoto Co., Inc. and Group companies have established systems for appropriate response to information security incidents and other emergency situations in which information flows all the way to the CEO.



Rigorous management of personal information

To securely manage customer data and other personal information, the Ajinomoto Group informs relevant organizations of clearly defined rules and procedures as part of its organizational business management.

At Ajinomoto Co., Inc., the Personal Information Management Guidelines under the Information Security Regulations specify rules and procedures for securely handling personal information. The guidelines are based on the ISO 27001 standard for information security management systems.

When operations are outsourced, the contractor's business and systems are assessed to ensure a similar high level of information security. The Company has been building a system for managing customer personal information more strictly on the collection of personal information for campaigns, consumer surveys, etc. The rules demand the selection of personal information managers under the jurisdiction of organizational managers, and clarify the persons responsible for or in charge of the collection, storage and deletion of personal information, as well as who might access or use the collected data.

Following revisions to the Personal Information Protection Law in Japan in May 2017, the Company has revised its internal processes and handling guidelines, and is regularly educating personal information managers in each organization. Regarding transfer of personal information among Group companies out from Europe, the Group complies with the requirements of the EU's General Data Protection Regulation (GDPR), which went into effect in May 2018.

Performance

GRI418-DMA

Information Security Initiatives

Main information security trainings in fiscal 2018

- Group training for line managers in business and sales divisions: Three times, 220 participants
- Group training for line managers in production and R&D divisions: Three times, 187 participants
- Group training for new hires: 87 participants
- Comprehension test on information handling via e-learning for all employees of Ajinomoto Co., Inc.: 3,560 participants (89.4%)

The Company also conducted training on targeted mail attacks for new employees.

Ongoing initiatives to prevent leakage of confidential information

In Japan, the Ajinomoto Group introduced an AI-driven user behavior detection system on standard PCs for thorough detection of fraud. After adoption in four companies including Ajinomoto Co., Inc., it is currently being expanded into other Group companies.

The Group builds a consistent vulnerability response strategy by conducting annual external security checks of each Group company's website.

Information security inspections

Ajinomoto Co., Inc. conducts annual information security inspections at all worksites. The inspections mainly focus on the basic elements of proper information handling, including management of IT equipment, confidential information, and personal information. The Company also conducts annual checks of external cloud service use and its management status.