Information security

Basic policy

The FineToday Group Code of Conduct and Ethics (see p. 60) calls for managing confidential information and personal information appropriate and preventing its misuse. This is intended to prevent cases such as loss or leakage of such information. Based on this code, the Group strives to protect and properly manage the important information assets it holds, through establishment of related rules and regulations, including the FineToday Group Information Security Policy, and sharing with employees of all business sites information on the importance of and our responsibility for information management.

– Information security rules and regulations

- Information Security Policy
- Information System Management Regulations
- Information System Use Regulations
- Rules on bring your own device (BYOD) policies, external storage, information devices, antivirus measures, and software
- Confidential Information Management Regulations
- Regulations on Handling of Information Assets
- The FineToday Group Global Personal Information Protection Policies
- Privacy Policy
- Personal Information Protection Regulations
- Regulations on Handling of Specific Personal Information

– Subjects of the FineToday Group Information Security Policy

1. Purpose
2. Definitions
3. Information security promotion structure
4. Outsourcee assessment
5. Education, inspection, auditing
6. Practical procedures
7. Duties of employees and others

Information security system

FineToday Group has appointed the Group Chief Information Security Officer (CISO) holding comprehensive responsibility for handling of information assets and information systems throughout the Group. In this way, the Group strives to maintain a robust information security system.

Each Group company appoints a person responsible for managing the handling of information assets and information systems inside the company. It also maintains and thoroughly puts into practice rules and regulations on control of confidential information, protection of personal information, information system administration, and information security measures, as well as carrying out activities such as security measures, education, and drills. The CISO oversees these activities and provides additional instructions as needed.

Furthermore, periodic meetings on information security are held to continually improve the information security system of the Group as a whole.

Handling of personal information

FineToday Group has established The FineToday Group Global Personal Information Protection Policies in recognition of its responsibility to handle personal information safely and securely.

These policies apply to all Group companies. The implementation plans of Group companies and promotional campaigns will establish individual policies and rules on the handling of personal information in line with this policy and with applicable laws, regulations, etc.

Website **Privacy Policy**
https://www.finetoday.com/en/privacy/

Information security

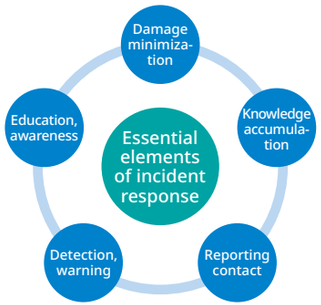
Responding to information security incidents

FineToday Group adopts an advanced zero-trust security model to enhance its measures to counter information security incidents. For example, it configures access controls to prevent unauthorized access to confidential information through business systems. It also has established the Security Operation Center (SOC) to monitor for external threats and detect and report cyberattacks 24 hours/day, 365 days/year. Group internal hotlines also accept reports concerning information security.

In FY2023, FineToday Group organized a Computer Security Incident Response Team (CSIRT) that specializes in responding to information security incidents. The CSIRT members come from FineToday's IT, general affairs, and corporate communications sections. The Group recognizes the importance of acting quickly in response to any incidents. Instead of relying on its systems and structures alone, the Group plans to have staff undergo continual specialized education and drills. The FineToday Chief Information Officer (CIO), who is responsible for Group cybersecurity, will respond to any serious incidents through an emergency response structure. To improve response capabilities even more, plans call for conducting drills that involve related business sections as well.

– Roles of the CSIRT

- Improving response capabilities through regular drills and training of team members
- Taking leadership in responding to information security incidents and minimizing their damage (internal and external cooperation)
- Serving as a single contact point for internal and external reporting



Cybersecurity assessment

FineToday took an independent cybersecurity assessment in FY2022. It strives to counter constantly changing cybersecurity risks by assessing risk levels objectively and, based on the results of this assessment, defining and taking actions to strengthen its responses further.

– Information security KPIs <FineToday Group>

Total number of cybersecurity incidents, including intrusions	0
Total number of violations of information security related to leaks of customer personal information	0
Total number of customers affected by intrusions on company data	0
Total amounts of fines/penalties paid in connection with information security violations or other cybersecurity incidents	0 yen

Information security education and training

FineToday Group provides education and training for executives and employees to prevent information security incidents and enhance its systems for managing them. In FY2023, FineToday will carry out new drills for responding to the cyberthreat of targeted email attacks.

– State of information security education and training (FY2022) <FineToday>

e-Learning	
Eligible persons	All employees other than executives, temporary employees, and contractors
Topics	Preventing information security intrusions
Employees eligible for training	380
Employees who underwent training (participation rate)	376 (99%)