Specific Management Plans and Resource Allocation

Safety precautions	
Strengthening knowledge and skills of personnel	Enhancement of employees' cyber security awareness: New employees are required to complete the education training on information security arranged for new employees. Each employee receives a follow-up training every year.
	Enhancement of cyber security awareness: Electronic newsletters or notices about cyber security are sent from time to time to help employees get to know cyber security practices and understand types of the cyber security attacks occurring externally. 14 newsletters/notices were sent in 2022.
	Cyber attack drills: Phishing email testing is conducted twice a year to verify cyber security awareness of employees.
	Respect of intellectual property right: iST prohibits using illegally or cracking portable software.
	Enhancement of cyber security skills: Cyber security technicians are designated from time to time to participate in external training on cyber security tools or programs on hacker attack and defense technology to enhance cyber security literacy and skills. iST arranged for 26 technicians to participate in training in 2022.
Avoiding information disclosure	Encryption: Document encryption software is installed to protect confidential information files and reduce the risk of unauthorized disclosure of confidential information.
	Authorization: Access to the files is controlled by setting levels of authorization based on necessity.
	Network management: Warnings are issued, and inspection is conducted, for abnormal network traffic. Transmitting data to an external unit must be applied for and approved.
	Access control: Employees are not allowed to bring in personal storage devices or use personal equipment to take photos or film.USB ports are banned to be used in storage devices.
Conducting routine maintenance works	Audit and improvement: Systems are inspected and improved periodically. New technologies are adopted to enhance data protection. Compliance with requirements of the management system is secured through internal audits conducted periodically and audits conducted by external cyber security certification units. In 2022, an internal audit and an external verification audit were conducted, and the information security task force held a meeting every month to review relevant matters.
Ensuring services being available	Backup management: Important systems are backed up and are renewed or upgraded for cyber security subject to the annual plan. A backup and recovery test was conducted in 2022.
	Cybersecurity: To enhance protection of internal and external cyber attacks, the firewall policy is adjusted and review, the detection of cyber attacks is activated, the anti-virus system is updated periodically, and bugs are repaired and prevented. Enhanced protection is provided for important machines. Micromolecule firewalls are adopted to enhance lateral protection. iST has joined SP-ISAC Cyber Security Framework to receive significant intelligence to share. In 2022, the vulnerability assessment was conducted and information system vulnerabilities were patched as much as possible.