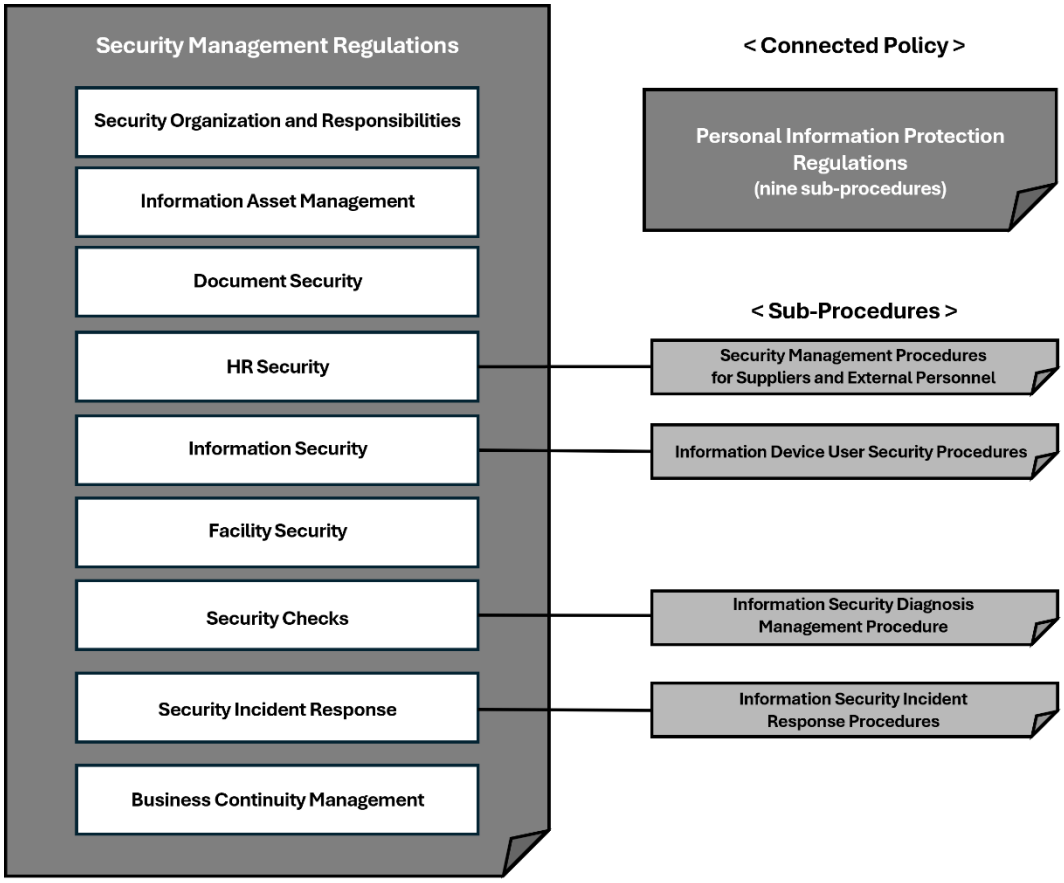
Security Management Regulations

Department : Information Security Officer

SK Innovation (hereinafter "SKI") has established administrative, technical, and physical protection measures to ensure the business continuity of its assets, including company information, information systems/devices, equipment, and facilities, against threats such as theft, tampering, destruction, and interruption. The Information Protection Policy comprises the Security Management Regulations and four sub-procedures, with personal information governed by the specialized Personal Information Protection Regulations. This policy applies to all SKI workplaces, employees, supplier employees engaged in SKI's business, and all visitors to SKI. It reflects relevant laws such as the Act on Promotion of Information and Communications Network Utilization and Information Protection, the Act on the Protection of Information and Communications Infrastructure, and the Act on Prevention of Divulgence and Protection of Industrial Technology. The policy is periodically reviewed and updated to reflect changes in the environment, including legal amendments.



[Figure] Diagram for Security Management Regulations and Sub-procedures Relationship

◇ Security Organization and Responsibilities

SKI appoints a Chief Information Security Officer (CISO) and reports this appointment to the Ministry of Science and ICT in accordance with the Act on Promotion of Information and Communications Network Utilization and Information Protection. The CISO forms an information protection organization and develops and implements an annual information protection plan, including inspections, improvements, awareness programs, and mock drills, in line with SKI's policy.

◇ Information Asset Management and Document Security

SKI defines all information and related information systems, personnel, facilities, equipment, etc., as information assets and establishes graded protection management standards based on

their importance. Specifically, SKI's documents are classified as core secrets, secrets, and internal use only, with strict controls on their creation, use, storage, and destruction according to their classification. Documents and information assets containing personal information are governed by detailed regulations in the "Personal Information Protection Regulations."

◇ HR Security

SKI stipulates the roles and responsibilities of not only its members but also the employees of suppliers engaged in SKI's business to comply with SKI's rules and regulations. When joining SKI or signing a contract, employees must sign information security pledges and undergo information protection training before starting work. During employment, SKI supervises the safe use of information assets in accordance with its information protection policy. Upon retirement or contract termination, employees must return business assets and accounts and sign pledges not to leak company information acquired during their employment. Additionally, SKI conducts regular awareness-raising activities such as information protection training and information protection letters to encourage employees to voluntarily practice information protection. For external personnel, who statistically pose a higher security risk, additional security measures are stipulated through the "Security Management Procedures for Suppliers and External Personnel."

◇ Information Security

SKI defines and manages technical information protection measures for information systems and devices as information security. Information devices (desktop PCs, laptops, tablets, etc.) must apply authentication functions such as ID/PW to prevent sharing with others and install security programs to detect and block malicious code. Additionally, information devices must apply security functions such as restricting the use of external Internet services unrelated to work, and specific user compliance requirements are stipulated in the "Information Device User Security Procedures." For information systems (hardware, software, applications, networks, etc.), SKI applies information security policies such as access control, account and authority management, and password management from the time of introduction, and conducts periodic risk assessments during their operation to ensure business continuity from information security threats.

◇ Facility Security

SKI designates restricted and controlled areas where its critical facilities or equipment are installed. Restricted areas are off-limits to unauthorized outsiders and require guided and monitored access. Controlled areas are areas where information assets require special protection, and entry is strictly prohibited except for authorized personnel. SKI thoroughly manages access to restricted and controlled areas by deploying security personnel and installing access control devices. Additionally, items brought into or out of protected areas require prior review and approval, and their history is managed in accordance with SKI policy.

◇ Security Checks

SKI periodically plans and conducts checks to ensure compliance with the information protection policy. Security checks evaluate the level of security by comprehensively considering not only SKI's policies but also information protection-related laws and recent incident cases. Vulnerabilities in information security found through inspections are shared with relevant organizations for improvement and continuous history management. The procedures and methods for security checks are detailed in the "Information Security Diagnosis Management Procedure."

◇ Security Incident Response and Business Continuity Management

SKI prepares for security incidents in advance so that SKI's business can grow stably. SKI defines the types of security incidents by identifying the scope and scale of damage to SKI and establishes a business continuity management plan to ensure that business is not interrupted in the event of an incident. In addition, SKI has established "Information Security Incident Response Procedures" that describe the roles and methods from incident reception to investigation, analysis, recovery, and prevention of recurrence so that SKI can respond quickly in the event of any incident.