Information Protection Policy

SK Telecom (SKT) is fully committed to its new mandate for the digital age, which is creating new values by leveraging digital technologies, making sure technologies, products, and services it provides can guarantee the customers' rights. SKT always strives to bring more benefits across society to make more people enjoy the products of digital technologies. For information protection, SKT aims to maintain information accuracy and completeness based on confidentiality, integrity and availability, while ensuring business continuity by providing access to information and systems when needed. Therefore, setting targets, developing plans and ensuring implementation is always done on a Company-wide scale, and a corporate system is also being developed to prevent information security breaches based on the latest security schemes and processes more rigorous than those required by law. By doing so, SKT is offering communications infrastructure and services users can trust.

SK Telecom puts the first priority on protecting personal information and human rights. To this end, it is offering training to all of its employees to raise awareness and working to fully establish the corporate culture aligned with the mission. When government agencies request data, SKT ensures to comply with the processes and restrictions stipulated by the applicable laws, and carefully reviews to prevent any potential infringement on users' rights. It is also reinforcing core capabilities for information protection by advancing its data security platform and infrastructure, which are built on 5G and AI technologies.

A. Policy Scope

This Policy applies to all types of information assets, both tangible and intangible, owned by all employees and the Company. SKT also expects its external stakeholders including customers and partner companies to comply with the Policy.

B. Governance

SKT is operating an information protection implementation system under the board of directors and the ESG committee where its top management including CEO, COO and CSPO manage information protection risks across the Company. In accordance with the Personal Information Protection Law and other applicable laws, SKT has appointed CISO/CPO who is an expert in information protection and ICT with longer than 20 years of experience to manage information protection by the Company. CISO/CPO also leads a weekly brief session on information protection issues and tasks.

C. Management System

(1) Management Process

SK Telecom has introduced the latest and best security system and process more rigorous than required by the applicable laws in terms of network infrastructure, data and service. Information protection is

included in the key risk management areas of the corporate risk management system.

(2) Management Scope

Network infra security	• Undertake national ICT infra inspection annually on the core ICT infra for mobile phone operation • Conduct annual ISMS (Information Security Management System certification program governed by the Ministry of Science & ICT) certification • Inspect technical and administrative vulnerabilities of major server and network equipment
Data security	• Acquired ISMS and ISMS-P (Information Security Management System certification program managed by the Ministry of Science & ICT and the Personal Information Protection Commission) certifications • Encrypt important data to prevent unauthorized access • Control access and logging through access control solutions that grant server/DB access only to pre-authorized users
Service security	• Maintain a safe service environment by conducting security vulnerability checks, mock hacking/trainings for new/changed services • Install and operate access control devices such as intrusion prevention/detection systems

(3) System Certification

SK Telecom has been receiving audits both by its internal team and an outside agency to maintain its highest information protection standards. The Company has acquired information/personal information protection management system certifications such as ISMS, ISMS-P in addition to ISO/IEC 27001, 27017, 27018 certifications based on the international standards and is maintaining the certifications thorough regular renewals.

(4) Prevention of Breach

SK Telecom is operating a security control center 24/7 by having hacking detection/analysis/blocking system in place to respond to cybersecurity threats. For secure operation, it is also conducting system security inspections and mock hackings to eliminate any potential vulnerabilities.

D. Personal Information Protection

(1) Personal Information Protection Principles

① Minimum collection: Information should be collected only to the minimum extent required for the stated business purpose, which should be clearly informed to the customer before obtaining consent.

② Safe storage: Customer's personal information must be stored and managed securely from internal and external access.

③ Usage aligned with the purpose of consent: Personal information should only be used and provided for the purposes to which the customer has consented.

④ Strengthening external management: Personal information provided to external parties such as subcontractors or affiliates should be protected by strengthening the management of such external parties.

⑤ Timely destruction: Personal information that has been withdrawn, terminated, or expired should be appropriately classified and destroyed to prevent any further usage.

(2) Personal Information Protection Process

SK Telecom complies with all relevant laws, including the Personal Information Protection Act, and pursuant to its provisions, discloses the privacy policy on its website so that customers can easily access it at any time. SKT uses the collected personal information for customers, such as for service provision and quality improvement, and manages it safely through technical and administrative measures beyond the level specified by the relevant laws.

① Personal information collection

Except as indicated below, SK Telecom will not sell, exchange, lease any of your personal information to any organization or individual. SK Telecom collects personal information only to the extent consented by the customer for its service provision. In accordance with the Personal Information Protection Act, SKT notifies all subscribers of the items of collected personal information, the purpose of collection and the retention period. SKT utilizes the collected personal information only within the scope of the stated purpose and immediately destroys the personal information after achieving the purpose. Customer information can only be provided to third-party organizations with the consent of the customer or as stipulated by separate laws and regulations. It is also strictly prohibited to rent, sell or provide personal information to third parties for purposes other than those ‘required by laws’ or ‘transaction/service provision’.

② Customers’ right to control their own personal information

SK Telecom periodically updates its personal information policy to inform users or their legal representatives of their rights and how to exercise them. Users can view, modify, delete, or request access to their personal information at any time through ‘myT’ page or the 114 Customer Center on the T world website.

③ Response to cyber threats to customers

SK Telecom has established and operates a dedicated organization to respond to the latest cyber threats to customers. The Company has also expanded its security scope from traditional areas such as system hackings or customer data leaks to social engineering crimes such as smishing or voice phishing, and is establishing strategies and conducting customer protection activities to preemptively respond to such new threats.

④ Response procedure for customer data breach

In the event of security incidents such as customer information breach/leakage, or confirming such risks, SK Telecom immediately reports it to the Customer Information Protection Department, and supports the preservation of relevant evidence for external investigations and legal responses. SKT also notifies/reports to relevant organizations within 72 hours after detecting a customer information breach incident.

E. Information Protection Education & Change Management

(1) Information Protection Education

SK Telecom offers information protection training for all employees and subcontractors at least once a year to prevent the risk of customer information misuse or leakage and enhance the corporate brand value. The training program is designed based on the positions and tasks of the recipients, and improved by incorporating feedback.

(2) Change Management

SK Telecom is strengthening the responsibility of its employees and external companies by developing specific implementation plans for customer information protection, and granting incentives/penalties based on the protection level. It is also promoting various activities such as campaigns and PR initiatives that can continuously improve the mindset for customer information protection.

(3) Strengthening the protection of personal information of partners

SK Telecom regularly diagnoses the risks of its business partners at least once a year to protect customers' personal information and privacy and prevent information leakage incidents. It also conducts regular diagnosis on its distribution network, along with the targeted diagnosis based on data analysis, while reviewing and improving the customer information handling system, and providing raise awareness education for customer information protection.

Addendum (May 28, 2024)

This Policy is effective as of May 30, 2024.

Young Sang Ryu, SK Telecom President & CEO



* SK Telecom updates this Information Protection Policy in accordance with the corporate policy management rules, and implements and discloses this Policy both internally and externally to improve its information protection status.