SK Telecom 정보보호 정책

SK텔레콤㈜은 디지털 시대에 새로운 임무를 부여 받았습니다. 디지털 기술을 활용해 새로운 가치를 창출하되, 고객의 권리를 보장할 수 있도록 기술과 상품, 서비스를 제공해야 합니다. 아울러, 디지털 기술의 장점을 누구나 누리며 사회에 더 유익한 결과를 가져올 수 있도록 책임을 다해야 합니다. SK텔레콤㈜의 정보보호의 핵심 원칙은 기밀성, 무결성, 가용성 기반으로 정보의 정확성과 완전성을 유지하며, 필요 시 정보와 시스템에 접근 가능하도록 보장하여 업무 연속성을 유지하는 것을 목표로 하고 있습니다. 또한, 정보보호에 관한 목표 설정부터 구체적인 이행 계획 수립, 이행까지 전사적으로 실현하고 있습니다. 법이 정한 수준 이상의 최신 보안 시스템과 프로세스를 적용해 정보보안 침해 예방 시스템을 구축하고 있으며, 고객이 안심하고 이용할 수 있는 통신 인프라 및 서비스를 운영하고 있습니다.

SK텔레콤㈜은 개인정보보호와 인권 보호를 최우선 가치로 두고 있습니다. 이를 위해 전 구성원을 대상으로 개인정보보호 교육을 실시하여 인식을 제고하고, 관련 문화를 정착시키는 데 노력하고 있습니다. 또한, 정부 기관 등의 자료 요청에 대해서는 현행법에서 규정한 절차와 제한에 따라 진행하며, 이용자의 권리를 침해하지 않도록 검토합니다. 더불어, 5G와 AI 기술을 결합한 정보보안 플랫폼과 보안 인프라를 고도화 하여 정보보호의 핵심 역량을 강화하고 있습니다.

가. 적용범위

본 정책은 회사의 모든 임직원과 회사가 보유하고 있는 유무형의 모든 정보자산에 대하여 적용합니다. 아울러, 고객, 협력사 등 외부 이해관계자에도 본 정책의 준수를 기대합니다.

나. 정보보호 거버넌스

SK텔레콤㈜은 이사회와 ESG위원회의 총괄 아래 CEO를 비롯한 COO, CSPO 등 주요 최고 경영진이 전사 차원의 정보보호 리스크를 관리하는 정보보호 추진체계를 구축하고 있습니다. 개인정보보호법 등 관련 법률에 따라 정보보호최고책임자(CISO) 겸 개인정보보호책임자(CPO)를 정보보호 담당으로 지정했습니다. CISO/CPO는 정보보호, 정보기술 분야의 업무를 20년 이상 수행한 경력이 있는 전문 인력을 선정했으며, 정보보호최고책임자(CISO)주관으로 매주 정보보호 이슈 및 업무보고 회의를 진행하고 있습니다.

다. 정보보호 관리체계

(1) 정보보호 관리 프로세스

SK텔레콤㈜은 네트워크 인프라, 데이터, 서비스 영역에서 법령이 정한 수준 이상의 최신, 최선의 보안 시스템과 프로세스를 적용해 운영하고 있습니다. 또한, SK텔레콤㈜ 전사 통합 리스크 관리체계에서 핵

심 리스크 관리 영역으로 포함되어 관리하고 있습니다.

(2) 정보보호 관리 영역

네트워크 인프라 보안	• 이동전화 운용 등 핵심 정보통신 인프라를 대상으로 매년 국가 정보통신 기반 시설 점검 수검 • ISMS(과학기술정보통신부 주관 기업 정보보호 인증제도) 인증 매년 수행 • 주요 서버·네트워크 장비 대상 기술적·관리적 취약점 점검 수행
데이터 보안	• ISMS 및 ISMS-P(과학기술정보통신부·개인정보보호위원회 주관 정보보호 및 개인정보보호 관리체계 인증제도) 인증 취득 • 중요 데이터는 암호화 처리를 동해 비인가 접근 원천 차단 • 서버·DB 접속은 사전 인가자만 접근 제어 솔루션을 통해 접근 통제 및 로깅
서비스 보안	• 신규·변경 서비스는 보안 취약점 점검, 모의해킹·모의훈련 등을 시행하여 안전한 서비스 환경 유지 • 침입차단시스템·침입탐지시스템 등 접근 통제 장치 설치 및 운용

(3) 정보보호 시스템 인증

SK텔레콤㈜은 최고의 정보보호 수준을 유지하기 위해 매년 내부 감사와 제3자 독립기관으로부터 감사를 시행하고 있습니다. ISMS, ISMS-P 인증 등 정보보호 및 개인정보보호 관리체계 인증과 함께 국제 표준인 ISO/IEC 27001, 27017, 27018 인증을 획득하였으며, 정기적인 갱신을 통해 인증을 꾸준히 유지하고 있습니다

(4) 정보보호 침해 예방

SK텔레콤㈜은 사이버 보안 위협에 대응하기 위해 해킹 공격 탐지·분석·차단 시스템을 구축하여 24시간×365일 통합보안관제센터를 가동하고 있습니다. 아울러 시스템 보안 진단, 해커 관점에서의 모의해킹을 통해 취약점을 제거하여 시스템을 안정적으로 운영하고 있습니다.

라. 개인정보보호

(1) 개인정보보호 원칙

① 최소 수집의 원칙: 사업목적에 맞는 최소한의 정보를 고객에게 구체적으로 알리고 이에 대한 동의를 받아야 한다.

② 안전보관의 원칙: 고객의 개인정보를 내·외부의 접근으로부터 안전하게 보관·관리해야 합니다.

③ 목적 내 활용의 원칙: 고객이 동의한 목적으로만 개인정보를 이용·제공해야 한다.

④ 외부 관리 강화의 원칙: 위탁업체 및 제휴업체 등 외부업체관리를 강화하여 외부에 제공된 개인정보를 보호해야 한다.

⑤ 적시 파기의 원칙: 동의 철회, 해지, 기간 만료된 개인정보를 활용하지 않도록 적정하게 분류·파기해야 한다

(2) 개인정보보호 프로세스

SK텔레콤㈜은 개인정보보호법을 비롯한 모든 개인정보 관련 법률을 준수하고, 관련 법령에 따라 고객이 언제나 개인정보처리방침을 용이하게 열람할 수 있도록 홈페이지에 공개하고 있습니다. 수집한 고객의 개인정보는 SK텔레콤의 제반 서비스 제공과 품질 개선 등 고객을 위한 용도로 사용하며 관련 법령이 명시하는 수준 이상으로 기술적·관리적 보호 조치를 통해 안전하게 관리하고 있습니다.

① 개인정보 수집

SK텔레콤㈜은 서비스 제공을 위해 가입자의 사전 동의에 따라 고객이 동의한 범위에서만 개인정보를 수집하고 있습니다. 개인정보보호 관련 법령에 따라 모든 가입자에게 수집하는 개인정보 항목, 수집 목적, 보유 기간 등을 고지하고 있으며, 수집된 개인정보는 명시한 목적 범위 내에서만 활용하고 이용 목적을 달성한 개인정보는 즉시 파기합니다. 고객 정보의 제3자 기관 제공은 고객이 동의하거나 별도 법령에서 정한 경우에만 가능하며, '법의 요구' 또는 '거래/서비스 제공' 이외의 목적으로 개인정보가 제3자에게 임대, 판매, 또는 제공하는 것을 엄격히 금지하고 있습니다.

② 개인정보 자기통제권 보장

SK텔레콤㈜은 개인정보처리방침을 주기적으로 현행화하고 있으며, 이를 통해 이용자나 법정대리인의 개인정보보호 관련 권리와 행사 방법을 안내하고 있습니다. 이용자는 언제든지 T world 홈페이지 내 'myT' 페이지나 114 고객센터를 통해 자신의 개인정보를 조회하거나 수정·삭제할 수 있으며, 열람을 요청할 수 있습니다.

③ 고객에 대한 사이버 위협 대응

SK텔레콤㈜은 고객에 대한 최신 사이버 위협에 대응하기 위해 전담 조직을 신설하여 운영하고 있습니다. 기존 시스템 해킹, 고객정보 유출 대응 등 전통적인 보안 영역에서 스미싱, 보이스피싱 등 사회공학적 범죄로 보안 영역을 확장하여 새로운 위협에 선제 대응하기 위한 전략 수립과 고객 보호 활동을 수행하고 있습니다.

④ 고객정보 침해 대응 절차

SK텔레콤㈜ 고객정보의 침해, 유출 등의 사고가 발생하거나 사고 발생의 위험이 확인된 경우, 즉시 고객정보보호 총괄부서에 신고하게 되어 있으며, 사고 발생 시에는 외부기관 조사 및 법적 대응을 위한 관련 증거가 훼손되지 않도록 지원하고 있습니다. 고객정보사고 인지 후 72시간 이내에 관련 기관에 통지 및 신고 조치를 시행하고 있습니다.

마. 정보보호 교육 및 변화관리

(1) 정보보호 교육

SK텔레콤㈜은 고객 정보의 오남용 및 유출사고의 Risk를 사전 방지하고, SK텔레콤의 Brand Value를 제고 하기 위해 전체 임직원 및 수탁업체 대상으로 연간 1회 이상의 정보보호 교육을 실시하고 있습니다. 교육은 대상자의 직위와 업무에 맞게 필요한 내용으로 진행되며, 교육 결과에 대한 피드백을 통해 개선과 반영이 이루어지고 있습니다.

(2) 변화관리

SK텔레콤㈜은 고객정보보호 추진계획 수립 시 구체적인 계획 반영하고, 고객정보보호 수준에 따른 Incentive/Penalty 부여 등을 통해 구성원 및 외부업체의 고객정보보호 책임을 강화하고 있습니다. 캠페인, 홍보 활동 등을 통해 고객정보보호 Mind-set 이 지속적으로 향상시킬 수 있는 다양한 활동을 추진하고 있습니다.

(3) 협력사 개인정보보호 강화

SK텔레콤㈜은 고객의 개인정보와 사생활을 보호하고 정보 유출 사고를 예방하기 위해 협력사의 리스크를 연 1회 이상 주기적으로 정밀 진단하고 있습니다. 유통망 정기 진단과 데이터 분석을 통한 타깃 진단, 고객정보 취급 업무 체계 점검과 개선, 고객정보보호 인식을 제고하기 위한 교육도 함께 진행하고 있습니다.

부　칙 (2024년 5월 28일)

본 정보보호 정책은 2024년 5월 30일 부로 시행한다.

SK텔레콤 대표이사 사장 유영상

* SK텔레콤㈜는 사규관리규정에 따라 본 정보보호 정책을 업데이트하고, 정보보호 이행 정도의 향상을 위해 본 정책을 수행하고 대내·외적으로 공개합니다"