SK telecom

2025 SECURITY WHITE PAPER

고객의 신뢰를 지키는 정보보호,
투명하고 책임 있는 실행으로 이어가겠습니다.

SK텔레콤 정보보호백서

PART 1 정보보호 거버넌스

PART 2 정보보호 아키텍처

PART 3 개인정보보호

통합보안센터

2025

목차

변화하는 위협 환경 속에서
고객 신뢰를 지키기 위한
SK텔레콤의 정보보호 활동을
정리했습니다.

CONTENTS

INTRO 발간 개요

PART 1 정보보호 거버넌스

PART 2 정보보호 아키텍처

PART 3 개인정보보호

CLOSING 맺음말

발간 개요

백서 발간의 배경과 SK텔레콤이 지키고자 하는 정보보호의 원칙을 소개합니다.

INTRODUCTION

01 CEO 발간사

02 CISO 발간사

03 추천사

04 정보보호 혁신 추진 경과

05 정보보호 혁신 과제

CEO MESSAGE

CEO 발간사

SK텔레콤은 **고객 신뢰를 최우선으로** 정보보호의 기본을 다시 세우고,
고객이 누릴 **더 안전한 통신 서비스를 위한 변화와 실행**을 지속하고 있습니다.

고객 여러분과 이해관계자 여러분께,

SK텔레콤은 대한민국의 통신 인프라를 책임지는 기업으로서 고객의 일상을 연결하고 산업의 디지털 전환을 이끌어 왔습니다. 이제 통신 서비스는 단순한 연결 수단을 넘어 사회적 기반이 되었으며, 고객의 정보를 안전하게 보호하는 일은 통신사가 반드시 지켜야 할 책무이자 핵심 가치입니다.

최근 AI와 클라우드 등 디지털 서비스의 확산으로 사이버 위협이 더욱 정교해지고 있습니다. 이러한 환경에서 보안은 **고객 신뢰의 기반이자 지속가능한 성장을 뒷받침하는 경영의 핵심 어젠다**가 되었습니다.

SK텔레콤은 고객 신뢰를 회복하기 위해 정보보호 체계를 다시 점검하고, 조직·투자·기술 등 전 영역에 걸쳐 고객 보호 관점으로 실행력을 높이고 있습니다. 정보보호 투자를 확대하고, 통합보안센터를 중심으로 전사적 보안 관리 체계를 강화하여 경영진의 의사결정이 현장의 철저한 보안 실행으로 이어지도록 최선을 다하고 있습니다.

무엇보다 중요한 것은 고객이 체감할 수 있는 '실질적인 변화'입니다. SK텔레콤은 고객 정보를 더욱 안전하게 보호하고, 스미싱·보이스피싱 등 고객의 일상을 위협하는 사이버 범죄로부터 고객 피해를 예방하기 위한 선제적이고 다각적인 노력을 멈추지 않을 것입니다.

이번 정보보호백서는 SK텔레콤이 추진해 온 정보보호 및 개인정보보호 활동과 향후 개선 방향을 고객과 사회에 투명하게 설명해 드리기 위해 마련되었습니다. 완성된 결과를 선언하기보다, 더 안전한 통신 서비스를 만들기 위한 변화의 과정과 지속적인 실행 의지를 담고자 했습니다.

SK텔레콤은 고객의 정보를 안전하게 지키는 일을 그 무엇보다 우선으로 하겠습니다.
지속적인 투자와 실행을 통해 고객이 안심하고 이용할 수 있는 디지털 서비스 환경을 만들어 가겠습니다.

SK텔레콤 대표이사 사장
정재헌

CISO MESSAGE

CISO 발간사

정보보호는 **유기적으로 연결된 전사 실행체계로 작동할 때** 실질적인 효과를 가집니다.
이번 백서는 SK텔레콤의 정보보호 활동을 **일관된 실행체계**로 구축하여
빠르게 변화하는 위협에 대응하기 위한 보호 방안을 설명합니다.

고객 여러분과 이해관계자 여러분께,

디지털 서비스 환경이 빠르게 변화하면서 정보보호의 범위와 책임도 함께 확대되고 있습니다. AI, 클라우드, 공급망, 개인정보, 고객 접점 영역의 변화는 보안 위험이 특정 시스템이나 조직에 국한되지 않고 서비스 운영 전반에 영향을 줄 수 있음을 보여줍니다.

특히 최근 위협은 AI를 활용해 더 빠르고 정교하게 변화하고 있습니다. 피싱·사회공학·계정 탈취·악성 행위 자동화 등 다양한 위협이 AI와 결합하면서 기존 방식만으로는 충분히 대응하기 어려운 환경이 되고 있습니다. SK텔레콤은 AI 기반 위협 탐지·분석 역량을 강화하고, 새로운 AI 보안 이슈에도 유연하게 대응할 수 있는 보안 체계로 고도화하고 있습니다.

SK텔레콤은 변화하는 위협 환경에 대응하고 고객 신뢰를 높이기 위해 **정보보호 체계 전반**을, **전사 관점에서 재점검**하였습니다. 그 결과를 토대로 정보보호 혁신 과제를 구체화하고, 조직·정책·기술·고객 보호 전반의 개선을 단계적으로 추진하고 있습니다.

이번 백서에서는 각 활동이 왜 필요하고 어떤 기준과 체계로 운영되며 앞으로 어떻게 고도화될 것인지를 정리하였습니다.

고객 신뢰는 한 번의 조치와 노력으로 만들어지지 않습니다. 올바른 방향의 활동을 꾸준히 실행하고, 그 결과를 책임 있게 설명하는 과정이 쌓일 때 신뢰는 다시 세워질 수 있을 것입니다. SK텔레콤은 신속한 대응을 위해 추진할 과제와 시간이 소요되지만 반드시 필요한 보안 인프라의 구축·임직원 역량 강화를 균형 있게 추진해 나가겠습니다.

SK텔레콤 정보보호최고책임자 (CISO)
이종현

ENDORSEMENT

추천사

오늘날 정보보호는 디지털 사회에서 기업이 이용자와 맺는 신뢰 계약의 핵심이며, 수천만 가입자의 민감한 통신 데이터를 다루는 통신사에게 있어 그 책임은 더욱 무겁습니다. 정보보호는 기술적 조치에 그치지 않고, 개인정보 처리 원칙·프라이버시 거버넌스·구성원의 실천 문화가 유기적으로 작동할 때 비로소 실질적인 이용자 보호로 이어집니다.
SK텔레콤이 이번 백서를 통해 사고 이후의 개선 과정을 투명하게 공개하고, 정보보호와 프라이버시 체계 전반을 종합적으로 정리한 것은 책임 있는 기업이 취할 수 있는 가장 성숙한 대응이라 평가합니다. 이 백서가 통신산업은 물론 우리 사회의 정보보호·프라이버시 논의를 한 단계 심화시키는 의미 있는 계기가 되기를 기대합니다.

권헌영 교수
고려대학교 정보보호대학원

사이버 공격은 이제 특정 기업만의 문제가 아니라 우리 사회 전체의 신뢰와 직결되는 경영 과제가 되었습니다. 이때 무엇보다 중요한 것은 사고의 발생 여부가 아니라, 사고를 통해 무엇을 배우고 어떻게 개선해 나가는가에 있습니다. 그러한 점에서 SK텔레콤이 이번 정보보호백서를 통해 그동안의 개선 활동과 성과를 투명하게 공개하는 것은 매우 의미 있는 노력이라고 생각합니다. 정보보호는 일회성 프로젝트가 아니라 지속적인 점검과 개선, 투자와 훈련, 그리고 조직 문화의 정착을 통해 완성되는 여정입니다.
앞으로도 SK텔레콤이 정보보호에 대한 꾸준한 투자와 투명한 소통을 통해 국민과 고객으로부터 더욱 신뢰받는 기업으로 발전해 나가기를 바랍니다.

김승주 교수
고려대학교 정보보호대학원

이동통신망은 우리 사회의 핵심 인프라이며, 정보보호는 통신사업자의 가장 중요한 책무 중 하나입니다. 보안은 완성된 상태가 아니라 지속적으로 검증하고 개선해야 하는 과정입니다. 새로운 위협을 식별하고, 방어 체계를 점검하며, 발견된 문제를 개선하는 노력이 반복될 때 비로소 신뢰가 만들어질 수 있습니다.
최근 SK텔레콤은 정보보호를 경영과 운영의 핵심 과제로 인식하고 조직, 투자, 검증 체계를 강화하고 있습니다.
특히 정보보호 활동과 개선 과정을 외부에 공개하고 설명하려는 이번 백서 발간은 국내 정보보호 문화의 성숙에 기여할 수 있는 의미 있는 시도라고 생각합니다.

김용대 교수
카이스트 정보보호대학원

보안을 이미 완료된 결과가 아니라 진행형으로, 투명하게 담아낸 점이 인상 깊습니다. 특히 CEO 직속 통합보안센터와 이사회 보고 체계는 보안에 대한 진정성을 보여줍니다. 공격자는 끊임없이 새로운 침투 경로를 찾습니다.
그래서 꾸준한 점검을 통해 개선하고 검증하는 절차야말로 진정한 보안 역량입니다.
현장을 중심으로 이러한 피드백이 지속될 때, 보안 수준도 점차 성숙해집니다.
이번 백서가 산업 전반에 '일상화된 보안'의 중요성을 환기하는 계기가 되길 기대합니다.

박찬암 대표
㈜ 스틸리언

최근 빈발하는 해킹사고 및 개인정보유출 사고로 인해 정보보호는 기술적 과제인 동시에, 기업의 법적·사회적 책임이 함께 작동하는 준법 경영의 핵심 영역이 되고 있습니다. 특히 사고 예방과 대응 과정에서 사실관계의 투명한 공유, 책임 있는 조치, 재발방지 체계의 정비는 정부, 소비자 등 모든 이해관계자의 신뢰를 좌우하게 됩니다. AI를 활용한 사이버 공격에 대비한 준비도 철저히 해나가는 한편 또한 관련 법령과 글로벌 규범의 변화에 맞춰 내부 통제와 관리체계를 지속적으로 점검·개선하는 노력이 중요합니다.
이번 백서가 SK텔레콤의 정보보호 수준을 한층 더 끌어올리고, 책임 있는 보안문화를 확산하는 계기가 되기를 기대합니다.

이기주 회장
한국CISO 협의회

디지털 서비스가 고도화될수록 정보보호 및 개인정보보호는 기술 이슈를 넘어 사회적 신뢰를 설계하는 문제입니다. 특히 이용자 관점에서 '어떻게 보호되고 있는지'를 이해할 수 있도록 설명하고, 책임 있게 운영하고 실천하는 태도가 중요합니다.
정보보호백서는 기업의 운영 원칙과 실천적 개선 방향을 투명하게 공유하는 대표적인 수단이 될 수 있습니다. SK텔레콤의 백서가 신뢰 기반의 디지털 생태계를 확산하는 데 의미 있는 출발점이 되기를 바랍니다.

최경진 교수
가천대학교 법과대학

INNOVATION PROGRESS

정보보호 혁신 추진 경과

투명하게 공개하고, 책임 있게 대응하며, 지속적으로 실행합니다.

SK텔레콤은 사고 인지 이후 **고객 보호 조치, 개선 실행체계 구축**을 순차적으로 추진하며,
정보보호 역량 강화를 위한 후속 과제를 지속 이행하고 있습니다.

SK텔레콤 정보보호 혁신 추진 타임라인

'25.04
사고 인지 및 신고
- 사고를 자발적으로 인지·신고
- 관계기관 협력 조사 착수
- 고객 보호조치 안내

'25.05
개선 실행체계 가동
- 고객가치혁신TF 가동
- 그룹 정보보호혁신 특별위원회 출범
- 고객안심패키지 발표

'25.07
정보보호혁신안 발표
- 정보보호투자, 거버넌스 개편, 제로 트러스트 정보보호 체계 구축 등 중장기 목표 선언
- 정보보호 혁신 과제 수립 및 이행

'25.10~
대고객 안심 보안 서비스 확대
- 에이닷 AI 통화/문자 보안 서비스 런칭(10월)
- 대고객 모바일 보안 솔루션 제공(11월)
- 사이버 침해보상 보증제도 도입(12월)

우리가 지켜온 3가지 원칙

01 투명성

숨기지 않고, 있는 그대로 공개합니다.

SK텔레콤은 사고를 자발적으로 인지하고 관계기관에 신고하는 등 투명하게 사실을 공개했습니다.

02 책임성

문제의 원인부터 후속 조치까지 끝까지 책임집니다.

SK텔레콤은 사고 원인 규명과 고객 보호 조치를 우선 이행하고, 재발 방지를 위한 과제 이행 및 완료까지 책임 있게 관리합니다.

03 지속성

한 번의 대응이 아닌, 꾸준한 실행으로 이어갑니다.

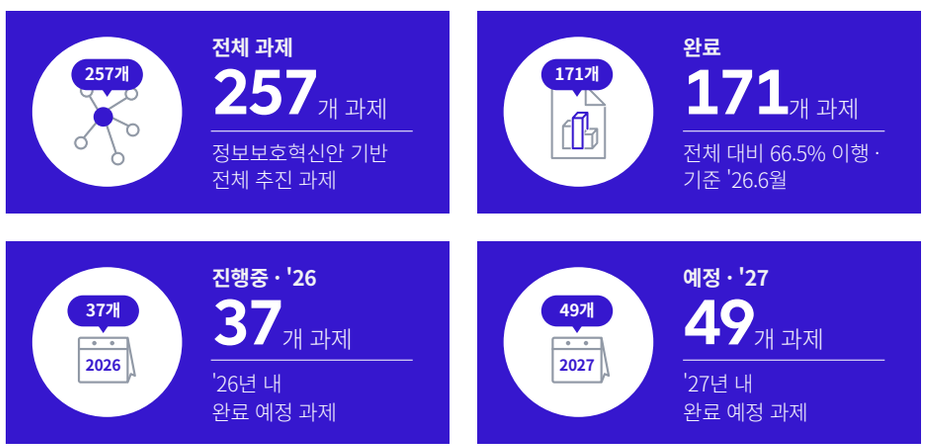
일회성 사후 조치에 그치지 않고, 재발 방지와 보안 고도화를 위한 활동을 지속 수행하여 고객 신뢰를 견고히 다져갑니다.

PROGRESS DASHBOARD

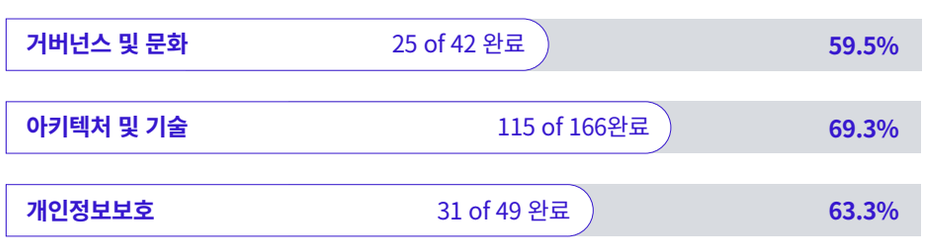
정보보호 혁신 과제

신뢰는 선언이 아니라 검증 가능한 지속적 실행에서 비롯됩니다.

SK텔레콤은 정보보호혁신안을 수립하고, 이를 바탕으로 **총 257개의 혁신 과제**를 선정하여 **거버넌스 및 문화 · 정보보호 아키텍처 및 기술 · 개인정보보호** 세 영역에서 단계적으로 이행하고 있습니다.



영역별 이행률 비교



정보보호 혁신과제 이행 현황

영역	대과제	실행 과제 수	완료	'26 진행중	'27 예정
거버넌스 및 문화	전사 Security Literacy 강화	6	4	-	2
	사고유형별 대응체계 고도화	11	7	2	2
	내부정보보안강화	2	2	-	-
	보안 정책 및 지침 제정	3	3	-	-
	보안 전문인력 확대/육성체계	7	5	-	2
	전사 Security Portal 외 4개 과제	13	4	2	7
아키텍처 및 기술	전사 IT/NW 통합 자산관리 체계	15	12	2	1
	주요 정보 암호화 확대	12	10	2	-
	전사 계정/권한관리체계 구축	16	14	2	-
	Micro Seg.기반 NW보안 강화	18	15	1	2
	AI기반 보안위협탐지 체계 강화	11	8	2	1
	DevSecOps	9	6	3	-
	공급망 보안 체계	6	4	2	-
	복구시나리오 고도화	13	10	2	1
	악성코드 탐지 강화 외 15개 과제	66	36	10	20
개인정보보호	개인정보보호 강화	16	6	3	7
	고객보호 서비스 개발	7	6	1	-
	스팸/스미싱 대응 고도화	14	8	2	4
	유심 인증키 암호화 적용	4	4	-	-
	개인정보 처리 시스템 이상행위 탐지 강화 외 5개 과제	8	7	1	-
합계		**257**	**171**	**37**	**49**

정보보호 거버넌스

책임 있는 의사결정과 체계적인 실행으로 정보보호 거버넌스를 운영합니다.

PART 01

01 개요

02 CEO 직속 통합보안센터

03 글로벌 표준 기반 정보보호정책 체계

04 정보보호 투자

05 모의훈련 및 임직원 보안 기본 역량 강화

06 6대 보안 실천 지침

07 정보보호 인증 감사

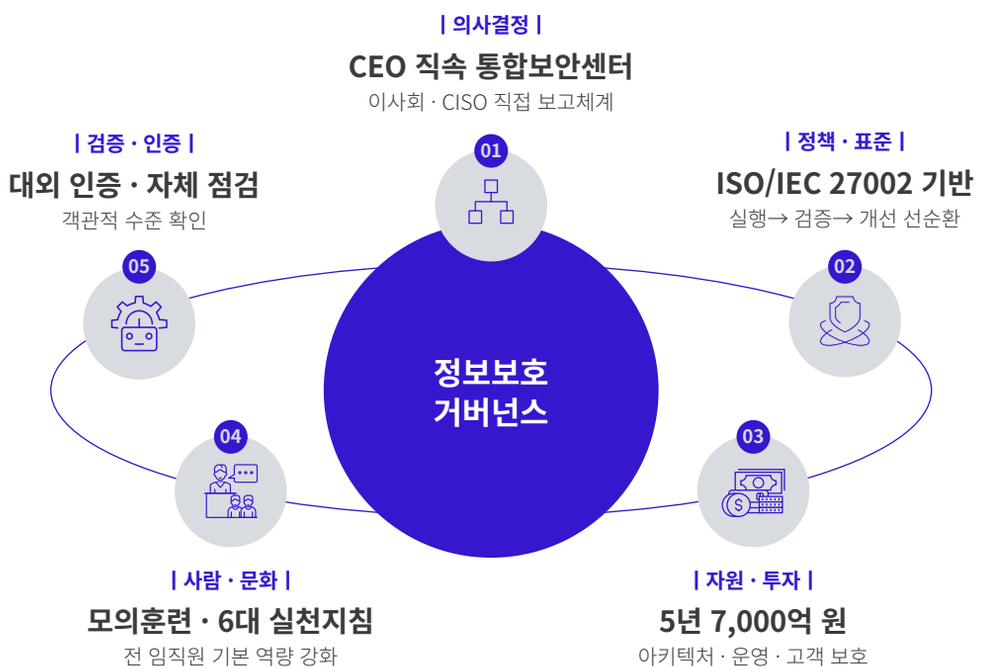
OVERVIEW

개요 – 정보보호 거버넌스

기준은 엄격하게, 보호는 철저하게

SK텔레콤은 정보보호 거버넌스를 **의사결정 · 정책 · 투자 · 문화 · 검증**의 다섯 축으로 재정립하여, 변화하는 위협 환경에 대응할 수 있는 **하나의 통합 운영체계**로 작동시키고 있습니다.

SK텔레콤 정보보호 거버넌스 체계



거버넌스 운영 원칙

01 CEO · CISO가 직접 책임

정보보호는 **최상위 의사결정의 책임**이라는 원칙 아래, CISO가 이사회에 직접 보고하는 독립적 운영구조를 두고 있습니다.

02 글로벌 스탠다드 기준의 정책 적용

ISO/IEC 27002 등 **국제 표준 정보보호 프레임워크**를 기반으로 정책과 절차를 정립하고, 표준이 실제 현장에서 효과적으로 작동하는지 정기적으로 검증합니다.

03 지속적 투자를 통한 보안 고도화

정보보호 투자(T+B) 기준 **5년간 약 7,000억** 원을 투입하여 보안 아키텍처 및 기술, 운영·대응 역량, 고객 보호 체계를 지속적으로 강화합니다.

04 전 임직원이 공감하고 실천하는 보안 문화

거버넌스는 특정 부서가 아닌 **전 임직원이 일상에서 실천**할 때 완성됩니다. 분기별 모의훈련과 6대 보안 실천 지침으로 일관성을 확보합니다.

05 외부 검증을 통한 객관적 수준 확인

자체 점검에 더해 **ISMS · ISMS-P 등 대외 인증**과 외부 감사를 정기적으로 수검함으로써, 운영 수준을 객관적 시각에서 점검·개선합니다.

CEO 직속 통합보안센터

전사 보안 컨트롤타워로서 신속하게 판단하고 대응합니다.

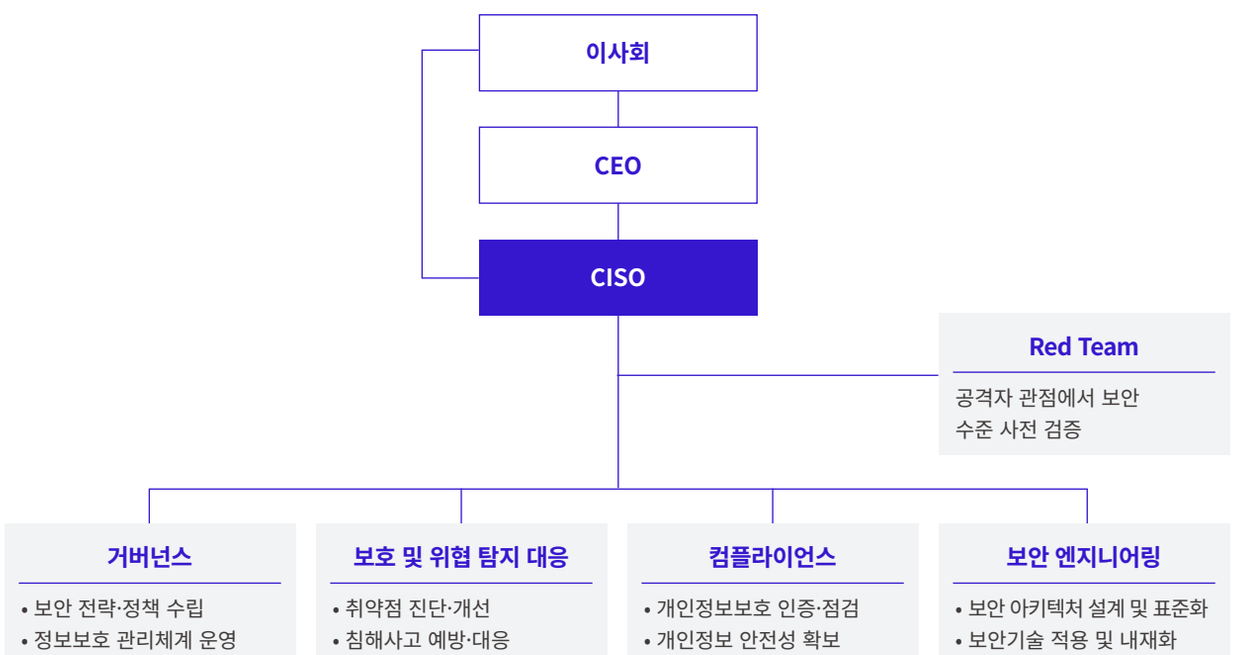
SK텔레콤은 **CEO 직속의 CISO 체계 아래 통합보안센터**를 중심으로 전사 관점에서 위험을 관리하며, **CISO가 이사회에 직접 보고하는 독립적 의사결정 체계**를 운영하고 있습니다.

통합보안센터는 보안 전략 수립, 보호 및 위협 탐지 대응, 개인정보보호 및 컴플라이언스, 보안 엔지니어링의 4개 기능을 연계하여 주요 보안 현안이 하나의 체계 안에서 일관되게 관리되도록 운영합니다.

이와 함께, 외부 공격자 관점에서 방어체계의 실전 대응력을 검증하는 CISO 직속 모의해킹 전담조직 **레드팀(Red Team)**을 운영하여, 보호 관점의 점검만으로는 확인하기 어려운 잠재 위험을 사전에 식별하고 즉시 개선 과제로 연결하고 있습니다.

CISO는 보안 현안과 주요 의사결정 사항을 **정기적으로 경영진과 이사회에 직접 보고**하여, 현장의 보안 이슈가 경영진의 판단과 자원 배분에 신속하게 반영될 수 있도록 거버넌스 체계를 운영하고 있습니다.

SKT 통합보안센터 조직도



글로벌 표준 기반 정보보호정책 체계

정책은 현장 검증과 개선으로 선순환되도록 합니다.

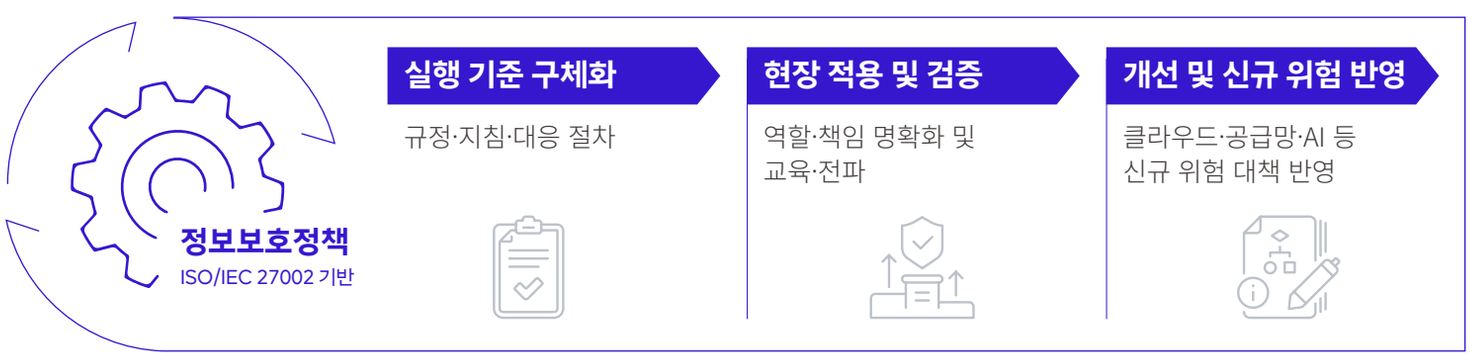
모든 임직원이 같은 기준으로 보안 활동을 수행하기 위해 명확한 정책과 절차가 필요합니다.
SK텔레콤은 **ISO/IEC 27002** 기반으로 정보보호정책 체계를 재정비하여,
실행 → 검증 → 개선의 선순환 구조로 운영하고 있습니다.

SK텔레콤은 **국제 정보보호 표준인 ISO/IEC 27002를 기반으로 정책 구조를 전면 재정비**하였습니다.
정책 구조를 국제 기준에 맞게 재편하는 한편, 보안 규정과 지침이 실제 업무 현장에서 실질적으로 활용될 수 있도록 실행 기준과 대응 절차를 구체화했습니다.

재정비된 정책은 현장 적용 과정에서 역할과 책임을 명확히 하고, 교육·전파와 검증을 통해 이행 수준을 지속적으로 점검합니다.
이를 통해 정책이 문서에 머무르지 않고 업무 수행 기준으로 작동하도록 운영하고 있습니다.

또한 클라우드·공급망·AI 등 급변하는 기술 환경과 새로운 보안 위협을 정책 체계에 반영하여, 신규 위험에 대응할 수 있는 기준을 지속적으로 보완하고 있습니다.

정보보호정책 운영 구조도



정보보호 투자

일회성이 아닌 지속 투자로 고객 신뢰를 지킵니다.

사이버 위협이 정교해지고 서비스 환경이 빠르게 변화할수록 정보보호 역량은 **지속적인 투자**로 뒷받침되어야 합니다. SK텔레콤은 **보안 아키텍처 · 운영·대응 역량 · 고객 보호** 세 영역에 투자를 집중하고 있습니다.

5-YEAR INVESTMENT

5년간 약

7,000 억 원

정보보호 공시(T+B) 기준 7,000억 원 투자

기준: 2025-2029 회계연도 누적 편성 금액

정보보호 투자를 디지털 인프라와 서비스 전반의 보안 수준을 높이기 위한 전략적 투자로 인식하고, 보안 아키텍처 전환부터 고객 보호 서비스 강화까지 **포괄적 관점**에서 추진합니다.

주요 투자 영역 및 방향

ARCHITECTURE

보안 아키텍처 고도화

- IAM, SASE, Micro Segmentation 도입 등 제로 트러스트 기반 보안 체계 확대
- 전사 자산관리 체계 구축 및 보호 대상 가시성 확대

OPERATIONS

AI 기반 보안 운영·대응 역량 강화

- AI 기반 보안 취약점 진단 자동화
- AI 기반 보안관제 체계 구축 및 보안 이벤트 통합 분석 고도화
- AI 기반 개인정보 비식별 처리 솔루션 도입

CUSTOMER PROTECTION

고객 보호 강화

- 개인정보보호 관리체계 고도화 및 고객 데이터 보호 조치 고도화
- 스미싱·보이스피싱 탐지·차단, 고객 알림·상담·모바일 보안 서비스 확대

모의훈련 및 임직원 보안 기본 역량 강화

강한 보안은 꾸준한 훈련과 실천으로 완성됩니다.

SK텔레콤은 보안 사고 발생 시 전사 임직원이 각자의 **역할과 할 일을 명확히 인지하고 대처**할 수 있도록 **분기별 모의훈련**을 시행하고, **임직원의 보안 기본 역량 강화**를 위한 **보안 인식 제고 프로그램**을 확대 운영하고 있습니다.

Runbook 기반 분기별 보안 모의훈련

보안 사고 대응 Runbook

보안 사고 시나리오 유형별 상세 수행 프로세스와 필요 활동을 정의하여, 사고 발생 시 일관된 대응을 보장하는 표준 절차서입니다.

PROCESSES	ACTIVITIES
8개 프로세스	**67개 활동**

보안 모의훈련 운영

Runbook의 실효성을 검증하고 임직원의 실전 대응 역량을 강화하기 위해 분기별 모의훈련을 시행합니다.

훈련 과정에서 도출된 개선 사항은 Runbook에 반영하여 대응 절차를 지속적으로 고도화 합니다.

목적	전사 위기대응 역량 강화
일정	'25.11월 시행 · '26년부터 분기 단위 지속
방식	시나리오 기반 도상훈련

임직원 보안 기본 역량 강화

보안 인식 제고 프로그램

모든 임직원이 업무 과정에서 기본적인 보안 원칙을 이해하고 실천할 수 있도록 보안 교육과 가이드를 운영하고 있습니다.
교육은 단순한 이수 활동에 그치지 않고 **실제 업무 판단으로 이어질 수 있도록** 시의성 있는 주제를 선정하고 전달 방식을 지속적으로 개선합니다.

교육 핵심 영역

개인정보보호
수집·이용·파기 원칙

안전한 시스템 이용
접근·계정·암호 관리

내부정보 보호
사내 주요 정보 유출 예방

생성형 AI 활용 유의사항
AI 시대 새로운 보안 원칙

6대 보안 실천 지침

일상 업무 속에서 보안이 실천되도록 합니다.

Security First 문화는 임직원이 고객 정보와 정보자산을 다루는 **모든 업무 과정에 보안을 먼저 고려**하는 것부터 시작됩니다. SK텔레콤은 **보안 실천 지침 제정 · 인식 제고 캠페인**을 통해 보안 실천을 일상 업무에 정착시키고 있습니다.

보안 실천 지침 제정

보안은 모든 임직원이 일상 업무 속에서 함께 실천해야 하는 기본 원칙입니다. SK텔레콤은 고객 정보, 시스템·데이터, 외부 협업 등 업무 전반에서 임직원이 준수해야 할 **6대 영역의 보안 실천 지침**을 제정하였습니다.

각 영역의 업무 과정에서 유의해야 할 사항과 기본 준수 기준을 제시하여, 임직원이 자신의 업무와 관련된 보안 책임을 이해하고 필요한 조치를 확인할 수 있도록 구성되어 있습니다.

보안 실천 문화 확산

SK텔레콤은 보안 실천 지침이 임직원의 업무 수행 과정에서 실질적으로 적용될 수 있도록 전사 공지, 팀 단위 기본지키기 워크숍, 임직원 단말 PC 화면보호기를 통한 전파 등 다양한 방식으로 반복 안내하고 있습니다. 또한 IT자산 내 고객정보 식별 캠페인을 통해 임직원이 자신의 업무 환경을 스스로 점검하고 보호 필요성을 인지하는 자율적 보안 문화를 만들어 가고 있습니다.

6대 보안 실천 지침

1 사용자 보안
정보보호를 위해 임직원이 준수해야 할 보안 지침

2 서비스 보호
서비스 개발·운영 과정 전반 보안 강화를 위한 지침

3 고객정보 보호
소중한 고객 정보를 안전하게 보호하기 위한 지침

4 내부정보 보호
사내 주요 정보 유출을 방지하기 위한 지침

5 정보자산 보호
정보자산의 등록~폐기까지 자산 보호를 위한 지침

6 물리 보안
회사 주요 시설과 자산을 안전하게 보호하기 위한 지침

6개 영역은 **전사 임직원이 매일 마주하는 업무 환경**에 맞춰 설계되었으며, 일상 속 보안 판단의 기준이 됩니다.

정보보호 인증·감사

정보보호 관리 수준을 객관적으로 검증하고 있습니다.

정보보호 체계는 구축하는 것만큼 **지속적으로 점검하고 개선**하는 것이 중요합니다.
SK텔레콤은 정보보호 인증, 주요 인프라 평가, 대내외 감사와 자체 점검을 통해
관리 수준을 객관적으로 확인하고 있습니다.

정보보호 인증 및 관리체계 운영

SK텔레콤은 ISMS 및 ISMS-P 등 국내 주요 인증을 통해 정보보호 및 개인정보보호 관리체계의 적정성을 인증 받고 있으며, 정기적인 심사와 개선 활동을 수행하여 인증 수준을 지속적으로 유지 및 발전시키고 있습니다.

이 외에도 SK텔레콤은 다양한 외부 평가와 내부 점검을 통해 정보보호 관리체계가 실제 운영 환경에서 효과적으로 작동하는지 지속적으로 확인하고 있습니다. 주요 점검과 감사 결과는 개선 과제 도출과 후속 조치로 연계되며, 이를 통해 정보보호 체계의 적정성과 운영 수준을 객관적으로 검증하고 있습니다.

대외인증

ISMS
정보보호
관리체계 인증

ISMS-P
정보보호 및
개인정보보호
관리체계 인증

점검

주요정보통신 기반시설 점검
중요 정보시스템의
기술적·관리적·물리적
보안 점검

5G 협의회 이통사 기지국 점검
기지국
보안 점검

위치정보 관리실태 점검
위치정보의 보호 및
이용 등에 관한 법률
준수 점검

자체 보안 점검
정기·비정기적
내부 점검 활동

외부 감사
전사 차원의
외부 점검

※ 2026년부터 ISMS-P 단일 인증 체계로 운영

정보보호 아키텍처

제로 트러스트 아키텍처를 기반으로 식별 → 보호 → 탐지 → 대응 → 복구
5단계가 하나의 흐름으로 작동하는 SK텔레콤의 통합 보안 아키텍처입니다.

PART 02

01 **개요**

02 **[식별]** 서버 및 SW 보안 가시성 확보

03 **[보호]** 다중방어체계

04 **[탐지]** AI 기반 위협 탐지

05 **[대응]** 사고 대응 절차 표준화

06 **[복구]** 침해 사고 복구

07 **차세대 보안 기술 개발**

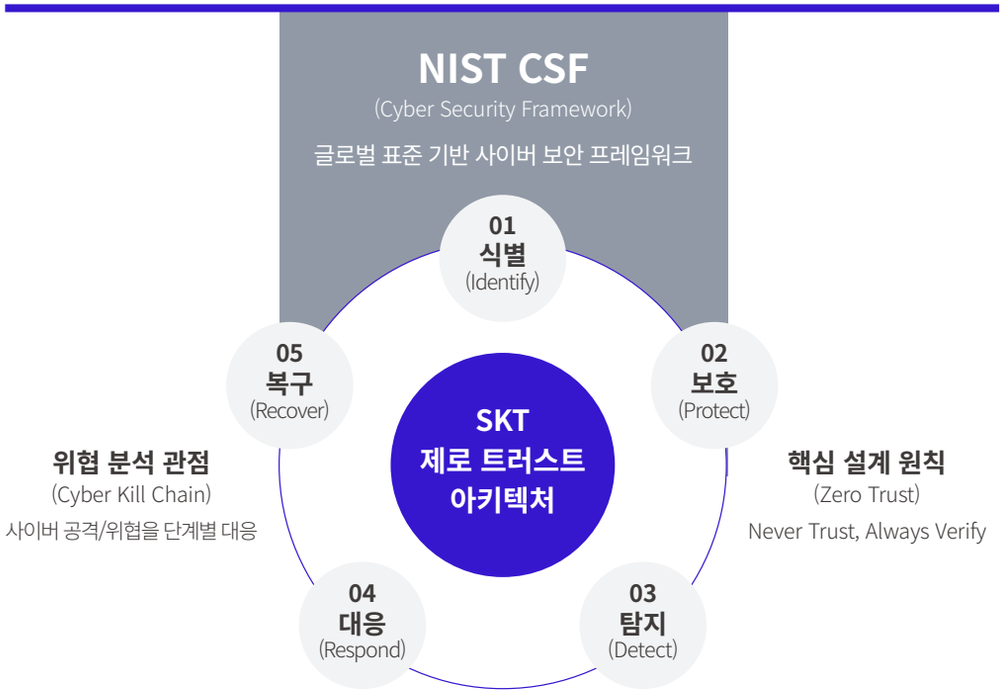
OVERVIEW

개요 – 정보보호 아키텍처

글로벌 표준 프레임워크 기반의 제로 트러스트 보안 원칙 적용

제로 트러스트 원칙을 핵심으로 **SK텔레콤 보안 아키텍처**를 새로 정의하였습니다.

NIST CSF 기반 제로 트러스트 아키텍처



보안 영역별 설명

1 식별	• 정보자산을 통합 관리시스템으로 관리, 자산 유형별 보안에 필요한 세부 정보 필수 관리 • 보안 취약점 스캔 도구와 통합 관리시스템이 연계되어 위험평가 워크플로우 자동화 및 누락 없는 조치
2 보호	• 다중방어체계(Multi-Layer Defense)로 고객 정보·핵심 시스템 접근통제 및 위험 확산 방지 • 비인가 정보 탈취 차단, 비인가 외부 전송 차단, 암호화로 정보 열람 차단
3 탐지	• 글로벌 위협 인텔리전스 기반의 선제적·능동적 위협 분석 및 통신 서비스 특화 위협 대응 • AI 기술을 활용한 탐지→분석→보고 프로세스 자동화
4 대응	• 전사 실전형 대응 매뉴얼·실무 Playbook 운영 및 경영진 참여 모의훈련 수행 • 탐지된 이벤트에 대해 대응체계 기반 위험도와 안정성을 고려한 IT자산 격리, 치료 등 즉각 대응
5 복구	• 중요 등급 국사 재난복구 시스템(DR) 구축, 다중 백업으로 서비스 연속성 및 백업 무결성 확보 • 보안 사고 유형별 복구 프로세스 및 백업·재해복구 시스템 운영

식별 보호 탐지 대응 복구

서버 및 SW 보안 가시성 확보

보호 대상의 가시성 확보가 보안의 출발점입니다.

통신 서비스는 네트워크·시스템·데이터·고객 접점이 복합적으로 연결되어 있어, **보호 대상의 정확한 식별**이 보안의 출발점입니다. SK텔레콤은 자산 식별과 위험평가 프로세스를 운영하고 이를 뒷받침할 자동화 기반의 자산관리 시스템을 단계적으로 구축하고 있으며, 공급망 보안관리를 통해 외부 요인으로 인한 보안 위험을 줄이고 있습니다.

변화하는 자산의 지속적 가시성 확보

보안 관리 대상 자산은 생성, 변경, 운영, 폐기의 생애주기를 거치며 끊임없이 변화합니다. 네트워크, 시스템, 데이터, 계정, 서비스 구성요소가 새롭게 추가되거나 운영 환경이 바뀌면 보안 조치가 필요한 대상과 우선순위도 함께 달라지므로, 자산을 정확하게 식별하는 일이 보안 관리의 출발점입니다.

SK텔레콤은 자산 식별과 위험평가 프로세스를 통해 자산별 중요도와 위험 수준을 관리하고 있으며, 자동화 기반의 관리 체계를 마련해 나가고 있습니다.

자동화 기반 자산관리 시스템 도입

변화하는 자산과 위험 상태를 수기 점검에 의존하지 않고 신속하게 파악할 수 있도록 자산 식별 · 위험평가 · 개선 조치를 연계하는 자동화 기반 시스템을 단계적으로 구축해 나가고 있습니다.

자동 수집	자동 분류	자동 연계 조치
자산 정보 현행화	**위험도 등급 산정**	**보호 체계 연동**

공급망 보안관리

외부 패키지 솔루션, 오픈소스, 자체 개발 소스코드 등 다양한 구성요소가 서비스에 활용되는 만큼, 소프트웨어 구성요소와 취약점 관리 체계를 강화하여 외부 요인으로 인한 보안 위험을 줄이고 있습니다.

공급업체 보안역량 평가

- 공급업체의 보안관리 수준을 사전에 평가하고 공급망 리스크를 관리
- 관리체계, 개발보안, 환경관리, 유통보안, 취약점 대응 등 5개 영역 항목 점검
- 평가 결과를 계약·구매 절차에 반영하여 안전한 공급망 확보

소프트웨어 구성요소 취약점 점검

- 납품 소프트웨어의 구성요소와 취약점 점검 의무화
- 주요 취약점 조치 후 계약·인수하도록 하여 서비스 보안성 강화

식별 **보호** 탐지 대응 복구

다중방어체계

핵심 자산은 겹겹이 보호합니다.

보호 대상이 식별되면, 그 다음 단계는 필요한 사람과 시스템만 적절한 권한으로 접근하도록 통제하고 위험이 확산되지 않도록 관리하는 것입니다. SK텔레콤은 **통합 계정 권한 관리, 네트워크 접근 통제, 중요정보 보호, 개발 단계 보안관리**를 연계하여 보호 수준을 강화하고 있습니다.

고객 정보와 핵심 시스템 보호체계 강화

식별 단계에서 보호해야 할 서비스·데이터·인프라를 파악했다면, 보호 단계에서는 대상에 적절한 보안 통제를 적용해야 합니다. 보호 대상의 중요도와 위험 수준이 다르기 때문에 모든 영역에 동일한 기준이 아니라, 서비스 운영에 미치는 영향에 기반하여 **필요한 보안 통제**를 정교하게 적용하는 것이 중요합니다.

비인가 접근 가능성을 낮추기 위해 사용자·관리자·시스템 계정의 역할과 권한을 기준에 따라 관리하고, 업무상 필요한 범위 내에서만 접근할 수 있도록 **최소권한 원칙**을 적용하고 있습니다. 특히 고위험·장기 미사용 권한은 정기 점검 및 폐기를 통해 오남용 가능성을 줄입니다.

업무·서비스 특성에 따라 필요한 연결만 허용하고, 중요 시스템과 데이터가 불필요하게 노출되지 않도록 접근 경로를 관리합니다. 이를 통해 내부에서 이상 상황이 발생하더라도 위험이 다른 영역으로 확산될 가능성을 낮춥니다.

데이터 · 개발 보안관리 확대

고객 정보와 주요 **데이터가 저장·전송·활용되는 전 과정**에서 강력한 암호화와 접근관리 기준이 적용되도록 관리합니다. 데이터가 처리되는 위치와 방식이 다양해지는 환경에서 정보 유출 위험을 낮추기 위한 기본 보호조치입니다.

서비스 **기획·설계·개발·배포 과정**에서 보안 요구사항을 점검하고, 취약점이 운영 환경으로 이어지지 않도록 사전 검토와 개선 활동을 수행하고 있습니다.

SKT
다중 방어체계
Multi-Layer Defense

01 사고인지
- 단말·시스템 보안관리 강화
- 시스템 취약점 예방

02 계정 · 권한 관리 및 인증 · 접근 통제
- 허가된 사용자만 접근
- 최소권한 원칙 적용

03 네트워크 보안
- 외부 침입·접근 차단
- 내부망에서 횡적 이동 위험 최소화

04 데이터 보호 (암호화·분류)
- 주요 데이터 암호화 적용
- 중요정보 구분 관리

식별 보호 **탐지** 대응 복구

AI 기반 위협 탐지

AI로 먼저 탐지하고, 한발 앞서 대응합니다.

SK텔레콤은 다양한 보안 정보를 통합하고, **AI 기반 보안위협 탐지·분석 체계**를 통해,
정상 활동으로 위장한 위협까지 조기에 식별하고 차단하여 피해를 방지합니다.
전사 사용자·PC·서버·네트워크·서비스에서 발생하는 이벤트 정보를 한곳에 모으고, AI를 활용하여
이상행위를 분석한 후 식별된 위협에 대해서 방어를 적용하는 3단계 탐지 대응 체계를 운영합니다.

STEP **01**

보안 정보 수집

보안 탐지의 사각지대가 없도록 다양한 시스템과 유형의 로그를 수집하고, AI가 이해하고 자동화할 수 있도록 데이터를 표준 포맷으로 변환하여 저장합니다.

사용자 행위
개인정보 조회·권한 변경

PC · 서버
로그인 시도·명령어 실행

네트워크
방화벽·Switch·DNS

서비스 이벤트
웹 접속·크리덴셜 스터핑

보안시스템 이벤트
EDR·NDR·IDS·WAF

외부 위협 정보
TI Feed·OSINT

STEP **02**

AI 기반 통합 분석

통합된 보안 정보를 패턴학습 및 상관분석을 통해 이상 행위를 탐지하고 AI를 통한 자동 분석과 전문 인력의 심화 검증을 통해 정·오탐을 명확히 판단합니다.

상시 보안 관제
전문 인력에 의한
24 x 365 관제

보안 정보 통합 분석
이기종 보안 정보 통합 및
상관분석

이상 행위 탐지
패턴 학습 및 비정상 행위
탐지

AI 기반 위협 분석
이벤트 분석 및 정·오탐 판단
자동화

STEP **03**

위협 식별 · 방어

정탐으로 판별된 이벤트에 대해서는 차단을 적용하고, 피해 여부 점검 및 유사 위협에 대한 탐지·차단 개선 활동을 수행합니다.

위협 식별
정탐 이벤트 대상
영향도 판단

위협 방어
차단 패턴, 취약점 패치
적용

확대 점검
유사 공격 발생 및
피해 여부 점검

식별 강화
위협 탐지 시나리오
지속 개선

식별 보호 탐지 **대응** 복구

사고 대응 절차 표준화

위기상황에서 빠르고 정확하게 대응하여 영향을 최소화합니다.

사고 대응의 핵심은 신속하고 일관된 실행 체계를 확보하는 데 있습니다.
SK텔레콤은 **사고 유형별 표준 대응 절차**와 **단계별 실행 방안**을 마련하여
신속하고 일관된 대응을 수행합니다.

SKT 침해사고 대응 체계

SK텔레콤은 침해사고 발생 시 전사 차원의 신속하고 일관된 대응을 통해 피해를 최소화하고, 법·규제 준수 의무 사항을 충족하며, 회사의 핵심 자산을 보호하기 위한 실행 절차와 구체적 대응 방법을 체계적으로 정의하였습니다.

모의훈련 계획 수립

모의훈련 계획
- 훈련 개요
- 훈련 목적
- 훈련 방식 등

Runbook 기반 훈련 시나리오 작성

Runbook 기반 모의훈련 시행

훈련개시	탐지	조사	대응	복구	훈련종료
• 훈련 목적 및 방식 설명	• 사고인지, 초동조치 • 비상대응 조직 구성	• 사고 영향 범위, 원인 분석 • 정보유출 경로, 규모 파악	• 자체 사고대응 또는 외부기관 지원 요청 • 언론·기관·고객 대응	• 기술적 복구 • 고객피해·기업 신뢰도 복구	• 훈련 결과 분석 • 개선 필요사항 Runbook 반영

사고 유형

랜섬웨어 / 웹 해킹 / DDoS / 정보 유출 / 악성코드 감염 / 개인정보 유출 / 계정 탈취 / 크리덴셜 스터핑

예)랜섬웨어 사고대응 시나리오

STEP 01	STEP 02	STEP 03	STEP 04	STEP 05
사고인지	**확산방지**	**사고분석**	**보고·신고**	**복구·정상화**
피해 시스템 식별/증상 확인	연동 시스템 감염 여부 조사	로그 수집 및 보존	정부 침해사고 신고	백업 데이터 무결성 확인 및 복구
▼	▼	▼	▼	▼
피해 시스템 분리 및 NW 차단	추가 감염시스템 격리	원인/경로 로그 분석/포렌식	전사 대응체계 가동	복구 확인 및 취약점 패치
▼	▼	▼	▼	▼
정보유출 여부 점검	전체 사고영향도 분석	심각도 판단 및 비상 대응조직 구성	전체 사고영향도 분석	전체 사고영향도 분석

식별 보호 탐지 대응 **복구**

침해 사고 복구

서비스 연속성을 보장하도록 회복탄력성을 확보합니다.

통신은 고객의 통화·문자·데이터를 넘어 **금융·인증·공공·산업 서비스**와 긴밀히 연결된 사회적 인프라입니다. SK텔레콤은 서비스 중요도에 따라 복구 기준을 체계화하고, 다중 백업·재해복구·정기 훈련을 유기적으로 연계하여 어떤 상황에서도 흔들리지 않는 **회복탄력성을 확보**하고자 합니다.

서비스 연속성 복구 체계

재해복구 체계

특정 시스템·거점에 문제가 발생해도 **서비스 연속성을 확보**할 수 있도록 중요 등급 **국사에 재난복구 시스템(DR)을 구축**하고, 대체 인프라·이중화 구조·복구 절차를 마련합니다.

- 핵심 서비스 우선 복구 적용
- 중요 국사 DR 운영
- 서비스 영향도 기반 복구 우선순위

다중 백업 체계

랜섬웨어 등 위협 상황에서도 안정적으로 복구되도록 주요 데이터·시스템의 다중 백업을 강화하고, 백업 데이터의 위협 노출을 차단합니다.

- 다중 복제 및 격리 보관
- 위변조 불가 백업 저장장치 운영
- 백업 무결성 정기 검증

정기 복구훈련

구축된 체계가 **실제 상황에서 정상적으로 작동하는지 검증**하는 것이 중요합니다. 랜섬웨어 시나리오 등 주요 상황을 가정한 정기 복구훈련을 시행합니다.

- 시나리오 기반 모의훈련
- 백업 데이터 복원 검증
- 조직 간 협업 절차 점검

Cybersecurity Technology

차세대 보안 기술 개발

변화하는 위협보다 한발 앞서가겠습니다.

보안기술은 단순한 도입을 넘어, 변화하는 위협에 신속하게 대응하기 위해 **지속적으로 내재화·고도화**되어야 합니다. SK텔레콤은 **인증 보안과 AI 기반 AX 위협 대응 기술**을 강화하여 고객 보호 중심의 보안 체계를 발전시키고 있습니다.

Passwordless 인증 체계 내재화

FIDO ALLIANCE 이사회 멤버

Passwordless 시스템 추진

로그인 방식을 **패스워드 기반에서 생체·인증서 기반으로 전환**하고, 국제 표준 기반 인증 체계를 공동 구축하고 있습니다.

PASSKEY
생체 기반 로그인
지문·얼굴 인식 등 디바이스 자체 인증

FIDO 표준
국제 표준 호환
FIDO Alliance 의사결정 직접 참여

기대 효과
- 피싱·크리덴셜 스터핑 등 비밀번호 기반 공격에 대한 방어 수준 향상
- 고객의 비밀번호 관리 부담 해소 · 사용자 편의성 향상
- 국내·외 다양한 서비스에 호환되는 표준 인증 환경 구축

Passkey by SK Telecom

소프트웨어 품질인증 최고 등급인 GS(Good Software) 인증 '1등급' 획득

FIDO(Fast Identity Online) 기반의 차세대 인증 솔루션으로 사내 시스템에 단계적으로 적용하여 Passwordless 업무 환경을 구축할 계획입니다.

인증보안 체계 고도화

통합신원관리 체계 강화

접근 주체 확장에 따른 접근 통제 기반 마련

사용자·시스템·AI 에이전트 등 접근 주체가 확장됨에 따라, 인증·권한·감사 체계를 신원 중심으로 통합합니다

01 **사용자 인증**
패스키 기반 비밀번호 없는 인증을 확대해 계정 탈취 위험을 줄이고, 안전한 접속 환경을 제공

02 **시스템 인증**
고정 인증정보 사용을 제거하고, 실행 시점의 신원 검증으로 시스템 접근을 보호

03 **AI 에이전트 인증**
AI 에이전트의 신원과 위임 권한을 식별하고, 도구 사용과 수행 권한 및 범위를 통제·감사

기대 효과
- 사용자·시스템·AI 에이전트 통합 보호
- 비밀번호·고정 인증정보 의존도 축소
- 통제와 감사가 가능한 보안 체계 확보

AX 위협 대응 AI 기술 개발

생성형 AI 보안 엔진 개발

AI 기반 보안 감사로 AX 리스크 관리

사내 AI 활용 중 발생할 수 있는 정보 노출과 오남용 위험을 AI 기반으로 탐지하고, 안전한 활용 환경을 지원합니다.

01 **보안 통합 분석**
전체 대화 맥락, 첨부파일, 정보 민감도 및 악용 가능성을 통합 분석

02 **위험 사용자·조직 식별**
사용자·조직별 AI 이용 패턴과 위험도를 분석해 고위험 대상을 식별

03 **실시간 운영 가이던스 제공**
AI 에이전트 분석 결과를 기반으로 보안 대응 가이드를 실시간 제공

기대 효과
- 생성형 AI 활용 과정에서의 보이지 않는 보안 리스크 가시화
- 개인정보·기밀정보·인증정보 등 유출 위험 차단 및 감사 체계 구축
- 안전하게 AI를 활용할 수 있는 AX 보안 기반 확보

개인정보보호

고객이 안심하고 서비스를 이용할 수 있도록 만드는 일상 속 보호 활동입니다.

PART 03

01 개인정보보호 거버넌스

02 Privacy by Design 원칙

03 개인정보 자기결정권 보장

04 Privacy First 문화

개인정보보호 거버넌스

CPO를 중심으로 개인정보보호 관리체계를 한층 더 강화하겠습니다.

CPO 중심의 책임과 의사결정 체계를 명확히 하여 **개인정보보호가 경영진 보고와 전사 실행으로 연결**되도록 거버넌스를 강화하고 있습니다.

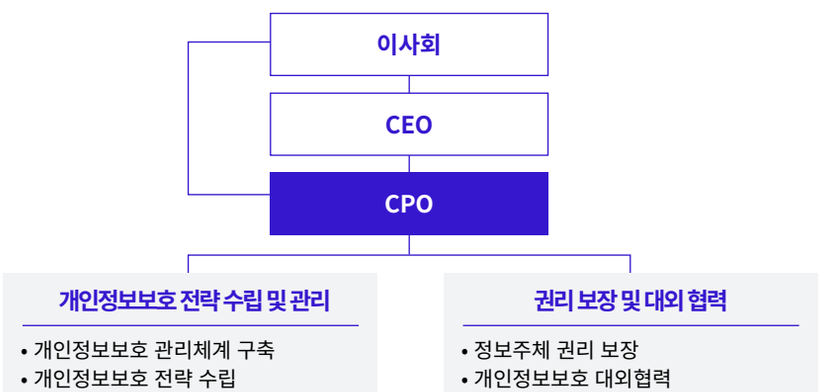
CPO 조직 신설 및 독립성 강화

SK텔레콤은 개인정보보호 강화를 위해 **CPO를 별도로 선임**하고 프라이버시 전담 조직을 정비하여 전략 수립, 실행 관리, 관련 법령 준수, 리스크 대응 기능을 강화하고 있습니다.

또한 개인정보 관련 주요 이슈와 현안을 **정기적으로 이사회에 직접 보고**하여, CPO의 독립성·신속한 의사결정·전사 영향력을 확보할 수 있는 기반을 마련하고 있습니다.

아울러 정보주체 권리 보장을 최우선으로 하여 개인정보의 열람·정정·삭제 등 권리 행사를 체계적으로 지원하고, 유관 기관과의 협력을 통해 개인정보보호 수준을 지속적으로 고도화하고 있습니다.

SKT CPO 조직도 및 보고체계



CPO – CISO 협업체계

CPO와 CISO는 각각 개인정보보호 정책·법적 준수사항 이행과 정보보호·기술적 보호조치를 담당하면서, 서비스 기획부터 운영·침해대응까지 상호 검증하는 협업체계를 구축하고 있습니다.

Privacy by Design 원칙

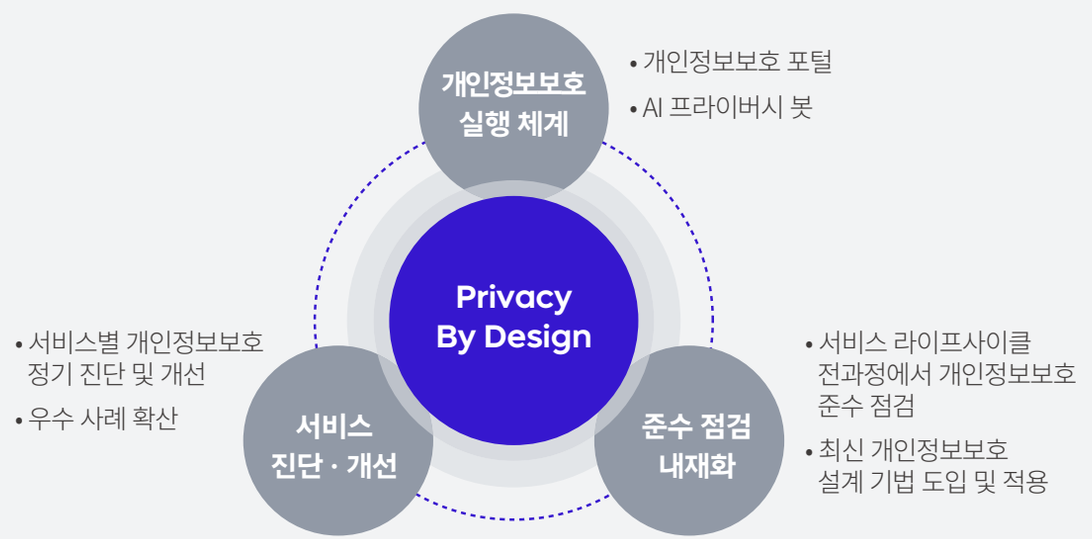
개인정보보호는 서비스 설계의 기본값입니다.

SK텔레콤은 Privacy by Design 원칙에 따라 개인정보보호를 **서비스 설계 · 개발 · 운영 · 폐기 전 과정**에 반영하고 있으며, **고객이 별도 조치를 하지 않아도 개인정보가 기본적으로 보호**되도록 운영하고 있습니다.

Privacy by Design 7대 원칙

1	사후 대응이 아닌, 사전에 위험을 예측하고 방지
2	별도의 설정 없이 개인정보가 자동으로 보호되도록 설계
3	개인정보보호를 시스템과 서비스 설계 초기 단계부터 반영
4	프라이버시 보호와 비즈니스 목적을 함께 달성
5	개인정보를 수집부터 파기까지 전 과정에서 안전하게 관리
6	개인정보 처리 방식과 보호조치는 이해관계자와 이용자가 알 수 있도록 명확하게 공개
7	개인정보의 최우선 가치는 개인의 권리 존중

Privacy by Design 실행 선순환 구조



개인정보보호가 **모든 시스템·프로세스 설계의 원칙**으로 **내재화**되는 구조

개인정보 자기결정권 보장

내 정보에 대한 선택권까지 보호합니다.

개인정보보호의 핵심은 **고객이 자신의 정보가 어떻게 처리되는지 이해**하고, 필요한 권리를 **쉽고 명확하게 행사**할 수 있도록 보장하는 데 있습니다. SK텔레콤은 **고객이 개인정보 처리 현황을 확인하고 권리를 행사**할 수 있는 체계를 강화하여 고객 중심의 개인정보보호 수준을 높이고 있습니다.

개인정보 자기결정권 보장

SK텔레콤은 개인정보 **처리방침 공개 · 권리 행사 · 이용 내역 통지 · 피해 구제** 4개 영역을 체계적으로 운영하여 개인정보 자기결정권을 보호하고 있습니다.
고객은 프라이버시센터·T world·주요 서비스 앱 등 다양한 채널에서 개인정보 처리방침을 확인하고, 열람·정정·삭제·처리정지 권리를 온라인으로 행사할 수 있습니다. 개인정보 이용 내역은 정기적으로 안내하며, 문의·상담·피해 구제 절차를 통해 접수된 사항은 **재발 방지와 보호수준 향상을 위한 개선 활동**으로 연계하고 있습니다.

4개 영역의 고객 권리 보장 체계

01 **개인정보 처리방침 공개**
개인정보 처리목적·수집항목 등 처리현황을 T world 등 주요 서비스 채널에서 상시 확인 가능

02 **정보주체 권리 보장**
열람·정정·삭제·처리정지 등 정보주체 권리를 쉽게 행사할 수 있도록 절차 안내(T world, 고객센터)

03 **개인정보 이용 내역 통지**
정기적으로 개인정보 이용 내역을 안내하여 고객이 직접 자신의 개인정보가 어떻게 활용되고 있는지 확인할 수 있도록 지원

04 **고객 피해 구제**
개인정보 관련 문의·상담·피해 구제 절차 운영 (고객센터·온라인 상담·PoC 게시판 문의 등)

개인정보 보호수준 강화

ISMS-P 인증 범위 확대 · 개인정보 암호화 대상 확대 등 기술적 보호조치를 함께 강화하여 관련 법령 준수와 실질적 보호수준을 균형 있게 고도화하겠습니다.

Privacy First 문화

개인정보보호를 최우선으로 내재화하고 있습니다.

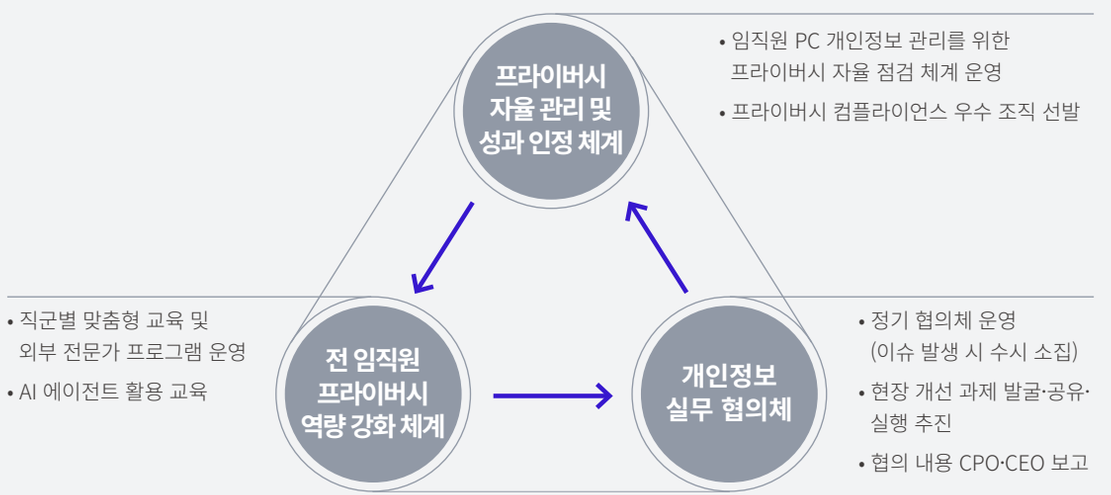
고객 정보 보호 수준은 모든 임직원이 **개인정보보호 원칙**을 이해하고 업무에 적용할 때 높아집니다.
SK텔레콤은 실제 업무 상황을 반영한 교육과 인식 제고 활동을 통해
Privacy First 실천 문화를 확산하고 있습니다.

개인정보보호 문화 확산과 인식 제고

개인정보보호는 규정과 시스템만으로 완성되지 않습니다. 고객 정보를 수집·이용·보관·파기하는 모든 업무 과정에서 임직원이 **개인정보보호 원칙을 이해하고 실제 상황에 맞게 판단할 때** 보호 수준이 높아집니다.

SK텔레콤은 개인정보보호를 전 임직원이 함께 실천해야 할 기본 원칙으로 정착시키고자, **실제 업무 사례 중심 교육과 캠페인 · 서약 등 참여형 활동**을 운영하고 있습니다. 이를 통해 개인정보보호가 별도 점검 항목이 아닌 **업무 시작과 의사결정 시점에 자연스럽게 고려되는 기준**으로 자리 잡도록 하고 있습니다.

Privacy First 문화 확산 3대 핵심 활동



규정 준수를 넘어, **임직원 스스로가 개인정보보호의 주체**가 되는
자발적인 프라이버시 보호 문화 정착 실현

맺음말

CLOSING

고객 신뢰를 위한 지속적인 약속

정보보호는 한 번의 조치로 완성되는 일이 아닙니다.
변화하는 위협과 서비스 환경에 맞춰 SK텔레콤은 점검과 개선을 멈추지 않겠습니다.

ROADMAP

추진 전략 및 중장기 로드맵

정보보호는 완료가 아니라 계속되는 약속입니다.

정보보호는 변화하는 위협을 지속적으로 검증하고 대응할 수 있는 구조로 발전해야 합니다. SK텔레콤은 **제로 트러스트 기반 보안 원칙과 AI 기반 운영 고도화**를 중심으로 중장기 정보보호 로드맵을 추진하고 있습니다.

중장기 정보보호 로드맵

	PHASE 01 (FY26) 정보보호 기반 강화	PHASE 02 (FY27) 제로 트러스트 체계 고도화	PHASE 03 (FY28) 국내 최고 수준 정보보호 역량
① 거버넌스	• ISO/IEC 27002 기반 정책 개편 • Red Team 신설 및 침투테스트를 통한 보안 수준 강화 • 정기 모의훈련 분기 단위 확대 운영	• AI 보안 거버넌스 체계 확립 • ISMS-P 통합 인증·정기 감사 • 보안 전문기업과의 협력 체계 강화 및 공동 대응	• 공급망 보안 거버넌스 고도화 • AI 기반 보안운영 핵심성과지표 관리
② 아키텍처	• 정보보호 아키텍처 재설계 및 구현 • 전사 자산관리체계 구축 및 공급망 보안 강화 • 서비스망 보안 강화 (EDR, 망연계 등)	• 자산관리시스템 고도화, 위협 탐지 대응 자동화 • Micro-Segmentation 확대 적용 • 클라우드 네이티브 보안(CNAPP) 통합 플랫폼 운영	• AI 에이전트 기반 SOC 운영체계 구축 • 전사 IAM 체계 구축 완료 및 사외 확산
③ 보안 기술	• AX 보안 내재화를 위한 보안 기술 개발 • 사이버보안 AI 기술 개발 • 핵심 인프라 / 매체별 보안 강화	• 분산된 Trust Infra를 구조적으로 통합 관리 • Passwordless 기술 확산 • 차세대 인증시스템 구축	• 자체 개발 AI 보안기술 사외 확산 • AI를 통한 사기방지기술 고도화
④ 개인정보보호	• 개인정보보호 포털 및 AI 프라이버시 봇 구축 • AX기반 개인정보 관리 에이전트 개발 • 구매 프로세스 개선 및 공급망 프라이버시 관리	• 프라이버시 우수 사례 공유 체계 구축 • 서비스 전과정 프라이버시 점검 프로세스 정착 • 그룹-멤버사 및 기관과의 프라이버시 협력 체계 고도화	• AI 기반 예측·선제 대응형 개인정보보호 체계 구축 • 개인정보보호의 기업 신뢰 자산화 체계 구축 • 글로벌 기준 기반 규제 준수 및 대응

CLOSING MESSAGE

맺음말

고객 신뢰를 위한 지속적인 약속

SK텔레콤은 **고객 안심**을 최우선에 두고, **책임 있고 투명한 실행**을 통해
고객과 사회가 신뢰할 수 있는 정보보호 체계를 만들어 가겠습니다.

정보보호는 한 번의 조치로 완성되지 않습니다. 위협은 끊임없이 달라지고, 서비스 환경도 빠르게 진화합니다.
그렇기에 정보보호는 '완료'가 아니라 '계속되는 약속'이어야 합니다.

이번 정보보호백서는 SK텔레콤이 정보보호를 바라보는 관점과 방향을 공유하기 위해 마련되었습니다.
무엇보다 중요한 것은 현재의 조치를 소개하는 데서 한 걸음 더 나아가, 이러한 노력이 실제 업무와 서비스 현장에서 흔들림 없이 작동하도록 만드는 일입니다.

정보보호최고책임자로서 보안을 특정 시점의 대응이나 특정 조직의 과제로 한정하지 않겠습니다.
보안 원칙이 경영 의사결정과 서비스 운영, 고객 소통 전반에 일관되게 적용되도록 살피고, 필요한 보완을 꾸준히 이어가겠습니다.

SK텔레콤은 새로운 위협을 면밀히 분석하며, 고객 보호에 필요한 기술과 운영 역량을 한층 강화해 나가겠습니다.
개선의 과정과 결과를 고객에게 투명하게 공유하고, 고객의 목소리를 반영해 지속적으로 보완하여 고객과 사회가 신뢰할 수 있는 정보보호 체계를 만들어 가겠습니다.

감사합니다.

SK텔레콤 정보보호최고책임자 (CISO)
이종현

SK텔레콤의 세 가지 약속

1. 고객 안심 우선

보안 의사결정의 기준은 항상 고객의 안심입니다.
고객이 안전하게 통신 서비스를 이용할 수 있는 환경을 끝까지 지키겠습니다.

2. 책임 있는 실행

변화하는 위협에 맞춰 보안 기술과 운영 역량을 꾸준히 강화하며, 일회성이 아닌 지속 가능한 실행을 약속합니다.

3. 신뢰를 위한 소통

개선의 과정과 결과를 성실히 설명하고,
고객 신뢰를 높이는 소통을 이어가겠습니다.

Appendix

Appendix. 고객보호활동 (1) AI 기반 스팸·보이스피싱 차단

연간 11억 건 통신사기 차단

AI로 더 빨리 찾고, 고객에게 닿기 전에 막겠습니다.

스팸·보이스피싱은 고객의 통화와 문자 이용 과정에서 발생하는 **대표적인 일상 속 보안 위협**입니다. SK텔레콤은 **AI 기반 분석 기술**로 의심 통화·문자를 사전 탐지·차단하고 있습니다.

2025년 AI 기반 스팸·보이스피싱 차단 차단 성과

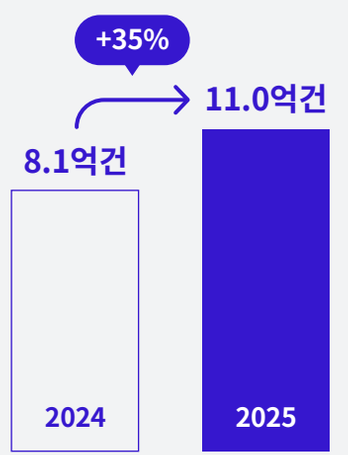
2025년 누적 차단 실적

한 해 동안 선제적으로 차단한 통신사기

11억 건

차단 음성 통화	차단 문자
음성 스팸·보이스피싱	스미싱·미끼문자
2.5억 건 차단	**8.5억 건 차단**

2025년 스팸 · 보이스피싱 차단 건수 추이



* 단위: 음성 스팸·보이스피싱 통화 + 미끼문자 통합 차단 건수/전년 대비 35% 증가

AI 기반 탐지 구조

스캠뱅가드 (ScamVanguard)

SKT 자체 개발 AI 금융사기 탐지 기술

에이닷 전화

통화 중 위험 징후를 실시간 분석하여 보이스피싱 가능성 즉시 경고

PASS 스팸필터링

의심 문자를 사전 식별하여 고객에게 실시간 알림

문자, 통화, 악성 URL 등 금융사기 관련 통합 분석 AI 모델

미끼 문자, 신고되지 않은 보이스피싱 의심 번호, 사칭 웹사이트에 대한 종합 분석 수행

Appendix. 고객보호활동 (2) · 대고객 안심 보안 서비스

고객의 안심을 지키는 통합 안심 보안 서비스 패키지

통신 서비스에서 **유심 · 단말 · 통화 · 문자 · 매장**은 고객 식별과 이용의 중요한 기반입니다. SK텔레콤은 **고객 안심 패키지 · 통신사기 차단 솔루션 · 24시간 상담**을 하나의 보호 체계로 통합 운영하고 있습니다.

고객 안심 보안 서비스 — 통합 보호 체계

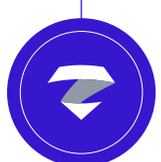
전화 · 문자보안

에이닷 전화

AI 기반 음성 분석으로 의심 통화 · 문자를 사전 인식 · 안심 메시지 안내

- 통화전 AI 기반 보호·차단
- 통화중 스팸·보이스피싱 탐지
- 이상 징후 통화·메시지 경고·차단

스마트폰 보안



짐페리움 MTD

글로벌 Top 보안 브랜드 협업으로 스마트폰에 가해지는 위협을 방어

- 기기 보호
- 악성앱 탐지·피싱 탐지
- 악성 또는 가짜 Wi-Fi 접속 탐지

네트워크 보안

고객 안심 패키지

모든 SK텔레콤 고객 기본 제공 – 보안 부가 서비스 4종 외

- 복제 유심/단말 비정상인증 차단
- 유심 보호 서비스
- 음성스팸·보이스피싱 전화 차단, 문자·스팸스미싱 문자 차단

24시간 고객 안심 상담 · 전국 대고객 보안 서비스

24h

CALL CENTER · 365일 24시간

T 안심 24시간 보안센터

24시간 365일 전화 상담 가능한 보안 특화 전문 고객센터

2,500

전국 매장OFFLINE

T 안심매장

전국 2,500여 매장에서 보안 전문 상담 제공

3,000

VISITING · 방문 상담

B 안심지킴이

3,000여 명 유선보안 전문가 방문 시 홈 보안 Care 서비스 상담

Appendix. 용어집 (1)

용어집

CNAPP (Cloud-Native Application Protection Platform) – p.31
클라우드 환경에서 애플리케이션, 인프라, 설정, 권한 등 보안 위험을 통합적으로 관리하는 보안 플랫폼

Cyber Kill Chain – p.18
사이버 공격이 진행되는 단계를 나누어 각 단계별로 탐지·차단·대응하기 위한 분석 체계

DDoS (Distributed Denial of Service) – p.22
다수의 기기를 이용해 특정 서비스에 과도한 트래픽을 보내 정상 이용을 방해하는 공격

EDR (Endpoint Detection and Response) – p.21, p.31
PC·서버 등 단말에서 발생하는 이상행위를 탐지하고 분석·대응하는 보안 솔루션

FIDO Alliance (Fast IDentity Online Alliance) – p.24
비밀번호 없는 인증 기술 표준을 만들고 확산하기 위해 구성된 글로벌 협의체

IAM (Identity and Access Management) – p.13, p.31
사용자와 시스템 계정을 관리하고, 필요한 권한만 부여하도록 통제하는 계정·권한 관리 체계

IDS (Intrusion Detection System) – p.21
네트워크나 시스템에서 의심스러운 접근이나 공격 징후를 탐지하는 보안 시스템

Micro Segmentation – p.13, p.31
네트워크를 세분화하여 침해 발생 시 피해가 다른 영역으로 확산(lateral movement)되지 않도록 통제하는 방식

MTD (Mobile Threat Defense) – p.35
스마트폰 등 모바일 기기의 악성 앱, 피싱, 네트워크 위협을 탐지·차단하는 모바일 보안 솔루션

NDR (Network Detection and Response) – p.21
네트워크 통신 흐름을 분석해 이상행위나 침해 징후를 탐지·대응하는 보안 솔루션

NIST CSF (Cybersecurity Framework) – p.18
미국 국립표준기술연구소에서 만든 조직의 사이버보안 활동을 식별, 보호, 탐지, 대응, 복구 관점에서 관리하도록 제시한 글로벌 보안 프레임워크

OSINT (Open Source Intelligence) – p.21
공개된 웹사이트, 게시글, 도메인 정보 등 누구나 접근 가능한 정보를 수집·분석하는 활동

Privacy by Design – p.27
서비스와 시스템을 설계하는 초기 단계부터 개인정보보호를 기본적으로 반영하는 원칙

SASE (Secure Access Service Edge) – p.13
네트워크 접속과 보안 기능을 클라우드 기반으로 통합해 어디서 접속하든 일관된 보안을 제공하는 체계

SOC (Security Operations Center) – p.31
보안 이벤트를 모니터링하고 위협을 탐지·분석·대응하는 보안 운영 조직 또는 기능

TI Feed (Threat Intelligence Feed) – p.21
악성 IP, 도메인, 파일 정보 등 최신 위협 정보를 보안시스템에 제공하는 데이터

Appendix. 용어집 (2)

용어집

WAF (Web Application Firewall) – p.21
웹사이트와 웹 애플리케이션을 대상으로 하는 공격을 탐지하고 차단하는 웹 방화벽

계정 탈취 – p.5, p.22
공격자가 타인의 아이디와 비밀번호 등을 이용해 계정에 무단으로 접근하는 행위

다중 백업 – p.18, p.23
데이터를 여러 위치나 방식으로 복제해 장애나 사고 발생 시 복구할 수 있도록 하는 백업 방식

다중방어체계 (Multi-Layer Defense) – p.18, p.20
여러 보안 장치를 단계적으로 적용해 하나의 방어선이 뚫려도 다른 방어선이 작동하도록 하는 보안 방식

딥페이크 (Deepfake) – p.31
인공지능 기술로 사진, 영상, 음성을 조작해 실제처럼 보이게 만드는 기술

랜섬웨어 – p.22, p.23
데이터를 암호화하거나 시스템 사용을 막은 뒤 금전을 요구하는 악성코드 또는 공격 방식

보이스피싱 – p.34, p.35
전화로 금융기관, 수사기관 등을 사칭해 개인정보나 금전을 탈취하는 사기 수법

스미싱 (Smishing) – p.34, p.35
문자메시지에 포함된 악성 링크를 통해 개인정보나 금융정보를 탈취하는 사기 수법

스캠뱅가드 (ScamVanguard) - p.34
SK텔레콤이 자체 개발한 AI 기반 모바일 금융사기 탐지·방지 기술/서비스

스팸 (Spam) – p.34, p.35
이용자가 원하지 않는데도 반복적으로 전송되는 광고성 또는 불필요한 정보

악성코드 감염 – p.22
악의적인 프로그램이 단말이나 시스템에 설치되어 정보 유출, 시스템 장애 등 피해를 일으키는 상태

위협 인텔리전스 (Threat Intelligence) – p.18
사이버 위협을 탐지하고 대응하기 위해 활용하는 공격 정보, 침해 징후, 위협 동향 정보

위협 탐지 – p.21
시스템, 단말, 네트워크 등에서 공격이나 이상행위의 징후를 찾아내는 활동

재난복구 시스템 (DR, Disaster Recovery) – p.18, p.23
장애, 재해, 침해사고 발생 시 주요 시스템과 서비스를 복구하기 위한 체계

크리덴셜 스터핑 (Credential Stuffing) – p.21, p.22
다른 곳에서 유출된 아이디와 비밀번호를 여러 서비스에 대입해 로그인을 시도하는 공격

포렌식 (Forensic) – p.22
사고 원인과 피해 범위를 확인하기 위해 로그, 파일, 시스템 기록 등을 분석하는 조사 활동

SK telecom