



KT&G  
정보보안정책



KT&G Information Security Policy



# KT&G 정보보안 정책

## 개요

### 제정 목적

주식회사 케이티앤지(이하 “KT&G”)는 소비자의 신뢰를 최우선 가치로 삼으며, 정보자산의 안전한 보호를 통해 지속가능한 경영과 사회적 책임을 실현하고자 합니다. KT&G는 ‘정보통신망 이용촉진 및 정보보호 등에 관한 법률’, ‘개인정보보호법’ 와 같은 국내외 정보보호 관련 법규와 규정을 준수하고 엄격한 원칙에 따라 정보자산과 고객, 구성원 등의 개인정보를 철저히 보호하여, 소비자에게 안정적이고 믿음직한 서비스를 제공하도록 노력하겠습니다.

### 적용범위

본 정책은 KT&G 및 KT&G 국내외 자회사의 모든 임직원, 그리고 협력업체(파트너사)를 포함한 비즈니스 파트너의 모든 구성원에게 적용되며, 현지 국가의 법규, 조직의 정관, 사규 등에 특별한 조항이 있을 경우를 제외하고는 본 정책에 따라 업무를 수행해야 합니다.

### 책임범위

KT&G는 정보보안 및 개인정보보호에 대한 최고책임기구인 기업비밀보호위원회에서 기업비밀보호최고책임자 (CSO : Chief Security Officer)와 정보보호최고책임자 (CISO : Chief Information Security Officer)를 선임하고, 정보보호 관련 사규 제·개정, 정보보호 인증 및 보안 시스템 구축 등 정보보호를 위한 활동 계획을 검토하고 심의 의결합니다.

## 기본 원칙

### 정보보호 체계 점검

정보보호 담당 부서는 주기적으로 관련법령의 개정 및 정보보호를 위한 요구사항을 기반으로 사규 및 정책 등을 관리하며, 기업비밀보호운영과 개인정보 컴플라이언스에 대한 점검 및 내부 감사를 수행합니다.

### 정보보호 체계의 지속적인 개선

KT&G는 정보보호 관련 규정에 근거하여 정보보호 관리 체계를 적절하게 운영하고 있으며, 정보보호 체계의 유지와 수준 향상을 위해 지속적으로 개선활동을 수행합니다. 또한 정보보호 관리에 대한 객관적인 공신력을 확보하기 위해 정보보호 국제표준 인증, 국내 정보보호 및 개인정보보호 관리체계 인증을 취득하고 있으며, 이를 유지하기 위해 매년 정보보호 체계와 인증 수준을 검토하고 강화하고 있습니다.

### 정보자산 보호

정보자산에 대한 기밀성, 무결성, 가용성을 보장할 수 있도록 정보자산 관리에 대한 권한이 부여된 자만 정보자산에 접근 가능할 수 있도록 통제해야 합니다 또한, 직무 수행에 필요한 정보로의 접근만 허용하도록 합니다.

### 정보보호 리스크 관리

KT&G는 정보자산의 위협 및 관리를 위해 정보보호 리스크 식별 프로세스를 마련하고 있습니다. 이에 따라 주기적으로 정보보호 위험요소 진단 활동을 수행하고 도출된 위험요소에 대해 개선조치를 이행해야 합니다.

### 보안 위협 대응

정보보호 활동에 대한 상시 모니터링을 통해 보안 위협을 방지해야 합니다. 보안 위협 발생 시 정보보호 규정과 운영 지침 및 침해사고 대응 매뉴얼을 준수하여 신속히 대응하고 피해를 최소화해야 합니다. 이후 재발방지 대책을 수립하고 실행해야 합니다.

### 구성원의 책임과 역할

정보보호는 전사적인 책임이며, 정보보호의 지속적인 유지와 발전을 위해 모든 구성원의 적극적인 참여와 협력이 요구됩니다.

KT&G의 모든 구성원은 정보보호 관련 법규와 KT&G 정보보호 관련 규정을 준수하고, 정보보호 교육 이수 및 모의훈련 참여를 통해 정보보호 인식 수준을 강화시켜야 합니다.

### 외부 인력의 책임과 역할

KT&G와 계약관계에 의한 파트너사 및 외주업체 직원, 용역업체 직원 등이 KT&G의 정보자산에 접근하는 경우에는 반드시 본 정책을 비롯하여, KT&G 정보보호 관련 규정과 정보보호 관련 법규를 준수해야 합니다.