정보보호 정책

넥센타이어는 ZERO TRUST(아무도 믿지 않는다)라는 보안 원칙을 가지고, 고객과 임직원 및 협력사를 비롯한 주요 이해관계자의 소중한 정보자산을 보호하는 것을 최우선으로 삼아 정보유출 사고와 침해사고 건수 ZERO를 위해 최선을 다하고 있습니다. 개인정보보호 활동이 더 이상 선택이 아닌 필수임을 인식하고 경영진의 적극적 지원 의지를 담아 정보보호 원칙을 수립하여, 전 임직원이 스스로 참여하는 정보보호 문화를 만들고자 합니다.

이에 관리 보안, 기술 보안, 물리 보안등 주요 영역별로 정보보호체계 및 컴플라이언스 대응, 시스템 보안, 사이버 모의 대응훈련, 임직원 인식제고 활동을 시행하고 있습니다.

모든 임직원은 정보보호 정책을 기초로 하여 규정과 지침을 준수하여 정보자산을 보호해야 하는 책임이 있습니다. 또한 고객정보를 위탁 받아 처리하는 수탁사 및 주요 협력사도 대상에 포함됩니다.

정보보호 방침

1. 임직원은 정보자산을 보호하기 위해 정보보호 정책 및 규정 및 지침을 준수한다
2. 임직원은 정보자산을 사적 용도로 사용하지 않고 외부에 무단 공개하지 않는다
3. 임직원은 승인되지 않는 정보자산의 접근과 자료를 유출하지 않는다
4. 임직원은 정보보호 관련 법적 요구사항을 준수하고 사회적 책임을 다한다
5. 경영진은 정보보호에 필요한 예산과 자원은 확보하도록 적극적으로 지원한다
6. 경영진은 정보보호정책을 수립하고 이를 이행하도록 적극적으로 지원한다
7. 경영진은 솔선수범하여 정보보호 정책을 준수한다

정보보호 규정

1. 정보보호 규정 및 지침

규정 및 지침에 권고된 필수 요구수준은 회사의 일관된 정보 보호 수준 유지를 위해 반드시 준수해야 합니다.

1) 정보보호 규정

i. 인원 보안 지침

ii. 정보자산 관리 지침

iii. 보안사고 대응 지침

iv. 정보보호 조직 운영 지침

v. 사용자 보안 지침

vi. 기술적 보안 지침

vii. 물리적 보안 지침

viii. 정보보호 위험관리 지침

ix. 협력업체 보안관리 지침

x. 개인정보보호 지침

2. 정보보호 사고 대응 체계

정보보안 침해사고 발생 시 신속한 초기 대응을 통해 피해를 최소화하고 추가적인 피해가 없도록 사고 대응 체계가 구축되어 있으며, 정기적인 모의 훈련을 통해 사고 대응체계를 관리합니다.

[정보보안 침해사고 대응 프로세스]

i. 사고인지

ii. 의심내역 신고 (정보보호 부서 및 정보보호 책임 대상)

iii. 사고 대응팀 구성

iv. 4단계 사고 대응 프로세스
   a) 초동조치 b) 원인분석 c) 문제해결 d) 사후조치

v. 관련 신고기관에 현황 보고 (필요 시)

vi. 재발방지 대책 수립 및 적용

vii. 모니터링 및 사후관리

문서명	넥센타이어 정보보호 정책	**버전**	1.0
제정일자	2023.06.26	**개정일자**	-
제·개정부서	정보보호팀	**관리부서**	ESG팀