NEXAUTO	넥스오토 위험관리 방법론 및 관리절차 지침	문서번호 : HDH-BO-A-5
개정일 : 2025-03		개정차수 : 1

개정이력

차수	재(개)정 일자	시행일자	주요 개정 내용
1	2025-03-11	2025-03-11	초도 제정

목 차

1. 개요

1.1 목적

이 지침은 넥스오토 내 정보보호 위험요소를 체계적으로 식별, 평가, 대응 및 모니터링함으로써 정보자산의 기밀성, 무결성, 가용성을 유지하고, 보안 사고 발생 가능성을 최소화하며 지속 가능한 보안관리 체계를 구축하는 데 목적이 있다.

1.2 적용범위

1.2.1 본 지침은 조직의 모든 정보자산, 정보시스템, 네트워크, 사용자, 업무환경을 대상으로 한다.

1.2.2 임직원, 협력업체, 외부 사용자를 포함하여 조직이 통제 가능한 보안환경에 적용한다.

2. 위험관리 기본 원칙

2.1 선제적 관리 : 위험이 현실화되기 전에 사전 식별 및 대응

2.2 주기적 점검 : 정기적 위험 평가 및 관리체계 검토

2.3 문서화 : 위험 식별, 분석, 대응 활동은 모두 문서로 기록

2.4 책임 명확화 : 각 단계별 역할과 책임을 명확히 정의

3. 정보보안 위험관리 방법론

3.1 자산 식별 (Asset Identification)

3.1.1 식별 대상 : 서버, 네트워크 장비, DB, 사용자 계정, 문서, 소프트웨어 등

3.1.2 분류 기준 : 중요도(CIA 기준), 소유자, 위치, 처리 정보 유형

3.2 위협 및 취약점 식별 (Threat & Vulnerability Identification)

3.2.1 위협 예시

1) 외부 공격 : 해킹, 피싱, 랜섬웨어 등

2) 내부 위협 : 인가되지 않은 접근, 정보 유출, 실수

3.2.2 취약점 예시

1) 보안 패치 미적용, 잘못된 설정, 약한 암호, 미사용 서비스 미차단 등

3.3 위험 분석 (Risk Analysis)

3.3.1 정성적 분석

1) 위험 매트릭스(가능성 × 영향도)를 사용한 위험 등급 분류

3.3.2 정량적 분석

2) 자산 가치 × 위협 발생 확률 × 취약점 활용 확률 = 기대 손실

위험수준	설명	비고
높음(High)	즉시 조치 필요. 보안 위협 현실화 가능성 높음	
중간(Medium)	조치 계획 수립 필요. 모니터링 대상	
낮음(Low)	추후 재평가 필요. 위험 수용 가능	

3.4 위험 평가 및 우선순위화 (Risk Evaluation)

3.4.1 조직의 위험 수용 기준(Risk Appetite)에 따라 위험을 분류

3.4.2 경영진 보고 및 대응 우선순위 지정

3.5 위험 대응 (Risk Treatment)

대응 방식	설명	예시	비고
회피(Avoid)	위험 원인 제거	특정 서비스 중단	
완화(Mitigate)	위험 수준 감소	암호화, 방화벽 도입, 접근제어	

전가(Transfer)	외부에 전가	보험, 외주 위탁	
수용(Accept)	위험 수용	영향이 낮거나 비용이 과도할 경우 문서화 후 승인	

3.6 위험 모니터링 및 재평가 (Monitoring & Review)

3.6.1 KRI(주요 위험지표) 설정

3.6.2 보안 사고 발생 시 원인 분석 및 위험 평가 갱신

3.6.3 연 1회 정기 평가, 신규 시스템 도입 시 추가 평가

4. 위험관리 절차 흐름

[자산 식별] → [위협 및 취약점 식별] → [위험 분석] → [위험 평가] → [대응 전략 수립 및 실행] → [모니터링 및 보고] → [주기적 재평가]

5. 정보보안 위험관리 책임 분담

5.1 CISO(정보보안최고책임자) : 전사 위험관리 총괄, 정책 승인

5.2 정보보안그룹 : 위험 평가 및 대응 전략 수립, 시행, 모니터링

5.3 시스템 관리자 : 보안 패치, 설정 변경 등 기술적 대응 수행

5.4 사용자/직원 : 보안 교육 이수, 정책 준수, 위협 인지 및 보고

6. 문서 및 기록 관리

6.1 모든 위험 식별, 평가, 대응 활동은 문서화

6.2 보안 사고 대응 및 개선은 별도 사고보고서 및 개선보고서로 관리

6.3 문서 보존 기간 : 최소 3년 이상 보관

7. 정기 점검 및 감사

7.1 자체 감사 : 연 1회 이상 위험관리 프로세스 전반 감사

7.2 외부 인증 대비 점검 : ISMS-P, ISO27001 등 대비한 갭 분석 수행

7.3 내부 교육 및 인식 제고 : 위험 인식 교육, 보안 캠페인 시행