1.1.1 구 분	작 성	검 토	승 인
직 책	관리/물리 보안담당자	기술 보안담당자	CSO
성 명	정금 매니저	송대준 책임매니저	김상두 전무
서 명			
일 자	2026-05-12	2026-05-12	2026-05-12

(주)넥스오토 NEXAUTO	정보자산 분류 및 위험도 평가 절차 지침	문서번호 NEX-IS-A-05
제정일: 2026-05-12		개정차수: 0

개정 이력

차수	제(개)정 일자	시행일자	주요 개정 내용
0	2026-05-12	2026-05-12	초도 제정 기존지침 (위험관리 방법론 및 관리절차 지침 / 정보자산 위험관리 절차 지침) 문서 병합

(주)넥스오토 NEXAUTO	정보자산 분류 및 위험도 평가 절차 지침	문서번호 NEX-IS-A-05
제정일: 2026-05-12		개정차수: 0

목 차

(주)넥스오토 NEXAUTO	정보자산 분류 및 위험도 평가 절차 지침	문서번호 NEX-IS-A-05
제정일: 2026-05-12		개정차수: 0

1. 개요

1.1 목적

본 지침은 넥스오토의 정보자산을 체계적으로 식별·분류하고, 자산별 중요도 및 위험도를 정량적으로 평가하여 적정한 보호대책을 수립함으로써 정보자산의 기밀성(C)·무결성(I)·가용성(A)을 유지하고 보안 사고 발생 가능성을 최소화하는 데 목적이 있다.

1.2 적용 범위

본 지침은 넥스오토의 모든 정보자산(정보·소프트웨어·하드웨어·설비·인력)에 적용되며, 임직원·협력업체·외부사용자를 포함하여 조직이 통제 가능한 모든 보안 환경에 적용한다.

2. 위험관리 기본 원칙

2.1 선제적 관리: 위험이 현실화되기 전에 자산을 식별하고 위협에 사전 대응한다.

2.2 주기적 점검: 연 1회 이상 정기 평가와 관리체계 검토를 통해 최신 위협 트렌드를 반영한다.

2.3 문서화: 식별·분석·대응의 전 과정을 기록하여 추적 가능성을 확보한다.

2.4 책임 명확화: 각 단계별 역할과 책임을 명확히 정의하고 이행 여부를 관리한다.

2.5 DoA 준수: 위험수용수준(DoA)은 40점으로 설정하며, 이를 초과하는 위험은 반드시 '감소(Reduce)' 조치를 시행한 후 기본통제규칙에 재반영한다.

3. 정보자산 유형 분류 절차 및 기준

3.1 자산의 정의

정보자산이란 조직의 업무 수행에 필수적인 데이터, 시스템, 네트워크 장비, 문서, 소프트웨어, 사용자 계정, 인력 등 조직이 가치를 두어 보호할 필요가 있는 모든 대상을 말한다.

3.2 분류 기준 (5대 유형)

유형코드	분류	세부 항목 예시	자산번호 체계
RD/QM/MA 등	정보 (Information)	설계자료, 개발소스, 품질데이터, 측정데이터, 인사·회계·구매 등 업무 문서	NEX-[부서코드]-[일련번호]
SW	소프트웨어 (S/W)	PLM, MES, ERP, OS, DB(Oracle·MS-SQL), 보안솔루션, 그룹웨어 등	NEX-SW-[일련번호]
HW	하드웨어 (H/W)	서버(AIX·Linux·Windows), 네트워크 장비, 정보보안장비, 단말기, 저장장치 등	NEX-HW-[일련번호]
FC	설비·시설 (Facility)	전산실, 사무실, 보호구역, 생산라인, 금고, 기계실 등	NEX-FC-[일련번호]
HR	인력 (Human)	국내·해외사업장 임직원, 연구소 인력, 공동개발·외부협업 인원	NEX-HR-[일련번호]

3.3 분류 절차

3.3.1 정보보안그룹이 자산 식별 요청 및 등록 템플릿을 배포한다.

3.3.2 부서별 자산 관리자가 자산 정보(명칭, 소유자, 보관장소, 연동시스템 등)를 입력한다.

3.3.3 정보보안그룹이 5대 유형 기준에 따라 자산을 분류하고 정보자산관리대장에 등록한다.

3.3.4 CSO가 분류 결과를 승인하고, 변경 발생 시 수시 갱신한다.

3.3.5 자산 목록은 연 1회 이상 정기 검토한다.

4. 정보자산 중요도 평가 절차 및 기준

4.1 평가 항목 및 점수 체계

자산 가치(X)는 아래 4개 항목의 합산으로 산출한다.

4.1.1 기밀성(C) · 무결성(I)

등급	점수	기밀성(C) 기준	무결성(I) 기준	비고
E	3.0	경영층 승인 필요 (최고 기밀)	변경 불가 (CSO 승인 필요)	Extremely High
H	2.3	부서장 승인 필요	승인 후 변경	High
M	1.5	부서원 접근 가능	변경 후 승인	Medium
L	0.8	사내한 접근 가능	사후 확인	Low
N	-	공개 정보	임의 수정 가능	해당 없음

4.1.2 가용성(A)

등급	점수	가용성(A) 기준
M	2.0	비가용 시 업무에 심각한 영향 (핵심 시스템)
L	1.0	비가용 시 업무에 일부 영향 (보조 시스템)
N	-	비가용성 영향 요인 없음

4.1.3 유출영향도(AI — Asset Impact)

등급	점수	유출영향도(AI) 기준
E	2.0	유출 시 매우 심각한 타격 (회사 존립 위협 수준)
H	1.5	유출 시 심각한 타격 (주요 고객 계약 취소, 대규모 배상)
M	1.0	유출 시 보통 수준의 영향 (평판 하락, 일부 손실)
L	0.5	유출 시 미약한 영향
N	-	영향 없음

4.2 보안등급 분류 기준

4개 항목의 합산 점수(X = C + I + A + AI)에 따라 아래 4단계 등급을 부여한다.

등급	합산 점수	레이블	정의
비밀	8.0 초과	SECRET	회사 핵심 기밀 정보로 유출 시 중대한 재무적·법적 손실 또는 사업상 치명적 피해가 발생할 수 있는 문서
대외비	6.0 초과 ~8.0 이하	CONFIDENTIAL	외부 유출 시 업무 수행, 고객 신뢰, 대외 이미지 또는 사업상 손실이 발생할 수 있는 문서
사내한	4.0 초과 ~6.0 이하	RESTRICTED	회사 내부 임직원 간 공유 가능한 일반 업무 문서로 외부 유출 시 영향이 경미한 문서
관리제외	4.0 이하	표시없음	공개된 정보 또는 보안 관리가 불필요한 문서

4.3 등급별 통제 차별화 기준

통제 항목	비밀	대외비	사내한	관리제외
승인 권한	경영층 승인	부서장 승인	팀장/부서 승인	승인 불필요

접근 권한	지정된 최소 인원만 접근 가능	관련 부서 및 승인 인원만 접근 가능	임직원 열람 가능	제한 없음
문서 레이블	“비밀” 표시 필수	“대외비” 표시 필수	“사내한” 표시 권장	표시 불필요
저장/보관	암호화 저장 및 접근 권한 통제 필수	권한 제한 저장	사내 시스템 저장	일반 보관
외부 전송	원칙적 금지	승인 후 가능	업무 목적 내 가능	제한 없음
출력물 관리	출력 · 복사 제한 및 관리대장 권장	출력물 관리 필요	일반 관리	관리 제외
폐기 방법	완전 삭제 또는 파쇄	파쇄/완전삭제 권장	일반 폐기 가능	일반 폐기
대표 예시	M&A 계획, 핵심 기술자료, 미공개 재무자료	고객정보, 계약조건, 프로젝트 계획	공지사항, 일반 회의록, 교육자료	공개 브로셔 홈페이지 자료

4.4 평가 절차 및 주기

구분	내용	주기
최초평가	자산 등록 시 중요도 최초 평가 및 등급 부여	최초 1회
정기평가	전체 자산에 대한 정기 재평가	연 1회
수시평가	자산 변경, 평가 기준 변경, 보안사고 발생 시	발생 시

5. 위험분석 및 위험평가 절차 및 기준

5.1 핵심 개념

5.1.1 용어 정의

① 위협 (Threat): 해킹, 피싱, 랜섬웨어, 내부자 위협, 재해, 물리적 침해 등

② 취약점 (Vulnerability): 보안 패치 미적용, 잘못된 설정, 약한 암호, 과도한 권한, 미사용 서비스 미차단 등

③ 위험 (Risk): 자산가치(X) × 발생가능성(Y) × 비즈니스영향도(Z)

④ DoA (수용수준): 위험수용수준 40점. DoA 초과 시 반드시 감소(Reduce) 조치 시행 후 기본통제규칙 반영

5.2 발생 가능성 (Y 벡터) 평가 기준

등급	점수	기준	예시
Almost Certain	10	매년 1회 이상 발생 가능	과거 1년 내 유사 사례 다수 발생
Likely	8	2~3년에 1회 발생 가능	업계 평균 발생 주기 2~3년
Possible	6	3~5년에 1회 발생 가능	가능성 낮으나 현실적 위협 존재
Unlikely	4	5~10년에 1회 발생 가능	특수 상황에서만 발생, 사례 드묾
Rare	2	10년에 1회 이하 발생 가능	극히 예외적 사건

5.3 비즈니스 영향도 (Z 벡터) 평가 기준

Z 벡터는 아래 4개 항목을 각각 평가한 후, 그 중 가장 높은 점수를 Z 값으로 사용한다.

5.3.1 비즈니스 영향 / 금전적 손실 (공통 기준)

등급	점수	비즈니스 영향 기준	금전적 손실 기준
Catastrophic	3.5	핵심 업무 전면 중단, 기업 운영 불가	수십억 원 이상 손실, 대규모 배상 · 소송

Major	2.6	주요 부서 업무 장기 중단	수억 원대 손실, 주요 계약 취소
Moderate	1.7	부분적 업무 지연 · 장애	수천만 원대 손실, 단기 손해
Minor	1.0	경미한 영향	수백만 원대 손실
Insignificant	0.5	무시 가능한 수준	사실상 무손실

5.3.2 고객 영향도

등급	점수	기준
고객사 영향	2	핵심 고객사 불만 · 계약 취소 가능, 납품 불이행
2차사 영향	1	일부 고객 불편 발생, 서비스 장애
없음	0	고객 영향 없음, 내부 이슈, 외부 노출 無

5.3.3 준거성 영향

등급	점수	기준
법규 위반 사항	1	법적 제재, 과징금 · 형사처벌 가능 (개인정보보호법 위반 등)
대외 신뢰 하락	0.5	평판 손상, 언론 노출, 협력사 신뢰 하락
없음	0	영향 없음, 내부적 이슈로 종결

5.4 위험 점수 산출 공식 ★★★★★★5/26일 자동차 위험평가 문서 분석★★★★★

5.4.1 위험 점수 = X (자산 가치) × Y (발생 가능성) × Z (비즈니스 영향도)

5.4.2 DoA(위험수용수준) = 40점 | Z = 4개 항목 중 최댓값 사용

5.5 위험 등급 분류

위험 등급	종합 점수 구간	관리 기준
High (높음)	7.5 이상	즉각적 조치 필요. 경영진 보고 후 감소(Reduce) 대책 수립 및 시행.
Medium (중간)	5.0 ~ 7.4	개선계획 수립 및 정기 점검. DoA 초과 시 Reduce 조치 시행.
Low (낮음)	5.0 미만	모니터링 중심 관리. DoA 미만 시 수용(Accept) 가능.

5.6 평가 절차

5.6.1 자산별 위협 및 취약점 수집 (정보보안그룹 주관, 시스템관리자 지원)

5.6.2 Y · Z 벡터 점수 산정 및 위험 점수 계산

5.6.3 위험 등급 산정 (High / Medium / Low)

5.6.4 DoA(40점) 초과 항목에 대한 위험처리 방안 수립

5.6.5 결과 보고서 작성 및 CSO 보고 · 승인

5.6.6 기본통제규칙에 반영 및 1년 후 Feedback 재평가

6. 위험처리 방안 절차 및 기준

6.1 처리 방안 4가지

방안	설명	적용 사례
감소	통제 강화를 통해 위험 수준을 낮춤 (DoA 초과 시 우선 적용)	방화벽 도입, 접근제어 강화, 암호화, 모니터링 강화

회피	위험의 원인이 되는 활동 · 자산 자체를 제거 · 중단	특정 서비스 중단, 위험 프로세스 폐기
전가	보험 · 계약을 통해 위험의 재정적 책임을 외부로 이전	사이버보험, 아웃소싱, 계약서 면책 조항
수용	DoA 미만 위험을 문서화 후 현 수준 유지	비용 대비 효과가 낮은 낮은 위험

6.2 처리 절차

6.2.1 위험 대응 전략 수립 및 책임자 지정 (정보보안그룹)

6.2.2 실행 계획 수립 및 CSO 검토 · 승인

6.2.3 실행 후 효과 검증 및 잔여 위험 확인

6.2.4 결과 문서화 (위험처리계획서 및 이행결과서 보관)

6.2.5 조치 결과는 시행 1년 후 Feedback 반영하여 기본통제규칙으로 재반영

7. 위험관리 책임 분담

7.1 CSO: 전사 위험관리 총괄 및 최종 정책 승인. DoA 초과 위험에 대한 처리 방향 결정.

7.2 정보보안그룹: 위험 평가 실시, 대응 전략 수립, 이행 모니터링, 정보자산관리대장 등록 · 갱신.

7.3 시스템 관리자: 기술적 보안 패치 · 설정 변경 등 기술적 대응 수행. 취약점 정보 및 시스템 구조 제공.

7.4 부서 자산 관리자: 자산 정보 식별 · 등록, 중요도 평가 정보 제공, 변경 발생 시 즉시 통보.

7.5 임직원 전체: 보안 정책 준수, 위협 인지 시 즉시 보고, 보안 교육 이수.

8. 문서 · 기록 관리 및 사후 점검

8.1 문서 보존: 모든 위험관리 기록(자산목록, 평가결과, 처리계획서, 이행결과서)은 최소 3년 이상 전자 문서 시스템에 보관한다.

8.2 정기 감사: 연 1회 이상 자체 감사를 실시하며, ISMS-P · ISO 27001 등 외부 인증 대비 갭 분석을 수행한다.

8.3 지속적 개선: 위험 조치 결과는 시행 1년 후 Feedback을 반영하여 기본통제규칙으로 통상 실시 추진한다.

8.4 재평가 트리거: 신규 시스템 도입, 보안사고 발생, 조직 · 업무 변경, 평가 기준 변경 시 수시 재평가를 실시한다.

(주)넥스오토 NEXAUTO	정보자산 분류 및 위험도 평가 절차 지침	문서번호 NEX-IS-A-05
제정일: 2026-05-12		개정차수: 0

부록 A — 자산 분류 기준표

유형	자산번호 체계	분류 항목 예시	비고
정보	NEX-[부서]-NNN	설계 · 개발 · 품질 · 측정 · 인사 · 회계 · 구매 · 물류 · 안전 · 전산 등 업무 문서	
소프트웨어	NEX-SW-NNN	PLM, MES, ERP, OS, DB, 보안솔루션, 그룹웨어, 홈페이지 등	
하드웨어	NEX-HW-NNN	서버, DB서버, 웹서버, 네트워크장비, 정보보안장비, 단말기, 저장장치 등	
설비 · 시설	NEX-FC-NNN	전산실, 사무실, 기계실, 보전창고, 생산라인, 금고, 현장사무실 등	
인력	NEX-HR-NNN	국내 · 해외사업장 임직원, 연구소, 공동개발, 외부협업 인원	

부록 B — 등급별 통제 요약표 (기본통제규칙 연계)

기본통제 정책	비밀	대외비	사내한	관리제외
정책 · 세부지침 적용	●	●	●	○
보안서약서	●	●	●	—
문서고 운영 · 등급 표기	●	●	○	—
파일서버(NAS)/PLM 저장통제	●	●	●	—
암호화	●	●	권고	—
DLP · 매체제어	●	●	●	—
반출입 통제 · HDD 봉인	●	●	○	—
로그 모니터링	●	●	●	○
보안감사 대상	●	●	●	—

● 필수 적용　○ 권고 적용　— 해당 없음