(주)넥스오토 NEXAUTO	보안점검 및 감사 지침	문서번호 NEX-IS-A-08
제정일: 2026-06-29		개정차수: 2

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	2026-06-29	2026-06-29	2026-06-29

(주)넥스오토 NEXAUTO	보안점검 및 감사 지침	문서번호 NEX-IS-A-08
제정일: 2026-06-29		개정차수: 2

개정 이력

차수	제(개)정 일자	시행일자	주요 개정 내용
0	2024-08-01	2024-08-01	초도 제정
1	2025-08-04	2025-08-04	협력사 · 해외법인 · 임시직 파견자 조항 추가 관리/물리 담당자 변경
2	2026-06-29	2026-06-29	취약점 도출 및 개선조치 조항 추가

(주)넥스오토 NEXAUTO	보안점검 및 감사 지침	문서번호 NEX-IS-A-08
제정일: 2026-06-29		개정차수: 2

목 차

(주)넥스오토 NEXAUTO	보안점검 및 감사 지침	문서번호 NEX-IS-A-08
제정일: 2026-06-29		개정차수: 2

1. 보안점검 및 감사지침

1.1 목적

본 지침서는 당사 정보보호 규정에 따라, 정보보안그룹 주관의 전사 보안점검을 체계적으로 운영하고, 각 부서의 보조적 자체점검을 통해 정보보안 수준을 강화함을 목적으로 한다.

1.2 적용 범위

본 지침은 전 임직원 및 외부 협력사, 파견자, 해외법인, 해외주재원을 포함하며, 정보보안 활동에 영향을 미치는 모든 조직 및 시스템에 적용된다.

2. 보안점검 체계

2.1 점검 유형 및 주체

2.1.1 전사 보안점검

① 주관: 정보보안그룹

② 대상: 전 부서 및 사업장

③ 주기: 분기 1회 이상

④ 목적: 조직 전반의 보안 통제 현황을 체계적으로 점검하고 취약점 개선

2.1.2 부서별 자체 보안점검 (보조)

① 주관: 각 팀 보안담당자

② 대상: 각 부서 내 보안관리 항목

③ 주기: 월 1회

④ 목적: 일상적인 보안관리 상태를 자체 점검하고, 전사점검 시 사전 보완자료로 활용

3. 전사 보안점검 (정보보안그룹 주관)

3.1 목적 및 특징

3.1.1 정보보안그룹이 주관하며, 회사 전체의 보안상태를 종합적으로 점검

3.1.2 부서 자체점검과는 별도로 수행되는 독립된 점검체계

3.1.3 도출된 취약점에 대해서는 책임 부서가 개선조치 이행

3.2 점검 절차

3.2.1 분기별 점검 계획 수립 및 대상 부서 공지

① 정보보안그룹은 연간 또는 분기별 보안점검 계획을 수립한다.

② 점검 목적, 범위, 일정, 점검 항목을 정의한다.

③ 점검 대상 부서에 사전 공지하며 필요 시 증적자료 제출을 요청한다.

④ 고위험 부서는 우선 점검 대상으로 선정할 수 있다.

⑤ 조직 변경 및 보안사고 발생 부서는 수시 점검 대상으로 추가할 수 있다.

3.2.2 사전 자료 수집 및 점검 준비

① 대상 부서는 정보보안그룹의 요청에 따라 시스템 현황 및 계정목록등 필요한 자료를 제출한다.

② 정보보안그룹은 제출 자료를 검토하여 중점 점검 항목 및 위험 요소를 사전 분석한다.

③ 필요 시 인터뷰 대상자 및 현장 점검 일정을 조율한다.

④ 점검 수행에 필요한 체크리스트 및 증적 확보 방안을 준비한다.

3.2.3 현장 점검 또는 문서 및 시스템 점검 실시

① 정보보안그룹은 현장 점검, 시스템 확인, 인터뷰, 문서 검토 등의 방식으로 점검을 수행한다.

② 점검 과정에서 운영 절차 준수 여부와 실제 운영 상태를 비교 확인한다.

③ 시스템 이벤트 로그 기록, OS 업데이트 현황, 계정 현황, 보안솔루션 설치 현황등을 확인한다.

④ 필요 시 샘플링 방식으로 계정, 문서, 자산 등을 검증할 수 있다.

⑤ 점검 수행 중 발견된 주요 위험사항은 즉시 해당 부서에 통보할 수 있다.

3.2.4 점검 결과 기록 및 취약점 분석 수행

① 점검 결과는 점검 체크리스트 및 점검보고서에 기록한다.

② 발견된 미흡사항 및 취약점은 평가결과(상 · 중 · 하) 에 따라 분류한다.

③ 정보보안그룹은 취약점의 발생 원인, 영향도 및 잠재 위험성을 분석한다.

④ 동일 또는 유사 취약점의 반복 발생 여부를 확인한다.

⑤ 법규 위반 또는 중대한 보안위험 발견 시 즉시 CSO 및 관련 부서에 보고할 수 있다.

3.2.5 종합 결과보고서 작성 및 경영진 보고

① 정보보안그룹은 점검 결과, 취약점 현황, 개선 상태 및 주요 위험사항을 종합하여 결과보고서를 작성한다.

② 보고서에는 부서별 보안수준 평가 및 주요 개선 필요사항을 포함할 수 있다.

③ 종합 결과는 CSO 및 필요 시 경영진에게 보고한다.

④ 점검 결과는 향후 보안정책 개선 및 위험관리 활동에 반영한다.

3.3 점검 항목 예시

3.3.1 접근통제 설정 및 로그 관리

3.3.2 계정 및 권한 관리

3.3.3 민감정보 취급 방식

3.3.4 문서보안 및 자산관리

3.3.5 클린데스크 정책 준수 여부

4. 부서별 자체 보안점검

4.1 개요

4.1.1 부서 자체점검은 정보보안그룹의 전사점검을 보조하는 선제적 조치로, 각 부서가 자율적으로 월 1회 실시한다.

4.1.2 점검 결과는 정보보안그룹에 제출하여 전사 점검의 기초자료로 활용된다.

4.2 절차

4.2.1 매월 정해진 시점에 자체점검 실시한다.

4.2.2 부서 담당자가 지정된 체크리스트 기준으로 점검한다.

4.2.3 개선 필요사항은 정보보안그룹이 도출한 취약점 기준에 따라 조치한다.

4.2.4 자체점검 결과는 3년간 보관, 정보보안그룹 검토 시 참고자료로 활용한다.

5. 협력사 보안점검

5.1 목적 및 특징

5.1.1 협력사의 정보보호 관리 수준 및 보안통제 이행 상태를 점검하여 공급망 보안위험을 최소화한다.

5.1.2 정보보안그룹 주관 하에 수행하며, 협력사 보안사고 예방 및 재발방지를 목적으로 한다.

5.1.3 협력사 보안점검 결과 미흡사항은 해당 협력사에 개선 요청하며 후속 조치를 확인한다.

5.2 점검 기준 및 주기

5.2.1 정보보안그룹은 연간 또는 반기별 협력사 보안점검 계획을 수립할 수 있다.

5.2.2 점검 대상은 당사 업무 수행에 필요한 정보자산 또는 시스템에 접근 가능한 협력사를 대상으로 한다.

5.2.3 협력사 보안점검은 연 1회 이상 실시하는 것을 원칙으로 한다.

5.2.4 필요 시 현장 방문 점검, 원격 점검, 문서 점검 등의 방법으로 수행할 수 있다.

5.2.5 협력사 보안사고 발생 또는 침해 우려가 확인된 경우 수시 특별점검을 실시할 수 있다.

5.3 점검 절차

5.3.1 사전 계획 및 통보

① 정보보안그룹은 점검 목적, 일정 및 점검 항목을 포함한 계획을 수립한다.

② 협력사 담당자에게 방문 일정, 점검 목적 및 주요 점검 내용을 사전 통보한다.

5.3.2 현장 및 시스템 점검

① 협력사의 업무에 영향을 최소화하도록 신속하고 정확하게 점검을 수행한다.

② 시스템 보안설정, 계정관리, 로그관리, 악성코드 대응체계 등을 점검할 수 있다.

③ 필요 시 보안진단 소프트웨어 및 점검 체크리스트를 활용할 수 있다.

5.3.3 사고 대응 점검

① 협력사 보안사고 발생 시 즉시 긴급 보안점검을 수행할 수 있다.

② 침해원인 분석, 임시조치 및 재발방지 대책 수립 여부를 확인한다.

③ 필요 시 협력사에 개선 가이드라인 제출 및 후속조치를 요구할 수 있다.

5.3.4 결과 분석 및 개선조치

① 점검 결과는 협력사 정보보안 점검 체크리스트 및 결과보고서에 기록한다.

② 미흡사항에 대해서는 개선 권고사항 및 조치 기한을 통보한다.

③ 개선 결과는 증적자료 또는 재점검을 통해 확인한다.

6. 해외법인 보안점검

6.1 목적 및 특징

6.1.1 해외법인의 정보보호 수준을 유지하고 글로벌 보안통제를 일관되게 적용하기 위하여 실시한다.

6.1.2 국내 본사 정보보안그룹 주관 하에 수행하며 해외법인의 자체 보안활동을 지원한다.

6.2 점검 기준 및 주기

6.2.1 정보보안그룹은 해외법인 보안점검 계획을 연간 단위로 수립한다.

6.2.2 해외법인 보안점검은 분기별 1회 이상 실시할 수 있다.

6.2.3 필요 시 보안솔루션을 활용한 원격 점검으로 대체할 수 있다.

6.2.4 필요 시 불시 보안점검 및 현장 방문 점검을 수행할 수 있다.

6.2.5 해외법인은 월 단위 자체 보안점검 및 보안교육 활동을 수행할 수 있다.

6.3 점검 절차

6.3.1 사전 계획 수립

① 본사 정보보안그룹은 연간 해외법인 점검계획을 수립한다.

② 점검 대상 및 일정은 해외법인 보안책임자에게 사전 공유한다.

6.3.2 점검 수행

① 해외법인 보안책임자는 본사 점검 체크리스트 기준에 따라 보안점검을 수행한다.

② 정보보안그룹은 시스템 설정, 계정 현황, 로그 관리, 보안솔루션 운영 상태 등을 확인할 수 있다.

③ 필요 시 현장 방문을 통한 실사 점검을 수행할 수 있다.

6.3.3 결과 보고 및 개선

① 해외법인은 점검 결과를 본사 정보보안그룹에 제출한다.

② 정보보안그룹은 점검 결과를 분석하고 취약점 개선 여부를 확인한다.

③ 주요 취약점 및 반복 위반사항은 CSO에 보고할 수 있다.

7. 임시직 · 파견자 및 제3자 아웃소싱 보안점검

7.1 목적 및 특징

7.1.1 외부 인력 및 아웃소싱 수행 과정에서 발생 가능한 정보유출 및 비인가 접근 위험을 예방하기 위하여 실시한다.

7.1.2 계약서, 보안서약서 및 내부 보안정책 준수 여부를 중점적으로 점검한다.

7.2 점검 기준 및 주기

7.2.1 외주인력 및 파견인력의 보안점검은 업무 수행 기간 동안 상시 수행할 수 있다.

7.2.2 주요 시스템 접근 권한 및 작업 내역은 필요 시 수시 점검한다.

7.2.3 작업 시작 전 · 작업 중 · 작업 종료 후 단계별 보안점검을 수행할 수 있다.

7.3 점검 절차

7.3.1 작업 전 점검

① 계약서, 보안서약서 및 접근권한 승인 여부를 확인한다.

② 작업 범위 및 허용 권한을 사전 검토한다.

7.3.2 작업 중 점검

① 외주인력의 작업 내역 및 시스템 접근 현황을 점검한다.

② 승인되지 않은 접근 시도 및 비인가 작업 여부를 확인한다.

③ 주요 서버 및 시스템에 미치는 영향을 수시 모니터링할 수 있다.

7.3.3 작업 종료 후 점검

① 작업 로그 및 보안시스템 로그를 검토한다.

② 외부 인력이 보유한 회사 자료의 삭제 여부를 확인한다.

③ 계정 회수 및 접근권한 종료 여부를 확인한다.

7.3.4 위반사항 조치

① 보안 위반사항 발견 시 즉시 정보보안그룹 및 CSO에 보고한다.

② 필요 시 외주업체에 재발방지 대책 제출을 요구할 수 있다.

③ 중대한 위반사항은 계약상 손해배상 및 제재 절차를 검토할 수 있다.

8. 취약점 도출 및 개선조치

8.1 식별 및 보고

8.1.1 전사 보안점검, 부서별 자체점검, 협력사 보안점검, 해외법인 보안점검 및 외부인력 보안점검 결과는 정보보안그룹이 통합 수집하여 취약 여부를 분석한다.

8.1.2 각 부서, 해외법인 및 협력사는 점검 결과 및 요구 증적자료를 정해진 기간 내 제출하여야 하며, 취약점 판단은 정보보안그룹이 수행한다.

8.1.3 정보보안그룹은 점검 결과 확인된 미흡사항 및 취약점을 중요도(상 · 중 · 하) 기준에 따라 분류할 수 있다.

8.1.4 중대한 보안위험, 법규 위반 또는 침해사고와 연계된 사항 발견 시 즉시 CSO 및 관련 부서에 보고할 수 있다.

8.1.5 반복적으로 발생하는 취약점 및 미조치 항목은 지속관리 대상 항목으로 분류하여 관리할 수 있다.

8.2 개선 요청 및 조치

8.2.1 정보보안그룹은 도출된 취약점에 대해 해당 부서, 해외법인, 협력사 또는 외부업체에 개선 요청서를 전달한다.

8.2.2 개선 요청을 받은 조직 또는 담당자는 개선계획 및 조치일정을 수립하여 정보보안그룹에 회신하여야 한다.

8.2.3 부서는 개선요청 접수 후 4주 이내 개선 완료 후 결과를 회신하는 것을 원칙으로 한다.

8.2.4 긴급 조치가 필요한 항목 또는 중대 취약점은 우선적으로 개선하여야 하며, 정보보안그룹은 즉시 조치를 요구할 수 있다.

8.2.5 개선이 어려운 사항은 사유, 위험분석 결과 및 대체 통제방안을 제출하여야 하며, 필요 시 CSO 승인을

받아야 한다.

8.2.6 협력사 및 외부업체의 경우 개선 결과에 대한 증적자료 제출 또는 재점검을 요구할 수 있다.

8.2.7 해외법인의 경우 본사 정보보안그룹이 개선 진행 상태를 모니터링하고 필요 시 추가 보완조치를 요청할 수 있다.

8.2.8 외주·파견 인력 관련 보안 위반사항 발견 시 즉시 접근권한 회수, 작업중지 또는 추가 보안조치를 수행할 수 있다.

8.2.9 조치가 지연되거나 반복적으로 미이행될 경우 '지속관리 항목'으로 등록하며, 누적 시 보안책임자 및 CSO에 보고한다.

8.2.10 중대 취약점, 반복 위반 사항 또는 침해사고와 관련된 항목은 경영진에게 직접 보고될 수 있다.

8.3 개선결과 확인 및 이력관리

8.3.1 정보보안그룹은 개선조치 완료 여부를 증적자료 검토, 시스템 확인 또는 재점검을 통해 확인할 수 있다.

8.3.2 미조치 또는 조치가 미흡한 사항에 대해서는 추가 개선을 요구할 수 있다.

8.3.3 모든 점검 결과, 개선조치 결과 및 관련 증적자료는 최소 3년 이상 보관한다.

8.3.4 점검 결과 및 개선 현황은 향후 보안정책 개선, 위험관리 및 보안교육 자료로 활용할 수 있다.