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	2026-06-26	2026-06-26	2026-06-26

(주)넥스오토 NEXAUTO	모바일보안지침	문서번호 NEX-IS-A-03
제정일: 2026-06-26		개정차수: 4

개정 이력

차수	제(개)정 일자	시행일자	주요 개정 내용
0	2017-09-13	2017-09-13	초도 제정
1	2023-12-01	2023-12-01	디오토 상호변경
2	2024-08-01	2024-08-01	넥스오토 상호변경
3	2025-08-04	2025-08-04	관리/물리 담당자 변경
4	2026-06-26	2026-06-26	사내망 보호 VPN 항목 추가

목 차

1. 목적

본 정책은 모바일 업무 개발 및 사용에 대한 기본원칙을 수립함으로서 회사의 영업비밀을 안전하게 보호하고, 정보의 유출을 예방하는 것을 목적으로 한다

2. 적용범위

임직원이 사용하는 스마트폰, 휴대폰, PDA, 태블릿, 노트북 등 정보의 저장이 가능하고 다른 정보기기에 연결할 수 있는 모든 이동형 기기를 대상으로 한다.

3. 용어의 정의

3.1 모바일기기

스마트폰, PDA, 휴대폰, 노트북, 태블릿 등 휴대 가능하고 자료의 저장 기능이 있는 모든 기기를 의미한다.

3.2 모바일업무

3.2.1 모바일 기기를 통해 업무를 수행하는 일체의 행위를 의미한다.

3.2.2 회사 사업장내에서 내부 무선망을 사용하거나, 사업장 이외의 장소에서 유무선 인터넷을 사용하여 접속할 수 있도록 업무시스템을 제공하는 것을 의미한다.

3.3 스마트폰(Smartphone)

PDA와 휴대전화기의 기능이 결합하고 완전한 형태의 OS(운영체제)를 탑재하여 프로그램(앱) 설치가 가능하고 인터넷이나 부가적인 접속 기능을 통해 외부와 정보를 주고받을 수는 기기를 의미한다.

3.4 PDA(Personal Digital Assistance)

휴대 가능한 컴퓨터로 스마트폰과 유사하나 이동통신망 연결 기능이 없는 장비를 의미한다

3.5 휴대폰(Feature phone)

기기의 형태와 무관하게 전화 통화, 문자메시지 송수신을 주목적으로 하는 전화기를 의미한다.

3.6 노트북/랩탑(Laptop)

전원공급이 없는 이동간에 사용할 목적으로 만들어진 PC를 의미한다.

3.7 태블릿PC (Tablet PC)

노트북과 유사하나 터치스크린을 장착하여 별도의 키보드나 마우스 없이 조작이 가능한 장비를 의미한다.

3.8 임의개조(Jail Break, Custom Rom)

제조사에서 제한한 기능 활용을 목적으로 시스템 관리자 권한을 취득하도록 임의 변경된 OS를 설치하거나

유사한 프로그램을 설치하는 행위를 의미한다.

3.9 테더링 (Tethering)

이동통신망을 사용하는 모바일기기를 USB케이블 또는 무선으로 PC/노트북을 연결하여 인터넷에 접속하는 것을 의미한다.

3.10 앱 (App)

Application(응용프로그램)의 약자로 일반적으로 스마트폰에서 구동되는 프로그램을 의미한다

3.11 이동통신망

CDMA, GSM, LTE 등의 통신장치가 장착된 기기에서 음성, 데이터 통신이 가능하도록 한 네트워크를 의미한다

3.12 BYOD(Bring Your Own Device)

개인소유의 모바일 기기를 회사 업무에 활용하는 것을 의미한다

3.13 모바일보안심의팀

보안관리팀(현대), 보안관리팀(기아), 보안기술팀(현대/기아), 정보보안기획팀의 실무자로 구성된 협의체를 의미한다.

4. 모바일 업무지원

4.1 적용절차

4.1.1 본 절차는 기획단계 또는 발의 품의 이전에 검토 적용한다.

4.1.2 '4.2 적용기준'을 모두 만족하는 경우

① 업무 주관팀에서 모바일보안심의팀으로 협조전을 송부하고, 업무일 기준 10일 이내 검토의견이 없는 경우 IT 투자절차에 따른OOOO지침을 시행한다.

② 모바일보안실무팀에서 기각 사유가 있는 경우, 보안기술팀에서 모바일보안실무자 회의를 소집하여 재검토 및 조정한다.

4.1.3 '4.2 적용기준' 중 4.2.② 또는 4.2.③ 을 충족하지 못하는 경우

① 월 1회 개최되는 모바일보안실무팀 회의에서 검토 후 추진한다.

4.1.4 '4.2 적용기준' 중 4.2.①항을 충족하지 못하는 경우

① 현업 팀에서 모바일 업무개발 시 리스크, 목표사용량 등 포함한 내용 별도로 작성한다.

② 작성된 보고서를 경영층(현업본부장, CSO, CIO 등)에 보고 후 결정한다

4.2 적용기준

4.2.1 모바일기기를 통해 업무를 서비스 하기 위해서는 아래 조건을 모두 충족해야 한다.

① '5. 모바일업무 가능한 정보'의 허용기준을 충족해야 한다.

② '6. 모바일업무 타당성'에서 정한 평가기준을 충족해야 한다.

③ '7. 모바일기기 활용기준'을 충족해야 한다.

4.2.2 기존 모바일로 서비스되고 있는 업무도 4.2의 적용기준을 만족하도록 개선해야 하며, 특정시점을 기준으로(201x년 1월 이후) 적용기준을 만족하지 못하는 모바일 업무는 그 서비스를 중단한다

5. 모바일 업무 가능한 정보

5.1 허용 기준

5.1.1 미 분류, 비밀 또는 극비 정보를 포함하지 않는 경우

5.1.2 '5.3 비밀등급의 예외'에 해당하는 경우

5.1.3 비밀 정보는 회사에서 지급한 기기로, 사업장 내에서, 회사 무선랜을 사용하는 경우에만 허용한다,

5.2 정보자산분류

5.2.1 회사의 보안규정에서 정한 정보자산분류 기준을 준용한다.

5.2.2 최근 3개월 이내에 보안등급을 하향하여 재 분류한 경우 이전 기준을 사용한다.

5.2.3 최근 3개월 이내에 보안등급이 분류되지 않은 상태에서 민감한 자료로 판단이 되는 경우 비밀로 간주한다.

5.2.4 오토웨이 계정을 통한 로그인 후 조회되는 정보는 대외비 이상으로 간주한다.

5.3 비밀등급의 예외

5.3.1 입력/수집정보: 보안규정 내 비밀이상에 해당하는 정보라도 조회기능 없이 모바일기기 및 서버로 정보를 입력만 하는 경우는 대외비로 분류한다.

5.3.2 제한된 고객정보: 시스템 제한으로 고유식별정보 등 중요정보가 노출되지 않은 상태로 본인이 수집 및 입력한 정보에 한해 1일 100건 이상 조회 불가한 고객정보는 대외비로 분류한다.

6. 모바일업무 타당성

6.1 타당성 평가기준

6.1.1 '6.2 보안성 항목'에서 3건이상 만족해야 한다

6.1.2 '6.3 편의성 항목'에서 3건이상 만족해야 한다

6.1.3 두 항목의 결과를 더해 7건 이상 만족해야 한다

6.2 보안성 항목

6.2.1 대외비/비밀 등급이 혼재되어 있지 않을 것

6.2.2 기존 운영 방식보다 보안성이 떨어지지 않을 것

6.2.3 모바일 기기에 자료를 저장하지 않을 것

6.2.4 화면을 통해 자료가 노출되어도 감수할 수 있을 것

6.2.5 하루에 사용할 수 있는 정보를 제한할 수 있을 것 (건수, 크기, 횟수 등)

6.3 편의성 항목

6.3.1 PC로 처리가 불가능할 것

6.3.2 노트북으로 처리가 불가능할 것

6.3.3 장소에 구애받지 않고 사용할 요구가 있을 것

6.3.4 실시간 사용의 요구가 높을 것

6.3.5 사용계정 마다 매일 1회 이상의 로그인이 있을 것

7. 모바일기기 활용

7.1 회사기급 기기

7.1.1 공통사항

① '10. 모바일기기 보호'의 해당 사항을 모두 적용해야 한다

② 회사 지급 기기에는 직원이 임의로 프로그램을 설치하거나 삭제할 수 없으며, 회사가 지정한 앱, 프로그램만 설치 사용해야 한다.

7.1.2 사내 사용

① 회사 지급 기기는 특별한 사유가 없는 한 와이파이 전용(이동통신 기능이 없는) 기기를 지급한다.

② 회사 지급 기기는 사내망 접속 상태에서 처리 가능한 업무에 적용한다. 단, 회사에서 사내망을 제공하지 못한 경우 이동통신망을 허가할 수 있다

③ 회사지급 기기에는 암호화(DRM)된 파일만 저장해야 한다.

④ 단, 암호(DRM)해제된 파일의 저장/사용이 필요한 경우 보안관리팀에 사용자, 사용기기, 저장내용, 시용 기간, 보호조치 등을 협의 후 적용하며, 암호 해제된 파일을 사용하는 동안에는 해당기기의 사외반출을 제한한다.

7.1.3 사외 사용

가상환경(업무격리) 또는 전용 앱으로 제공되는 업무를 사용해야 한다

7.2 개인소유 기기

7.2.1 사내 사용

① 개인소유 모바일기기로 회사 회의자료, 시설 등을 메모, 녹취, 촬영하고자 하는 경우에는 아래 기준에 따라 사전 승인을 받아야 한다.

a. 회의, 발표, 출력물 등은 자료의 관리 책임자

b. 차량, 부품, 시설 등은 해당 관리 책임자

c. 상기 항목에 해당하지 않는 경우 보안팀

② 개인소유 모바일기기는 사내의 유·무선망을 접속하거나 사용할 수 없다

③ 개인소유 모바일기기를 회사 PC, 노트북 기타 장비로 연결하거나, 자료를 송신할 수 없다.

④ 개인소유 노트북은 사내 반입을 금지한다.

7.2.2 사내에서 이동통신망을 통한 업무 사용하거나 사외에서 사용

① 회사에서 지정한 종류의 기기만 사용한다

② 회사 지급장비와 동일한 통제를 적용 받고, 해당 기기 내 모든 자료를 회사가 파기할 수 있다는 사용자 동의서를 제출한다

③ '10. 모바일기기 보호'의 해당 사항을 모두 적용하거나

④ 가상환경(업무격리) 또는 전용 앱으로 제공되는 업무를 사용해야 한다

8. 모바일 인프라 보호

8.1 무선랜 보호

8.1.1 회사가 설치한 AP는 회사기기에 한정하여 접속을 허용한다.

8.1.2 회사 내에서 허가되지 않은 AP가 운영되지 않도록 관리적/기술적인 조치를 적용한다.

8.1.3 회사에서 승인하지 않은 테더링, 무선AP, 장비간 AdHoc 연결을 포함한 모든 연결은 실시간 차단한다.

8.1.4 업무상 AP의 설치, 사용기기의 등록이 필요한 경우 보안팀에서 승인할 수 있도록 절차를 수립하고, 허가된 범위 내에서 사용되는지 정기적으로 확인한다

8.2 모바일 기기 식별 및 관리

8.2.1 회사 업무에 사용되는 모바일 기기는 고유한 식별 정보를 등록 관리한다.

8.2.2 고유한 식별 정보는 USIM, 기기 Hardware ID, MAC Address 등 복제가 어렵고 개인정보를 포함하지 않는 정보를 사용한다

8.2.3 식별정보가 등록되지 않은 모바일 기기는 회사 네트워크에 연결할 수 없도록 제한한다.

8.2.4 기기를 등록한 사용자만 접속이 되도록 제한한다.

8.3 사내망 보호(VPN)

8.3.1 회사 VPN은 회사기기에 한정하여 접속을 허용한다.

8.3.2 회사 VPN에 접속하는 모바일기기는 MAC Address를 사전에 등록해야 하며, 등록된 계정과 MAC Address가 일치하고 부가인증(OTP)를 사용하여 접속이 되도록 한다.

8.3.3 회사 VPN계정은 아래 업무에 해당하는 경우에만 발급한다.

① 차량생산과 관련한 유지보수 업무

② 차량시험 업무

③ 전용선이 설치되지 않은 사업장 파견 업무

8.3.4 IT유지보수, 설비유지보수 업무는 지정된 보안서버(SAC) 또는 사업장 내에서 수행한다

8.3.5 상기 항목에 해당하지 않는 업무 또는 개인기기로 회사 VPN에 접속이 필요한 경우 보안팀의 승인을 받고, '7.2.2 항목을 준수해야 한다.

9. 모바일 앱 보호

9.1 사용동의

9.1.1 모바일 앱 설치 시, 모바일 업무에 대한 보안규정 준수를 동의하는 내용을 화면에 공지하고 동의하는 경우에 설치되도록 한다

9.1.2 모바일 앱 사용 시, 보안상 주의사항을 화면에 공지하고 동의하는 경우 로그인이 되도록 구현한다

9.2 계정저장 금지

9.2.1 오프라인 로그인 기능을 제공하지 않는다.

9.2.2 비밀번호 저장 옵션을 제공하지 않는다.

9.2.3 비밀번호는 마스킹 처리한다

9.2.4 비밀번호 변경주기는 기존 보안정책을 준용한다

9.3 접속기록 유지

9.3.1 앱 접속 시 접속시간, 디바이스ID, 사용자ID, IP, 사용내용을 기록하고 3년 이상 보관한다

9.3.2 사용자가 앱에 로그인하면 직전 접속정보를 표시한다

9.4 암호화

9.4.1 로그인 시 송신되는 계정정보는 암호화한다.

9.4.2 화면에 표시되는 정보 중 대외비 이상의 정보를 처리하는 경우 암호화하여 송수신 한다

9.5 자료저장 제한

9.5.1 화면에 표시되는 정보는 스트리밍 처리하여 모바일기기에 자료가 저장되지 않도록 구현해야 한다. 임시파일(Cache)을 사용하는 경우 로그오프 또는 세션만료 시 복구 불가능하도록 자동 삭제한다

9.5.2 메일을 포함한 메시지는 최근7일만 표시되도록 한다.

9.6 장치사용 통제

9.6.1 허용된 장소 외 카메라 사용을 제한한다

9.6.2 회사 앱이 동작중인 동안에는 화면캡쳐를 제한 한다.

10. 모바일 기기 보호

10.1 공통사항

10.1.1 사내에서만 사용 허가된 모바일기기는 반출·입 통제 대책을 수립 적용한다

10.1.2 공용 모바일기기 사용 후에는 저장한 자료를 모두 삭제해야 하고, 이를 강제할 수 있는 체계를 수립, 운영한다

10.1.3 업데이트, 시스템 패치 등이 정상적으로 적용되었는지를 확인하고, 이를 강제할 수 있는 체계를 수립, 운영한다

10.2 윈도OS 모바일기기

10.2.1 네트워크접속통제(NAC)가 항상 동작 중이어야 한다

10.2.2 매체통제프로그램(SEP)이 항상 동작 중이어야 한다

10.2.3 암호화 프로그램(DRM)이 항상 동작 중이어야 하고 저장된 자료는 암호화 상태를 유지하여야 한다.

10.2.4 자료유출방지프로그램(DLP)이 항상 동작 중이어야 한다.

10.2.5 분실 시 정보유출 위험 및 하드디스크 분리를 통한 보안우회를 통제할 수 있도록 디스크암호화를 적용해야 한다.

10.3 비 윈도OS 모바일기기

10.3.1 기기를 회사에 등록하고, 기기인증 절차를 따라야 한다.

10.3.2 회사가 허용한 앱 외, 임의로 앱을 설치할 수 없다

10.3.3 임의개조 하거나 타인에 제공, 대여할 수 없다,

10.3.4 5분이내 화면 잠금이 동작되어야 한다.

10.3.5 분실 시 원격삭제가 가능해야 한다

11. 사용자 모바일 보안 관리

11.1 임직원 준수사항

11.1.1 임직원은 모바일 보안정책을 준수하고 관련 보안교육을 이수해야 한다.

11.1.2 모바일업무에 사용되는 모든 모바일 기기는 기기정보와 사용자 정보를 등록한 후 사용한다.

11.1.3 회사 자료/정보를 개인 모바일 단말기에 저장/보관하지 않는다.

11.1.4 사외에서 와이파이에 연결한 경우에는 업무용으로 사용하지 않는다.

11.1.5 회사에 등록한 개인 모바일 기기를 도난·분실한 경우 원격삭제 조치를 받는다

11.1.6 위조된 웹사이트나 문자를 통한 사기(파밍/스미싱)에 주의하고, 악성코드가 설치되지 않도록 백신 등을 설치하여 관리한다

11.1.7 설치파일 또는 블랙마켓 등 비 정상적인 방법을 통해 취득한 앱은 설치하지 않는다.

11.1.8 회사가 지정 배포한 앱(프로그램), 보안프로그램, 백신은 항상 최신 상태로 업데이트 및 유지 관리한다.

11.1.9 모바일 업무시스템 사용 시 전자/서면 동의 내용을 반드시 확인하고 이를 준수한다.

11.1.10 바이러스, 악성코드 등에 감염되거나 해킹이 의심될 때에는 기기 포맷한다.