구 분	작 성	검 토	승 인
직 책	관리/물리담당자	기술담당자	CSO
성 명	정 금	송 대 준	김 상 두
서 명			
일 자	2026-02-09	2026-02-09	2026-02-09

개정 이력

차수	제(개)정 일자	시행일자	주요 개정 내용
1	2017-09-29	2017-09-29	초도 제정
2	2022-10-14	2022-10-14	조직도 변경
3	2023-12-01	2023-12-01	상호변경 조직도 변경
4	2024-08-05	2024-08-05	상호변경 조직도 변경
5	2025-08-03	2025-08-03	각 목차별 보안규정 내용수정
6	2025-01-13	2025-01-13	현대/넥스 통합에 따른 조직도 변경
7	2025-03-25	2025-03-25	관련 지침 및 양식 순서 변경
8	2026-02-09	2026-02-09	계열사 규정 일치화 및 규정 업데이트

목 차

제1장 총칙

제1절 정보보안 개요

제1조 (목적) 본 규정은 (주)넥스오토(이하 '회사' 또는 '당사'라 한다.)의 정보보호 활동을 위한 기반 조직을 구성하고, 비 인가자의 부적절한 행위로부터 당사 근무인원 및 시설을 안전하게 보호하는 것과 정보시스템에 의하여 처리, 저장, 소통되는 자료를 바이러스, 해킹 등의 위협으로부터 보호하고 취약요인을 제거하여 회사의 정보보호 관리를 지속적으로 이루어지게 하는 것을 목적으로 한다.

제2조 (적용범위) 회사의 업무 관련 보안은 관계법령에 저촉되지 않는 범위 내에서 본 규정이 정하는 바에 의한다.

① 본 규정은 당사에 근무하는 모든 임직원에 대하여 적용함을 원칙으로 한다

② 본 규정은 당사가 보유한 유·무형의 모든 자산 및 임직원에 의해 파생된 자산과 활동을 포함한다.

③ 본 규정에 정한 범위 내에서 당사의 출입자, 계약 관계에 있는 업체 및 기타 업무상 조정 통제를 받는 단체의 임직원들도 적용한다.

제3조 (용어의 정의)

① 관리적보안

보안 조직 구성 및 운영, 보안정책 및 절차관리, 보안교육, 보안점검, 보안사고조사 등의 보안활동을 의미한다.

1. 전사보안책임자(CSO) (Chief Security Officer 이하 “정보보안담당임원”)
   회사의 대표로부터 정보보호에 대한 권한을 위임받아 보안정책 수립, 교육, 점검 등 보안에 관련한 모든 업무시행 및 관리감독의 주체가 되는 임원을 의미한다.
2. 정보자산
   회사가 보유하고 있는 지적 재산권과 특허, 영업 비밀 등 기술상, 경영상의 내용 그 자체와 이를 포함하고 있는 문서, 전산 시스템, 소프트웨어, 영상 매체, 시설, 기타 유/무형의 모든 자산을 의미한다.
3. 영업비밀
   공공연히 알려져 있지 않으며, 독립된 경제적 가치가 있고, 비밀로 관리된 도면, 문서, 생산방법, 판매방법, 기타 영업활동에 유용한 기술상 또는 경영상의 정보를 말하며, 회사가 사용을 위하여 타사와의 계약관계 등을 통하여 도입한 타사의 영업비밀을 포함한다.
4. 보안문서
   영업비밀 중 전산화 되어 파일로 존재하거나 출력되어 문서로 존재하는 자료로써, 외부에 유출되는 경우 회사의 경영상 기술상의 손실이 발생할 수 있는 자료를 의미한다.
5. 기밀성(Confidentiality)
   정보자산이 전송, 백업, 보관 중에 허가 받지 않은 사람에게 노출되지 않아야 하는 성질
6. 무결성(Intgerity)
   정보자산이 파손되거나 고의로 변조되지 않고 완전하게 전송되고 보관되어야 하는 성질
7. 가용성(Availaility)
   장애가 발생했을 경우에도 정보자산의 이용이 지속적으로 가능하게 하는 성질

② 물리적보안

비인가 자로부터 회사의 시설 및 인원을 보호하기 위한 출입통제, 정보자산의 반·출입 통제, 상황모니터 등의 보안활동을 의미한다.

1. 상황모니터
   사업장내 설치된 CCTV 또는 경비인력 운영을 통해 안전, 사고 및 보안현황을 실시간 확인하는 것

에 관련한 활동을 의미한다.

2. 시설
   회사의 운영에 필요한 건축물, 장비 및 설비 일체를 의미한다.
3. 무인 경비시스템
   경비인력 없이 카메라 또는 센서 등을 이용하여 방범 및 방호하는 시스템을 의미한다.

③ 기술적보안
정보시스템의 보호 및 정보시스템을 통한 유출을 예방하기 위한 운영관리, 정보시스템 접근통제, 개발 및 유지보수, 침해사고관리 등의 보안활동을 의미한다.

1. 정보시스템
   사용자에게 원활한 서비스의 제공을 목적으로 하는 하드웨어 일체와 주변장치 및 운영체제를 포함한 각종 시스템 소프트웨어 및 DBMS를 총칭한다.
2. 네트워크
   회사의 사업을 영위하기 위해 사업장간에 송수신되는 정보 혹은 관련기관 간에 주고받는 각종 정보를 전달하여 주는 각종 시스템들을 다양한 형태로 연결시켜 주는 유무선 통신망을 의미한다.
3. 백업
   예상치 못하고 바람직하지 않은 사건에 의해 발생할 수 있는 정보서비스 혹은 정보자산의 손상을 최소화하고 이를 복구하기 위해 필요한 복사본을 만드는 것을 말한다.
4. 복구
   사전에 백업 받았던 복사본을 이용하여 이전의 상태로 전환하기 위한 RECOVERY와 단순히 백업 받았던 자료를 재 설치하는 RESTORE 작업을 총칭하여 말하며, 복구를 위해서는 반드시 백업이 선행되어야 한다.
5. 단말기
   전산시스템의 입출력 장치를 말하며, LAN 혹은 WAN으로 연결된 개인용 PC 및 프린터, 콘솔, 스캐너 장비 등이 포함된다.
6. PC
   데스크탑과 노트북을 말한다.
7. 모바일 기기
   휴대폰, 스마트 폰, PDA, 태블릿 PC 등을 말한다.
8. 보안사고(침해사고)
   보호관리 대상에 속하는 정보 및 정보시스템이 무단으로 파괴되거나, 유출, 변조되어 정보보안관리체계에 문제가 발생하는 경우를 말한다.
9. 보안시스템
   사용 권한이 없는 사람이 파일이나 장치 따위에 접근하지 못하도록 막고 보호하는 시스템을 말한다.
10. 공중망 (Public Network)
    불특정 다수에게 서비스 할 수 있도록 통신업체들이 구축한 통신망으로 일반적인 사용되는 인터넷 망을 말한다.

제4조 (책임과 역할)

① 임직원 및 계약관계에 있는 모든 인원

1. 본 규정 및 관련 지침에서 정하는 보안정책을 준수해야 한다.
2. 보안교육에 참석할 의무가 있고, 자체 점검 등 회사 보안활동에 적극 협조해야 한다.
3. 영업비밀을 과도하게 취득, 보관하거나 사외로 무단 반출하는 등 보안사고의 개연성이 있는 행위를 해서는 안 된다.
4. 회사의 정보자산 반출 시 정해진 절차에 따라야 하며, 임의 판단으로 반출할 수 없다
5. 출입증 및 업무시스템 계정은 타인에게 공유하지 않는다.
6. 보안사고를 발견하였을 경우 팀(부서)별 보안책임자 또는 보안담당조직에 즉각 해당 사실을 알려야

한다.

7. 회사의 보안규정을 위반하는 경우 다음과 같은 인원에 책임이 있다.
   가. 임직원이 보안규정 위반: 위반자 및 소속 팀(부서)장
   나. 방문자가 보안규정 위반: 출입허가를 요청한 임직원

② 방문자

1. 출입증을 소속회사의 직원이나, 타인에 대여, 공유하는 행위를 해서는 안 된다.
2. 카메라 또는 카메라폰과 같은 영상 기록장치를 이용한 임의 촬영을 금지한다.
3. 당사에서 공식적으로 제공된 자료 외 어떤 자료도 취득, 사용해서는 안 된다.
4. 당사에서 요구하는 보안조치 위반 시 사규와 관련법령에 따른 모든 책임을 진다.
   가. 출입증을 대여하거나 본 목적과 다르게 사용하는 등 오남용 적발 시 해당자는 출입증 회수 및 출입금지 조치되며, 소속사 대표이사에 재발방지 대책을 제출하도록 한다.
   나. 보호구역내에서는 당사의 통제에 따라야 하며 이를 위반 시 강제 퇴실 또는 퇴장된다.
   다. 당사 자료를 무단으로 취득, 활용하거나 유출을 시도하는 경우: 관련 법령에 따른 민형사상 책임을 진다

제2장 관리적보안

제1절 보안조직

제5조 (보안조직 구성 및 관리주체)

① 전사보안조직의 구성 및 관리는 정보보안그룹에서 주관한다.
② 정보보안그룹은 보안에 대한 임직원의 역할과 책임을 정의하고 그 현황을 유지한다.
③ '제8조 보안조직 업무분장'에 따로 정하지 않은 내용은 보안협의체의 심의과정을 통하여 정의한다.

제6조 (보안협의체 운영) 보안에 대한 정책 결정, 전달 및 이행을 위해 전사보안책임자(CSO), 정보보안그룹을 구성원으로 하는 협의체를 구성하고 최소 반기 별로 운영해야 한다.

제7조 (보안조직도) 관리보안 담당자는 담당자의 팀, 성명, 연락처를 포함한 보안 조직도(첨부 참조)를 작성하여 전사보안 책임자에게 보고 후 관리한다.

제8조 (보안조직 업무분장) 책임과 역할 (제5장 첨부 보안조직도 참조)

① 전사보안책임자(CSO) (보안담당임원)

1. 대표이사 또는 대표이사의 권한을 위임받은 임원으로 한다.
2. 보안총괄책임자로서 보안에 관련한 모든 정책을 결정한다.
3. 정보보안그룹의 전사보안담당자를 선임한다.
4. 보안업무를 기획, 시행하도록 전사보안담당자에 지시하고 시행 상황을 관리감독 한다.
5. 전사보안책임자(CSO)는 정보통신망법상 CISO(Chief Information Security Officer)의 역할을 겸임할 수 있다.

② 정보보안그룹

정보보안그룹은 관리보안담당자, 물리보안담당자, 기술보안담당자로 역할을 구분하고, 규정에서 정한 보안업무를 수행한다.

1. 관리보안담당자
   가. 전사보안책임자(CSO)가 선임한 자로 회사 모든 보안업무를 전사보안책임자(CSO)에 보고 하고

시행한다.

나. 회사의 보안규정을 수립하고 교육, 공지 등을 활용하여 적용한다.

다. 보안관련 법령 및 관련사의 보안정책 변경 등 외부환경 변화에 따른 회사의 보안정책을 재 검토하고 필요 시 보안규정에 반영하거나 보안교육, 점검 등의 조치를 시행한다.

라. 보안의식 제고를 위해 매월 특정일을 '보안의 날'로 지정하여 자체점검을 시행한다.

마. 보안교육 및 홍보를 실시한다.

바. 보안사고 발생 시 외부 수사기관과 연계하여 진행한다. 사고 처리 완료 후에는 재발 방지 대책을 수립하고, 필요한 경우 인사 주관부서에 징계처리를 요청한다.

사. 정보자산의 정기적인 점검을 통해 취약성 조사 및 대응방법을 마련하여 보안사고를 사전에 예방한다.

아. 회사 정보보호실태를 분기별로 전사보안책임자(CSO)에게 보고한다.

자. 정보보호 활동 계획 및 예산에 대한 운영 및 승인을 시행한다.

차. 반기 1회 이상 정기적으로 팀 보안 담당자 회의를 개최하여 보안 정책의 하부조직 전파에 노력한다.

카. 교육계획을 수립 및 시행하고, 각종 보안 이벤트 시행, 모니터링, 정보자산에 대한 정기적인 점검 등을 통한 보안사고 예방활동을 수행한다.

타. 보안사고 발생 시 이에 대한 관리적인 조사, 조치활동을 담당한다.

2. 물리보안담당자

가. 각 팀(부서)에서 요청하는 보안구역설정을 검토, 승인하고, 그 결과를 요청부서에 회신하고 이를 현황으로 관리해야 한다.

나. 물리보안시스템을 운영하며 관련된 절차를 수립하고, 그 절차에 따라 운영현황을 관리하며 필요 시 전사보안책임자에 보고, 조치한다.

3. 기술보안담당자

가. 정보기술 관련한 전 부문의 보안업무를 총괄하여 수립 및 시행한다.

나. 정보기술 보안운영계획을 수립하고 시행한다.

다. 정보기술 보안에 관련한 별도의 세부 지침을 마련하여 시행한다.

라. 정보기술 보안시스템의 관리 및 성과분석을 실시한다.

마. 전산자산의 안정적 운영 및 보안대책을 마련하고 실시한다.

바. 정보기술(IT) 업무를 수행하는 자로 전사보안책임자(CSO)가 지명한 직원으로 한다.

사. '제4장 기술적 보안'에 규정된 내용을 계획하고 시행한다.

아. 전산자산의 취약점이 발견되면 전산담당자에게 개선을 요청해야 하며, 패치를 실시한다.

자. 내·외부 전산장비에 대한 보안점검을 실시한다.

차. 보안규정 상의 보안업무 수행사항을 적용 및 실행한다.

카. 보안사고 발생 시 기술적인 조사, 조치 등을 지원한다.

타. 위 각 호에 대한 결과를 전사보안책임자(CSO)에게 보고한다.

③ 팀(부서)별 보안책임자

각 팀의 팀(부서)장으로 해당 팀(부서)내 보안업무를 수행, 조정, 감독한다.

1. 팀(부서)내 각종 기업비밀의 보안성 검토 및 보안문서 여부를 결정한다.

2. 팀(부서)내 자체 보안점검이 정상적으로 이행되고 있는지 확인하고 감독한다.

3. 팀(부서)내 시건 장치 등이 적절히 사용, 관리되고 있는지 확인하고 감독한다.

4. 팀(부서)원 보안교육 실시를 주관한다.

5. 팀(부서)보안담당자를 임명한다.

6. 팀(부서)내 보안사고 발생시 또는 발생할 우려가 있는 경우 전사보안담당자에게 통보한다.

7. 팀(부서)의 업무와 관련 있는 장소가 보안상 출입을 제한할 필요가 있는 경우 물리보안담당자에 보호구역 설정을 요청한다.

8. 회사의 보안정책이 효과적으로 이행될 수 있도록 적극 지원한다.

④ 팀(부서)별 보안담당자

1. 팀(부서)별 보안책임자가 임명한 자로 팀(부서)보안책임자의 권한을 대행하여 팀(부서)내 보안현황을 관리하고, 보안점검, 보안교육 등 팀(부서)과 관련한 보안활동을 수행한다.
2. 매월 보안의 날 시행 후 팀(부서)내 보안현황, 문제점 등을 팀(부서)보안책임자에 보고하고, 지시에 따라 개선을 이행한다.
3. 정보보안그룹이 소집하는 팀보안담당자 회의에 참석하여, 팀(부서) 입장을 대변하여 보안정책 결정에 참여하며, 정해진 보안정책을 팀 내 전파하는 역할을 수행한다.

제2절 보안정책 운영

제9조 (운영 목적)

① 보안정책 운영 목적은 당사 업무의 연속성을 보장하고, 모든 보안 사고를 사전에 방지하여 당사 업무 및 정보자산의 피해를 최소화하는데 있다.
② 보안정책은 문서화되어야 하며 제·개정 시에는 전사보안책임자(CSO)의 승인을 득해야 한다.
③ 보안정책은 사내한 사항임으로 임직원은 허가 없이 외부에 유출해서는 안 된다.

제10조 (보안정책 준수)

① 회사의 임직원은 본 규정을 비롯한 제반 보안정책을 준수하여야 하며, 위반 시 회사 규정 및 관계법령에 의거 조치한다.
② 회사 내 제3자는 당사의 보안정책을 준수하여야 하며 위반 시 계약 및 관계법령에 따라 처리한다.

제11조 (제·개정 절차)

① 보안정책의 제·개정 및 폐지는 정보보안그룹이 관련부서 간 협의를 거쳐 전사보안책임자(CSO)가 승인한다. 경미한 사항은 정보보안그룹 책임 하에 시행할 수 있다.
② 직원 신상에 중대한 영향을 미치는 사항 등에 대해서는 사규총괄부서와 사전 협의토록 한다.
③ 단, 세부 업무절차의 제·개정은 관련 부서장이 자율 운영하되, 보안규정 및 지침의 개정이 필요할 경우 정보보안그룹과 협의하여 제·개정을 진행하여야 한다.

제12조 (보안정책 해석)

① 이 규정과 관련 지침 및 업무절차 간에 효력 또는 해석에 대하여 이의가 생길 때에는 1차적으로 정보보안그룹의 해석을 따른다.
② 조문의 해석이 책임한계의 구분 또는 중대한 사실에 영향을 미칠 때에는 사규총괄부서의 유권해석을 따른다.

제13조 (유지관리) 보안정책 유지관리를 위한 정보보안그룹의 책임은 다음과 같다.

① 보안정책은 최소 1년 주기로 개정 필요성에 대한 검토가 있어야 하며, 변경이 필요한 경우에는 즉시 보완하여야 한다.
② 개정된 보안정책은 임직원 및 관련자가 인지할 수 있도록 즉시 공지한다.
③ 주기적으로 보안점검을 실시하여 보안정책의 효과성을 재평가해야 한다.

제3절 보안서약서

제14조 (관리주체)

① 영업비밀의 법적인 보호와 임직원의 보안인식제고를 위해 정보보호서약서를 작성하여 제출토록 한다.

② 관리보안담당자는 징구 대상과 서약서 징구 현황을 표로 관리해야 하며, 누락이 있는지 정기적으로 점검하고 누락이 확인되는 경우 원인을 파악 후 전사보안책임자(CSO)에 보고, 조치한다.
③ 임직원, 제3자 구분 없이 정보보호 서약서를 제출한 인원만 당사 사업장 출입 및 정보자산을 사용할 수 있다.
④ 서약서를 제출하지 않은 인원에는 사업장 출입권한 및 시스템 사용권한을 부여해서는 안되며, 이에 대한 관리 책임은 관리보안담당자에 있다.

제15조 (임직원)
① 임직원은 입사시 정보보안에 대한 중요성을 숙지하여 '정보보호 서약서'를 작성 후 채용담당자에게 제출(징구)해야 한다. '정보보호 서약서'는 관련 법령 및 정보의 기밀사항에 관하여 지켜야 할 사항을 명시해야 한다.
② 관리보안담당자는 재직 중인 임직원을 대상으로 2 년간 1 회이상 정기적으로 '정보보호 서약서'를 징구해야 한다.
③ 임직원은 퇴사시 본인이 보호해야 할 영업비밀의 내용과 보호기간, 부정경쟁방지 등에 관한 법령 준수 및 법적 책임 등이 포함된 '퇴직자 보안 준수 서약서'를 작성 제출(징구)해야 한다.
④ 임직원은 보직변경 시 '정보보호 서약서'를 제출(징구)해야한다.

제16조 (제3자(일반용역, 외주(아웃소싱)인원)))
① 일반용역을 포함한 외주인원은 계약 시 '회사정보 보호 서약서'를 작성하여 해당 팀 보안담당자에게 '회사정보 보호 서약서'를 제출하여야 한다.
② 계약서는 회사에서 정한 표준계약서를 사용해야 하며, 표준계약서에는 회사의 보안규정을 준수할 것과 외주인원 및 외주인원의 소속 사에 보안책임이 있음을 공지하는 내용이 포함되어야 한다.
③ 기술용역 또는 기술자료 교환이 있는 계약의 경우 회사의 정보자산보호/관리를 위해 당사의 보안점검에 외주인원 소속사도 포함이 되어 있음을 고지하는 문구를 포함한 계약서를 사용해야 한다.

제 4 절 보안교육

제17조 (보안교육계획 수립)
① 정보보안그룹은 전사 연간 보안교육계획을 최소 차기 회계연도 시작 1개월 전에 수립한다
② 전년도 보안이슈 사항을 반영하여 당해년도 보안교육 계획을 수립한다.

제18조 (보안교육 실시)
① 정보보안그룹은 다음 각호에 해당하는 보안교육을 실시하여야 한다.
1. 채용시 보안교육(신입, 경력)
2. 개인정보 보호교육
3. 전사 보안교육
4. 팀보안담당자교육
5. 개인정보취급자 보안교육
6. 협력사 보안교육

제19조 (임시직, 파견자 및 제3자 아웃소싱에 대한 교육)
① 임시직이나 파견자에게 당사 보안규정 및 업무에 따른 보안 필요사항을 주지시키고, 장기 근무 시는 당사 임직원에 준해 동일한 교육을 받게 한다.
② 제3자의 경우에는 업무를 개시하기 전에 당사의 보안 규정에 관하여 숙지할 수 있도록 교육을 실시한다.
③ 비밀유지 의무 준수 및 위반 시 처벌 내용 등에 대한 교육을 실시한다.

제20조 (교육 사후관리)

정보보안그룹은 임직원들의 보안준수 현황을 점검하고, 점검결과에 따른 우수, 열위직원에 대해 인사평가, 승진, 보직 등 인사에 연계되도록 협의하여야 한다.

제21조 (보안담당자 양성)

정보보안그룹에서는 부서(팀) 보안담당자에 대한 교육, 양성계획을 수립, 운영하여야 한다.

제5절 퇴직자 관리

제22조 (퇴직자 처리 절차)

① 퇴직자 처리 절차는 퇴직 예정자의 정보자산, 접근권한 및 영업비밀 보호를 위하여 사전 확인, 퇴직 면담, 권한 회수 및 보안조치 절차를 포함하여 수행한다.

② 인사담당부서는 퇴직 예정자 발생 시 관련 부서 및 정보보안 담당부서에 퇴직 예정 사실을 공유하여야 한다.

③ 팀(부서)보안책임자는 퇴직 예정자에 대하여 업무 인수인계, 정보자산 반납 및 영업비밀 보호 의무를 안내하고 관련 사항을 확인하여야 한다.

④ 퇴직 예정자는 재직 중 취득한 영업비밀, 개인정보 및 내부정보를 외부에 유출하거나 무단 사용하여서는 아니 되며, 회사의 정보보호 정책을 준수하여야 한다.

⑤ 퇴직 예정자는 퇴직 처리 전 다음 각 호의 문서를 제출하여야 한다.

1. 퇴직자 보안 준수 서약서
2. 퇴직 프로세스 확인서
3. 기타 회사가 필요하다고 판단하는 보안 관련 서류

⑥ 팀(부서)보안책임자 및 인사담당부서는 퇴직 예정자와의 면담을 통해 다음 사항을 확인하여야 한다.

1. 영업비밀 및 중요정보 보호 의무 안내
2. 회사 자산 및 저장매체 반납 여부
3. 업무자료 및 중요정보 인계 여부
4. 개인 보관 자료 삭제 또는 파기 여부
5. 경쟁업체 이직 여부 및 보안 유의사항 안내

⑦ 기술보안담당자 및 물리보안담당자는 퇴직 발령 후 관련 절차에 따라 시스템 접근권한 및 출입권한을 회수하여야 한다.

⑧ 퇴직자의 계정, 시스템 사용기록 및 접근권한 회수 여부 등 보안로그는 정기적으로 점검하여야 하며, 미회수 또는 이상사항 발견 시 즉시 조치 후 전사보안책임자(CSO)에 보고하여야 한다.

⑨ 퇴직 처리 완료 후 관련 서류 및 점검 이력은 회사 정책에 따라 보관 및 관리한다.

제23조 (인사담당부서)

① 퇴직자에 대해 '퇴직자 보안 준수 서약서'를 퇴직서류에 포함하여 징구해야 한다.

② 퇴직자 영업비밀유지서약서를 제출하지 않는 인원에는 해당양식을 송부하여 제출을 독려해야 하며, 미제출시 정상적 퇴직절차가 지연될 수 있음을 공지한다.

③ 인사담당부서는 퇴직 후 동종업계로 전직한 사실을 인지한 경우 당사에서 취득한 영업비밀이 제공되었는지를 확인하고 전직금지 가처분 신청 등 관련 법적 조치를 취한다.

제24조 (팀(부서)보안책임자)

① 팀 내 퇴직이 예정되거나, 퇴직명령이 발령된 직원에 대해 재직기간 동안 습득한 모든 영업비밀은 경우를 막론하고 대외로 유출하여서는 안되며 이를 위반할 시 '퇴직자 보안 준수 서약서'에 의거하여 민형사상의 책임을 질 수 있음을 공지할 의무가 있다.

② 퇴직(예정)자가 근무기간 동안 습득한 모든 영업비밀을 소속 팀(부서)에 인계 하도록 하고, 개인이 소지한 영업비밀은 회사에 반납 또는 재사용 불가한 상태로 파기하도록 요청하고 퇴직자 면담서류 등에 이에 대한 사항을 기록한다.

제25조 (임직원)

임직원은 퇴직자가 동종업종 또는 경쟁사에 재취업하는 것을 인지하였을 경우 즉각 전사 보안담담부서에 통보해야 한다.

제26조 (기술보안담당자 및 물리보안담당자)

① 퇴직 명령 일을 기준으로 24시간 이내에 퇴직자에 대한 출입 및 시스템상의 모든 접근 권한을 절차에 따라 모두 삭제 한다.

② 정기적으로 퇴직자의 권한이 정상적으로 회수되고 있는지 현황을 확인하고 누락이 확인되면 그 원인을 확인하고 개선조치를 이행한다.

③ 업무인수/인계를 목적으로 팀(부서)보안담당자가 서면으로 요청하는 경우 최대 2주 기간 동안 권한 삭제를 유예할 수 있다. 권한 회수 유예로 문제가 발생하는 경우 팀(부서)보안담당자에도 책임이 있다.

④ 퇴직자에 의한 중요정보 유출 방지를 위하여 적절한 보안성검토 및 교육을 실시하여야 한다.

⑤ 퇴직발령 게시 지연 등의 사유로 권한회수가 정상적으로 처리되지 않은 경우, 그 차이 기간 동안 출입/시스템 사용기록을 모두 확인하고, 팀(부서)보안담당자에 확인을 요청하고 그 결과를 포함하여 전사보안책임자(CSO)에 보고 한다

제6절 보안 위반자 관리

제27조 (보안위반 조치)

① 위반사항의 경중을 판단하여, 경미한 위반의 경우 전사보안담당자 명의의 주의조치를 해당 직원 및 소속 팀(부서)장에 통보하며, 중요한 위반이라고 판단되는 경우 전사보안책임자(CSO)보고 후 규정에 따라 조치한다.

② 보안 위반에 대한 징계는 취업규칙과 인사규정 또는 보안규정에 정한 징계 종류 및 절차에 따른다.

③ 유사사고 재발방지를 위해 대책을 수립/시행하고 이력을 관리한다, 징계 결과는 임직원 전원에게 공지한다

제28조 (임직원)

① '정보보안 규정' 및 관련 지침/절차를 위반한 사실을 인지하는 경우 정보보안그룹에 즉시 위반 사실을 통보해야 한다.

② 본인의 실수 또는 의도하지 않게 정보가 노출, 제공되었음을 확인하는 경우 전사 정보보안그룹에 관련사실을 통보해야 한다.

제29조 (위반자 경중 판단 기준)

① 경미한 위반

1. 위반 내용이 실수 또는 과실에 의한 단순한 규칙/지침 위반이라고 인정되는 경우
2. 위반이력이 없는 임직원이 규정, 절차 등의 미 인지로 규칙/지침을 위반한 경우 중 중대한 위반의 사유가 되지 않는 경우
3. 본인의 위반사실을 통보해온 경우 중 중대한 위반에 사유가 되지 않는 경우
4. 위반회수에 따라 다음과 같이 조치를 상향 한다

가. 1 회 위반: 당사자 구두 경고
나. 2 회 위반: 당사자 서면 경고(시말서) 및 팀(부서)장 구두경고
다. 3 회 위반: 당사자 및 팀(부서)장 서면 경고(시말서)

라. 4 회 이상: 고의적 정책 미 준수로 중대한 위반으로 상향

② 중대한 위반
1. 고의로 보안 규정, 절차, 지침을 우회하는 행위를 한 경우
2. 보안사고와 직, 간접적으로 관련된 사안으로 인정되는 경우
3. 중대한 과실이거나, 동일한 위반을 반복적으로 지적 받는 경우
4. 인사징계위원회에 회부하여 경고 이상의 징계 조치를 시행한다.

제30조 (보안위반의 신고 및 통보)
① 임직원은 '정보보안 규정' 및 관련 지침/절차를 위반한 사실을 인지하였거나, 본인의 실수 또는 의도치 않게 정보가 유출/제공되었음을 확인한 경우 즉시 전사 보안주관부서(정보보안그룹)에 해당 사실을 통보해야 한다.
② 전사 보안주관부서는 접수된 위반 사항의 경중을 판단하여 조치를 시행한다.

제31조 (위반 사항의 경중 판단 기준)
① 경미한 위반: 다음 각 호에 해당하는 경우로, 단순 과실 및 규정 미인지에 의한 사안을 포함한다.
1. 실수 또는 과실에 의한 단순 규칙/지침 위반
2. 위반 이력이 없는 임직원이 절차를 인지하지 못해 발생한 사안 중 중대한 피해가 없는 경우
3. 위반자가 본인의 위반 사실을 자진 신고한 경우
4. 위반 횟수에 따른 단계적 조치(구두 경고 → 서면 경고 → 시말서 제출 등) 대상인 경우

② 중대한 위반: 다음 각 호에 해당하는 경우로, 고의성이 있거나 보안 사고로 직결되는 사안을 말한다.
1. 고의적인 보안 정책 미준수 및 반복적인 위반(4 회 이상)으로 인해 통제가 불가능하다고 판단되는 경우
2. 보안 사고로 인해 회사에 막대한 손실을 초래하거나 외부 정보 유출이 발생한 경우
3. 보안 사고를 은폐하거나 조사를 방해한 경우

제32조 (보안위반 조치 및 징계)
① 경미한 위반 시 조치: 위반 횟수 및 사유에 따라 다음과 같이 조치하며, 전사보안담당자 명의로 해당 직원 및 소속 팀(부서)장에게 통보한다.
1. 1 회 위반: 당사자 구두 경고
2. 2 회 위반: 당사자 서면 경고 및 팀(부서)장 구두 경고
3. 3 회 위반: 당사자 및 팀(부서)장 서면 경고(시말서 징구)
② 중대한 위반 시 조치: 전사보안책임자(CSO)에게 즉시 보고하며, 사내 인사규정 및 보안규정에 따라 징계위원회에 회부하여 엄중히 조치한다.
③ 재발 방지 대책: 위반 사항 발생 시 즉시 대책을 수립/시행하고 관리 대장을 통해 이력을 관리한다. 징계 확정 시 보안 의식 고취를 위해 보안 사고의 유형과 징계 결과(개인정보 제외)를 사내에 공지할 수 있다.
④

제7절 정보자산 분류

제33조 (분류 주체 및 주기)
① 팀(부서) 보안책임자는 회사의 정보자산 분류 기준을 숙지하여야 하며, 정보 생성자(문서 작성자)가 최초 분류를 적정하게 수행하도록 공지 · 지도 · 점검하여야 한다.
② 임직원은 문서를 생성하는 경우 분류 기준에 따라 보안등급을 지정하여야 하며, 문서는 항상 분류된 상

태로 관리하여 회사 보안정책이 준수되도록 하여야 한다.

③ 팀(부서) 보안담당자는 다음 각 호에 따라 분류의 적정성을 검토 · 조정하여야 한다.

1. 업무 변동사항 발생 시: 2주 이내
2. 특별한 변동사항이 없는 경우: 연 1회 정기 점검

④ 등급이 분류된 정보자산은 식별이 가능하도록 자산관리번호, 관리자, 보관위치 등을 확인할 수 있는 관리 인덱스를 부착 · 등록하여야 한다.

제34조 (정보자산의 보안등급 구분 기준)

① 정보자산의 중요성 등급은 기밀성, 무결성, 가용성 측면에서 각 자산이 보안 위협에 노출되었을 경우 회사에 미치는 현재적 손실 규모를 반영하여 측정한다.

② 회사 내 정보자산에 대한 중요도는 주요 정보에 대해 기밀성, 무결성, 가용성 등의 보안요구사항을 고려하여 중요도 등급을 부여함으로써 이루어진다.

③ 정보자산의 보안등급은 비밀 (SECRET), 대외비 (CONFIDENTIAL), 사내한 (RESTRICTED)으로 구분한다.

④ 비밀 · 대외비 · 사내한 등급은 당사의 영업비밀 또는 보호대상 정보에 해당하며, 「영업비밀 관리기준」 및 관련 규정을 준수하여야 한다.

⑤ 사내한 (RESTRICTED) 등급은 사내 모든 임직원이 자유롭게 공유하고 열람할 수 있으나, 외부에 유출될 경우 회사의 이미지 저하나 사기 저하 등 부정적인 영향을 초래할 우려가 있는 정보를 말한다.

⑥ 대외비 (CONFIDENTIAL) 등급은 제한된 부서/인원만 열람할 수 있고, 외부에 노출될 경우 업무 추진에 차질이 생기거나 회사에 직간접적인 손해를 끼칠 우려가 있는 정보를 말한다.

⑦ 비밀 등급은 업무상 직접 관련이 있는 임직원에 한하여 제한적으로 열람을 허용하며, 외부 노출 시 상당한 재무적 손실, 사업계획 변경 · 폐기, 영업손실 등을 초래할 우려가 있는 정보를 말한다.

⑧ 임직원(계약관계에 있는 자 포함)에 의해 작성된 모든 문서는 최초 분류 전까지 '대외비'로 간주한다.

⑨ 추가적인 보안등급 지정이 필요한 경우, 전사보안책임자(CSO)의 승인을 받아 '극비 (Top Secret)' 등급을 지정할 수 있다.

⑩ 외부 반입 문서에 대한 등급 분류 기준은 별도로 수립하여 전사보안책임자(CSO)의 승인을 받은 후 운영하여야 한다.

제35조 (보안등급 표시 기준)

① 전자문서 및 출력문서는 다음 기준에 따라 등급을 명확히 표시하여야 한다.

② 전자문서의 경우

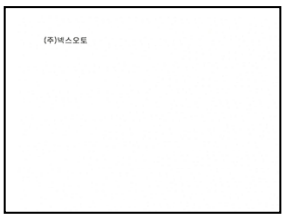
1. 우측 상단에 '비밀, '대외비', '사내한'을 적색 사각형 안에 표시한다.
2. 파일명에 등급을 포함할 수 있다.

③ 출력문서의 경우

1. 우측 상단에 '비밀, '대외비', '사내한'을 적색 사각형 안에 표시한다.
2. 좌측 상단에는 회사 자산임을 표시한다.
3. 우측 하단에는 문서에 대한 경고문구를 표시한다.

④ 등급 표시 예시는 별첨 서식에 따른다.

정보자산 종류	전자문서	출력문서

등급 표시 예시	우측 상단에 적색 사각형 안에 표시 	좌측 상단에 넥스오토 자산임을 표시 우측 하단에 경고문구 표시 

제36조 (정보자산 가치평가)

① 정보자산의 가치는 기밀성, 무결성, 가용성 기준에 따라 평가하며, 3단계 등급으로 구분한다.

② 중요도 평가 등급은 다음과 같다.

1. H(High): 중요도 점수 8~9점 (비밀 수준)
2. M(Medium): 중요도 점수 5~7점 (대외비 수준)
3. L(Low): 중요도 점수 1~4점 (일반 수준)

③ 평가는 매년 상반기에 실시하며 다음과 같이 구분한다.

1. 최초평가: 자산 최초 등록 시
2. 신규평가: 신규 자산 발생 시
3. 정기평가: 연 1회 전체 자산 평가
4. 수시평가: 평가 기준 변경 또는 자산 중요도 변경 시

제37조 (정보자산의 보관 및 관리)

① 정보보안그룹은 팀(부서) 단위에서 작성할 수 있는 정보자산분류기준(템플릿)을 제공해야한다.

② 임직원은 보안문서 등급 분류 시 소속 부서 업무 단위로 등급을 부여하며, 이에 따른 관리 대장을 작성하여 운영해야 한다.

③ 정보자산 목록의 작성 단위, 책임자, 갱신 방법 및 보고 체계는 다음과 같다.

④ 작성 단위

1. 부서 정보자산목록: 팀(부서) 단위
2. 전사 정보자산목록: 부서 정보자산목록을 종합

⑤ 작성 책임자

1. 부서 정보자산목록: 팀(부서)보안책임자(정), 보안담당자(부)
2. 전사 정보자산목록: 정보보안그룹

⑥ 갱신 방법

자산별 소유관계 및 보안등급을 명확히 정의하고 지속적으로 보완

⑦ 갱신 주기

1. 부서 목록: 분기 1회 (변경 발생 시 수시)
2. 전사 목록: 연 1회

⑧ 보고 의무

1. 팀(부서)보안책임자는 정보자산 변경 발생 시 즉시 정보보안그룹에 통보
2. 정보보안그룹은 전사 정보자산관리 현황을 연 1회 전사보안책임자(CSO) 및 최고경영층에 보고

제38조 (정보자산 보호대책)

① 방화벽, 침입탐지시스템, 접근통제장치, 시건장치 등을 활용하여 정보자산을 보호한다.
② 정보자산은 보안등급에 따른 취급 절차를 준수하여야 한다.
③ 사내한 이상 정보자산은 외부인의 접근을 제한하여야 한다.

제39조 (정보자산의 배포 및 파기)
① 중요 정보자산을 배포할 경우 보안솔루션을 활용하고 해당 부서장의 승인을 받아야 한다.
② 중요 정보자산을 외부 반출하는 경우 사전 승인을 받아야 한다.
③ 중요 정보자산을 폐기할 때에는 복구가 불가능하도록 완전 파기 또는 영구 삭제하여야 한다.
④ 정보자산 재사용 및 폐기 과정에서 개인정보 및 중요정보가 복구되지 않도록 안전한 절차를 수립·이행하여야 한다.
⑤ 저장 기능이 있는 자산이 고장·훼손·오삭제된 경우 원칙적으로 불용 처리하며, 복구가 필요한 경우 승인 후 외부 전문업체에 의뢰할 수 있다.

제40조 (정보자산 실사)
① 정보보안그룹은 팀(부서) 보안담당자의 협조를 받아 연 1회 전사 정보자산 실사를 실시하고, 그 결과를 전사보안책임자(CSO)에 보고하여야 한다.

제41조 (기타 세부사항) '정보자산 위험관리 절차 지침'을 따른다.

제8절 정보자산 위험관리

제42조 (목적) 넥스오토 내 정보보호 위험요소를 체계적으로 식별, 평가, 대응 및 모니터링함으로써 정보자산의 기밀성, 무결성, 가용성을 유지하고 보안 사고 발생 가능성을 최소화하는 데 그 목적이 있다.
제43조 (관리항목)
① 서버, 네트워크 장비, 소프트웨어, 문서 등 전사 정보자산을 식별하고, 조직의 기준에 따라 유형별로 분류하여 자산 목록을 현행화하여야 한다.
② 식별된 자산에 대하여 기밀성(C), 무결성(I), 가용성(A)을 기준으로 자산의 가치와 중요도를 평가하고 등급을 부여해야 한다.
③ 자산별 위협과 취약점을 식별하고, 발생 가능성과 영향도를 분석하여 위험 등급을 산정하여야 한다.
④ 평가된 위험 수준이 수용 가능한 수준을 초과하는 경우, 위험 회피, 완화, 전가, 수용 중 적절한 대응 전략을 수립하여 조치하여야 한다.
⑤ 수립된 위험 처리 대책의 이행 여부를 점검하고, 잔류 위험에 대해 정기적인 재평가와 모니터링을 실시해야 한다.
⑥ 정보보안그룹은 위험 평가를 주관하고, CSO는 최종 위험 수준 판단 및 대응 전략을 승인하며, 각 부서는 자산 정보 제공 및 위험 처리 이행에 협조해야 한다.
⑦ 연 1회 이상 또는 중대한 환경 변화 발생 시 위험 평가를 갱신하고, 모든 과정은 문서화하여 기록 관리하여야 한다.

제44조 (기타 세부사항) '위험관리방법론 및 절차지침'과 '정보자산 위험관리 절차 지침'을 따른다.

제9절 영업비밀 관리기준

제45조 (영업비밀의 분류)
① 당사 영업비밀
1. 영업비밀은 최초 문서의 작성(기안)자가 분류한다.

2. 문서등급의 조정권한은 팀(부서)장 또는 상위 결재자에게 있으며, 문서의 유통범위에 대한 관리감독 책임을 가진다.
3. 문서의 내용이 보안문서와 일반문서가 혼합되어 있는 경우 상위등급의 내용으로 문서의 등급을 지정하여야 한다.
4. 영업비밀의 분류 시 분류기준 및 참고항목을 고려하여 등급을 결정해야 한다. 분류기준에 해당사항이 없는 경우라도 보안문서로 지정하여 관리할 수 있다.

② 타사 영업비밀

1. 제3자로부터 계약관계에 의해 타사의 영업비밀을 취득 시에는 제공자가 정당한 권한을 가진 자인가를 확인하여야 한다.
2. 타 회사에 근무경력이 있는 임직원은 이전 회사의 보안의무를 지고 있으므로 이전 회사의 영업비밀을 회사 내에서 공개, 사용하지 않아야 한다.
3. 업무적으로 제공받은 타사의 영업비밀은 제공자가 결정한 등급으로 분류한다.
4. 해당 등급이 없는 경우 차 상위등급으로 분류한다.

제46조 (영업비밀의 보관 및 관리)

① 영업비밀은 생성시 원본 문서에 해당 등급을 표기해야 하며, 생성과정에 있는 중간산출물 및 해당내용의 일부를 사용한 문서도 동일한 방법으로 관리되어야 한다. 기 생성된 문서 중 보안등급이 구분되지 않는 문서의 경우 소급하여 등급 분류를 시행한다.

② 출력된 영업비밀에는 그 등급이 매 페이지마다 쉽게 식별 가능하도록 표기되어야 하며, 출력 시 표기하지 못한 문서의 경우 출력 후 고무인 등을 활용하여 표기한다.

③ 출력된 영업비밀은 개방된 장소에 보관해서는 안되며, 시건 장치가 있는 장소에 보관하고 팀(부서) 보안책임자가 지정하는 자가 관리한다.

④ 출력된 영업비밀은 보존기간이 만료되면 1 개월 이내에 복원할 수 없는 형태로 파기한다. 단, 업무적 이유로 파기를 유예할 필요가 있는 경우 목적과 유예기간 등을 서면으로 보안 주관부서에 보고 후 보관한다.

⑤ 전자상의 보안문서는 출력 시 문서열람 프로그램 또는 기타 시스템을 통해 워터마크 또는 회사 자산임을 증빙하는 문구를 포함하여 자동 출력되도록 해야 한다. 또한 파일 암호화, 보안이 적용된 저장공간 사용 등 회사에서 제공한 문서보안시스템을 적용하여 안전하게 보관해야 한다.

⑥ 보안문서는 업무목적 외에는 복사, 인용, 가공 등의 재생산을 해서는 안 된다. 보안문서의 재생산 시에는 당사 보안정책을 준수해야 하며, 전달받은 문서의 경우 전달자가 요구하는 보안사항을 이행해야 한다.

⑦ 영업비밀이 휴지통, 공용 회의실 등 직원이 통제할 수 없는 장소에 방치된 경우 문서의 출력자, 해당 팀장을 보안규정위반으로 조치 한다.

제47조 (영업비밀의 이관)

① 보직 변동으로 해당 영업비밀을 소유할 필요가 없는 경우 전보자는 '업무인수인계서'에 취급 영업비밀의 인수인계 내용을 작성하고, 전자문서 및 출력문서 등 모든 종류의 영업비밀을 인수자에 인계한다.

② 팀(부서)별 보안책임자는 인계/인수 절차에 따라 영업비밀이 적절히 이관되었는지 확인하고 인계자 소유하고 있는 영업비밀이 모두 파기되었는지 확인한다.

③ 업무상 이유로 기존 영업비밀의 일부를 전보된 부서에서 사용할 필요가 있는 경우 그 목적과 파일의 목록을 이전 팀(부서)보안책임자에 서면으로 보고 후 활용할 수 있다. 서면보고 과정 없이 보유하는 경우 이유를 막론하고 고의적인 정보취득으로 보안위반자 처리규정에 따라 조치한다.

제48조 (영업비밀의 배포 및 반출)

① 영업비밀을 본인의 업무와 직접적으로 관련이 없는 곳으로 반출할 사유가 발생하거나 국가기관 등 외부에서 요청한 자료의 범위에 영업비밀이 포함되는 경우 전사보안담당자의 사전 승인을 얻어 반출한다.
② 본인의 업무 수행을 위해, 사외 반출하는 경우 반출처와 반출일시, 반출 내역을 회사가 정한 양식에 따라 작성하여, 주간 단위로 팀(부서)보안책임자에 보고하고, 결재를 받아 보관한다. 단, 기술자료(도면)를 배포/접수할 수 있는 시스템이 구축된 경우 별도의 기록을 작성하지 않고 시스템 로그로 대체한다.
③ 영업비밀의 반출 이력은 2 년 이상 보관되어야 하며, 필요 시 쉽게 조회 가능한 상태로 관리되어야 한다. 사내 배포의 경우 영업비밀의 소유권자(작성자)의 판단에 따라 회사가 정하는 보호조치가 적용된 상태로 필요한 인원에 한정하여 배포한다.
④ 본인이 작성한 영업비밀이 아닌 경우 배포, 반출할 수 없으며, 작성자의 승인을 얻거나 작성자에 반출, 재 배포를 요청해야 한다.

제49조 영업비밀의 파기
① 전자문서 형태의 영업비밀은 회사가 정하는 소프트웨어를 활용하여 복원 불가한 상태로 파기해야 하며, 사본도 같은 방법으로 파기한다.
② 전자문서 이외의 영업비밀은 문서세단기를 사용하여 원형을 확인할 수 없는 상태로 파기해야 한다. 임직원이 사용할 수 있는 문서세단기가 설치되지 않은 경우 전사보안책임자는 별도의 파기절차를 수립하여 운영해야 한다.
③ 전자문서 파기용 소프트웨어를 지정, 공지하지 않은 경우 파기에 대한 책임은 전사보안책임자(CSO)에 있다.
④ 문서의 파기는 해당문서의 생산자 및 사용자에 의해 임의로 실시해서는 안 되며, 반드시 소속 팀(부서)별 보안책임자의 책임하에 이루어져야 한다.

제10절 준거성

제50조 전사보안담당자는 보안관련법령이 개정되거나, 고객사의 보안정책이 변경되는 경우 내부규정, 절차, 지침에 영향이 있는지 전사보안담당자를 통해 검토해야 하고 필요 시 개정해야 한다.

제51조 검토 결과, 개정이 불필요하다고 판단되는 경우에는 검토 이력을 문서로 유지해야 한다.

제52조 전사보안책임자(CSO)는 법령개정 및 고객사 정책변경 등 변경사항을 내부규정 변경사항과 함께 전 임직원이 인지할 수 있도록 공문 또는 게시판을 통하여 공지해야 하며, 필요 시 별도 교육을 실시해야 한다.

제53조 기술보안담당자는 시스템의 취약점을 주기적으로 점검하여, 내부 규정 또는 외부 법령에 위반사항이 없도록 확인하고 개선이 필요한 경우 전사보안담당자, 전사보안책임자(CSO)에 보고하고 조치 한다.

제11절 보안점검 및 관리

제54조 (목적)
회사에서 정한 보안통제가 적절히 이행되고 있는지 확인함으로써, 잠재적인 정보보안 침해의 가능성과 그로 인한 피해를 최소화하는데 그 목적이 있다.

제55조 (시행 주체 및 주기)

① 전사보안책임자의 주관 하에 사전 계획에 따라 시행하며 점검을 시행할 인원은 전사보안담당자가 지명하고 전사보안책임자(CSO)가 승인한 임직원으로 한다.
② 점검은 분기별 1 회로 시행한다.
③ 단, 솔루션을 이용하여 점검 가능하며 해당 솔루션으로 점검 진행 시 정기 점검으로 갈음한다.
④ 솔루션을 활용한 평가 진행시 예약검사를 이용하여 업무중 휴게시간, 점심시간 등으로 셋팅하여 진행한다.
⑤ 보안점검은 임직원의 일상적인 준수사항 위주로 시행한다.
⑥ 다음의 경우 상기 일정과 별도로 점검을 실시할 수 있다.
가. 전사보안책임자(CSO)가 필요하다고 인정할 때
나. 보안사고의 발생 우려가 있을 때 또는 보안사고 발생시

제56조 (점검 대상)
본 규정 제 2 조 적용범위에서 정한 범위를 대상으로 한다.

제57조 (점검 절차)
① 전사보안담당자는 점검 시행 전 점검 목적, 대상, 일정 및 주요 점검항목 등을 포함한 점검계획을 수립하고 대상 팀(부서)에 사전 공지하여야 한다.
② 대상 팀(부서)은 전사보안담당자의 요청에 따라 점검에 필요한 자료 및 증적을 제출하여야 하며, 필요 시 인터뷰 및 현장 확인에 협조하여야 한다.
③ 전사보안담당자는 현장점검, 문서점검, 시스템 확인 등의 방법으로 보안점검을 수행하며, 운영 절차 준수 여부 및 보안통제 이행 상태를 확인할 수 있다.
④ 전사보안담당자는 점검 결과를 기록하고 확인된 취약점 및 미흡사항에 대하여 중요도 및 영향도를 검토하여야 한다. 필요 시 동일 또는 유사 취약점의 재발 여부를 확인할 수 있다.
⑤ 전사보안담당자는 점검 결과 확인된 미흡사항에 대하여 관련 팀(부서)에 개선을 요청할 수 있으며, 해당 팀(부서)은 개선계획 및 조치일정을 수립하여 회신하여야 한다.
⑥ 전사보안담당자는 개선조치 완료 여부를 확인하기 위하여 증적자료 제출 또는 재점검을 요청할 수 있으며, 미조치 또는 조치가 미흡한 사항에 대해서는 추가 개선을 요구할 수 있다.
⑦ 전사보안담당자는 점검 결과, 주요 취약점, 개선 현황 및 미조치 사항 등을 포함한 종합 결과를 전사보안책임자(CSO)에 보고하여야 한다.

제58조 (점검 시행)
① 임직원은 정당한 사유 없이 점검요청을 지연하거나, 거부할 수 없다. 부득이한 경우 전사보안책임자(CSO)서면 보고 후, 승인된 경우에 한하여 일정을 조정할 수 있다.
② 점검이 완료되면 전사보안담당자는 그 현황을 전사보안책임자(CSO)에 보고하고 [경미한 위반]으로 확인된 사항은 관련 팀(부서)보안책임자에게 개선을 요청한다.
③ 팀(부서)보안책임자는 요구된 개선사항에 대한 조치방법/일정을 전사보안담당자에 회신하고, 계획에 따라 조치 후 완료여부를 전사보안담당자에 통보하는 것으로 개선조치를 종료한다. 조치는 통보받은 시점부터 4 주 이내에 완료해야 하며, 그 이상의 기간이 소요될 것으로 판단되는 경우 전사보안담당자를 통해 전사보안책임자(CSO)에 별도 보고 한다.
④ 전사보안담당자는 팀(부서)에 요청한 개선사항의 완료가 모두 확인되면, 전사보안책임자(CSO)에 점검에 대한 개선완료 보고한다. 단, 완료보고는 점검완료 시점부터 30 일을 초과할 수 없으며, 4 주 이내 완료 통보하지 않은 팀(부서)는 '미 조치'로 처리한다.
⑤ 전사보안담당자는 점검 결과 [중대한 위반]으로 판단되는 사항에 대해서는 전사보안책임자(CSO)보고 후 당사 규정에서 정한 절차에 따라 조치한다.
⑥ 모든 점검 결과 및 위반자 처리 결과는 3 년 이상 유지해야 한다.
⑦ 자체 점검을 이행하지 않거나, [중대한 위반]에 대한 조치를 소홀히 한 경우 전사보안책임자(CSO) 책임이 있으며, 고객사의 보안점검/감사 시 불이익의 사유가 될 수 있다.

제59조 (협력사 보안점검 기준 및 절차)

① 협력사 점검 기준 및 주기

1. 정보보안그룹 주관 하에 사전 계획을 수립하여 점검을 실시한다.
2. 보안점검 대상은 당사 주관장사 협력사 기준으로 보안점검을 실시한다.
3. 방문 점검을 기본으로 하며, 주기는 연 1 회 실시한다.
4. 협력사 사이버침해사고 피해사고 접수 또는 인지시에 수시 방문 점검을 실시한다.
5. 협력사 사이버침해사고 발생 접수 또는 인지시에 수시 방문 점검을 실시한다.

② 협력사 보안점검 절차

1. 보안점검시행전 협력사 담당자에게 최대 7 일 전까지 방문자/목적/방문일시/점검내용들을 통보한다.
2. 협력사 보안실시는 실무에 방해되지 않도록 신속 및 정확하게 실시한다.
3. 협력사 사이버 침해사고 발생시 즉시 협력사 방문 후 보안진단 소프트웨어나 점검목록을 이용하여 임시 진단을 실시해야 한다.
4. 보안관리 실태를 확인하고, 협력사 정보보안점검 체크리스트를 통한 평과 후 부적합 부분에 대한 개선을 사항을 배포하고, 일주일 후 개선여부를 확인한다.
5. 협력사 사이버 침해사고 발생 시 즉시 협력사 방문 후 보안집단 소프트웨어나 점검목록을 이용하여 임시 진단을 실시하며, 즉시 보안조치 진행 후 재발방지 근본대책(협력사 대표이사 승인본) 징구 및 가이드라인을 제시한다.

제60조 (해외법인 보안점검 기준 절차 및 주기)

① 국내 본사의 정보보안그룹 주관 하에 사전 계획을 수립하여 실시한다.
② 정보보안그룹은 해외법인의 보안점검 계획을 연초에 연간계획(분기별 1 회)을 수립하여 실시한다.
③ 단, 솔루션을 이용하여 점검 가능하면 해당 솔루션으로 점검 진행 시 정기 점검으로 갈음한다.
④ 필요 시 정보보안그룹의 승인 하에 해외법인의 불시 보안점검을 실시할 수 있다.
⑤ 부서(팀)보안책임자는 보안의 날 행사 시 자체 보안점검 및 교육을 실시한다.
⑥ 연간 1 회 해외법인 현장 방문 점검을 실시하여 정보보안 강화를 지원한다.

제61조 (해외법인 보안점검 절차)

① 본사 정보보안그룹의 연간 계획에 따라 해외법인 보안책임자가 정기적으로 점검을 실시한다.
② 본사가 제공한 보안의 날 점검 체크리스트에 따라 매 월 보안 활동을 수행한다.
③ 점검 결과를 해외법인 보안 책임자에게 보고하고 본사에 전달한다.
④ 본사 보안 담당자는 해외법인의 보안 점검 결과를 모니터링하고 피드백을 제공한다.
⑤ 보안점검 결과를 분석하고 취약점을 지속적으로 개선한다.

제62조 (임시직, 파견자 및 제 3 자 아웃소싱)

① ① 계약서, 회사정보보호서약서, 내부정책에 명시된 정보보호 및 개인정보보호 요구사항에 따라 외부자의 보호대책 이행 여부를 주기적인 점검 또는 감사 등 관리·감독하여야 한다.

② ② 외주인력에 대한 시스템 및 정보자산 접근권한은 업무 수행에 필요한 최소 범위 내에서만 부여하여야 하며, 사전 승인 절차를 거쳐야 한다.

③ 외주인력 계정은 개인별로 발급하여야 하며, 계정 공유를 금지한다.

④ 외주인력의 접근권한은 계약기간 및 업무 수행 기간에 한하여 부여하며, 계약 종료·업무 종료·퇴사 시 즉시 회수하여야 한다.

⑤ 외주인력의 원격접속은 회사에서 승인한 보안통제 수단(VPN, 접근통제 시스템 등)을 통해서만 허용할 수 있다.

⑥ 외주인력의 중요정보 및 주요 시스템 접근 시 접근기록 및 작업이력을 보관하고 필요 시 모니터링할 수 있다.
⑦ 외주인력의 보안 점검은 일 1 회 이상 실시하며, 주요 업무서버에 영향이 있는지 수시로 점검한다.
⑧ 외주인력의 작업 시작 전 · 작업 중 · 작업 후 보안점검을 수행할 수 있다.
⑨ 계약서 및 서약서에 명시된 작업 범위를 벗어난 비인가 접근 시도 여부를 수시 점검하여야 한다.
⑩ 외주인력 프로젝트 완료 후 철수 시 작업 내용, 작업 로그, 보안시스템 로그 기록 등에 대한 보안성 검토를 실시하여야 한다. 또한 외주인력이 보유 중인 회사 자료 및 대외비 이상 등급의 정보 존재 여부를 확인하고 발견 시 즉시 삭제 또는 반납 조치하여야 한다.
⑪ 외주인력 계정 및 접근권한 부여 현황은 정기적으로 검토하며, 불필요하거나 미사용 계정은 즉시 삭제 또는 비활성화하여야 한다.
⑫ 외주인력의 보안점검 시 위반사례가 발견되면 전사보안책임자(CSO)에 보고하고, 필요 시 외주업체 대표자에게 재발방지 대책 제출 요구, 계약 제한 및 민 · 형사상 조치를 검토할 수 있다.

제63조 기타 자세한 사항은 '보안준수측정 지침', '보안점검 및 감사 지침'을 따른다

제12절 해외주재원 보안관리

제64조 정보보안 교육
① 해외 법인에 직원을 파견할 때, 해당 법인의 보안시스템 현황 및 사용법 교육을 실시한다.
② 해외 법인 파견직원 대상으로 보안수칙 준수 및 해외 정보유출 피해사례를 집중 교육한다.
③ 교육진행 완료후 교육일지를 필히 기록으로 남겨야 한다.

제65조 보안서약서 징구
① 해외법인에 재직 중인 근로자가 퇴직할 때, 업무기간 중 취득한 비밀 등 중요자료에 대한 누설 및 사적이용 금지를 내용으로 하는 보안서약서를 징구한다.
② 년에 1 회이상 보안서약서를 재징구한다.

제66조 자료 무단반출 방지
① 보안솔루션을 통하여 각종 보안자료의 무단 반출 여부를 확인하고 로그를 남긴다.
② 암호화되지 않거나 무단으로 자료를 반출할 경우 당사 위반자 처리규정에 의거 징계한다.
③ 해외주재원의 자료 이용 및 외부 반출현황을 월 1 회이상 검토한다.

제67조 기타 자세한 사항은 '해외주재원 보안관리지침'을 따른다

제 3 장 물리적 보안

제13절 보호구역 설정

제68조 (보호구역의 정의)
① 보호구역이라 함은 업무수행에 있어 비밀보호가 필요한 지역을 말하며, 그 중요도에 따라 '제한구역'과 '통제구역'으로 구분하며, 보호구역의 세분화 관리를 위하여 '사업장구역'을 추가하여 구분할 수 있다.
② 제한구역: 상주직원 이외에 출입이 금지되는 보안상 중요한 구역으로, 비 인가자의 출입 시 사전에 반드시 해당 구역 업무담당자의 승인을 받고 상시 동행해야 하는 구역을 말한다.
③ 통제구역: 비 인가자의 출입이 금지되는 보안상 극히 중요한 구역으로, 비 인가자의 출입 시 사전에 반드시 관리책임자의 승인을 받아야 출입이 가능한 지역을 말한다.

④ 사업장구역: 비밀이나 중요시설, 자재 및 중요문서 등을 보호하기 위하여 일반출입자에 대한 감시가 요구되는 지역으로, 별도의 승인내역 없이 출입할 수 있는 구역이나, 회사의 보안 관리범위에 있는 지역을 말한다.

제69조 (보호구역의 지정)

① 사업장 보안책임자는 비밀보호의 중요도에 따라 보호구역을 지정하여야 한다.
② 회사의 영업비밀 및 자산의 보호를 위하여 외부인의 출입을 제한하여야 하는 지역은 제한구역 이상으로 지정하며, 비인가자 및 외부인은 절차에 따라 승인 후 출입한다
③ 제한구역 이상으로 설정된 지역은 비 인가자의 진입을 방지하기 위한 통제장치의 설치 및 보호활동을 하여야 하며, 출입기록을 유지하여야 한다.
④ 비밀보호를 위해 임직원의 출입을 통제하여야 할 필요가 있는 지역은 통제지역으로 지정하며, 사진촬영 및 비인가 임직원의 출입을 제한한다.
⑤ 통제구역은 팀(부서)보안책임자의 의견을 수렴하여 물리보안담당자가 설정하고 전사보안책임자 (CSO)에 보고 후 시행한다.
⑥ 사업장구역은 제한구역 및 통제구역 외 지역으로 관리한다.

제70조 (보호구역 표시)

① 보호구역의 출입 시 쉽게 확인이 가능한 출입문 중앙 또는 잘 보이는 곳에 부착한다.
② 보호구역의 표지는 시설보호 및 출입통제지침 3.2 항을 따른다.

제71조 (보호구역 해제) 보호구역의 지정 목적이 소멸되었거나, 관리 환경 변화로 인해 보호구역 유지가 불필요하다고 판단될 경우 다음 절차에 따라 해제를 진행한다.

① 해제 사유 발생 및 검토
보호구역 지정 목적 소멸(프로젝트 종료, 자산의 외부 반출, 부서 이동 등) 시 주관 부서장은 해제 사유를 명시하여 보안 부서에 검토를 요청한다.
② 보안성 검토 및 타당성 확인
정보보안그룹(또는 보안 담당 부서)은 해당 구역의 자산 및 정보가 보호받아야 할 가치가 더 이상 없는지, 잠재적 위험은 없는지 물리적·관리적 측면에서 검토한다.
③ 해제 승인 절차
검토 결과를 바탕으로 '보호구역 해제 요청서'를 작성하며, 최초 지정 시의 승인권자(전사보안책임자 등)의 최종 승인을 득한다.
④ 통보 및 공고
해제 승인 즉시 임직원에게 공지하여 해당 구역의 보안 등급 변경 사실을 알리고, 혼선을 방지한다.
⑤ 현장 조치
1. 보호구역 표지 및 안내문 제거
2. 출입 통제 장치(잠금장치, 출입 기록 시스템 등) 권한 회수 및 일반 구역 전환
3. 보안 관련 기록 보존 및 최종 보고

제72조 출입관리

① 임직원은 본인 근무지역 및 제한지역의 출입이 가능하며, 외부인은 회사 내 업무목적으로 필요한 경우에 방문을 요청하여야 하고, 방문신청은 외부인을 관리/통제할 수 있는 부서에서 신청 및 승인한다.
② 외부인은 경비실 또는 사무동 입구에서 신분확인 및 방문증을 수령하여 출입하여야 한다.
③ 업무적 계약이나 장기적으로 사업장내 출입하는 인원은 장기출입증 발급 후 출입하여야 한다.
④ 출입허가를 받은 외부인이 제한구역 이상의 구역에서 업무를 수행할 때에는 담당책임자의 통제를 따라야 하며 이를 위반 시 강제 퇴실 또는 퇴장 조치한다.
⑤ 통제구역 내에서의 활동은 전사보안책임자가 승인하고 물리보안담당자의 관리하에서 가능하다.

제73조 출입증 운영

① 임직원 출입등록: 당사의 임직원은 출입 지문등록 및 태그를 발급한다.

1. 출입지문 등록 및 태그: 전 임직원 의무적 지문등록 및 출입의 목적으로 사용가능
2. 출입등록 해제 및 태그반납: 퇴사 또는 직무변경에 의해 당사 근무자로 인정되지 않는 경우 출입 지문등록 해제 및 태그를 반납해야한다.

② 외부인출입증: 당사 임직원이 출입허가를 요청한 자에 발급하는 출입증

③ 차량출입증: 사업장내 진입하기 위한 차량에 발급하는 출입증

1. 임직원차량출입증: 출입승인은 받은 차량에 발급하며, 차량 전면유리에 부착
2. 임시차량출입증: 사전 승인된 방문차량으로 일일차량출입증, 장기차량출입증으로 구분하여 발급하는 출입증

제14절 자산 반출·입 통제

제74조 반출·입 통제항목

① 반출·입 통제 항목은 일반자산 및 정보자산으로 분류한다.

② 일반자산 통제 항목

1. 생산 및 운영에 필요한 자재 및 부품, 완성품 또는 이에 준하는 자산
2. 기타 정보보안그룹에서 선정한 일반자산

③ 정보자산 통제 항목

1. 컴퓨터 류(휴대형 포함), 서버 류, 저장매체 류 등의 정보처리 및 저장 장치 또는 이에 준하는 자산
2. 기타 정보보안그룹에서 선정한 정보자산

④ 기타 통제하기 어려운 세부 항목에 대하여서는 정보보안그룹에서 검토 및 선정하여 세부 지침에 명기할 수 있으나, 최소한으로 분류토록 한다.

⑤ 반출·입 통제 관리

1. 당사 소유 및 비 소유 자산 등의 모든 통제 대상 자산에 대하여 사업장내 반출입시에는 반드시 해당 자산에 대하여 관리, 통제할 수 있는 부서(팀)의 승인 절차를 반드시 운영토록 한다.
2. 승인받은 외부인에 의한 자산 반출·입일지라도 업무 목적 이외의 행위를 할 경우 승인을 한 임직원에게도 책임이 있다.
3. 관리, 통제할 수 있는 부서(팀)의 승인이 있더라 하더라도 당사 보안 목적 달성을 저해하는 항목에 대하여서는 정보보안그룹에서 반출·입을 통제할 수 있다.

제15절 CCTV운영 및 시설감시

제75조 (기본원칙)

① 차량 및 인원이 출입하는 지역은 상시 감시하여야 한다.

② 중요(보안)시설에 대하여는 CCTV 및 보안요원(인원)에 의한 감시를 하여야 하며, 사업장 특성에 따라 운영이 불가한 경우 무인경비시스템을 운영할 수 있다.

③ CCTV 는 보안 및 화재, 도난 등에 대한 구체적이고 실질적인 위험 발생 우려가 있는 장소에 한하여 설치되어야 하며, 설치목적에 맞게 운영되어야 한다.

④ CCTV 를 설치·운영할 때에는 주 출입구 등 쉽게 인지가 가능한 장소에 CCTV 가 설치 운영 중임을 알아볼 수 있도록 안내판을 설치(부착) 하여야 한다.

제76조 (관리책임)

① 물리보안담당자는 경비인력/CCTV 의 관리 및 운영에 대한 책임을 지며 업무를 위탁하는 경우 위탁 계약서에 관계법령에 의거 개인정보보호에 관한 준수사항을 규정하여야 한다.

② 전사보안담당자는 사업장 출입 등의 목적으로 수집된 개인정보 및 CCTV 운영에 따라 수집된 영상정보에 대하여 물리보안담당자가 수집 목적 외 조작·유출 등 오남용 하지 않도록 관리·감독하여야 한다.

제77조 (정보의 처리)

① 보관기간이 만료된 개인정보(영상정보 포함)는 지체 없이 삭제하여야 하며, 복원이 불가능하도록 파기하여야 한다.

② 영상정보를 취급(모니터링)하는 장소 및 보관장소는 제한구역 이상의 보호구역으로 설정하여 관계자 외 접근을 통제하여야 한다.

③ 영상정보는 CCTV 의 설치 목적 이외의 용도로 활용되거나, 접근권한을 부여받은 자 이외의 타인에게 열람 제공되어서는 안 된다. 다만 법령에 의하거나 정보주체의 요청에 의하여 열람 및 자료를 제공하여야 할 경우에는 사전 전사보안책임자(CSO)의 인가를 득해야 한다.

제16절 업무연속성 관리

제78조 (업무연속성 관리절차 내 보안의 반영)

① 천재지변, 화재, 폭동 등과 같은 비상사태 발생에 대비하여 전사에 걸쳐 업무연속성 계획을 개발하고 유지하기 위한 조직 및 관리 프로세스가 수립되어야 한다.

② 비상사태 발생시 정보시스템의 계속적 운영과 업무 중단 시 최단 시간 내에 업무를 재개할 수 있도록 업무 우선순위에 따라 비상계획이 수립되고 운영 되어야 한다.

③ 업무연속성 계획의 변경 절차가 수립되어야 하며, 변경된 업무연속성 계획을 관련 임직원에게 교육하고 공지하여야 한다.

④ 업무연속성 계획은 정기적으로 테스트되고 그 유효성이 검증되어야 한다.

제79조 (기타 세부 사항) 본 규정에 언급되지 않은 사항 및 세부적인 내용은 '시설보호 및 출입통제지침', 'CCTV 운영 및 시설 감시지침' 및 '정보자산반출 통제지침'에 따른다

제 4 장 기술보안

제17절 사용자보안지침

제80조 (목적) 업무상 목적으로 회사에서 지급한 업무용 단말기의 정보기술보호를 위한 요구사항을 제공함에 그 목적이 있다.

제81조 관리항목

① 업무용 단말기 도입, 운영 및 폐기에 대한 지침이 마련되어야 한다.

② 회사의 정보자산을 이용하는 사용자는 사용자보안지침을 준수하여야 하고, 추가로 모바일 기기로 업무를 수행하는 경우 '모바일보안지침'을 적용한다. 사용자는 본 지침을 위반하여 발생한 손실에 대한 책임을 진다.

③ 사용자는 회사에서 지급한 H/W 및 S/W 의 변경을 임의로 하여서는 안되며, 이동형 저장장치는 승인절차를 거친 후 사용해야 한다.

④ 개인 소유의 PC, Tablet PC, CD-Writer, 외장형 저장장치, 데이터케이블 등 전산장비는 회사에 반입 및 사용할 수 없으며, 업무상 필요한 경우 승인절차에 따라 사용하여야 한다.
⑤ 회사 소유 정보자산은 개인 목적으로 반출할 수 없으며, 출장·이동업무·수리 등 필요한 경우 승인절차 후 반출하여야 한다.
⑥ 외부에 내부정보를 제공하는 경우 반드시 관리 책임자의 사전 또는 사후 승인절차를 거쳐야 하며, 미승인 정보 제공에 대한 책임은 사용자에게 있다.
⑦ 인터넷 사용 시 회사의 보안정책을 준수해야 하며, 승인되지 않은 인터넷 망 사용이나 비인가 소프트웨어(불법 S/W 포함) 설치를 금지한다.
⑧ PC 로그인 및 화면보호기 비밀번호를 설정하여야 하며, 화면보호기 암호시간은 10 분으로 설정하여야 한다.
⑨ 패스워드는 영문자, 숫자, 특수문자를 포함한 8 자리 이상으로 설정하여야 하며, 3 개월 주기로 변경하고 6 개월간 재사용을 금지한다.
⑩ 패스워드는 자신과 관련된 정보나 타인이 추측하기 쉬운 값으로 설정하여서는 안 되며, 타인과 공유하거나 노출하여서는 안 된다. 노출 시 즉시 변경하여야 한다.
⑪ 공용 PC 를 구축할 경우 관리자를 지정해야하며 공용 PC 에는 보안문서를 저장할 수 없다.
⑫ 공유폴더 사용 시에는 반드시 비밀번호가 설정된 공유폴더를 사용하여야 하며, 이때 업무적으로 인가된 사용자만 접근 가능하도록 설정하여야 한다. 또한 Everyone, Domain Users 등 기본 계정은 삭제하여 비인가 접근을 방지하고, 사용 목적이 종료되면 즉시 공유를 해제하여야 한다.
⑬ 사용자는 주기적으로 보안패치 업데이트를 실시하여야 하며, 보안패치 적용 후 업무시스템 및 대외 업무시스템의 정상 동작 여부를 확인하여야 한다. 이상 발생 시 즉시 기술보안담당자에게 알려 조치를 받아야 한다.
⑭ 업무 관련 전자메일은 회사에서 제공하는 전자메일 서비스를 사용하여야 하며, 발신인이 불분명하거나 의심스러운 메일은 열람하지 말고 삭제하여야 한다. 중요정보 전송 시에는 암호화 또는 비밀번호 설정 등 보호조치를 하여야 한다.
⑮ 사용자 PC 는 악성코드 실행방지솔루션 등의 정보보호 기능을 설정·활용하여야 하며, PC 내 기밀정보 보호, 악성코드 감염 예방, 소프트웨어 지적재산권 준수 의무를 이행하여야 한다.

제82조 (기타 세부 사항) '사용자보안지침' 및 '모바일보안지침'을 따른다.

제18절 네트워크보안

제83조 (목적) 사내 네트워크 구성 및 외부 네트워크와의 연결 시 요구되는 정보보호 수준을 향상시켜 안정적인 네트워크 인프라를 운영함에 그 목적이 있다.

제84조 (관리항목)
① 사내 네트워크 및 외부와 연결되는 모든 네트워크의 설치, 변경, 해지 작업은 승인 후 수행하여야 한다.
② 사내 네트워크는 외부에서 접근이 통제되는 별도의 네트워크를 구축해야 한다.
③ 사설 IP 및 공인 IP 의 신규 부여, 회수 및 변경은 네트워크 운영담당자가 관리하여야 하며, 그 이력을 유지하여야 한다.
④ 외부에서 사내 네트워크에 접속하는 경우에는 회사가 승인한 VPN 을 사용하여야 하며, VPN 계정 및 권한은 업무상 필요한 범위 내에서 부여·관리하여야 한다. VPN 계정의 발급, 변경, 회수, 접속기록 보관 및 점검 등에 관한 세부사항은 제 76 조를 따른다.
⑤ 중요 네트워크는 분리 및 이중화하여야 하며, FA 망 및 서버망 등 주요 업무망은 장애 시에도 중단이 없도록 구성하여야 한다.
⑥ 허가되지 않은 유·무선 전산장치의 회사 네트워크 사용을 금지하며 AP 는 주 1 회 이상 접속장비, 설정값, 백업 및 최신 펌웨어 상태를 점검하여야 한다.

⑦ 외부 방문객 또는 개인 PC 의 네트워크 사용 시 기술보안담당자의 승인이 필요하며, 기술보안담당자는 해당 인원에 대해 접근 권한을 설정하여야 한다.
⑧ 모든 무선 네트워크는 암호화하여 운영하여야 하며, OA 망과 GUEST 망은 분리하여 관리하여야 한다.
⑨ 네트워크장비 설정 내용 백업 등 장애발생에 대비해야 하며, 접근 통제가 이루어져야 한다.
⑩ 네트워크의 도입, 운영, 폐기에 대한 지침이 마련되어야 한다.

제85조 (기타 세부 사항) '네트워크보안지침'을 따른다.

제19절 정보유출통제

제86조 (목적) 사내 중요정보에 대한 IT 통제지침을 제시함으로써 정보자산의 보안성과 안정성을 유지하는데 필요한 사항을 정함에 그 목적이 있다.

제87조 (관리항목)
① 인터넷을 통한 모든 정보의 송수신은 회사의 보안시스템을 통하여야 하며, 승인되지 않은 별도의 인터넷 회선은 차단되어야 한다.
② 대용량 파일의 송수신은 승인된 절차와 통제수단을 통하여 수행하여야 한다.
③ PC 내 대외비 이상 중요문서는 암호화하여 보관하여야 하며, 비밀등급 이상의 문서는 허가 없이 저장하여서는 안 된다. 문서 삭제 및 이동 또한 승인 하에 수행하여야 한다.
④ 정기적인 보안패치 운영관리를 수행하여야 하며, PC 내 방화벽 또는 백신의 유효성과 업데이트 상태를 주기적으로 확인하여야 한다.
⑤ 이동식 저장매체는 통제 솔루션 또는 이에 상응하는 운영관리를 적용하여야 하며, 승인된 사용자만 사용할 수 있어야 한다.
⑥ 비인가 · 비보안 USB 등 이동식 매체의 반입을 금지하며, 회사에서 제공하는 보안 USB 만 사용하여야 한다.
⑦ 이동식 저장매체의 사용자, 지급, 회수, 등록 및 예외 현황은 관리대장으로 수시 관리하여야 하며, 민감정보 저장 시 암호화 또는 접근통제를 적용하여야 한다.
⑧ 저장매체 변경 또는 처분 시 재사용 또는 불용 여부를 결정하여 승인받아야 하며, 재사용 시 완전삭제 후 사용하고, 폐기 시 완전파괴 또는 전용 소자장비를 사용하여 복구가 불가능하도록 하여야 한다.
⑨ 저장매체 폐기 시 폐기 일자, 담당자, 사유, 방법, 사진 등을 포함한 폐기관리대장을 기록 · 보관하여야 한다.
⑩ 외부업체를 통하여 저장매체를 폐기하는 경우 폐기 절차를 계약서에 명시하고, 완전 폐기 여부를 확인하여 최종 보고하여야 한다.
⑪ 서버시스템에 대한 정보유출 통제는 시스템보안지침에 따라 관리하여야 한다.

제88조 (기타 세부 사항) 세부 사항은 '정보유출통제지침'을 따른다.

제20절 시스템보안

제89조 (목적) 시스템의 도입, 설치, 운영 폐기 시 다양한 보안 위협 및 취약성으로부터 안전하게 보호하고, 운영 관리하는데 그 목적이 있다.

제90조 (관리항목)
① 시스템의 도입, 운영, 폐기 프로세스에 대한 지침이 마련되어야 한다.

② 시스템의 도입 및 변경은 계획 수립, 보안성검토 및 승인 후 수행하여야 하며, 이후 자산관리 목록을 갱신하여야 한다. 보안점검항목이 지정되어 있어야 한다.
③ 시스템은 물리적 보안이 확보된 통제구역(전산실 또는 이에 준하는 시설)에 설치되어야 한다.
④ 시스템 설치 시 관리자를 지정하고 기본계정 및 불필요 계정을 삭제하는 등 적절한 보안설정을 적용하여야 하며, 반기 1 회 전체 계정에 대한 검토를 실시하여야 한다.
⑤ 시스템 사용자 계정의 등록, 변경, 삭제는 공식적인 승인절차로 이루어져야 하며 이력관리가 되어야 한다.
⑥ 모든 사용자에게는 유일한 계정을 부여해야 하며, 계정공유현황을 분석해야 한다. 또한 비밀번호는 영문, 숫자 혼용 8 자리 이상이며, 3 개월 이내 변경되어야 한다.
⑦ 데이터베이스와 서버 등 주요 시스템에 접근한 모든 기록은 유실되지 않도록 3 년 이상 보관해야 하며, 비인가자의 접근을 차단하기 위한 통제 절차를 반드시 운영해야 한다
⑧ 중요 업무 시스템은 개발과 운영시스템이 분리되어야 한다.
⑨ 어플리케이션의 개발 및 변경은 공식적인 승인 절차를 준수하여야 하며, 보안성 검토 및 기능 검증 테스트 후 운영에 반영되어야 한다.
⑩ 테스트데이터는 주민등록번호, 계좌번호 등과 같은 개인 정보 및 중요정보를 포함하여서는 안 된다.
⑪ 시스템에 대한 주기적인 취약점 점검 및 조치가 및 이루어져야 하며, 시스템 성능 점검을 통해 도입 또는 폐기 여부를 검토하여야 한다.
⑫ 유지보수는 인가된 직원 또는 인가된 절차에 따라 수행하여야 하며, 작업 내역과 의심 결함을 기록하여야 한다. 유지보수 시 시스템 담당자는 동석하여야 한다.
⑬ 보안패치는 취약점 확인, 타당성 검토 및 테스트 후 적용하여야 하며, 패치 적용 현황을 관리하여야 한다.
⑭ 운영체제, 데이터베이스에 대한 백업 및 원격지 소산이 되어야 한다.
⑮ 시스템 장애에 대비한 복구계획이 마련되어야 하며 최소 년 1 회 모의 훈련을 실시하여야 한다.

제91조 (기타 세부 사항) '시스템보안지침'을 따른다.

제21절 보안시스템운영

제92조 (목적) 보안시스템을 안정적, 효율적으로 운영 관리하기 위한 지침을 제공하는데 그 목적이 있다.

제93조 (관리항목)
① 보안시스템의 도입, 운영, 폐기에 대한 지침이 마련되어야 한다.
② 각 보안시스템에 대한 운용 매뉴얼을 마련하여야 한다.
③ 보안시스템은 인가된 사용자만이 접근해야 하며, 비밀번호는 영문, 숫자 혼합으로 8 자리 이상으로 설정되어야 한다.
④ 외부에서 접근 가능한 웹 시스템은 웹 방화벽 기준에 따라 보호하여야 한다.
⑤ 보안시스템 관리자는 로그 기능이 항상 가동되도록 하고, 주기적으로 모니터링 및 분석해야 하며, 관련 로그는 3 년 동안 보관해야 한다.
⑥ 보안시스템에 대한 취약점 분석 및 점검을 주기적으로 시행하여 개선한다.

제94조 (기타 세부사항) '보안시스템운영지침'을 따른다.

제22절 보안사고침해대응지침

제95조 (목적) 보안침해사고에 대한 대응 및 복구업무를 포함하며, 피해를 최소화하고 재발방지를 통하여 정보자산의 보안성과 안정성을 유지하는데 필요한 지침을 제공하는데 그 목적이 있다.

제96조 (관리항목) 보안침해사고 예방을 위하여 시스템 보안성 검토 및 취약점 점검 · 조치를 수행하여야 한다.

① 보안침해사고 발생 시 기술보안담당자는 긴급히 대응하고, 그 처리 결과를 전사보안책임자(CSO)에 보고해야 한다.

② 모든 임직원은 침해사고 발견 시 임의 처리 없이 즉시 전사보안책임자(CSO) 또는 부서장에게 보고해야 한다.

③ 외부 침입 흔적이 의심되는 경우 기술보안담당자는 보안진단 도구 등을 이용하여 점검해야 하며, 데이터 변조나 불법 접근이 확인될 경우 해당 서비스를 중지한다.

④ 침입자 식별을 위한 증거 수집 및 보안사고 대응의 모든 기록을 유지 · 관리해야 한다.

⑤ 필요 시 외부 유관업체 및 대외기관에 통보하고 협조를 요청한다.

⑥ 침해사고로 인한 시스템 장애 시 신속한 복구 및 서비스 정상화를 수행하며, 장애복구 모의훈련을 연 1 회 이상 실시한다.

⑦ 보안침해사고 발생 시 원인 분석, 확산 방지 및 피해 최소화를 위한 조치를 수행하여야 한다.

⑧ 조치된 사안에 대해 취약점 점검 및 개선조치를 통해 근본 해결책을 강구하고, 재발방지 대응책을 마련한다.

⑨ 공개가 허용된 침해사고는 임직원에게 공지 또는 교육하여 보안 인식을 강화시켜야 한다.

제97조 (기타 세부사항) '보안침해사고대응지침'을 따른다.

제23절 재해복구대응

제98조 (목적) 재해 및 비상 상황 발생 시 중단된 정보시스템을 목표 시간 내에 복구하여 업무 연속성을 보장하는 데 그 목적이 있다.

제99조 (관리항목)

① 재해 발생 시 신속한 의사결정을 위해 전사보안책임자(CSO)를 중심으로 한 재해복구 대응 조직을 구성하고 역할을 정의해야 한다.

② 장애 복구 시간이 허용 범위를 초과할 것으로 예상될 경우, 즉시 재해를 선포하고 비상 체제로 전환하여야 한다.

③ 각 정보자산별 목표 복구 시간(RTO)과 목표 복구 시점(RPO)을 설정하여 관리하여야 한다.

④ 재해복구 계획의 실효성 검증을 위해 연 1 회 이상 모의훈련을 실시하고 결과를 반영하여 절차를 보완해야 한다.

⑤ 재해 종료 후에는 원인 분석 및 대응 과정에 대한 사후 보고서를 작성하여 재발 방지 대책을 강구해야 한다.

제100조 제 3 조 (기타 세부사항) '재해복구대응지침'을 따른다.

제24절 취약점 점검

제101조 (목적) 정보시스템의 보안 취약점을 사전에 발견하고 제거하여 외부 공격으로부터 정보자산을 안전하게 보호하는 데 그 목적이 있다.

제102조 (관리항목)

① 서버, 네트워크, 보안 시스템 등 전사 정보자산을 대상으로 주기적인 취약점 점검 계획을 수립하여야 한다.
② 연 1 회 이상의 종합 점검을 실시하며, 주요 시스템은 분기 또는 월별 점검을 통해 보안 패치 상태를 확인해야 한다.
③ 자동화 도구, 수동 점검 및 모의 해킹 등 다양한 방법을 병행하여 점검의 실효성을 확보해야 한다.
④ 발견된 취약점은 위험도에 따라 우선순위를 정하여 개선 조치하고, 조치 결과를 기록·관리하여야 한다.

제103조 (기타 세부사항) '취약점점검지침'을 따른다.

제25절 서버 접근통제 운영

제104조 (목적) 서버 및 데이터베이스에 대한 접근 권한을 체계적으로 통제하여 비인가자의 접근 및 정보 유출을 방지하는 데 그 목적이 있다.

제105조 (관리항목)
① 서버 접근 권한은 업무상 필요한 인원에게만 '최소 권한 부여' 원칙에 따라 허용되어야 한다.
② 권한 신청은 부서장 검토와 정보보안팀 승인을 거쳐야 하며, 관리자 권한은 CSO 의 최종 승인을 득해야 한다.
③ 외부 인력의 접근은 보안서약서 징구 후 특정 기간 내에서만 허용하며, 작업 완료 후 즉시 권한을 회수해야 한다.
④ 모든 서버 접속 및 작업 내역은 로그로 수집하여 3 년 이상 보관하고 주기적으로 모니터링해야 한다.
⑤ 인사이동이나 퇴사 발생 시 해당 계정의 권한을 즉시 삭제 또는 정지하여야 한다.

제106조 (기타 세부사항) '서버접근 통제운영지침'을 따른다.

제26절 소스코드 이관

제107조 (목적) 소프트웨어 개발 및 유지보수 시 발생하는 소스코드의 이관 절차를 규정하여 지적 자산의 유출을 방지하는 데 그 목적이 있다.

제108조 (관리항목)
① 소스코드 이관 시 사유와 목적이 명확한 계획을 수립하고 보안성 검토를 선행하여야 한다.
② 이관되는 소스코드 내에 개인정보, 계정 정보 등 중요 정보가 포함되지 않도록 점검하여야 한다.
③ 이관은 승인된 보안 저장소나 암호화된 전송 수단을 이용해야 하며, 이관 이력을 기록·관리하여야 한다.
④ 수신된 소스코드는 인가된 자만이 접근할 수 있도록 권한을 제한하고 안전하게 보존해야 한다.

제109조 (기타 세부사항) '소스코드이관지침'을 따른다.

제27절 저장매체 불용처리

제110조 (목적) 저장매체의 폐기나 교체 시 저장된 중요 정보를 완전히 삭제하여 외부 유출을 원천 차단하는 데 그 목적이 있다.

제111조 (관리항목)
① 저장매체의 외부 반출이나 폐기 시 정보보안그룹의 관리 하에 보안 조치를 수행하여야 한다.
② 정보의 중요도에 따라 디가우징, 파쇄, 완전포맷 등 복구가 불가능한 삭제 방법을 적용하여야 한다.
③ 개인 지급 매체는 사용자 본인이 삭제하며, 공용 시스템 매체는 정보보안그룹 책임 하에 삭제를 진행한다.
④ 모든 불용처리 내역은 날짜, 방법, 담당자 등을 포함하여 기록하고 증빙 자료를 보관하여야 한다.

제112조 (기타 세부사항) '저장매체 불용처리지침'을 따른다.

제28절 데이터 백업 및 복구

제113조 (목적) 시스템 장애나 데이터 손실 시 신속한 복구를 위해 체계적인 백업 운영 기준을 정함으로써 가용성을 확보하는 데 그 목적이 있다.

제114조 (관리항목)
① DB, OS 설정파일, 중요 문서 등 백업 대상을 선정하고 주기적인 백업 정책을 수립·운영하여야 한다.
② 백업 데이터는 물리적으로 분리된 안전한 장소 또는 원격지에 소산 보관하여야 한다.
③ 연 1회 이상 실제 복구 테스트를 실시하여 백업 데이터의 정합성과 복구 절차의 유효성을 검증하여야 한다.
④ 백업 및 복구 수행 내역은 전자문서로 기록하여 관리하고, 사고 발생 시 보고 자료로 활용한다.

제115조 (기타 세부사항) '데이터 백업 복구 절차 지침'을 따른다.

제29절 수작업 생산 절차

제116조 (목적) IT 시스템(MES 등) 장애로 자동화 생산이 불가능할 경우, 수작업 전환을 통해 생산 중단을 방지하고 업무 연속성을 확보하는 데 그 목적이 있다.

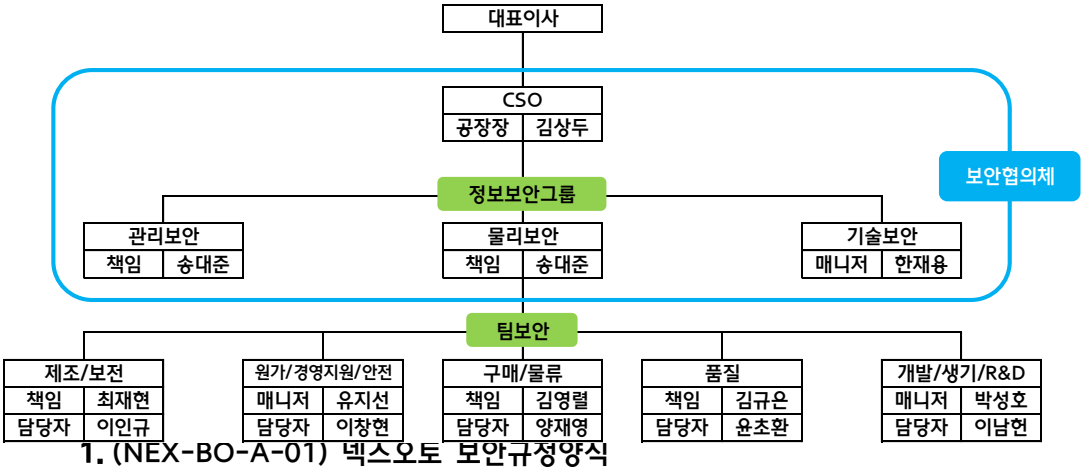
제117조 (관리항목)
① 시스템 장애 발생 시 즉시 상황을 전파하고, 사전에 정의된 기준에 따라 장애 선언 및 수작업 전환을 결정해야 한다.
② 수작업에 필요한 필수 생산 데이터(서열 정보 등)를 확보하여 현장에 배포하는 절차를 마련해야 한다.
③ 수작업 생산 중에도 품질 및 안전 수칙을 준수해야 하며, 모든 생산 실적은 별도로 기록 관리해야 한다.
④ 시스템 복구 후에는 수작업 기간의 데이터를 누락 없이 시스템에 입력하여 정합성을 확보해야 한다.

제118조 (기타 세부사항) '수작업생산절차지침'을 따른다.

제119조 제 5 장 첨부

제120조 별첨

① 보안조직도



1. (NEX-BO-A-01) 넥스오토 보안규정양식
2. (NEX-BO-A-02) 넥스오토 개인정보보호지침
3. (NEX-BO-A-03) 넥스오토 모바일보안정책
4. (NEX-BO-A-04) 넥스오토 보안준수측정지침
5. (NEX-BO-A-05) 넥스오토 위험관리방법론 및 절차지침

② 물리영역

1. (NEX-BO-P-01) 넥스오토 시설보호 및 출입통제지침
2. (NEX-BO-P-02) 넥스오토 CCTV운영 및 시설감시지침
3. (NEX-BO-P-03) 넥스오토 정보자산 반출입 통제지침
4. (NEX-BO-P-04) 넥스오토 경비운영지침

③ 기술영역

1. (NEX-BO-T-01) 넥스오토 사용자보안지침
2. (NEX-BO-T-02) 넥스오토 네트워크보안지침
3. (NEX-BO-T-03) 넥스오토 정보유출통제지침
4. (NEX-BO-T-04) 넥스오토 시스템보안지침
5. (NEX-BO-T-05) 넥스오토 재해복구대응지침
6. (NEX-BO-T-06) 넥스오토 취약점점검지침
7. (NEX-BO-T-07) 넥스오토 서버접근통제운영지침
8. (NEX-BO-T-08) 넥스오토 소스코드이관지침
9. (NEX-BO-T-09) 넥스오토 저장매체 불용처리지침
10. (NEX-BO-T-10) 넥스오토 보안침해사고대응지침