





개인정보보호 관리계획

☐ 관 리 본

☐ 비관리본

관 리 번 호 : 25(SK-P)-02

	작 성	검 토		승 인
직 책	개인정보보호 담당자(부)	본사 개인정보보호 담당 부서장/부장	현장 개인정보보호 책임자(정) /상무	개인정보보호 책임자/ 대표이사
성 명	나지훈	나왕주	장정한	이일환
서명/날인				

2025년 1월 02일



(주)신광티앤이

주소 : 서울시 강서구 허준로 217 , 204호 (가양동, 가양테크노타운)

TEL : (02)464-4252 FAX : (02)464-3065



개인정보보호 관리계획

문서번호

SK-P

개정차수

1

1.2 목 차

제,개정일자

2025.1.02

페이지

1/1

장 번 호	제 목	제·개 정 일 자	개 정 번 호	비 고
1 장	총칙	2024.02.15	0	-
2 장	내부 관리계획의 수립 및 시행	2024.02.15	0	-
3 장	개인정보보호 책임자의 역할 및 책임	2024.02.15	1	-
4 장	개인정보보호교육	2024.02.15	1	-
5 장	기술적 안전조치	2024.02.15	1	-
6 장	정기적인 자체검사	2024.02.15	1	-
7 장	관리적 안전조치	2024.02.15	1	-
8 장	물리적 안전조치	2024.02.15	1	-
9 장	개인정보 침해대응 및 피해구제	2024.02.15	1	-

개인정보 보호 내부관리 계획

- 개인정보 내부관리 계획은 일반적으로 아래와 같은 내용을 포함하여야 한다.

개인정보 보호 내부관리 계획 목차

제1장 총칙

- 1조.(목적)
- 2조.(적용범위)
- 3조.(용어 정의)

제2장 내부관리계획의 수립 및 시행

- 4조.(내부관리계획의 수립 및 승인)
- 5조.(내부관리계획의 공표)

제3장 개인정보관리책임자의 역할과 책임

- 6조.(개인정보관리책임자의 지정)
- 7조.(개인정보관리책임자의 역할과 책임)
- 8조.(개인정보보호 담당자의 역할과 책임)
- 9조.(개인정보 취급자의 범위 및 의무와 책임)

제4장 개인정보 보호 교육

- 10조.(개인 정보 보호 책임자 및 담당자 교육)
- 11조.(개인정보취급자의 교육)

제5장 기술적 안전조치

- 12조.(접근 권한의 관리)
- 13조.(접근통제)
- 14조.(개인정보의 암호화)
- 15조.(접속기록의 보관 및 점검)

제6장 정기적인 자체검사

- 16조.(보안 프로그램 설치 및 운용)
- 17조.(관리용 단말기의 안전조치)

개인정보 보호 내부관리 계획 목차

제7장 관리적 안전 조치

18조.(개인정보 보호조직 구성 및 운영)

19조.(개인정보 유출 사고 대응)

20조.(위험도 분석 및 대응)

21조.(수탁자에 대한 관리 및 감독)

제8장 물리적 안전조치

22조.(물리적 안전조치)

제9장 개인정보 침해대응 및 피해구제

23조.(권익침해 구제방법)

제1장 총칙

1조. 목적

개인정보 보호 내부 관리계획(이하 '본 계획' 또는 '내부 관리계획' 이라 한다)은 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 '정보통신망법' 이라 한다)의 내부 관리계획의 수립 및 시행 의무에 따라 제정된 것으로 (주)신광티앤이(이하 '회사' 라 한다)가 취급하는 개인정보를 체계적으로 관리하여 개인정보가 분실, 도난, 누출, 변조, 훼손, 오·남용 등이 되지 아니하도록 함을 목적으로 한다.

2조. 적용범위

계획은 정보통신망을 통하여 수집, 이용, 제공 또는 관리되는 개인정보뿐만 아니라 서면 등 정보통신망 이외의 수단을 통해서 수집, 이용, 제공 또는 관리되는 개인정보에 대해서도 적용되며, 이러한 개인정보를 취급하는 내부 임직원 및 외부업체 직원에 대해 적용된다.

3조. 용어 정의

본 계획에서 사용하는 용어의 뜻은 다음과 같다.

1. “개인정보”란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.

① 고유식별정보 : 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호

② 민감정보 : 사상, 신념, 노동조합·정당가입·탈퇴, 정치적 견해, 건강, 성생활, 유전정보, 범죄경력 정보 등에 관한 정보와 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보

2. “처리”란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.

3. “정보 주체”란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.

4. “개인 정보파일”이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.

5. “개인 정보처리자”란 업무를 목적으로 개인정보파일을 운영하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인등을 말한다.

6. “개인정보 보호책임자”란 개인 정보취급자의 개인정보 처리에 관한 업무를 총괄해서 책임지거나 업무처리를 최종적으로 결정하는 자로서, 법 제31조에 따른 지위에 해당하는 자를 말한다.

7. “개인정보 보호담당자”란 개인정보 보호책임자를 보좌 하여 개인정보취급자의 교육, 보안PC 포함 자체보안점검, 문서 관리 등을 담당하는 자를 말한다.

8. “개인 정보취급자”란 개인정보처리의 지휘, 감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 임직원, 파견근로자, 시간제근로자 등을 말한다.

9. “개인정보 처리시스템”이란 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템을 말한다. (DRM PC , AIS 등록 PC)

10. “위험도 분석”이란 개인정보 유출에 영향을 미칠 수 있는 다양한 위험요소를 식별, 평가하고 해당 위험요소를 적절하게 통제할 수 있는 방안 마련을 위한 종합적으로 분석하는 행위를 말한다.

10. “비밀번호”란 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴

퓨터 또는 정보통신망 등에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.

11. “정보통신망”이란 “전기통신기본법” 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집, 가공, 저장, 검색, 송신 또는 수신하는 정보통신체계를 말한다.

12. “공개된 무선망”이란 불특정 다수가 무선접소강치(AP)를 통하여 인터넷을 이용할 수 있는 망을 말한다.

13. “모바일 기기”란 무선망을 이용할 수 있는 PDA, 스마트폰, 태블릿PC 등 개인정보 처리에 이용되는 휴대용 기기를 말한다.

14. “바이오 정보”란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다

15. “보조 저장매체”란 이동형 하드디스크, USB메모리, CD, DVD 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 용이하게 연결, 분리할 수 있는 저장매체를 말한다.

16. “내부망”이란 물리적 망분리, 접근 통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.

17. “접속기록”이란 개인정보취급자 등이 개인정보처리시스템에 접속한 사실을 알 수 있는 계정, 접속일시, 접속자 정보, 수행업무 등을 전자적으로 기록한 것을 말한다. 이 경우 “접속”이란 개인정보처리시스템과 연결되어 데이터 송신 또는 수신 가능한 상태를 말한다.

18. “관리용 단말기”란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리시스템에 직접 접속하는 단말기를 말한다.

제2장 내부 관리계획의 수립 및 시행

4조. 내부 관리계획의 수립 및 승인

- 1) 개인정보 보호책임자는 회사의 개인정보 보호와 관련한 법령 및 규정 등을 준수할 수 있도록 내부 의사결정 절차를 통하여 내부 관리계획을 수립하여야 한다.

2) 개인정보보호 책임자는 내부 관리계획의 각 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부 관리계획을 수정하여야 한다.

3) 개인정보보호 책임자는 제1항, 제2항에 따라 내부관리계획을 수립하거나 수정하는 경우에는 대표이사로부터 내부결재 등의 승인을 받아야 하며, 그 이력을 보관, 관리하여야 한다.

4) 개인정보처리자는 내부관리계획의 세부 이행을 위한 각종 지침 등을 마련하여 시행할 수 있다.

5) 개인정보보호 책임자는 연 1회 이상으로 내부관리계획의 이행 실태를 점검, 관리하고 그 결과에 따라 적절한 조치를 취하여야 한다.

5조. 내부 관리계획의 공표

1) 개인정보보호 책임자는 제4조제3항에 따라 승인된 내부관리계획을 모든 임직원 및 관련자에게 알림으로써 이를 준수하도록 하여야 한다.

2) 내부관리계획은 임직원 등이 언제든지 열람할 수 있는 방법으로 비치하거나 제공하여야 한다.

제3장 개인 정보보호 보호 책임자의 의무와 책임

6조. 개인 정보보호 책임자의 지정

1) 회사는 “개인정보 보호법” 제31조와 같은 법 시행령 제32조에 따라 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인 정보보호 책임자로 정한다.

7조. 개인정보보호 책임자의 역할과 책임

1) 개인 정보보호 책임자는 다음 각 호의 업무를 수행한다.

- 개인 정보보호 계획의 수립 및 시행
- 개인 정보처리 실태 및 관행의 정기적인 조사와 개선
- 개인 정보 처리와 관련한 불만의 처리 및 피해 구제
- 개인 정보 유출 및 오용, 남용 방지를 위한 내부통제시스템의 구축
- 개인 정보보호 교육 계획의 수립 및 시행
- 개인 정보파일의 보호 및 관리 감독
- “개인 정보보호법” 제30조에 따른 개인정보 처리방침의 수립, 변경 및 시행
- 개인 정보 보호 관련 자료의 정리
- 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기

2) 개인 정보보호 책임자는 제1항의 업무를 수행함에 있어서 필요한 경우 개인정보의 처

리 현황, 처리 체계 등에 대하여 수시로 조사하거나 관계 당사자로부터 보고를 받을 수 있다.

3) 개인 정보보호 책임자는 개인 정보보호와 관련하여 이 법 및 다른 관계 법령의 위반 사실을 알게 된 경우에는 즉시 개선조치를 하여야 하며, 필요하면 대표이사에게 개선조치를 보고하여야 한다.

4) 개인 정보보호 책임자는 개인정보 관련 업무의 효율적 운영을 위하여 개인정보 관리 전담 인원을 직원 중 1인 이상 개인정보 담당자로 임명한다

8조. 개인 정보보호 담당자의 역할 과 책임

1) 개인정보보호 담당자는 다음 각 호의 업무를 수행한다.

- 개인정보취급자의 개인정보 보호 교육 실시
- 개인정보취급자의 개인정보 보호 업무를 지도
- 개인정보 처리시스템의 사용자 권한 설정 등 제반 보호 장치에 관한 사항 확인
- 시스템 로그 파일 등 접속기록의 주기적인 분석 및 오남용 사고 예방
- P2P 프로그램 혹은 불법 소프트웨어 삭제 확인
- 시스템 암호,하드암호,윈도우 로그인 암호를 설정하며 화면보호기 암호 설정 및 시간 5분 이내 설정 확인
- 기타 개인정보 보호를 위해 필요한 사항등

2) 개인 정보보호 담당자는 개인정보보호책임자를 보좌하여 개인정보보호 업무에 대한 실무를 관리한다.

9조. 개인정보 취급자의 범위 및 의무와 책임

1) 개인정보 취급자의 범위는 회사 내에서 고객들의 개인정보 수집, 보관, 처리, 이용, 제공, 관리 또는 파기 등의 업무를 수행하는 자를 말하고, 정규직 이외에 임시직, 계약직 직원도 포함될 수 있다.

2) 개인정보 취급자는 개인 정보보호와 관련하여 다음과 같은 역할 및 책임을 이행한다.

- ① 개인 정보보호 활동 참여
- ② 내부관리계획의 준수 및 이행
- ③ 개인정보의 기술적·관리적 보호조치 기준 이행
- ④ 임직원 또는 제3자에 의한 위법·부당한 개인정보 침해행위에 대한 점검 등

제4장 개인정보 보호 교육

10조. 개인 정보보호 책임자 및 담당자 교육

- 1) 회사는 개인 정보보호 책임자 및 담당자를 대상으로 연2회 이상 개인정보 보호와 관련된 교육을 실시한다.

11조. 개인정보취급자의 교육

- 1) 개인 정보보호 책임자 및 담당자는 개인정보의 적절한 취급을 보장하기 위하여 다음 각 호의 사항을 정하여 개인 정보취급자에게 필요한 개인정보 보호 교육 계획을 수립하고 실시하여야 한다.
 - 교육 목적 및 대상
 - 교육 내용 (개인 정보보호에 관련된 법령, 사례 등)
 - 교육 일정 및 방법 (월 2회)
- 2) 개인 정보보호 책임자 및 담당자는 제4장에 따라 개인정보 보호 교육을 실시한 결과 또는 이를 입증할 수 있는 관련 자료 등을 기록, 보관하여야 한다.

제5장 기술적 안전조치

12조. 접근 권한의 관리

- 1) 회사는 개인 정보 처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.
- 2) 회사는 전보 또는 퇴직 등 인사이동이 발생하여 개인 정보취급자가 변경되었을 경우 지체 없이 개인 정보 처리시스템의 접근 권한을 변경 또는 말소하여야 한다.
- 3) 회사는 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.
- 4) 회사는 개인 정보 처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인 정보취급자 별로 사용자 계정을 발급하여야 하며, 다른 개인 정보취급자와 공유하지 않도록 하여야 한다.
- 5) 회사는 개인 정보처리시스템, 인터넷 홈페이지 등에 개인 정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 다음 각 호의 사항을 적용하여야 한다.
 - ① 영대문자, 영소문자, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성

- ④ IDMS 비밀번호 변경은 계정 연장 신청 시 변경

7) 회사는 권한 있는 개인 정보취급자들의 기술적 관리 보호조치를 아래와 같은 일정으로 시행 관리 한다.

구분	세목	대상자	매년												비고
			1월	2월	3월	4월	5월	6월	7월	8월	9월	10월	11월	12월	
수시점검	개인정보 보호교육 시행	전근로자													월 2회 시행
수시점검	개인정보 보호 점검 시행	전근로자													월 1회 시행
수시점검	개인 컴퓨터 관리	전근로자													상시
수시점검	바이러스 예방	전근로자													상시
수시점검	고객정보 폐기 지침 준수	전근로자													상시
수시점검	개인 사물함 정리 정돈	전근로자													상시
수시점검	이면지 확인	전근로자													상시

13조. 접근통제

1) 회사는 정보통신망을 통한 인가되지 않은 내,외부자의 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 조치를 하여야 한다.

① 개인 정보처리시스템에 대한 접속 권한을 IP(Internet Protocol)주소 등으로 제한하여 인가받지 않은 접근을 제한

② 개인 정보처리시스템에 접속한 IP주소 등을 분석하여 불법적인 개인정보 유출 시도 탐지 및 대응

2) 회사는 개인 정보취급자가 정보통신망을 통해 외부에서 개인 정보처리시스템에 접속하려는 경우 가상사설망(VPN:Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다.

3) 회사는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인 정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치를 하여야 한다.

4) 회사는 고유식별정보를 처리하는 인터넷 홈페이지를 통해 고유식별정보가 유출, 변조, 훼손되지 않도록 연 1회 이상 취약점을 점검하고 필요한 보완 조치를 하여야 한다.

5) 회사는 개인 정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인 정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 하여야 한다.

6) 회사에서 별도의 개인 정보처리시스템을 이용하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 제1항을 적용하지 아니할 수 있으며, 이 경우 업무용 컴퓨터 또는 모바일 기기의 운용체제나 보안프로그램 등에서 제공하는 접근 통제 기능을 이용할 수 있다.

7) 는 업무용 모바일 기기의 분실, 도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.

14조. 개인정보의 암호화

1) 회사는 고유식별번호(주민·여권·운전면허,외국인등록번호), 비밀번호,바이오정보에 대해서는 안전한 암호 알고리즘으로 암호화하여 저장하여야 한다. 단 비밀번호를 저장하는 경우에는 복호화 되지 않도록 일방향 암호화하여 저장하여야 한다.

2) 회사는 고유식별번호 및 비밀번호, 바이오정보를 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 않도록 일방향 암호화(해쉬함수)하여 저장하여야 한다.

3) 제 1항에 따른 개인정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다. 또한 업무와 관련된 메일은 사내 대표 메일만을 사용하여야 한다

4) 회사는 내부망에 고유식별정보를 저장하는 경우에는 암호화 하여야 한다.

5) 회사는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립, 시행하여야 한다.

6) 회사는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

15조. 접속기록의 보관 및 점검

1) 회사는 개인 정보취급자가 개인 정보처리시스템에 접속한 기록을 1년 이상 보관, 관리하여야 한다.

2) 회사는 개인정보의 분실, 도난, 유출, 위조, 변조 또는 훼손 등에 대응하기 위하여 개인 정보처리시스템의 접속기록 등을 반기별로 1회 이상 점검하여야 한다.

3) 회사는 개인 정보취급자의 접속기록이 위,변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.

제6장 정기적인 자체감사

16조. 보안 프로그램 설치 및 운용

1)회사는 악성프로그램 등을 방지, 치료할 수 있는 백신소프트웨어 등의 보안 프로그램을 설치, 운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다.

① 보안프로그램의 자동 업데이트 기능을 사용하거나, 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지.

② 악성프로그램 관련 정보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 즉시 이에 따른 업데이트를 실시

③발견된 악성프로그램 등에 대해 삭제 등 대응 조치

17조. 관리용 단말기의 안전조치

1) 회사는 개인정보 유출 등 개인정보 침해사고 방지를 위하여 관리용 단말기에 대해 다음 각 호의 안전조치를 하여야 한다.