개정 이력

차수	제(개)정 일자	시행일자	주요 개정 내용
1	2017-09-29	2017-09-29	초도 제정
2	2023-12-01	2023-12-01	디오토 상호변경
3	2023-12-05	2023-12-05	정기점검 시행내용변경
4	2024-08-01	2024-08-01	넥스오토 상호변경
5	2024-08-01	2024-08-01	개인정보보호지침 내용변경

목 차

1. 개요

1.1 목적

본 지침은 회사가 정보통신망 이용촉진 및 정보보호 등에 관한 법률 및 개인정보 보호법 등에 따라 처리하는 개인정보가 분실・도난・누출・변조・훼손되지 않도록 회사가 취하여야 하는 보호조치의 구체적인 내용을 정하는 것을 목적으로 한다.

1.2 적용범위

① **본 지침은** 업무 수행을 위하여 회사 서비스 이용자(고객) 및 임직원 개인정보를 취급하는 내/외부 담당자 및 해당 정보를 처리하는 정보시스템에 **적용된다.**

② **본 지침은 서비스 제공을 목적으로 정보통신망을 통하여 수집, 이용, 제공 또는 관리되는 개인정보뿐만 아니라 정보통신망 이외의 수단을 통하여 수집, 이용, 제공 기타 처리되는 개인정보에 관해서도 적용된다**

③ **본 계획에서 언급되지 않는 사항은 관련 법규 및 회사의 기타 사규에 따른다.**

1.3 용어정의

1.3.1 '개인정보'라 함은 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.

1.3.2 '정보주체'라 함은 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.

1.3.3 '개인정보파일'이라 함은 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합체를 말한다.

1.3.4 '처리'란 개인정보의 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그 밖에 이와 유사한 행위를 말한다.

1.3.5 '개인정보 보호책임자'라 함은 개인정보의 처리에 관한 업무를 총괄해서 책임지는 자를 말한다. (정보통신망 이용촉진 및 정보보호 등에 관한 법률상의 개인정보관리책임자와 개인정보보호법상의 개인정보 보호책임자를 총칭한다)

1.3.6 '개인정보 취급자'란 개인정보처리자의 지휘•감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 직접 개인정보에 관한 업무를 담당하는 자와 그 밖에 업무상 필요에 의해 개인정보에 접근하여 처리하는 임직원, 파견근로자, 시간제근로자 등을 말한다.

1.3.7 '개인정보처리시스템'이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다.

1.3.8 '비밀번호'라 함은 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터 또는 정보통신망에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.

1.3.9 '바이오정보'라 함은 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.

1.3.10 '접속기록'이라 함은 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무 내역에 대하여 식별자, 접속일시, 접속지를 알 수 있는 정보, 수행업무 등 접속한 사실을 전자적으로 기록한 것을 말한다.

1.3.11 '정보통신망'이라 함은 전기통신기본법 제2조 제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말한다.

1.3.12 '인증정보'라 함은 개인정보처리시스템 또는 정보통신망을 관리하는 시스템 등이 요구한 식별자의 신원을 검증하는데 사용되는 정보를 말한다.

1.3.13 'P2P(Peer to Peer)'라 함은 정보통신망을 통해 서버의 도움 없이 개인과 개인이 직접 연결되어 파일을 공유하는 것을 말한다.

1.3.14 '공유설정'이라 함은 컴퓨터 소유자의 파일을 타인이 조회•변경•복사 등을 할 수 있도록 설정하는 것을 말한다.

1.3.15 보조저장매체'라 함은 이동형 하드디스크(HDD), USB메모리, CD(Compact Disk), DVD(Digital Versatile Disk), 플로피디스켓 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 용이하게 분리할 수 있는 저장매체를 말한다.

2. 개인정보 보호책임자의 의무와 책임

2.1 개인정보 보호책임자 지정

2.1.1 회사는 개인정보가 분실 · 도난 · 누출 · 변조 · 훼손되는 것을 방지하기 위하여 개인정보의 처리에 관한 업무를 총괄해서 책임지는 개인정보 보호책임자를 지정한다.

2.1.2 개인정보 보호책임자는 「신용정보의 이용 및 보호에 관한 법률」에 의한 신용정보 관리·보호인 또는 개인정보 처리 관련 업무를 담당하는 부서의 장 중에서 지정한다.

2.2 개인정보 보호책임자의 의무와 책임

개인정보 보호책임자는 다음 각 호의 임무를 수행한다.

2.2.1 개인정보 보호 계획의 수립 및 시행

2.2.2 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선

2.2.3 개인정보 처리와 관련한 불만의 처리 및 피해 구제

2.2.4 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축

2.2.5 개인정보 보호 교육 계획의 수립 및 시행

2.2.6 개인정보파일의 보호 및 관리·감독

2.2.7 개인정보취급방침 및 개인정보처리방침의 수립·변경 및 시행

2.2.8 개인정보 보호 관련 자료의 관리

2.2.9 처리목적이 달성되거나 보유기간이 지난 개인정보의 파기

2.3 개인정보취급자의 범위 및 의무와 책임

2.3.1 개인정보취급자는 회사의 지휘·감독을 받아 개인정보를 수집, 보관, 처리, 이용, 제공, 관리 또는 파기 등의 업무를 하는 자를 말한다.

2.3.2 개인정보취급자는 개인정보보호와 관련하여 다음과 같은 역할 및 책임을 이행한다.

① 개인정보보호 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
⑤ 기타 개인정보보호를 위해 필요한 사항의 이행

3. 개인정보의 안전성 확보조치

3.1 개인정보취급자 접근통제 및 인증

3.1.1 회사는 개인정보처리시스템 접근에 대해 통제체계를 수립하여 관리하여야 한다.

3.1.2 회사는 개인정보처리시스템에 대한 접근권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.

3.1.3 회사는 개인정보취급자의 퇴직, 전보 등 인사이동이 발생하는 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소해야 한다.

3.1.4 회사는 개인정보처리시스템에 대한 접근권한 부여, 변경, 말소 등의 내역을 최소 5년간 보관한다.

3.1.5 회사는 개인정보처리시스템에 접속할 수 있는 사용자 계정을 발급하는 경우, 개인정보취급자 별로 한 개의 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

3.1.6 회사는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 가상사설망(VPN), 전용선 등의 안전한 접속 수단과 공인인증서 등의 안전한 인증 수단을 적용하여야 한다.

3.2 개인정보의 암호화

3.2.1 회사는 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호, 비밀번호, 신용카드번호, 계좌번호, 바이오정보를 정보통신망을 통하여 송•수신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.

3.2.2 회사는 비밀번호, 바이오정보는 복호화되지 않도록 일방향 암호화하여 저장하여야 한다. 단, EMV(국제 신용카드규격)에 따라 3DES 암호화 방식이 적용되는 카드 비밀번호는 예외로 한다.

3.2.3 회사는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ: Demilitarized Zone)에 고유식별정보 등 주요정보를 저장 및 관리하지 아니하여야 한다. 단, 거래로그를 관리하기 위한 경우에는 예외로 하되 이 경우 반드시 암호화하여 저장·관리하고 업무목적이 종료된 경우에는 주요정보를 포함한 거래로그 폐기 등 보호조치를 시행하여야 한다.

3.2.4 회사는 정보통신망을 통해 이용자의 개인정보 및 인증정보를 송•수신할 때에는 안전한 보안서버 구축 등의 조치를 통해 이를 암호화해야 한다. 보안서버는 다음 각 호 중 하나의 기능을 갖추어야 한다.

① 웹서버에 SSL(Secure Socket Layer) 인증서를 설치하여 전송하는 정보를 암호화하여 송•수신하는 기능
② 웹서버에 암호화 응용프로그램을 설치하여 전송하는 정보를 암호화하여 송•수신하는 기능
③ 기타 인터넷 망의 경우 VPN을 설치하여 전송하는 정보를 암호화하여 송•수신하는 기능

3.2.5 개인정보처리자는 업무용 컴퓨터에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화 저장하여야 한다.

3.3 접속기록의 위변조 방지

3.3.1 회사는 개인정보처리시스템에 대한 개인정보취급자의 접속내역을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 6개월 이상 보관·관리하여야 한다.

3.3.2 회사는 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 별도 저장장치 등에 정기적으로 백업하여 안전하게 보관하여야 한다.

3.4 보안프로그램의 설치 및 운영

3.4.1 회사는 개인정보처리시스템 및 개인정보취급자의 업무용 컴퓨터 등에 악성 프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안프로그램을 설치·운영해야 한다.

3.4.2 회사는 제1항의 보안프로그램의 자동 업데이트 기능을 사용하거나, 월 1회 이상 주기적으로 업데이트를 실시해야 한다.

3.4.3 회사는 악성 프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 실시해야 한다.

3.5 개인정보처리시스템 보안

3.5.1 회사는 외부 네트워크를 내부 네트워크에 연결할 경우 내부 네트워크를 보호하기 위해서 침입차단시스템(FW)과 침입탐지시스템(IPS 등)을 설치·운용하여야 한다.

3.5.2 회사는 개인정보취급자를 대상으로 다음 각 호의 사항을 포함하는 비밀번호 작성규칙을 수립하고, 이를 적용·운용하여야 한다.

① 다음 각 목의 문자 종류 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성

a. 영문 대문자(26개)
b. 영문 소문자(26개)
c. 숫자(10개)
d. 특수문자(32개)

② 연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않는 것을 권고

③ 비밀번호에 유효기간을 설정하여 분기별 1회 이상 변경

3.5.3 회사는 고객, 직원 등이 안전한 비밀번호를 이용할 수 있도록 비밀번호 작성규칙을 수립하고, 이행한다.

3.5.4 회사는 취급 중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통해 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 PC에 조치를 취하여야 한다.

3.6 물리적 접근제한

3.6.1 회사는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를

별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립 · 운영하여야 한다.

3.6.2 회사는 개인정보가 포함된 서류, 보조저장매체 등을 잠금 장치가 있는 안전한 장소에 보관하여야 한다.

3.7 **출력 및 복사 시 보호조치**

3.7.1 개인정보취급자는 개인정보처리시스템에서 개인정보의 출력 시(인쇄, 화면표시, 파일생성 등) 용도를 특정하여야 하며, 용도에 따라 출력 항목을 최소화 한다.

3.7.2 회사는 개인정보가 포함된 종이 인쇄물, 개인정보가 복사된 외부 저장매체 등 개인정보의 출력•복사물을 안전하게 관리하기 위해 출력•복사 기록 등 필요한 보호조치를 갖추어야 한다.

3.8 **정보보호책임자의 의무와 책임**

정보보호책임자(CSO)는 개인정보의 안전성 확보 조치 계획의 수립, 시행 및 관리, 감독 임무를 수행한다.

4. 정보보호 교육 및 정기 감사

4.1 개인정보보호 교육

4.1.1 회사는 개인정보 보호 및 침해사고 예방을 위하여 다음과 같이 개인정보보호 교육을 실시한다.

① 교육횟수: 연 1회 이상

② 교육대상: 개인정보 보호책임자, 개인정보취급자

③ 교육내용 및 방법: 개인정보의 안전한 처리 및 침해사고 예방을 위한 교육을 실시하며, 전체 집체 교육, 부서별 교육, 그룹웨어 활용 교육 등 구체적 상황에 맞는 방법을 통해 교육을 실시한다.

※ 온라인을 통한 교육도 병행한다.

4.1.2 개인정보 보호책임자는 교육실시 내역에 대한 근거자료를 최소 3년간 보관해야 한다.

4.2 정기 점검의 시행

4.2.1 회사는 개인정보의 기술적·관리적 보호조치가 제대로 이행되고 있는지를 정기적으로 점검하여야 한다.

- **상/하반기 담당 임원 주관 개인정보취급자를 대상으로 개인정보 보호조치여부 점검. (6월/12월)**

4.2.2 회사는 임직원 및 이용자의 개인정보를 위탁 처리하는 협력사를 대상으로 정기적인 관리·감독을 실시하여야 한다.