	대표	부문장	실장
결재			

유니원커뮤니케이션즈
개인정보 내부 관리계획

2026. 01. 30. (신규제정)

목 차

제1장 총 칙

제1조(목적) 유니원커뮤니케이션즈(이하 '회사') 개인정보 내부 관리계획은 「개인정보 보호법」 제29조와 같은 법 시행령 제30조 그리고 '개인정보의 안전성 확보조치 기준'(제2016-35호)에 따라 개인정보를 처리함에 있어서 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 및 물리적 안전조치에 관한 사항을 정하는 것을 목적으로 한다.

제2조(용어 정의) 개인정보 내부 관리계획에서 사용하는 용어의 뜻은 다음과 같다.

1. "개인정보"란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 쉽게 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.
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. "정보주체"란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
4. "개인정보파일"이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.
5. "개인정보처리자"란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.
6. "개인정보 보호책임자"란 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지는 자로서 영 제32조제2항에 해당하는 자를 말한다.
7. "개인정보 보호담당자"라 함은 개인정보 보호책임자를 보좌하여 개인정보보호업무에 대한 실무를 총괄하고 관리하는 자를 말한다.
8. "개인정보취급자"란 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 임직원, 파견근로자, 시간제근로자 등을 말한다.
9. "개인정보처리시스템"이란 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템을 말한다.
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.
11. "비밀번호"란 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터 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.

12. "정보통신망"이란 「전기통신기본법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말한다.
13. "공개된 무선망"이란 불특정 다수가 무선접속장치(AP)를 통하여 인터넷을 이용할 수 있는 망을 말한다.
14. "모바일 기기"란 무선망을 이용할 수 있는 PDA, 스마트폰, 태블릿PC 등 개인정보처리에 이용되는 휴대용 기기를 말한다.
15. "바이오정보"란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.
16. "보조저장매체"란 이동형 하드디스크, USB메모리, CD(Compact Disk), DVD(Digital Versatile Disk) 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 용이하게 연결·분리할 수 있는 저장매체를 말한다.
17. "내부망"이란 물리적 망분리, 접근 통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.
18. "접속기록"이란 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무 내역에 대하여 개인정보취급자 등의 계정, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 전자적으로 기록한 것을 말한다. 이 경우 "접속"이란 개인정보처리시스템과 연결되어 데이터 송신 또는 수신이 가능한 상태를 말한다.

제3조(적용 범위) 회사가 개인정보를 처리하거나 회사의 개인정보 처리 업무를 위탁받아 처리하는 수탁자에게는 본 개인정보 내부 관리계획이 적용된다.

제2장 내부 관리계획의 수립 및 시행

제4조(내부 관리계획의 수립 및 승인) ① 개인정보 보호담당자는 회사가 개인정보보호를 위한 전반적인 사항을 포함하여 관련한 법령 및 규정 등을 준수할 수 있도록 내부 의사결정 절차를 통하여 내부 관리계획을 수립하여야 한다.

② 개인정보 보호담당자는 내부 관리계획의 각 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부 관리계획을 수정하여야 한다.

③ 개인정보 보호담당자는 제1항, 제2항에 따라 내부 관리계획을 수립하거나 수정하는 경우에는 개인정보 보호책임자로부터 내부결재 등의 승인을 받아야 하며, 그 이력을 보관·관리하여야 한다.

④ 개인정보처리자는 내부 관리계획의 세부 이행을 위한 각종 지침 등을 마련하여

시행할 수 있다.

⑤ 개인정보 보호책임자는 연 1회 이상으로 내부 관리계획의 이행 실태를 점검·관리하고 그 결과에 따라 적절한 조치를 취하여야 한다.

⑥ 개인정보 보호책임자는 점검 결과 미흡 사항이 확인된 경우 필요한 개선조치를 시행하고, 그 결과를 기록·관리하여야 한다.

제5조(내부 관리계획의 공표) ① 개인정보 보호책임자는 제4조제3항에 따라 승인된 내부 관리계획을 모든 임직원 및 관련자에게 알림으로써 이를 준수하도록 하여야 한다.
② 내부 관리계획은 임직원 등이 언제든지 열람할 수 있는 방법으로 비치하거나 제공하여야 한다.

제3장 개인정보 보호책임자의 역할 및 책임

제6조(개인정보 보호책임자의 지정) ① 회사는 「개인정보 보호법」 제31조와 같은 법 시행령 제32조에 따라 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자를 개인정보 처리 관련 업무를 담당하는 부서의 장으로 정한다.

제7조(개인정보 보호책임자의 역할 및 책임) ① 개인정보 보호책임자는 다음 각 호의 업무를 수행한다.

1. 개인정보 보호 계획의 수립 및 시행
2. 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
3. 개인정보 처리와 관련한 불만의 처리 및 피해 구제
4. 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
5. 개인정보 보호 교육 계획의 수립 및 시행
6. 개인정보파일의 보호 및 관리 감독
7. 「개인정보 보호법」 제30조에 따른 개인정보 처리방침의 수립·변경 및 시행
8. 개인정보 보호 관련 자료의 관리
9. 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기

② 개인정보 보호책임자는 제1항의 업무를 수행함에 있어서 필요한 경우 개인정보의 처리 현황, 처리 체계 등에 대하여 수시로 조사하거나 관계 당사자로부터 보고를 받을 수 있다.
③ 개인정보 보호책임자는 개인정보 관련 업무의 효율적 운영을 위하여 개인정보 관리 전담부서의 직원 중 1인 이상을 개인정보 보호 담당자로 임명한다.

제10조(개인정보의 수집에 대한 고지) ① 정보주체로부터 제9조 1항의 규정에 의한 동의를 받고자 하는 경우 또는 개인정보를 제3자로부터 제공받은 경우에는 미리 다음 각 호의 사항을 서면 또는 인터넷 홈페이지 등을 통하여 내용을 쉽게 확인할 수 있도록 정보주체에게 고지하거나 서비스 이용약관에 명시하여야 한다.

1. 개인정보보호책임자의 성명, 소속, 전화번호, 전자우편주소
2. 개인정보의 구체적인 수집목적 및 이용목적
3. 동의 철회, 열람 또는 정정 요구 등 정보주체 및 법정대리인의 권리와 그 행사방법
4. 정보주체로부터 수집하고자 하는 개인정보 항목
5. 수집하는 개인정보의 보유·이용기간 및 법적 근거 등 보유 근거
6. 기타 개인정보에 대한 처리 또는 관리 방식

제11조(개인정보 취급자의 제한) ① 개인정보 보호책임자는 개인정보를 취급할 수 있는 자를 다음 각 호의 1에 해당하는 자로 정하여 최소한으로 제한하여야 한다.

1. 정보주체를 직접 상대로 하여 업무를 수행하는 자
2. 개인정보 보호책임자 등 개인정보관리 업무를 수행하는 자
3. 데이터베이스를 포함한 전산 관련 업무를 수행하는 자
4. 기타 업무상 개인정보의 취급이 불가피한 자

제5장 개인정보 보호 교육

제12조(개인정보 보호책임자의 교육) ① 회사는 개인정보 보호책임자를 대상으로 연 1회 이상 개인정보 보호와 관련된 교육을 실시한다.

제13조(개인정보취급자의 교육) ① 개인정보 보호책임자는 개인정보의 적정한 취급을 보장하기 위하여 다음 각 호의 사항을 정하여 개인정보취급자에게 필요한 개인정보 보호 교육 계획을 수립하고 실시하여야 한다.

1. 교육 목적 및 대상
2. 교육 내용
3. 교육 일정 및 방법

② 개인정보 보호책임자는 제4장에 따라 개인정보 보호 교육을 실시한 결과 또는 이를 입증할 수 있는 관련 자료 등을 기록·보관하여야 한다.

제10조(개인정보의 수집에 대한 고지) ① 정보주체로부터 제9조 1항의 규정에 의한 동의를 받고자 하는 경우 또는 개인정보를 제3자로부터 제공받은 경우에는 미리 다음 각 호의 사항을 서면 또는 인터넷 홈페이지 등을 통하여 내용을 쉽게 확인할 수 있도록 정보주체에게 고지하거나 서비스 이용약관에 명시하여야 한다.

1. 개인정보보호책임자의 성명, 소속, 전화번호
2. 개인정보의 구체적인 수집목적 및 이용목적
3. 동의 철회, 열람 또는 정정 요구 등 정보주체 및 법정대리인의 권리와 그 행사방법
4. 정보주체로부터 수집하고자 하는 개인정보 항목
5. 수집하는 개인정보의 보유·이용기간 및 법적 근거 등 보유 근거
6. 기타 개인정보에 대한 처리 또는 관리 방식

제11조(개인정보 취급자의 제한) ① 개인정보 보호책임자는 개인정보를 취급할 수 있는 자를 다음 각 호의 1에 해당하는 자로 정하여 최소한으로 제한하여야 한다.

1. 정보주체를 직접 상대로 하여 업무를 수행하는 자
2. 개인정보 보호책임자 등 개인정보관리 업무를 수행하는 자
3. 데이터베이스를 포함한 전산 관련 업무를 수행하는 자
4. 기타 업무상 개인정보의 취급이 불가피한 자

제5장 개인정보 보호 교육

제12조(개인정보 보호책임자의 교육) ① 회사는 개인정보 보호책임자를 대상으로 연 1회 이상 개인정보 보호와 관련된 교육을 실시한다.

제13조(개인정보취급자의 교육) ① 개인정보 보호책임자는 개인정보의 적정한 취급을 보장하기 위하여 다음 각 호의 사항을 정하여 개인정보취급자에게 필요한 개인정보 보호 교육 계획을 수립하고 실시하여야 한다.

1. 교육 목적 및 대상
2. 교육 내용
3. 교육 일정 및 방법

② 개인정보 보호책임자는 제4장에 따라 개인정보 보호 교육을 실시한 결과 또는 이를 입증할 수 있는 관련 자료 등을 기록·보관하여야 한다.

제6장 기술적 안전조치

제14조(접근 권한의 관리) ① 회사는 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.

② 회사는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체없이 개인정보처리시스템의 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 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자 별로 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

⑤ 회사는 개인정보처리시스템, 접근통제시스템, 인터넷 홈페이지 등에 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 다음 각 호의 사항을 적용하여야 한다.

1. 문자, 숫자의 조합·구성에 따라 최소 8자리 또는 10자리 이상의 길이로 구성
   - 최소 8자리 이상 : 두 종류 이상의 문자를 이용하여 구성한 경우
     ※ 문자 종류 : 알파벳 대문자와 소문자, 특수문자, 숫자
   - 최소 10자리 이상 : 하나의 문자종류로 구성한 경우
     ※ 단, 숫자로만 구성할 경우 취약할 수 있음
2. 비밀번호는 추측하거나 유추하기 어렵도록 설정
   - 동일한 문자 반복(aaabbb, 123123 등), 키보드 상에서 나란히 있는 문자열(qwer 등), 일련번호(12345678 등), 가족이름, 생일, 전화번호 등은 사용하지 않음
3. 비밀번호가 제3자에게 노출되었을 경우 지체 없이 새로운 비밀번호로 변경해야 함

⑥ 회사는 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 한다.

제15조(접근통제) ① 회사는 정보통신망을 통한 인가되지 않은 내·외부자의 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 조치를 하여야 한다.

1. 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol)주소 등으로 제한하여 인가받지 않은 접근을 제한
2. 개인정보처리시스템에 접속한 IP(Internet Protocol)주소 등을 분석하여 불법적인

개인정보 유출 시도 탐지 및 대응

② 회사는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 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 개인정보처리시스템, 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 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 하여야 한다.

⑥ 회사에서 별도의 개인정보처리시스템을 이용하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 제1항을 적용하지 아니할 수 있으며, 이 경우 업무용 컴퓨터 또는 모바일 기기의 운영체제(OS : Operating System)나 보안프로그램 등에서 제공하는 접근 통제 기능을 이용할 수 있다.

⑦ 회사는 업무용 컴퓨터 또는 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.

⑧ 회사는 보안 패치 미적용, 백신 미설치, 공용 컴퓨터 등 보안성이 낮은 기기 환경에서 개인정보 취급이 발생하지 않도록 사전 고지하고, 개인정보취급자의 개인정보 열람·처리·저장·전송 행위를 업무 기준 및 관리 절차에 따라 제한하여야 한다.

제16조(개인정보의 암호화) ① 회사는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하는 경우에는 이를 암호화하여야 한다.

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

③ 회사는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.

④ 회사가 내부망에 고유식별정보를 저장하는 경우에는 암호화 하여야 한다. 다만, 위험도 분석 결과에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.

⑤ 회사는 제1항, 제2항, 제3항, 또는 제4항에 따라 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.

⑥ 회사는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다.

⑦ 회사는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

제17조(접속기록의 보관 및 점검) ① 회사는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 보관·관리하여야 한다. 다만, 5만 명 이상의 정보주체에 관하여 개인정보를 처리하거나, 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다.

② 회사는 개인정보의 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 특히 개인정보를 다운로드한 것이 발견되었을 경우에는 내부 관리계획으로 정하는 바에 따라 그 사유를 반드시 확인하여야 한다.

③ 회사는 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.

제18조(악성프로그램 등 방지) ① 회사는 악성프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다.

1. 보안 프로그램의 자동 업데이트 기능을 사용하거나, 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지
2. 악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 즉시 이에 따른 업데이트를 실시
3. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치

제7장 관리적 안전조치

제19조(개인정보 보호조직 구성 및 운영) ① 회사는 개인정보의 안전한 처리를 위하여 다음 각 호의 사항을 포함하는 개인정보 보호 TF팀을 구성하고 운영하여야 한다.

1. 개인정보 보호책임자의 지정
2. 개인정보 보호책임자의 지휘·감독 하에 개인정보 보호책임자의 업무를 지원하는 담당자의 지정
3. 개인정보를 처리하는 개인정보취급부서의 지정

② 개인정보 보호 TF팀의 설치, 변경 및 폐지는 대표 및 임원진으로부터 승인을 받아 정한다.

③ 개인정보취급부서에서는 개인정보 보호 TF팀과 충분히 협의, 조정하여 개인정보를 처리하여야 한다.

④ 개인정보 보호 TF팀은 제7조에 따른 업무를 수행하여야 하며, 그 밖에 개인정보의 안전성 확보를 위하여 회사가 필요하다고 판단되는 사항을 수행할 수 있다.

제20조(개인정보 유출 사고 대응) ① 회사는 개인정보의 유출 사고 발생 시 신속한 대응을 통해 피해 발생을 최소화하기 위해 개인정보 유출 사고 대응 계획을 수립하고 시행하여야 한다.

② 제1항에 따른 개인정보 유출 사고 대응 계획에는 긴급조치, 유출 통지·조회 및 신고 절차, 고객 민원 대응조치, 현장 혼잡 최소화 조치, 고객불안 해소조치, 피해자 구제조치 등을 포함하여야 한다.

③ 회사는 개인정보 유출에 따른 피해복구 조치 등을 수행함에 있어 정보주체의 불편과 경제적 부담을 최소화할 수 있도록 노력하여야 한다.

제21조(개인정보 최소 제공 및 마스킹 기준) ① 회사는 개인정보의 처리, 내부 공유, 보고, 점검 및 감사 대응 과정에서 개인정보의 과도한 노출을 방지하기 위하여 업무 목적 달성에 필요한 최소한의 개인정보만 제공하여야 한다.

② 제1항에 따라 개인을 직접 식별할 필요가 없는 경우에는 성명, 사번, 연락처, 계정정보 등 개인정보에 대해 일부 마스킹 또는 비식별 처리 기준을 적용하여 제공한다.

③ 마스킹 적용 대상 개인정보 항목, 처리 방식 및 적용 기준은 내부관리계획에 포

함하여 운영하며, 개인정보취급자에게 사전 고지하여 준수하도록 한다.

④ 마스킹 기준의 적용 여부 및 예외 사항은 개인정보 보호책임자의 관리 하에 운영될 수 있다.

제22조(개인정보 처리업무의 위탁 관리) ① 회사는 개인정보 처리업무를 외부에 위탁하는 경우, 위탁받는 자가 개인정보를 안전하게 처리하도록 관리·감독하여야 한다.

② 회사는 개인정보 처리업무를 위탁하는 경우, 위탁의 목적, 범위, 개인정보 보호 관련 사항을 계약서 또는 이에 준하는 문서에 명시하여야 한다.

③ 개인정보 보호책임자는 개인정보 유출 등 문제가 발생한 경우 또는 필요한 경우에 한하여 수탁자의 개인정보 처리와 관련된 사항을 확인할 수 있다.

제8장 물리적 안전조치

제23조(물리적 안전조치) ① 회사는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 한다.

② 회사는 개인정보가 포함된 서류를 잠금장치가 있는 안전한 장소에 보관하여야 한다.

③ 회사는 개인정보가 포함된 보조 저장매체를 별도로 사용하지 않는다. 불가피하게 사용하는 경우에는 개인정보 보호책임자의 사전 승인 하에 관리 절차에 따라 사용한다.

제24조(개인정보의 파기) ① 회사는 개인정보를 파기할 경우 다음 각 호 중 어느 하나의 조치를 하여야 한다.

1. 완전파괴(소각·파쇄 등)
2. 전용 소자장비를 이용하여 삭제
3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

② 회사는 개인정보의 일부만을 파기하는 경우, 제1항의 방법으로 파기하는 것이 어려울 때에는 다음 각 호의 조치를 하여야 한다.

1. 전자적 파일 형태인 경우 : 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독

2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 해당 부분을 마스킹, 천공 등으로 삭제