kt ds

개인정보 내부관리계획서

2020. 07.13

정보보안센터

본 자료는 기업비밀(Ⅲ)로서 사내 직원 외 타인의 열람, 취급과 외부유출(반출)을 금하며, 위반 시에는 관련 법령 및 사규에 의거 처벌됩니다

제·개정 이력

문서번호	SEC-PO-002
문 서 명	SEC-PO-002-개인정보 내부관리계획서
비밀구분	대외비

No.	개정일자	버전	개정 내용 요약	비고
1	2015.06.19	1.0	신규 제정	제정
2	2016.01.12	1.1	개인정보 누출 통지 조항 추가	개정
3	2016.06.27	1.2	정보통신망법[시행2016.9.23] 개정 및 관련 고시 내용 반영, 개인정보보호법 개정[시행2016.9.30] 반영	개정
4	2017.12.08	1.3	개인정보보호법[시행2017.10.19] 개정 내용 반영 및 용어 보완	개정
5	2018.12.14	1.4	- '개인정보처리자'와 '개인정보취급자'의 의미 구분 명확화 - 조직개편 내용 반영(부서 현행화) - 고유식별번호 범위(여권번호) 추가 - 타 법령에 따른 개인정보 보유기준 추가 - 제3자 제공 동의(기재)항목 추가 - 위험도 분석 및 대응 조항 추가 - 재해 및 재난 대비 안전조치 조항 추가	개정
6	2019.09.16	1.5	개인정보의 안전성 확보조치 기준[시행2019.06.07] 개정 내용 반영	개정
7	2020.07.13	1.6	데이터3법 따른 정보통신망법, 개인정보보호법 개정 사항 반영	개정

목 차

2015.06.19 제정
2016.01.15 개정
2016.06.27 개정
2017.12.08 개정
2018.12.14 개정
2019.09.16 개정
2020.07.13 개정

제1장 총 칙

제1조(목적)

본 계획은 개인정보보호법의 내부관리계획의 수립 및 시행 의무에 따라 제정된 것으로 ㈜케이티디에스(이하 "회사"라 함)가 처리하는 모든 정보를 보호함에 있어 필요한 세부적인 사항에 관해 규정함으로써 정보의 분실, 도난, 유출·위조·변조 또는 훼손, 오·남용 등이 되지 아니하도록 함을 목적으로 한다.

제2조(적용범위)

본 계획은 정보통신망, 서면 등을 통하여 수집, 이용, 제공 또는 관리되는 모든 정보에 대해서 적용하며, 이러한 정보를 처리하는 내부 임직원 및 협력사 직원에 대해 적용된다.

제3조(용어 정의)

이 계획에서 사용하는 용어의 정의는 다음 각 호와 같다.

1. "정보보호"라 함은 정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 발생할 수 있는 정보의 훼손, 위조·변조, 유출 등을 방지하기 위한 기술적·관리적 수단을 마련하고 수행하는 것을 말한다.
2. "개인정보"라 함은 회사가 서비스 제공을 위해 고객으로부터 제공받은 주민등록번호 등 특정 개인을 식별할 수 있는 정보와 통화내역, 서비스이용 기록, 구매내역 등 서비스를 이용하는 과정에서 생성되는 정보, 다른 정보와 용이하게 결합하여 개인 식별이 가능한 정보 등 특정

개인과 관련된 모든 정보 및 가명정보를 말한다.

3. "가명정보"라 함은 가명 처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용 결합 없이는 특정 정보를 알아볼 수 없는 정보를 말한다.
4. "가명처리"라 함은 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것을 말한다.
5. "민감정보"라 함은 사상, 신념, 노동조합/정당의 가입/탈퇴, 정치적 견해, 건강, 성생활, 유전정보, 범죄경력자료 등으로서 정보주체의 사생활을 현저히 침해할 우려가 있는 대통령령으로 정하는 개인정보
6. "정보보호최고책임자(CISO)" 라 함은 회사 정보보호 분야 기획과 집행의 조정, 통제 등 정보보호 업무의 총괄 기능을 수행하는 자를 말한다.
7. "개인정보보호책임자"라 함은 회사 내에서 개인정보를 처리하는 업무 및 사업을 주관하는 임원이나, 회사의 개인정보보호 업무 및 조직을 총괄하는 자를 말한다.
8. "개인정보처리자"라 함은 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.
9. "개인정보취급자"라 함은 개인정보처리자의 지휘·감독을 받아 개인정보를 처리(개인정보의 수집, 생성, 연계, 연동 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기 그 밖에 이와 유사한 행위)하는 업무를 담당하는 자로서 내부 임직원 및 협력사 직원 등을 말한다.
10. "개인정보처리시스템"이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템 및 이용자의 개인정보를 보관·처리하는 파일시스템 등을 말한다.
11. "접속기록"이라 함은 이용자 또는 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무 내역에 대하여 개인정보취급자 등의 계정, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등 접속한 사실을 전자적으로 기록한 것을 말한다.
12. "패스워드"라 함은 "비밀번호"라고 표기하기도 하며, 이용자 및 개인정보취급자 등이 시스템 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.

13. "보안서버"라 함은 정보통신망에서 송·수신하는 정보를 암호화하여 전송하는 웹서버를 말한다.
14. "인증정보"라 함은 개인정보처리시스템 또는 정보통신망을 관리하는 시스템 등이 요구한 식별자의 신원을 검증하는데 사용되는 정보를 말한다.
15. "협력사"라 함은 회사와 계약을 통해 업무의 일부를 위탁 받거나 회사에 용역을 제공하는 법인으로서, 업무상 회사 정보시스템에 접속하거나 회사의 정보 및 개인정보 처리하는 법인을 말한다.
16. "협력사 직원"이라 함은 회사와 계약 또는 제휴를 맺은 협력사 소속직원과 협력사와 계약에 의해 위탁 또는 제휴 업무를 수행하는 모든 인력을 말한다.

제2장 내부관리계획의 수립 및 시행

제4조(내부관리계획의 수립)

① 개인정보보호책임자는 회사의 개인정보 보호를 위한 전반적인 사항을 포함하여 개인정보 보호에 관한 내부관리계획을 수립하여야 하며, 개인정보보호와 관련한 법령 및 관련 규정을 준수하도록 수립하여야 한다.

② 개인정보보호책임자는 개인정보보호 관련 법령의 제·개정 사항 등을 반영하기 위하여 주기적으로 내부관리계획의 타당성과 개정 필요성을 검토하고, 개정할 필요가 있다고 판단되는 경우 개정안을 작성하여야 한다.

제5조(내부관리계획의 공표)

① 개인정보보호책임자는 제4조에 따라 수립한 내부관리계획을 회사 임직원들에게 공표하여야 한다.

② 내부관리계획은 임직원이 언제든지 열람할 수 있는 방법으로 사내 게시판 등에 게시 또는 비치하여야 하며, 변경사항이 있는 경우에는 이를 공지하여야 한다.

제3장 개인정보보호책임자의 의무와 책임

제6조(개인정보보호책임자 지정)

① 회사는 다음 각 호의 어느 하나에 해당하는 지위에 있는 자 중에서 1인 이상을 개인정보보호책임자로 임명하여야 한다.

1. 회사의 임원
2. 개인정보와 관련하여 고객의 고충처리를 담당하는 부서의 장

② 제1항에 의한 회사 개인정보보호를 총괄하는 개인정보보호책임자는 정보보호최고책임자(CISO)인 정보보안센터장으로 임명한다.

제7조(개인정보보호책임자의 역할과 책임)

① 개인정보보호책임자는 개인정보보호를 위하여 다음 각 호의 임무를 수행한다.

1. 개인정보보호 관련 의무와 책임의 규정 및 총괄관리
2. 개인정보보호 내부관리계획의 수립 총괄
3. 개인정보의 기술적·관리적 보호조치 기준 이행 총괄
4. 임직원 또는 제3자에 의한 위법·부당한 개인정보 침해행위에 대한 점검, 대응, 사후 조치 총괄
5. 고객으로부터 제기되는 개인정보에 관한 고충이나 의견의 처리 및 감독 총괄
6. 임직원 및 개인정보처리업무 수탁자 등에 대한 교육 총괄
7. 본 규정에 명시된 개인정보보호와 관련된 제반 조치의 시행 총괄
8. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항
9. 개인정보의 분실, 도난, 훼손, 위조·변조, 유출 등이 발생한 경우의 대응 절차 및 방법에 관한 사항
10. 기타 고객의 개인정보보호에 필요한 사항

② 개인정보보호책임자는 개인정보취급자를 최소한으로 제한하여 지정하고 수시로 관리·감독하여야 하며, 임직원에 대한 교육 및 보안서약 등을 통해 개인정보 침해사고를 사전에 예방한다.

③ 개인정보보호책임자는 개인정보 관련 업무의 효율적 운영을 위하여 부서 개인정보관리자를 1인 이상 임명할 수 있다.
④ 개인정보를 처리하는 부서의 경우 부서 개인정보관리자를 지정하여야 하며, 해당 부서장으로 한다.
⑤ 개인정보보호책임자는 법 위반 사실 인지 시 즉시 개선조치를 시행하고, 필요하면 사업주 또는 대표자에게 개선조치를 보고한다.

제8조(개인정보취급자의 범위 및 의무와 책임)

① 개인정보취급자의 범위는 회사 내에서 개인정보 수집, 보관, 이용, 제공, 관리 또는 파기 등의 업무를 수행하는 자를 말하고, 정규직 이외에 임시직, 계약직 직원 그리고 협력사 직원 등에도 포함된다.
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. 기타 고객의 개인정보보호를 위해 필요한 사항의 이행

제9조(개인정보보호 교육 및 훈련)

① 개인정보보호책임자는 개인정보보호에 대한 직원들의 인식제고를 위해 노력해야 하며, 개인정보의 오용 또는 유출 등을 적극 예방하기 위해 개인정보취급자를 대상으로 매년 정기적으로 아래의 내용을 포함하여 연 1회 이상의 개인정보보호 교육을 수립·실시한다.
1. 교육 목적 및 대상
2. 교육 내용
3. 교육 일정 및 방법
② 교육 방법은 집체 교육뿐만 아니라, 인터넷 교육, 그룹웨어 교육 등 다양한 방법을 활용하여 실시하고, 필요한 경우 외부 전문기관이나 전문요원에 위탁하여 교육을 실시할 수 있다.
③ 개인정보보호에 대한 중요한 전파 사례가 있거나 개인정보보호 업무와 관련하여 변경된 사항이 있는 경우, 개인정보보호책임자는 수시 교육을 실시

할 수 있다.

④ 개인정보보호 교육 시행 시 교육참석자의 본인 확인이 가능한 기록을 보유하여야 한다.

⑤ 교육 훈련 효과를 높이기 위하여 교육 훈련에 대한 기록(교육 주제, 참석자, 교육 자료 등)을 남기고 교육 훈련 후 검토를 통한 교육 훈련 결과가 차기 교육에 반영하도록 한다.

제4장 개인정보의 기술적·관리적·물리적 조치

제10조(개인정보의 수집, 이용 동의)

① 개인정보를 수집하는 경우, 그 목적에 필요한 최소한의 개인정보를 수집하고, 개인정보의 수집·이용목적, 수집하는 개인정보의 항목, 개인정보의 보유 및 이용기간 등을 알리고 동의를 얻어야 한다. 단, 필요한 최소한의 개인정보 이외의 개인정보를 제공하지 아니한다는 이유로 그 서비스의 제공을 거부하여서는 안 된다. 이 경우 필요한 최소한의 개인정보는 해당 서비스의 본질적 기능을 수행하기 위하여 반드시 필요한 정보를 말한다.
또한, 수집동의 획득 시, 개인정보보호법 시행규칙에 따라 동의서 내용을 정보주체가 알아보기 쉽게 표기해야 한다.

② 개인정보의 수집·이용·제공·위탁 시 항목별로 개별동의를 얻도록 하여 개인정보 활용 여부에 대한 이용자의 선택권을 보장하도록 해야 한다. 또한 서비스 제공을 위한 계약 체결과 개인정보 활용에 대한 동의를 구분하여야 한다.

③ 개인정보는 동의 받은 이용목적 범위 내에서만 이용해야 하며, 공개된 개인정보(전화번호부, 공개된 게시판 등)라도 공개목적 이외에는 이용하면 안 된다.

④ 개인정보를 수집하는 목적은 명확히 특정되어 있어야 하며, 목적을 달성하기 위하여 직접적으로 필요한 범위 내에서 최소한의 정보만 수집하여야 하고, 서비스 제공과 관련 없는 고유식별번호(주민번호, 여권번호, 면허번호, 외국인등록번호) 및 종교, 사상 등 민감한 개인정보는 수집하면 안 된다.

⑤ 필수 서비스 외에 부가서비스, 제휴 등의 서비스 및 개인정보 제공을 거부한다는 이유로 필수 서비스의 제공을 거부하여서는 안된다.

⑥ 관련 법령에 의해 주민번호 대체수단 적용 요건을 갖춘 웹사이트는 주민등록번호 이외의 본인확인 수단을 제공해야 한다.

⑦ 개인정보의 수집·이용, 제공·위탁에 대한 동의의 보호조치 방법은 "개인정보보호가이드"를 참조한다.

⑧ 개인정보처리자가 정보주체 이외로부터 수집한 개인정보를 처리하는 때에는 정보주체의 요구가 있으면 즉시 관련 사항(개인정보의 수집 출처, 개인정보의 처리 목적 등)을 정보주체에게 알려야 한다.

제11조(만14세 미만 아동의 동의 획득)

① 만 14세 미만의 아동의 경우 개인정보 수집·이용·제공 등의 동의를 받으려면 그 법정 대리인의 동의를 받아야 한다. 이 경우 법정대리인의 동의를 받기 위하여 필요한 최소한의 정보는 법정대리인의 동의 없이 해당 아동으로부터 직접 수집할 수 있다.

② 법정대리인은 만 14세 미만 아동의 개인정보 수집·이용·제공 등의 철회, 열람 또는 오류 정정 등의 요구를 할 수 있다.

③ 제2항에 따라 수집한 법정대리인의 개인정보는 법정대리인의 동의를 얻기 위한 목적으로만 이용하여야 하며, 법정대리인의 동의 거부가 있거나 동의 의사가 확인되지 않는 경우 파기하여야 한다.

④ 법정대리인으로부터 동의를 획득하는 방법은 서면이나 전자적인 방법으로 할 수 있으며, 전자적인 방법으로 이용하고자 할 경우에는 SMS, 공인인증서, 신용카드 등 한가지 이상의 방법으로 제공하여야 한다.

제12조(개인정보의 관리 및 파기)

① 고객이 서비스 가입·해지 등을 위해 제출한 이용신청서, 개인정보이용동의서 등의 구비서류는 전자적 형태로 보관하여야 하며, 기타 개인정보가 포함된 문서를 사업장 내 보관할 경우 시건 장치가 있는 장소에 보관하고 잠금 조치를 하여야 한다.

② 개인정보처리자는 가입·해지 등을 위해 제출한 구비서류를 보유 목적 외의 용도로 이용하거나 제3자에게 제공하여서는 안 된다.

③ 개인정보는 정당한 사유가 없는 한 사용 목적 등이 달성되었을 경우 지체없이 파기하여야 한다.

④ 개인정보 파기 시에는 복구가 불가능한 형태로 파기하여야 한다.

1. 전자적인 파일 형태의 경우 : 복원이 불가능한 방법으로 영구삭제
2. 기록물, 인쇄물, 서면 등 그 밖의 기록매체인 경우 : 파쇄 또는 소각

⑤ 제2항과 3항에도 불구하고 다음 각 호와 같이 법령에 특별한 규정이 있을 경우 관련 법령이 정하는 기간 동안 보유할 수 있으며, 법령에 따라 보존한다는 점을 표시하여야 한다.

1. 전기통신사업법 제83조 제3항, 제5항에 의하여 보관하는 성명, 주민번호, 주소, 전화번호, 아이디, 가입일 또는 해지일의 경우 1년
2. 국세기본법 제85조의3 규정에 의하여 보관하는 성명, 주민번호, 전화번호,

청구지 주소, 요금납부내역(청구액, 수납액, 수납일시, 요금납부 방법)등의 경우 5년

3. 통신비밀보호법 제15조의2 제2항에 따른 가입자의 전기통신 일시, 전기통신 개시·종료 시간, 발·착신 통신번호 등 상대방의 가입자번호, 사용도수, 정보통신망에 접속된 정보통신기기의 위치를 확인할 수 있는 발신기지국의 위치추적자료의 경우 12개월(단, 시외·시내전화역무와 관련된 자료인 경우 6개월)
4. 통신비밀보호법 제15조의2 제2항에 따른 컴퓨터통신 또는 인터넷의 사용자가 전기통신역무를 이용한 사실에 관한 컴퓨터통신 또는 인터넷의 로그기록자료의 경우 3개월
5. 통신비밀보호법 제15조의2 제2항에 따른 컴퓨터통신 또는 인터넷의 사용자가 정보통신망에 접속하기 위하여 사용하는 정보통신기기의 위치를 확인할 수 있는 접속지의 추적자료의 경우 3개월

제13조(개인정보처리방침의 작성 및 관리)

① 개인정보처리방침을 작성할 때에는 다음 각 호의 사항을 반드시 포함하여야 한다. (자세한 작성 방법은 "개인정보보호가이드"를 참조)

1. 개인정보의 수집·이용 목적, 수집하는 개인정보의 항목 및 수집방법
2. 개인정보를 제3자에게 제공하는 경우 제공받는 자의 성명(법인인 경우에는 법인의 명칭을 말한다), 제공받는 자의 이용 목적과 제공하는 개인정보의 항목, 제공받는 자의 보유·이용기간
3. 개인정보의 보유 및 이용 기간, 개인정보의 파기절차 및 파기방법(관련 법령에 따라 개인정보를 보존하여야 하는 경우에는 그 보존근거와 보존하는 개인정보 항목을 포함한다)
4. 개인정보 처리위탁을 하는 업무의 내용 및 수탁자(해당되는 경우에만 처리방침에 포함한다)
5. 이용자 및 법정대리인의 권리와 그 행사방법
6. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항
7. 개인정보보호책임자의 성명 또는 개인정보보호 업무 및 관련 고충사항을 처리하는 부서의 명칭과 그 전화번호 등 연락처

② 제1항에 따라 개인정보처리방침을 변경하는 경우에는 변경 이유와 내용을 지체 없이 공지하고, 다음 각 호의 방법 중 어느 하나 이상의 방법으로

이용자가 언제든지 변경된 사항을 알아 볼 수 있도록 조치하여야 한다.

1. 운영하는 인터넷 홈페이지의 첫 화면의 공지사항 란 또는 별도의 창을 통하여 공지하는 방법
2. 서면·모사전송·전자우편 또는 이와 비슷한 방법으로 이용자에게 공지하는 방법
3. 점포·사무실·대리점 등 내부의 보기 쉬운 장소에 써 붙이거나 비치하는 방법

제14조(수탁사에 대한 관리·감독)

① 사업부서의 장은 개인정보를 처리하는 수탁사에 대하여 다음 각 호의 사항을 관리하여야 한다.

1. 개인정보의 처리 현황
2. 개인정보처리시스템의 접속현황
3. 개인정보처리시스템의 접근 대상자 및 개인정보취급자 관리
4. 목적 외 이용·제공 및 재위탁 금지 준수여부
5. 암호화 등 안전성 확보조치 이행여부
6. 그 밖에 개인정보의 보호를 위하여 필요한 사항

② 사업부서의 장은 수탁사에 대하여 제1항 각 호의 사항에 대한 실태를 점검하여 시정을 요구하고, 수탁사는 이를 시행하여야 한다.

③ 사업부서의 장은 ITO업무 중 개인정보를 처리하는 수탁사에 대하여 개인정보보호 자체점검 결과를 매월 1회이상 정기적으로 BA부서에 전달하여야 한다.

제15조(이용자의 보호)

① 상품 및 서비스의 관리를 담당하는 부서의 장은 이용약관, 가입신청서 등에 개인정보 수집목적, 수집항목, 개인정보 보유기간, 개인정보 수집·이용에 대한 동의·반대 처리 방법 등을 고지하여야 한다.

② 이용자가 본인 정보의 열람·수정, 제3자 제공내역, 개인정보 위탁·제공 등에 대한 동의의 철회를 요청할 경우에는 본인임을 확인하고 지체 없이 필요한 조치를 취하여야 하며, 이용자의 요구에 응할 수 없을 경우 해당 사유를 이용자에게 안내하여야 한다.

③ 동의의 철회 또는 제2항에 따른 개인정보의 열람·제공 또는 오류의 정정을

요구하는 방법은 개인정보의 수집방법보다 쉽게 제공하여야 한다.

④ 법정대리인이 14세 미만 아동의 개인정보에 대한 동의철회, 열람, 오류정정 요구 등을 할 경우 특별한 사유가 없는 한 법정대리인 관계 및 본인확인 후 요구에 응하여야 한다.

⑤ 개인정보를 처리하는 웹사이트 등을 운영하는 부서의 장은 수집한 이용자의 개인정보 처리위탁, 제3자 제공 내역 등 이용내역을 연 1회 이상 이용자에게 통지하여야 한다. 다만, 연락처 등 이용자에게 통지할 수 있는 개인정보를 수집하지 아니한 경우에는 통지하지 않을 수 있다.

제16조(위험도 분석 및 대응)

① 개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 위험분석을 연 1회 이상 수행하고, 위험 감소를 위한 위험조치 계획을 수립·시행하여야 한다.

② 위험분석의 방법은 위험분석의 목적, 용도, 대상자산의 관리조직·업무특성 등을 전반적으로 고려하여 합리적이고 적합한 방법을 채택하여 시행하여야 한다.

제17조(접근권한의 관리)

① 개인정보보호책임자는 개인정보처리시스템에 대한 접근 권한을 최소한의 인원에게만 부여하고, 개인정보취급자 이외에는 개인정보처리시스템에 접근하지 못하도록 관리·감독하여야 한다

② 개인정보보호책임자는 개인정보취급자 퇴직 등 인사 상 변동사항이 발생하였을 경우 지체 없이 개인정보처리시스템의 접근권한에 대한 말소를 요청한다.

③ 제2항에 의한 접근권한 부여, 변경 또는 말소 내역은 기록하고, 그 기록을 최소 5년간 보관하여야 한다.

제18조(접근통제)

① 개인정보보호책임자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 시스템을 설치 및 운영한다.

1. 개인정보처리시스템에 대한 접속 권한을 IP 주소 등으로 제한하여 인가

받지 않은 접근을 제한
2. 개인정보처리시스템에 접속한 IP 주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지

② 개인정보보호책임자는 개인정보취급자가 생일, 주민등록번호, 전화번호 등 추측하기 쉬운 숫자나 개인관련 정보를 패스워드로 이용하지 않도록 하고, 다음 각 호의 문자 종류 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성하도록 하여야 한다.
1. 영문 대문자(26개)
2. 영문 소문자(26개)
3. 숫자(10개)
4. 특수문자(32개)

③ 개인정보보호책임자는 비밀번호에 유효기간을 설정하여 분기별 1회 이상 변경이 가능하도록 조치하여야 한다.

제19조(개인정보의 암호화)

① 비밀번호의 소유자가 비밀번호를 분실한 경우, 본인확인 절차를 거친 후 다음 각호의 방법으로 비밀번호를 변경하여야 한다.
1. 소유자가 직접 비밀번호 변경(인터넷, ARS 등)
2. 랜덤한 임시 비밀번호를 생성하여 안전한 방법으로 제공하고 소유자가 비밀번호를 변경하도록 안내

② 개인정보처리시스템에 비밀번호를 저장할 경우 복호화 되지 않도록 안전한 일방향 암호화하여 저장하여야 하고 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호, 신용카드번호, 계좌번호, 바이오정보를 저장할 경우 안전한 양방향 암호화 알고리즘으로 암호화 하여야 한다.

③ 안전한 일방향 암호화 알고리즘은 SHA-256 이상의 암호화 알고리즘을 지칭하며, 안전한 양방향 암호화 알고리즘은 보안강도 128bit 이상의 AES, ARIA, SEED를 지칭한다. 부득이 별도의 다른 양방향 암호화 알고리즘을 적용해야 하는 경우 개인정보보호책임자의 승인을 득하여야 한다.

④ 알고리즘을 이용해 개인정보를 암호화 한 경우, 암호화에 사용한 암호키는 다음 각 호와 같이 관리되어야 한다.
1. 암호키는 프로그램의 소스코드 내 저장 금지
2. 암호키는 권한 있는 자만 이용할 수 있도록 접근통제 및 권한 부여 최소화

3. 암호키는 관리대장에 기록하여 소속 부서장의 책임하에 별도 잠금 장치가 있는 안전한 장소에 보관
4. DB, 어플리케이션 및 도입 솔루션에 의존적인 특별한 경우는 보안성승인 시 개인정보보호책임자의 승인을 얻어 별도의 방법으로 암호키 관리

⑤ 개인정보 및 인증정보를 송·수신할 때에는 다음 각 호 중 하나의 기능을 갖춘 안전한 보안서버 구축 등의 조치를 통해 암호화하여야 한다.

1. 웹서버에 SSL 인증서를 설치하여 전송하는 정보를 암호화하여 송·수신하는 기능
2. 웹서버에 암호화 응용프로그램을 설치하여 전송하는 정보를 암호화하여 송·수신하는 기능

⑥ 개인정보를 PC에 저장하는 것은 원칙적으로 금지한다. 다만, 업무상 저장이 필요할 경우에는 회사의 DRM을 이용하여 개인정보를 암호화 한 후 저장하고, 목적이 달성되는 즉시 파기하여야 한다.

⑦ 개인정보의 암호화 적용의 보호조치 방법은 "개인정보보호가이드"를 참조한다.

제20조(접속기록의 보관 및 점검)

① 개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리하는 경우에는 개인정보취급자 등의 계정, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등의 접속기록을 저장하여야 한다.

② 개인정보보호책임자는 제1항의 접속기록에 대해 월 1회 이상정기적으로 확인. 감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 1년 이상 접속기록을 보존·관리 하여야 한다. 다만, 5만명 이상의 정보주체에 관하여 개인정보를 처리하거나, 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다

③ 개인정보를 다운로드 한 것이 발견되었을 경우에는 사유를 반드시 확인하여야 한다.

④ 개인정보보호책임자는 제1항의 접속기록에 대해 위·변조 방지를 위해 정기적으로 별도의 저장매체에 백업 보관하여야 한다.

⑤ 개인정보 접속기록 저장 및 보관의 보호조치 방법은 "개인정보보호가이드"를 참조한다

제21조(보안프로그램의 설치 및 운영)

① 개인정보보호책임자는 업무용 컴퓨터(PC) 등을 이용하여 정보를 처리하는 경우 정보가 분실, 도난, 유출·위조·변조 또는 훼손되지 아니하도록 안전성 확보를 위한 백신 프로그램 등의 보안 프로그램을 설치·운영하여야 한다.
② 보안 프로그램은 항상 최신의 버전으로 업데이트를 적용하여야 한다.
③ 보안 프로그램의 최신 업데이트를 적용하기 위하여 자동 업데이트 설정 및 실시간 감시 기능을 적용하여야 한다.

제22조(물리적 접근제한)

① 개인정보보호책임자는 개인정보와 개인정보처리시스템의 안전한 보관을 위한 물리적 잠금 장치 등의 물리적 접근방지를 위한 보호조치를 취하여야 한다.
② 개인정보보호책임자는 물리적 접근방지를 위한 별도의 보호시설에 출입하거나 개인정보를 열람하는 경우, 그 출입자에 대한 출입사실 및 열람 내용에 관한 관리대장을 작성하도록 하여야 한다.
③ 개인정보보호책임자는 물리적 접근제한 관리대장의 출입 및 열람 내용을 주기적으로 검토하여 정당하지 않은 권한으로 출입하거나 열람하는 경우가 있는지를 점검하여 확인하여야 한다.

제23조(출력 복사 시 보호조치)

① 개인정보보호책임자는 개인정보가 포함된 정보를 출력하거나 복사할 경우에 개인정보 유출사고를 방지하기 위한 보호조치를 취하여야 한다.
② 개인정보보호책임자는 민감한 개인정보 또는 다량의 개인정보가 포함된 정보를 출력하거나 복사할 경우 출력·복사자의 성명, 일시 등을 기재하여 개인정보 유출 등에 대한 책임 소재를 확인할 수 있는 강화된 보호조치를 추가로 적용할 수 있다.
③ 개인정보취급자는 개인정보의 이용을 위하여 출력 및 복사한 개인정보의 이용 목적이 완료된 경우 분쇄기로 분쇄하거나 소각하는 등의 안전한 방법으로 파기하여야 한다.

제24조(영상정보처리기기의 설치 및 운영관리)

① 공개된 장소에 영상정보처리기기를 설치할 경우 개인정보보호책임자의 사전 승인을 득하여야 한다.

② 제1항에 의해 영상정보처리기기를 설치한 경우 정보의 주체가 쉽게 인지할 수 있도록 다음 각호의 내용이 포함된 안내판을 설치하여야 한다.

1. 설치 목적 및 장소
2. 촬영 범위 및 시간
3. 관리책임자의 성명 및 연락처

제25조(재해 및 재난 대비 안전조치)

① 개인정보처리자는 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검하여야 한다.

② 재해·재난 발생 시 개인정보처리시스템 백업, 복구 계획은 "사내 IT 인프라 관리 및 운영 기준"의 시스템 백업 절차 및 가이드와 재해 복구 절차 및 가이드를 따른다.

제5장 개인정보보호 감사

제26조(자체감사 주기 및 절차)

① 개인정보보호책임자는 내부관리계획에서 정하는 개인정보보호 규정을 임직원들이 성실히 이행하는지를 주기적으로 점검하여야 한다.

② 개인정보보호 자체 감사는 연 1회 이상 실시한다.

제27조(자체감사 결과 조치)

① 개인정보보호책임자는 개인정보 보호에 관한 자체감사 실시 결과, 관리·운영상의 문제점을 발견하거나 관련 직원이 본 계획의 내용을 위반할 때에는 시정·개선 등 필요한 조치를 취하여야 한다.

② 개인정보보호책임자는 위반사실에 대한 시정·개선 조치가 이행되지 않거나, 심각한 영향이 발생할 수 있는 우려가 되는 경우 임직원에 대한 인사조치 등의 필요한 추가 조치를 취할 수 있다.

제6장 개인정보 침해·유출사고 예방 및 대응

제28조(예방 활동)

① 개인정보보호책임자는 주요 정보시스템에 대한 실시간 탐지 및 대응이 가능하도록 모니터링 체계를 갖추어야 하며, 주요 시스템 로그 및 이벤트를 분석하여 침입 흔적이나 시도 유무를 점검하여야 한다.

② 개인정보처리자는 개인정보 침해사고가 발생했거나 의심되는 경우, 즉시 피해 최소화를 위한 초동 조치를 취하고 개인정보보호책임자에게 지체 없이 보고하여야 한다.

제29조(대응 및 복구)

① 개인정보침해사고가 발생 할 경우 개인정보보호책임자는 신속한 대응·복구를 위하여 다음 각호의 활동을 실시하여야 한다.

1. 침해사고 원인분석 및 사고 유형의 정의
2. 정보시스템에 대한 취약점 제거
3. 침해사고 재발방지 대책수립 및 시행

② 개인정보가 유출 된 경우 관련 유관부서 및 유관기관과 협의를 통해, 정보주체의 추가 피해를 예방하기 위하여 필요한 조치를 취해야 한다.

③ 개인정보보호책임자는 전자적 침해사고 발생을 대비하여 관련 유관부서 및 유관기관의 비상연락 체계를 현행화하여 관리하여야 한다.

제30조(개인정보 유출·위조·변조 또는 훼손 통지)

① 개인정보보호책임자는 개인정보의 유출·위조·변조 또는 훼손(분실·도난·유출·위조·변조 또는 훼손 등) 사실을 안 때에는 지체 없이 다음 사항을 해당 이용자에게 알리고 보호위원회 또는 전문기관(한국인터넷진흥원) 등에 신고하여야 한다. 유출·위조·변조 또는 훼손된 개인정보 항목 및 발생시점 확인 못한 경우는 먼저 확인된 사항을 통지·신고 후 추가 확인 사항은 확인 즉시 통지·신고 한다.

1. 유출·위조·변조 또는 훼손된 개인정보 항목
2. 유출·위조·변조 또는 훼손 발생 시점과 그 경위

3. 이용자가 취할 수 있는 조치
4. 개인정보보호책임자 등 대응 조치
5. 이용자가 상담 등을 접수할 수 있는 부서 및 연락처

② 정당한 사유없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 되며, 다만 이용자의 연락처를 알 수 없는 등 정당한 사유가 있는 경우에는 아래의 방법으로 통지를 갈음할 수 있다.

1. 위 ①항 각 호의 사항을 인터넷 홈페이지에 30일 이상 게시
2. 천재지변이나 그 밖의 정당한 사유로 홈페이지 게시가 곤란한 경우에는 전국을 보급지역으로 하는 둘 이상의 일반일간신문에 1회 이상 공고

③ 통지·신고 방법

1. 통지 매체 : 전자우편, 서면, 모사전송, 전화 또는 이와 유사한 방법으로 이용자에게 통지
2. 신고 매체 : 보호위원회 또는 한국인터넷진흥원에 서면(전자문서 포함)이나 통지 매체로 신고
3. 유출 수준 : 1천명 이상

부 칙

① (시행일) 본 계획은 2015년 06월 19일부터 시행한다.
② (경과조치) 본 계획 시행전에 추진한 업무는 종전 보안정책 및 지침에 준용하여 적용한다.

부 칙

① (시행일) 본 계획은 2016년 01월 15일부터 시행한다.
② (경과조치) 본 계획 시행전에 추진한 업무는 종전 계획에 준용하여 적용한다.

부 칙

① (시행일) 본 계획은 2016년 06월 27일부터 시행한다.
② (경과조치) 본 계획 시행전에 추진한 업무는 종전 계획에 준용하여 적용한다.

부 칙

① (시행일) 본 계획은 2017년 12월 08일부터 시행한다.
② (경과조치) 본 계획 시행전에 추진한 업무는 종전 계획에 준용하여 적용한다.

부 칙

① (시행일) 본 계획은 2018년 12월 14일부터 시행한다.
② (경과조치) 본 계획 시행전에 추진한 업무는 종전 계획에 준용하여 적용한다.

부 칙

① (시행일) 본 계획은 2019년 09월 16일부터 시행한다.
② (경과조치) 본 계획 시행전에 추진한 업무는 종전 계획에 준용하여 적용한다.

부 칙

① (시행일) 본 계획은 2020년 08월 05일부터 시행한다.

② (경과조치) 본 계획 시행전에 추진한 업무는 종전 계획에 준용하여 적용한다.