서울시사회서비스원
개인정보 내부 관리계획

2024. 4.

서울시사회서비스원

순번	구분	시행 일자	제정·개정 주요내용
1	제정	2020. 3. 30.	1. 제1조(목적)~제27조(개인정보의 파기) 신설
2	일부개정	2022. 10.	1.개인정보 보호법 개정에 따른 가명정보 내용 추가 2. 제1조(목적) 개정 - '개인정보의 안전성 확보조치 기준(개인정보보호위원회고시 제2021-2호)' 개정 사항 반영 3. 제2조(용어 정의) - 정보보호자 관련 용어 추가 1) 개인정보 보호책임자 2) 개인정보 관리책임자 3) 개인정보 보호담당자 - 개인정보취급자의 범위 확대 - 가명정보와 관련된 용어 추가 1) 익명정보, 추가정보, 재식별 - 관련 법령상 정의하고 있는 용어 중 변경된 사항 반영 1) 개인정보 2) 접속기록 - 바이오정보를 생체정보와 생체인식정보로 구분하여 정의 4. 제3조(적용 범위)제2항, 제3항 추가 - 제1항 적용 범위 확대 - 가명정보가 개인정보에 포함됨에 따른 표기 기준 정의 5. 제4조(내부관리계획의 수립 및 승인) - 전면 개정 6. 제5조(내부관리계획의 공표) - 전면 개정 7. 제6조(개인정보 보호책임자의 지정) - 근거 조항 추가 - 분야별 보호 책임자 명칭 변경(범위 동일) 8. 제7조(개인정보 보호책임자의 역할 및 책임) - 가명정보 관리책임자의 역할 및 책임 추가 9. 제8조(개인정보 취급자의 역할 및 책임) - 개인정보 취급자의 범위 항목 추가 10. 제9조(개인정보 보호 교육 계획의 수립) - 제1항 교육 목적 추가 11. 제10조(개인정보 보호 교육 실시) - 제20조(개인정보취급자의 교육)항목에서 조항 명칭 변경 - 교육 대상 확대

			- 제3항 변경 1) 교육 자료 기록·보관 12. 제10조의2(가명정보를 처리하는 자의 교육) 추가 13. 제11조(접근 권한의 관리) - 책임자 범위 확대 - 제11조 비밀번호관리를 하위 항목으로 이동 1) 기존 1,2호 내용 통합 2) 기존 3호 내용 2항 이동 3) 3호 비밀번호 유효기간 추가 14. 제12조(접근 통제) - 전면 개정 - 책임자 범위 확대 15. 제13조(개인정보의 암호화) - 전면 개정 - 책임자 범위 확대 16. 제14조(접속기록의 보관 및 점검) - 제1항, 제2항 기간 변경 - 제3항 추가 1) '개인정보의 안전성 확보조치 기준(개인정보보호위원회고시 제2020-2호)' 제8조제2항에 따른 다운로드 사유 확인이 필요한 기준을 책정하여 반영 - 책임자 범위 확대 17. 제20조(수탁자에 대한 관리 및 감독) - 전면 개정 18. 제21조(물리적 안전조치) - 제25조(물리적 접근제한)항목에서 조항 명칭 변경 - 책임자 범위 확대 - 제4항 보조저장매체 항목 추가 19. 제22조(재해 및 재난 대비 안전조치) - 책임자 범위 확대 20. 제23조(개인정보의 파기) - 책임자 범위 확대 21. 제24조(가명정보 기록의 작성·보관) 추가 22. 제25조(가명정보 및 추가정보 분리 보관) 추가 23. 제26조(가명정보 수탁자 관리·감독) 추가 - 가명정보 처리업무 외부 위탁 시, 문서에 포함될 사항 추가 24. 제26조의2(가명정보 및 추가정보에 대한 접근권한 분리) 추가

			25. 제26조의3(가명정보의 재식별 금지) 추가 26. 제27조(개인정보 유출 등의 통지) - 제1항 1) 5호 조치·절차 추가 - 제2항 대응팀 명칭 변경 27. 제28조(개인정보 유출 등의 신고) 1) 행정안전부(장관) → 개인정보 보호위원회 2) 한국정보화진흥원 삭제 28. 제29조(권익침해 구제방법) - 제1항 1) 변경된 개인정보보호 유관 기관 적용 2) 연락처 현행화 - 제2항 행정심판 청구 추가 29. [별표2] 법적근거 - 시행령 및 고시 변경에 따른 기관명, 제정번호, 법조문 현행화 30. 조항 순서 - 전면 개정 31. 소속 항목 - 전면 개정
3	일부개정	2022. 12.	1. 제2조(용어 정의) - 제7항 개인정보 관리책임자 정의 변경 2. 제6조(개인정보 보호책임자의 지정) - 개인정보 보호책임자 자격 정의 3. 제11조의2(접속 권한의 제한) - 인사이동에 따른 접속 제한 기준 정의
4	일부개정	2024. 4.	1. 제1조(목적) '개인정보의 안전성 확보조치 기준' 고시번호 변경 2. 제2조(용어 정의) - 13호 법 명칭 변경: 전기통신기본법 → 전기통신사업법 3. 제11조(접근 권한의 관리) - 제6항 비밀번호 오류 시 접근 제어 정의 4. 제13조(개인정보의 암호화) - 제2항 암호화 기준 정의

〈 목 차 〉

제1장 총 칙

제1조(목적)

서울시사회서비스원(이하 ‘본원’이라 한다) 개인정보 내부 관리계획(이하 ‘본 계획’ 또는 ‘내부 관리계획’이라 한다)은 ‘개인정보 보호법’(이하 ‘법’) 제29조와 같은 법 시행령(이하 ‘영’) 제30조 그리고 ‘개인정보의 안전성 확보조치 기준’(개인정보보호위원회 고시 제2023-6호, 2023. 9. 22.)에 따라 내부 관리계획의 수립 및 시행 의무에 따라 제정된 것으로 본원이 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)

본 계획에서 사용하는 용어의 뜻은 다음과 같다.

1. “개인정보”란 살아 있는 개인에 관한 정보로서 다음 각 목의 어느 하나에 해당하는 정보를 말한다.
   가. 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보
   나. 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보. 이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 한다.
   다. 가목 또는 나목을 법 제2조제1호의2에 따라 가명처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보(이하 "가명정보"라 한다)
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 관리책임자”란 개인정보처리시스템를 처리(취급)하는 각 부서의 장을 말한다.
8. “개인정보 보호담당자”란 개인정보 보호책임자를 보좌하고 본원의 개인정보보호 관련 현황관리, 관리실태 이행점검 및 관리감독 등을 수행한다.
9. “개인정보취급자”란 개인정보 관리책임자(개인정보 취급 부서의 장)·개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 임직원, 파견근로자, 시간제 근로자 등을 말한다.
10. “개인정보처리시스템”이란 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템을 말한다.
11. “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.
12. “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.
13. “정보통신망”이란 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호의 「전기통신사업법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말한다.
14. “공개된 무선망”이란 불특정 다수가 무선접속장치(AP)를 통하여 인터넷을 이용할 수 있는 망을 말한다.
15. “모바일 기기”란 무선망을 이용할 수 있는 PDA, 스마트폰, 태블릿PC 등 개인정보 처리에 이용되는 휴대용 기기를 말한다.
16. ”생체정보”란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 인증·식별하거나 개인에 관한 특징을 알아보기 위해 일정한 기술적 수단을 통해 처리되는 정보를 말한다.

16의2. “생체인식정보”란 생체정보 중 특정 개인을 인증 또는 식별할 목적으로 일정한 기술적 수단을 통해 처리되는 정보를 말한다.

17. “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.
18. “내부망”이란 물리적 망분리, 접근 통제시스템 등에 의해 인터넷 구간에서의 접근이 통제

또는 차단되는 구간을 말한다.

19. “접속기록”이란 개인정보취급자 등이 개인정보처리시스템에 접속한 사실을 알 수 있는 계정, 접속일시, 접속자 정보, 처리한 정보주체 정보, 수행업무 등을 전자적으로 기록한 것을 말한다. 이 경우 “접속”이란 개인정보처리시스템과 연결되어 데이터 송신 또는 수신이 가능한 상태를 말한다.
20. “관리용 단말기”란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리시스템에 직접 접속하는 단말기를 말한다.
21. “익명정보”란 시간・비용・기술 등을 합리적으로 고려할 때 다른 정보를 사용하여도 더 이상 개인을 알아볼 수 없는 정보를 말한다.
22. “추가정보”란 개인정보의 전부 또는 일부를 대체하는데 이용된 수단이나 방식(알고리즘 등), 가명정보와의 비교・대조 등을 통해 삭제 또는 대체된 개인정보를 복원할 수 있는 정보(매핑 테이블 정보, 가명처리에 사용된 개인정보 등) 등을 말한다.
23. “재식별”이란 특정 개인을 알아볼 수 없도록 처리한 가명정보에서 특정 개인을 알아보는 것을 말한다.

제3조(적용 범위)

① 본원(개인정보를 취급하는 내부직원(계약직 등 비정규직 포함) 및 외부업체 직원)이 개인정보를 처리하거나 본원의 개인정보 처리 업무를 위탁받아 처리하는 수탁자에게는 본 계획이 적용된다.

② “법 제2조제1호 다목”에 따라 가명정보는 개인정보로 취급한다. 단 익명정보는 그러하지 않는다.

③ 가명정보와 관련되어 수반되는 내용들은 동 내부 관리계획에 표기된 “개인정보”에서 수행·적용되는 항목들과 동일하게 취급되어져야 하므로 별도로 표기하지 아니한다. 단 가명정보만의 고유한 특징 업무를 수행·적용할 경우에는 별도의 항목으로 구분지어 표기한다.

제2장 내부 관리계획의 수립 및 시행

제4조(내부 관리계획의 수립 및 승인)

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

② 개인정보 보호책임자는 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 개인정보 보호담당자는 내부 관리계획의 세부 이행을 위한 각종 지침 등을 마련하여 시행할 수 있다.

⑤ 개인정보 보호책임자는 연 1회 이상으로 내부 관리계획의 이행 실태를 점검·관리 하고 그 결과에 따라 적절한 조치를 취하여야 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 내부직원(계약직 등 비정규직 포함), 외부업체 직원이 언제든지 열람할 수 있는 방법으로 비치하거나 제공하여야 한다.

제3장 개인정보 보호책임자의 역할 및 책임

제6조(개인정보 보호책임자의 지정)

① 본원은 법 제31조와 영 제32조에 따라 정보보호 및 개인정보 보호 업무자가 속한 실(부서)에서 2급 이상 직급자로 지정한다. 단, 분야별 보호책임자는 개인정보 관리책임자(개인정보 취급 부서의 장)로 지정한다.

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. 법 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 가명정보 및 추가정보 관리 업무에 대해 다음 각 호의 업무를 수행한다.

1. 가명정보에 대한 내부 관리계획의 수립·시행
2. 내부 관리계획의 이행실태 점검 및 관리
3. 가명처리 및 적정성 검토 현황 관리
4. 가명정보 및 추가정보에 대한 관리·감독
5. 가명정보 처리 현황 및 관련 기록 관리
6. 가명정보를 처리하는 자 교육계획의 수립 및 시행
7. 가명처리 및 가명정보 처리 위탁 사항에 대한 관리·감독(해당 시)
8. 가명정보에 대한 재식별 모니터링 및 재식별 시 처리 방안의 수립·시행
9. 그 밖의 가명정보 처리에 대한 보호에 관한 사항

③ 개인정보 보호책임자는 제1항의 업무를 수행함에 있어서 필요한 경우 개인정보의 처리 현황, 처리 체계 등에 대하여 수시로 조사하거나 관계 당사자로부터 보고를 받을 수 있으며, 임직원에 대한 교육 및 보안서약 등을 통해 개인정보 침해사고를 사전에 예방한다.

④ 개인정보 보호책임자는 개인정보 보호와 관련하여 이 법 및 다른 관계 법령의 위반 사실을 알게 된 경우에는 즉시 개선조치를 하여야 하며, 필요하면 소속 기관의 장에게 개선조치를 보고하여야 한다.

제8조(개인정보 취급자의 역할 및 책임)

① 개인정보취급자의 범위는 다음과 같으며 정규직 이외에 임시직, 파견근로자, 시간제근로자 등을 포함한다.

1. 본원에서 정보주체의 개인정보를 처리하는 업무를 수행하는 자
2. 개인정보 관리책임자(개인정보 취급 부서의 장)·개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자

② 개인정보취급자는 개인정보를 처리함에 있어서 개인정보가 안전하게 관리될 수 있도록 동 계획은 물론, 개인정보 보호와 관련한 법령 및 규정 등을 준수하여야 한다.

1. 내부 관리계획과 개인정보 보호와 관련 법령 및 규정 등의 준수 및 이행
2. 개인정보의 기술적·관리적 보호조치 기준 이행
3. 업무상 알게 된 개인정보를 제3자에게 제공 금지

제4장 개인정보 보호 교육

제9조(개인정보 보호 교육 계획의 수립)

① 개인정보 보호책임자는 개인정보의 적정한 취급을 보장하기 위하여 다음 각 호의 사항을 정하여 개인정보 취급자의 개인정보 보호 교육 계획을 수립하고 실시하여야 한다.

1. 교육 목적 및 대상
2. 교육 내용
3. 교육 일정 및 방법

② 개인정보 보호책임자는 수립한 개인정보 보호 교육 계획을 실시한 이후에 교육의 성과와 개선 필요성을 검토하여 다음년도 교육계획 수립에 반영하여야 한다.

제10조(개인정보 보호 교육 실시)

① 개인정보 보호책임자는 정보주체 개인정보 보호에 대한 직원들의 인식제고를 위해 노력해야 하며, 개인정보의 오·남용 또는 유출 등을 적극 예방하기 위해 직원을 대상으로 매년 연 1회 이상의 개인정보 보호 교육을 실시하여야 한다.

② 교육방법은 집합교육 뿐만 아니라 사이버교육, 부서 자체 내부교육 등 다양한 방법을 활용하여 실시하고, 필요한 경우 외부 전문기관이나 전문요원에 위탁하여 교육을 실시한다.

③ 개인정보 보호책임자는 개인정보 보호 교육을 실시한 결과 또는 이를 입증할 수 있는 관련 자료 등을 기록·보관하여야 한다.

제10조의2(가명정보를 처리하는 자의 교육)

① 개인정보 보호책임자는 가명정보를 처리하는 자에게 필요한 가명정보 보호 교육계획을 수립하고 실시하여야 한다.

② 가명정보 보호 교육은 다음과 같은 내용을 포함하여 시행하여야 한다.

1. 가명정보 처리에 관한 사항
2. 가명정보 및 추가정보의 안전조치에 관한 사항
3. 재식별 금지에 관한 사항

③ 가명정보를 처리하는 자에 대한 교육은 개인정보 보호교육과 함께 수행할 수 있으며 교육을 실시한 결과 또는 이를 입증할 수 있는 관련 자료 등을 기록·보관하여야 한다.

제5장 기술적 안전조치

제11조(접근 권한의 관리)

① 개인정보 관리책임자는 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.

② 개인정보 관리책임자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하여야 한다.

③ 개인정보 관리책임자는 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.

④ 개인정보 관리책임자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자 별로 한 개의 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

⑤ 개인정보 관리책임자는 개인정보처리시스템에 개인정보취급자 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
2. 연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않도록 노력
3. 비밀번호에 유효기간을 설정하여 반기별 1회 이상 변경

⑥ 개인정보 관리책임자는 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.

제11조의2(접속 권한의 제한)

① 직위해제(대기발령) 및 정직 처분자는 업무시스템 및 타인 정보를 확인할 수 있는 시스템 등에 대한 접근을 제한한다. 단, 개인 메일 등 본인의 정보만 확인할 수 있는 수준의 내부전산망 접속을 허용할 수 있다.

② 퇴직자의 경우 즉시 내부망 접근을 차단하여야 한다.

제12조(접근 통제)

① 개인정보 보호책임자는 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 개인정보 보호책임자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN: Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다.

③ 개인정보 보호책임자는 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 개인정보 보호책임자는 고유식별정보를 처리하는 인터넷 홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점을 점검하고 필요한 보완 조치를 하여야 한다.

⑤ 개인정보 보호책임자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 하여야 한다.

⑥ 개인정보 보호책임자는 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 개인정보취급자는 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.

제13조(개인정보의 암호화)

① 개인정보취급자는 고유식별정보, 비밀번호, 생체인식정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

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

③ 개인정보취급자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ:

Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.

④ 개인정보취급자가 내부망에 고유식별정보를 저장하는 경우에는 암호화 하여야 한다. 다만, 개인정보 영향평가의 결과 및 또는 암호화 미 적용시 위험도 분석 결과에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.

⑤ 개인정보취급자는 제1항, 제2항, 제3항에 따라 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.

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

⑦ 개인정보 보호책임자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다.

제14조(접속기록의 보관 및 점검)

① 개인정보 관리책임자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 보관·관리하여야 한다.

② 개인정보 관리책임자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 매월 1회 이상 점검하여야 한다. 특히, 개인정보처리시스템에 접속하여 개인정보를 다운로드한 경우 그 사유를 반드시 확인해야 한다.

③ 제2항에 따라 개인정보처리시스템에 접속하여 개인정보를 다운로드한 경우 그 사유 확인이 필요한 경우의 기준은 아래 각 호와 같다.

1. (업무시간 내) 개인정보취급자가 1일 1,000명이상 정보주체의 개인정보를 다운로드 한 경우
2. (업무시간 외) 개인정보취급자가 휴일에 500명 이상 정보주체의 개인정보를 다운로드 한 경우

④ 개인정보 관리책임자는 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.

제15조(악성프로그램 등 방지)

① 개인정보 보호책임자는 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

제16조(관리용 단말기의 안전조치)

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

1. 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치
2. 본래 목적 외로 사용되지 않도록 조치
3. 악성프로그램 감염 방지 등을 위한 보안조치 적용

제6장 관리적 안전조치

제17조(개인정보 보호조직 구성 및 운영)

① 본원은 개인정보의 안전한 처리를 위하여 다음 각 호의 사항을 포함하는 개인정보 보호조직을 구성하고 운영하여야 한다.

1. 개인정보 보호책임자의 지정
2. 개인정보 보호책임자의 지휘·감독 하에 개인정보 보호책임자의 업무를 지원하는 개인정보 보호담당자의 지정
3. 개인정보를 처리하는 개인정보 관리책임자 및 개인정보취급자 지정

② 개인정보 보호조직의 설치, 변경 및 폐지는 개인정보 보호책임자로부터 승인을 받아 정한다.

③ 개인정보 취급부서에서는 개인정보 보호조직과 충분히 협의, 조정하여 개인정보를 처리하여야 한다.

제18조(개인정보 유출사고 대응)

① 개인정보 보호책임자는 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 구제

조치 등을 포함하여야 한다.

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

제19조(위험도 분석 및 대응)

① 개인정보 관리책임자는 개인정보가 오·남용, 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 위험도 분석을 수행하고 필요한 보안조치 적용 등 대응방안을 마련하여야 한다.

② 제1항에 따른 위험도 분석은 개인정보 위험도 분석 기준을 활용하거나 위험요소를 식별 및 평가하는 등의 방법으로 수행할 수 있다.

제20조(수탁자에 대한 관리 및 감독)

① 위탁자는 개인정보의 처리 업무를 위탁하는 경우에 다음 각 호의 사항을 정하여 수탁자를 교육하고 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.

1. 교육 및 감독 대상
2. 교육 및 감독 내용
3. 교육 및 감독 일정, 방법

② 위탁자는 제1항에 따라 수탁자를 교육하고 감독한 결과에 대한 기록을 남기고 문제점이 발견된 경우에는 필요한 보안조치를 하여야 한다.

제7장 물리적 안전조치

제21조(물리적 안전조치)

① 개인정보 관리책임자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 한다.

② 개인정보 관리책임자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.

③ 개인정보처리자는 물리적 접근방지를 위한 별도의 보호시설에 출입하거나 개인정보를 열람하는 경우, 그 출입자에 대한 출입사실 및 열람 내용에 관한 관리대장을 작성하도록 하여야 한다.

④ 개인정보 관리책임자는 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안대책을 마련하여야 한다. 다만, 별도의 개인정보처리시스템을 운영하지 아니하고 업무용

컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 이를 적용하지 아니할 수 있다.

제22조(재해 및 재난 대비 안전조치)

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

② 개인정보 관리책임자는 재해·재난 발생 시 개인정보처리시스템 백업 및 복구를 위한 계획을 마련하여야 한다.

제23조(개인정보의 파기)

① 개인정보 관리책임자는 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 개인정보 관리책임자는 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

제8장 가명정보처리 안전조치

제24조(가명정보 기록의 작성·보관)

① 개인정보 관리책임자는 가명정보의 처리목적, 가명처리한 개인정보 항목, 가명정보의 이용내역, 제3자 제공 시 제공받는 자를 작성·보관하여야 한다.

② 개인정보 관리책임자는 가명정보 처리와 관련된 내용을 개인정보 처리방침에 포함하여 공개하여야 한다.

제25조(가명정보 및 추가정보 분리 보관)

① 추가정보는 가명정보와 분리하여 별도로 저장·관리하고 가명정보와 불법적으로 결합되어

재식별에 악용되지 않도록 접근권한을 최소화하고 접근통제를 강화하는 등 필요한 조치를 적용하여야 한다.

1. 추가정보와 가명정보는 분리하여 보관하는 것을 원칙으로 하고, 불가피한 사유로 물리적인 분리가 어려운 경우 DB 테이블 분리 등 논리적으로 분리*

   * 논리적으로 분리할 경우 엄격한 접근통제를 적용
2. 추가정보의 활용 목적 달성 및 불필요한 경우에는 추가정보를 파기하며, 이 경우 파기에 대한 기록 작성 및 보관
3. 추가정보에 대한 접근이력을 정기적(최소 월 1회)으로 점검하여 오남용 예방 및 접근통제를 강화

제26조(가명정보 수탁자 관리·감독)

① 위탁자가 가명정보 처리업무를 외부에 위탁하는 경우, 가명정보는 법 제26조에 따라 위탁업무 수행 목적 외 가명정보의 처리 금지에 관한 사항 등을 포함한 문서를 작성하여야 한다.

1. 재식별 금지
2. 재제공 또는 재위탁 제한
3. 재식별 위험 발생시 통지
4. 위탁업무 수행 목적 외 처리금지
5. 가명정보의 안전조치 사항
6. 위탁업무의 목적 및 범위
7. 관리·감독에 관한 사항

제26조의2(가명정보 및 추가정보에 대한 접근권한 분리)

① 가명처리가 완료되면 가명정보 또는 추가정보의 접근권한은 최소한의 인원으로 엄격하게 통제하여야 하며, 업무에 따라 차등적으로 부여 하여야 한다.

② 추가정보에 대한 접근권한과 가명정보에 대한 접근권한은 분리하여 관리해야 한다.

③ 가명정보 또는 추가정보에 대한 접근권한 부여, 변경 또는 말소에 대한 내역을 기록하도록 하고 이 기록은 최소 3년간 보관하여야 한다.

제26조의3(가명정보의 재식별 금지)

① 가명정보를 처리하는 자의 가명정보에 대한 재식 별 행위는 엄격하게 금지한다.

② 가명정보를 처리하는 자는 가명정보를 처리하는 중 특정 개인에 대한 재식별이 발생

하는 경우 즉시 처리를 중단하고 이를 가명정보 관리책임자에게 통보한 후 수립된 재식별시 처리 방안에 따라 즉시 조치하여야 한다.

제9장 개인정보 유출사고 대응 및 피해구제

제27조(개인정보 유출 등의 통지)

① 개인정보 보호책임자는 개인정보가 유출되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 각 호의 사실을 알려야 한다. 다만, 유출된 개인정보의 확산 및 추가 유출을 방지하기 위하여 접속경로의 차단, 취약점 점검·보완, 유출된 개인정보의 삭제 등 긴급한 조치가 필요한 경우에는 그 조치를 한 후 정보주체에게 알릴 수 있다.

1. 유출된 개인정보의 항목
2. 유출된 시점과 그 경위
3. 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
4. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처
5. 본원의 대응조치 및 피해 구제절차

② 개인정보 보호책임자는 개인정보가 유출된 경우 그 피해를 최소화하기 위하여 “개인정보 유출사고 대응팀”을 구성하고 필요한 조치를 하여야 한다.

제28조(개인정보 유출 등의 신고)

① 개인정보 보호책임자는 1천명 이상의 개인정보가 유출된 경우에는 본 계획 제22조에 따른 통지 및 조치 결과를 지체 없이 보호위원회 또는 전문기관(한국인터넷진흥원)에 신고하여야 한다. 이 경우 보호위원회 또는 대통령령으로 정하는 전문기관은 피해 확산 방지, 피해 복구 등을 위한 기술을 지원하여야 한다.

제29조(권익침해 구제방법)

① 정보주체는 아래의 기관에 대해 개인정보 침해에 대한 피해구제, 상담 등을 문의할 수 있다. 개인정보 불만처리, 피해구제 결과에 대해 보다 자세한 도움이 필요 시 아래의 기관에 문의할 수 있다.

1. 개인정보침해신고센터(https://privacy.kisa.or.kr/): 국번 없이 118
2. 개인정보분쟁조정위원회(https://www.kopico.go.kr/): 국번 없이 1833-6972

3. 대검찰청 사이버범죄수사단(https://www.spo.go.kr/): 국번 없이 1301

4. 경찰청 사이버안전국(https://cyberbureau.police.go.kr/): 국번 없이 182

② 개인정보보호법 제35조(개인정보의 열람), 제36조(개인정보의 정정·삭제), 제37조(개인정보의 처리정지 등)의 규정에 의한 요구에 대하여 공공기관의 장이 행한 처분 또는 부작위로 인하여 권리 또는 이익의 침해를 받은 자는 행정심판법이 정하는 바에 따라 행정심판을 청구할 수 있다.

※ 행정심판에 대해 자세한 사항은 중앙행정심판위원회(https://www.simpan.go.kr/) 참고

③ 개인정보보호 및 처리와 관련한 문의는 한국인터넷진흥원에서 운영하는 118 고객센터를 이용하여 상담 받을 수 있다.

※ 전화문의: 국번 없이 118(ARS 내선2번), 전자우편문의: privacyclean@kisa.or.kr

부 칙

제1조(시행일)

이 지침은 결재한 날로부터 시행한다.

붙임 1 개인정보 내부 관리계획 수립 대상

□ 「개인정보의 안전성 확보조치 기준」 제4조(내부 관리계획의 수립 · 시행)에 따라 다음과 같이 유형별로 내부 관리계획 수립 여부를 다르게 적용한다.

- 유형1(완화)에 해당하는 개인정보처리자는 내부 관리계획을 수립하지 아니할 수 있다.
- 유형2(표준) 및 유형3(강화)에 해당하는 개인정보처리자는 내부관리계획을 수립하여야 한다.

<table>
<tr><th colspan="2" rowspan="2">구 분</th><th colspan="4">개인정보처리자의 개인정보 보유량 (전체 총합)</th></tr>
<tr><th>1만명 미만</th><th>1만명~10만명 미만</th><th>10만명~100만명 미만</th><th>100만명 이상</th></tr>
<tr><td rowspan="7">유형</td><td>공공기관</td><td colspan="2" rowspan="3">유형2(표준)</td><td colspan="2" rowspan="3">유형3(강화)</td></tr>
<tr><td>대기업</td></tr>
<tr><td>중견기업</td></tr>
<tr><td>중소기업</td><td colspan="3">유형2(표준)</td><td>유형3(강화)</td></tr>
<tr><td>소상공인</td><td rowspan="2">유형1(완화)</td><td colspan="3" rowspan="2">유형2(표준)</td></tr>
<tr><td>개인</td></tr>
<tr><td>단체</td><td>유형1(완화)</td><td colspan="2">유형2(표준)</td><td>유형3(강화)</td></tr>
</table>

□ 「개인정보 내부 관리계획」 구성 항목

- 유형2(표준)에 해당하는 개인정보처리자는 아래 구성 항목의 제12호부터 제14호까지를 내부 관리계획에 포함하지 아니할 수 있다.

구성 항목	유형2 (표준)	유형3 (강화)
1. 개인정보 보호책임자의 지정에 관한 사항	○	○
2. 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항	○	○
3. 개인정보취급자에 대한 교육에 관한 사항	○	○
4. 접근 권한의 관리에 관한 사항	○	○
5. 접근 통제에 관한 사항	○	○
6. 개인정보의 암호화 조치에 관한 사항	○	○
7. 접속기록 보관 및 점검에 관한 사항	○	○
8. 악성프로그램 등 방지에 관한 사항	○	○
9. 물리적 안전조치에 관한 사항	○	○
10. 개인정보 보호조직에 관한 구성 및 운영에 관한 사항	○	○
11. 개인정보 유출사고 대응 계획 수립·시행에 관한 사항	○	○
12. 위험도 분석 및 대응방안 마련에 관한 사항		○
13. 재해 및 재난 대비 개인정보처리시스템의 물리적 안전조치에 관한 사항		○
14. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항		○
15. 그 밖에 개인정보 보호를 위하여 필요한 사항	○	○

붙임 2 법적 근거

「개인정보 보호법」

제29조(안전조치의무)
개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

「개인정보 보호법 시행령」

제30조(개인정보의 안전성 확보 조치)
① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 하여야 한다.
1. 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행
(이하 생략)

③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 행정자치부장관이 정하여 고시한다.

'개인정보의 안전성 확보조치 기준' (제2023-6호, 행정자치부 고시)

제4조(내부 관리계획의 수립·시행)
① 개인정보처리자는 개인정보의 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 의사결정 절차를 통하여 다음 각 호의 사항을 포함하는 내부 관리계획을 수립·시행하여야 한다. 다만, 1만명 미만의 정보주체에 관하여 개인정보를 처리하는 소상공인·개인·단체의 경우에는 생략할 수 있다.
1. 개인정보 보호 조직의 구성 및 운영에 관한 사항
2. 개인정보 보호책임자의 자격요건 및 지정에 관한 사항
3. 개인정보 보호책임자와 개인정보취급자의 역할 및 책임에 관한 사항
4. 개인정보취급자에 대한 관리·감독 및 교육에 관한 사항
5. 접근 권한의 관리에 관한 사항
6. 접근 통제에 관한 사항
7. 개인정보의 암호화 조치에 관한 사항
8. 접속기록 보관 및 점검에 관한 사항
9. 악성프로그램 등 방지에 관한 사항
10. 개인정보의 유출, 도난 방지 등을 위한 취약점 점검에 관한 사항
11. 물리적 안전조치에 관한 사항
12. 개인정보 유출사고 대응 계획 수립·시행에 관한 사항
13. 위험 분석 및 관리에 관한 사항
14. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항
15. 개인정보 내부 관리계획의 수립, 변경 및 승인에 관한 사항
16. 그 밖에 개인정보 보호를 위하여 필요한 사항

② 개인정보처리자는 다음 각 호의 사항을 정하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 사업규모, 개인정보 보유 수, 업무성격 등에 따라 차등화하여 필요한 교육을 정기적으로 실시하여야 한다.
1. 교육목적 및 대상
2. 교육 내용
3. 교육 일정 및 방법

③ 개인정보처리자는 제1항 각 호의 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부 관리계획을 수정하여 시행하고, 그 수정 이력을 관리하여야 한다.

④ 개인정보 보호책임자는 접근 권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부 관리계획의 이행 실태를 연1회 이상 점검·관리 하여야 한다.