개인정보 내부관리계획 규정

제정 2014.00.00.
개정 2017.02.23.
일부개정 2022.09.19.
일부개정 2026.01.28.

제1장 총칙

제1조(목적) 이 규정은 계양구가족센터 개인정보 내부관리계획으로 「개인정보보호법」 제29조 등에 따라 시설에서 처리하는 개인정보가 분실, 도난, 유출, 변조, 훼손 등이 되지 않도록 체계적이고 안전하게 관리함을 목적으로 한다. (2022.09.19. 개정)

제2조(적용범위) 계양구가족센터(이하 "시설"이라 한다) 개인정보 내부관리계획(이하 "내부관리계획"이라 한다)은 전자적 처리 여부를 불문하고 수기문서를 포함한 모든 형태의 개인정보와 이러한 개인정보를 처리 또는 취급하는 직원 및 외부업체 직원 등에 적용된다. (2022.09.19. 개정)

제3조(정의) 내부관리계획에서 사용하는 용어의 뜻은 다음과 같다.

1. "개인정보"란 살아있는 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.
2. "처리"란 개인정보의 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 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 책임지거나 업무처리를 최종적으로 결정하는 자를 말한다.
7. "분야별 관리책임자"란 개인정보파일 보유 부서장 및 영상정보처리기기 설치·운영 부서장을 말한다.
8. "개인정보취급자"란 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 직접 개인정보에 관한 업무를 담당하는 자와 그 밖의 업무상 필요에 의해 개인정보에 접근하여 처리하는 모든 자를 말한다.

9. “개인정보처리시스템”이란 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다.
10. “영상정보처리기기”란 폐쇄회로텔레비전(CCTV), 네트워크카메라 등 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 일체의 장치를 말한다.
11. “개인영상정보”라 함은 영상정보처리기기에 의하여 촬영·처리되는 영상정보 중 개인의 초상, 행동 등 사생활과 관련된 영상으로서 해당 개인의 동일성 여부를 식별할 수 있는 정보를 말한다.
12. “영상정보처리기기 운영자”라 함은「개인정보보호법」제25조제1항 각호에 따라 영상정보처리기기를 설치·운영하는 자를 말한다.
13. “고유식별정보”란 주민등록번호, 여권번호, 운전 면허번호, 외국인등록번호 등 법령에 따라 개인을 고유하게 구별하기 위해 부여된 정보를 말한다.
14. “정보통신망”이란 「전기통신기본법」제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말한다.
15. “내부망”이라 함은 물리적 망분리, 접근통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.
16. “접속기록”이라 함은 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무 내역에 대하여 식별자, 접속일시, 접속자를 알 수 있는 정보, 수행업무 등 접속한 사실을 전자적으로 기록한 것을 말한다.
17. “바이오정보”란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.
18. “보조저장매체”라 함은 이동형 하드디스크, USB메모리, CD(Compact Disk), DVD(Digital Versatile Disk), 플로피디스크 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 용이하게 연결·분리 할 수 있는 저장매체를 말한다.
19. “위험도 분석”이란 개인정보처리시스템에 적용되고 있는 개인정보 보호를 위한 수단과 개인정보 유출 시 정보주체의 권리를 해할 가능성 및 그 위험의 정도를 분석하는 행위를 말한다.
20. “모바일 기기”라 함은 무선망을 이용할 수 있는 PDA, 스마트폰, 태블릿PC 등 개인정보 처리에 이용되는 휴대용 기기를 말한다.
21. “공개된 무선망”이라 함은 불특정 다수가 무선접속장치(AP)를 통하여 인터넷을 이용할 수 있는 망을 말한다.

제2장 분야별 내부관리계획의 수립 및 시행

제4조(계획의 수립 및 시행) ① 분야별 관리책임자는 소관분야 개인정보보호를 위한 관련 법령과 규정의 준수 등 전반적인 사항을 포함하는 분야별 내부관리계획을 자체 실정에 맞게 수립하여 시행할 수 있다.

② 분야별 관리책임자는 개인정보보호 관련 법령의 제·개정 사항 등 개인정보의 안전성 확보를 위한 중요 사항의 변경이 있는 경우에는 이를 즉시 반영하여 소관 분야별 내부관리계획을 수정하여 시행하고, 그 수정 이력을 관리하여야 한다.

제5조(내부관리계획의 공표) 분야별 관리책임자는 제4조에 따라 수립·개정된 분야별 내부관리계획을 전 직원이 언제든지 열람할 수 있도록 시설 내부 인트라넷 게시판(공지사항) 등에 게재 및 공표하여야 한다.

제3장 개인정보 보호책임자의 의무와 책임

제6조(개인정보 보호책임자의 자격요건 및 지정) 시설 개인정보 보호책임자는 다음 각 호의 자격요건을 갖추어야 한다.

1. 개인정보 보호책임자(CPO: Chief Privacy Officer) 직제를 신설하거나, 정보주체의 개인정보 보호 업무를 위해 조직된 부서의 장 등을 지정할 수 있다.
2. 개인정보 보호책임자는 정보보안 관련 지식뿐만 아니라 개인정보 취급에 관한 법·제도적인 측면 등의 다양한 지식을 습득할 필요가 있다.
3. 개인정보 보호책임자의 지정 시 인사발령 등을 통해 공식적으로 책임과 역할을 부여하여야 한다.

제7조(개인정보 보호책임자 등의 의무와 책임) ① 개인정보 보호책임자는 개인정보 보호를 위하여 다음 각 호의 업무를 수행한다.

1. 개인정보 보호책임자는 개인정보의 처리에 관한 업무를 총괄해서 책임지는 역할을 수행하는 사람으로, 개인정보 보호를 위해 개인정보와 관련된 내부지침을 준수하도록 기술적·관리적 보호조치를 실시하고 관리·감독하는 책임을 진다.
2. 정보주체의 불만사항 접수 및 처리에 대한 책임을 지며, 개인정보를 취급하는 직원에 대해 교육훈련을 실시하여야 한다.

② '개인정보취급자'는 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 자로서 개인정보를 처리함에 있어서 개인정보가 안전하게 관리될 수 있도록 해야 한다.

제4장 개인정보의 기술적·관리적 안전조치

제8조(접근권한의 관리) ① 분야별 관리책임자는 '행정기관 정보시스템 접근권한 관리규정'(국무총리훈령)에 따라 개인정보처리시스템에 대한 접근권한을 관리하여야 한다.

② 분야별 관리책임자는 개인정보처리시스템의 자료 오·남용 및 불법 사용을 방지하기 위하여 다음 각 호의 사항을 포함하는 개인정보처리시스템별 접근권한 관리계획을 수립·시행하여야 한다.

1. 접근권한의 관리체계
2. 접근권한 관리 책임자·담당자의 역할 및 임무
3. 접근권한 대상자별 접근권한의 범위
4. 접근권한의 승인절차, 심사 내용 및 방법, 접근권한의 점검
5. 기타 접근권한의 효율적 관리를 위하여 필요한 사항

③ 개인정보보호책임자는 '개인정보처리시스템 접근권한 관리계획(표준안)'을 마련하여 분야별 관리책임자의 개인정보처리시스템 접근권한 관리계획 수립을 지원할 수 있다.: 별표 1

④ 분야별 개인정보 관리책임자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여야 하며, 또한 비밀유지의무 등에 대한 서약서를 받아야 한다.

제9조(비밀번호 관리) 개인정보취급자는 비밀번호 설정 시 다음 각 호의 사항을 반영하여 숫자와 영문자, 특수문자 등을 혼합하여 9자리 이상으로 정하고, 분기 1회 이상 주기적으로 변경 사용하여야 한다.

1. 사용자 계정(ID)과 동일하지 않은 것
2. 개인 신상 및 부서명칭, 전화번호 등과 관계가 없는 것
3. 일반 사전에 등록된 단어 사용을 피할 것
4. 동일 단어(문자) 또는 숫자를 반복하여 사용하지 말 것
5. 사용된 비밀번호는 재사용하지 말 것
6. 규칙적인 문자·숫자열 등을 사용하지 말 것
7. 동일 비밀번호를 여러 사람이 공유하여 사용하지 말 것
8. 응용프로그램 등을 이용한 자동 비밀번호를 다르게 부여할 것
9. 관리자계정과 사용자계정의 비밀번호를 다르게 부여할 것
10. 초기 할당된 임시 비밀번호는 사용자 로그인 후 즉시 변경

제10조(접근통제) ① 개인정보 보호책임자는 정보 통신망을 통한 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 IP주소 등을 분석하여 불법적인 개인정보 유출 시도를 탐지

② 개인정보 보호책임자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는 가상사설망(VPN: Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하여야 한다.
③ 개인정보 보호책임자는 다른 법령에 근거하여 정보주체의 본인확인을 위해 주민등록번호를 사용할 수 있는 경우에도 인터넷 홈페이지에서는 다른 인증수단을 통하여 정보주체의 본인을 확인하여야 한다.
④ 개인정보 보호책임자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터 및 모바일 기기 등에 조치를 취하여야 한다.
⑤ 고유식별정보를 처리하는 분야별 관리책임자는 인터넷 홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점을 점검하여야 한다.
⑥ 분야별 관리책임자가 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 접근통제 기능을 이용할 수 있다.
⑦ 분야별 관리책임자는 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.

제11조(개인정보의 암호화) ① 시행령 제21조 및 시행령 제30조제1항제3호에 따라 암호화하여야 하는 개인정보는 고유식별정보, 비밀번호 및 바이오정보를 말한다.
② 분야별 관리책임자는 제1항에 따른 개인정보를 정보통신망을 통하여 송·수신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.
③ 분야별 관리책임자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 단, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.
④ 분야별 관리책임자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ: Demilitarized Zone)에 설치된 장비에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.
⑤ 분야별 관리책임자가 내부망에 고유식별정보를 저장하는 경우에는 다음 각 호의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.
1. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과
2. 위험도 분석에 따른 결과
⑥ 분야별 관리책임자는 제1항에 따른 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.
⑦ 분야별 관리책임자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

제11조 1(가명정보의 처리)

① 시설은 통계작성, 과학적 연구, 공익적 기록보존 등의 목적을 위하여 필요한 경우 「개인정보보호법」 제28조의2에 따라 정보주체의 동의 없이 가명정보를 처리할 수 있다.

② 가명정보를 처리하는 경우에는 재식별되지 않도록 추가 정보의 분리보관 등 안전조치를 하여야 한다.

③ 가명정보의 처리 절차 및 관리에 관한 사항은 개인정보 보호책임자가 별도로 정한다.

제12조(접속기록의 보관 및 위·변조 방지) ① 분야별 관리책임자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 최소 6개월 이상 보관·관리하여야 한다.

② 분야별 관리책임자는 개인정보의 유출·변조·훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 반기별로 1회 이상 점검하여야 한다.

③ 분야별 관리책임자는 개인정보취급자의 접속기록이 위·변조 및 도난, 분실 등이 되지 않도록 정기적인 접속기록의 분석과 백업을 수행하여 안전하게 보관하여야 한다.

제13조(악성프로그램 등 방지) 분야별 관리책임자는 개인정보처리시스템 또는 업무용 컴퓨터에 악성 프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다.

1. 보안 프로그램의 자동업데이트 기능을 사용하거나, 또는 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지
2. 악성 프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제(OS) 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 실시

제14조(주민번호 대체수단 도입) 분야별 관리책임자는 정보주체가 인터넷 홈페이지에 회원으로 가입할 경우 주민등록번호를 사용하지 않고도 회원으로 가입할 수 있는 방법을 제공하여야 한다.

제15조(물리적 접근방지) ① 개인정보 보호책임자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 한다.

② 분야별 관리책임자는 개인정보가 포함된 서류, 보조기억매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.

③ 분야별 관리책임자는 정보보안 업무지침의 'USB메모리 등 휴대용 저장매체 보안관리 지침'에 따라 보조저장매체의 반출·입을 통제하여야 한다.

제5장 개인정보보호 교육

제16조(개인정보보호 교육 계획의 수립) ① 개인정보 보호책임자는 다음 각 호의 사항을 포함하는 연간 개인정보보호 교육계획을 수립하여야 한다.

1. 교육목적 및 대상
2. 교육내용
3. 교육 일정 및 방법

② 개인정보 보호책임자는 개인정보 보호 교육을 실시한 이후에 교육의 성과와 개선 필요성 등을 검토하여 다음연도 교육계획에 반영하여야 한다.

제17조(개인정보보호 교육의 실시) ① 개인정보보호 교육의 목적은 안전하게 개인정보가 관리될 수 있도록 개인정보취급자의 개인정보보호에 대한 인식을 제고시키고 개인정보보호 대책의 필요성을 이해시키는 것이다.

② 교육 방법은 집체교육 뿐 아니라 조직의 환경을 고려하여 인터넷 교육, 그룹웨어 교육 등 다양한 방법을 활용하여 실시하도록 하고, 필요한 경우 외부 전문기관이나 전문요원에 위탁하여 교육을 실시할 수도 있다.

③ 그 밖에 개인정보 보호를 위하여 필요한 사항으로는 개인정보처리자의 개인정보 운용(수집·이용·저장·제공·파기 등) 환경 및 중요도(민감정보 취급 등)를 고려하여 보안서약서 작성 등 개인정보 보호를 위하여 필요한 사항을 기술할 수 있다.

제6장 개인정보 침해대응 및 피해구제

제18조(개인정보 침해사고 대응) ① 개인정보 보호책임자는 개인정보 유출 및 침해 사고 발생에 대비하여 그 피해를 최소화하기 위하여 '시설 개인정보 침해사고 대응계획'을 수립·시행하여야 한다.: 별표 2

② 분야별 관리책임자는 개인정보가 유출되었음을 알게 되었을 때에는 지체 없이 개인정보 유출신고서를 작성하여 개인정보 보호책임자에게 보고하여야 한다.

③ 분야별 관리책임자는 개인정보가 유출되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 서면 등의 방법으로 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 지체 없이 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. 개인정보처리자의 대응조치 및 피해 구제절차

5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

④ 분야별 관리책임자는 제3항에도 불구하고 구체적인 유출 내용을 확인하지 못한 경우에는 해당 정보주체에게 개인정보가 유출된 사실과 유출이 확인된 사항만을 서면 등의 방법으로 먼저 알리고 나중에 확인되는 사항을 추가로 알릴 수 있다.

⑤ 개인정보 보호책임자는 제3항과 제4항에도 불구하고 1만명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 서면 등의 방법과 함께 인터넷 홈페이지에 정보주체가 알아보기 쉽도록 제3항 각 호의 사항을 7일 이상 게재하여야 한다.

⑥ 개인정보 보호책임자는 1만명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 제3항에 따른 통지 및 피해상황 최소화 조치내역을 지체 없이 행정안전부 또는 관련 전문기관(한국정보화진흥원·한국인터넷진흥원)에 신고하여야 한다.

제19조(정보주체의 권익침해 구제) ① 개인정보 보호책임자는 개인정보주체의 권익 보호를 위하여 기관 홈페이지 등에 개인정보 처리목적과 개인정보 처리 및 보유기간, 제3자 제공 현황 및 목적 외 이용에 관한 사항, 개인정보처리 위탁 등과 정보주체의 권리·의무 및 그 행사방법에 관한 사항 등을 게재하여야 한다.

② 분야별 관리책임자는 정보주체가 개인정보 열람거절 등의 행정 조치에 대하여 불복이 있는 경우 이의를 제기할 수 있도록 안내하여야 한다.

③ 분야별 관리책임자는 정보주체가 행정기관의 개인정보 처리조치에 대하여 불복이 있거나 개인정보침해 사항을 신고하고자 하는 경우에는 다음각 호의 관련기관을 안내하여야 한다.

1. 개인정보분쟁조정위원회: 02-405-5150 (www.kopico.or.kr)

2. 개인정보침해신고센터: (국번없이) 118 (privacy.kisa.or.kr)

④ 분야별 관리책임자는 개인정보 유출 또는 침해 사고로 의심되는 정황이 발견될 경우에는 개인정보 보호책임자에게 보고하여야 하며, 다음 각 호의 관련기관의 수사 필요시 적극 협조하여야 한다.

1. 대검찰청 사이버범죄수사단: 02-3480-3571 (cybercid@spo.go.kr)

2. 경찰청 사이버테러대응센터: 1566-0112 (www.netan.go.kr)