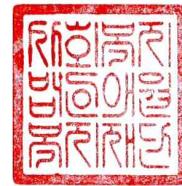


운 영 지 침



따뜻한 서비스, 건강한 공동체
신내종합사회복지관

개인 및 기관의 정보보호지침

제정 2012.12.20

제1조(목적) 이 규정은 「개인정보보호법」의 관련 조항에 따라 기관이 취급하는 개인·기관의 정보를 체계적으로 관리하여 개인·기관의 정보가 분실, 도난, 누출, 변조, 훼손, 오·남용 등이 되지 않도록 관련 사항에 대해 규정하는 것을 목적으로 한다.

제2조(적용범위) 이 규정은 개인·기관의 정보처리시스템, 컴퓨터 파일, 서면, 우편, 전화, 팩스, 이메일, 영상정보처리기기, 홈페이지, SNS 등 온라인 및 오프라인을 통해 수집, 이용, 제공 또는 관리되는 개인·기관의 정보에 대해 적용되며, 이러한 개인·기관의 정보를 취급하는 직원 및 외부업체 직원에 대해 적용된다.

제3조(용어 정의 및 책임자의 지정) 이 규정에서 사용하는 용어의 정의는 다음과 같다.

1. 기관이 관리하는 개인정보”란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보를 말한다.
2. “정보주체”란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의주체가 되는 사람을 말한다.
3. “개인·기관의 정보보호책임자”란 개인정보 처리에 관한 업무를 총괄해서 책임지거나 업무처리를 최종적으로 결정하는 자를 말하며 기관의 장을 말한다.
4. “개인·기관의 정보보호관리자”란 개인정보 처리에 관한 업무를 총괄하여 관리하는 자를 말하며 기관의 장이 직원 중 선정하여 그 임무를 부여한 자를 말한다.(외부업체위탁자포함)
5. “개인·기관의 정보취급자”란 개인정보를 보관, 처리, 이용, 제공, 관리 또는 파기 등의 업무를 하는 자를 말하며 개인정보를 사용하는 모든 직원을 말한다.
6. “개인·기관의 정보처리시스템”이란 개인정보를 처리할 수 있도록 체계적

으로 구성된 데이터베이스시스템을 말한다.

7.“개인·기관의 정보 자료”란 처리정보를 쉽게 검색할 수 있도록 일정한 형식에 따라 체계적으로 배열하거나 구성된 개인정보의 집합물로 컴퓨터 파일, 수기문서, 출력물 등을 말한다.

8.“영상정보처리기기”란 폐쇄회로텔레비전(CCTV), 네트워크카메라 등 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유무선망을 통하여 전송하는 일체의 장치를 말한다.

제4조(개인정보보호준수의무) 1.개인·기관의 정보보호책임자는 개인정보보호를 위한 법령 및 본 규정을 준수하여 하여야 한다.

2.개인정보보호책임자는 개인정보보호 관련 법령의 제·개정 사항 등을 반영하기위하여 이 규정을 개정할 필요가 있다고 판단되는 경우 개정하여야 한다.

제5조(공표) 이규정은 직원이 언제든지 열람할 수 있도록 하여야 하며, 변경사항이 있는 경우에는 이를 공지하여야 한다.

제6조(개인정보보호책임자의 의무와 책임) 개인정보보호책임자는 정보주체의 개인정보보호를 위하여 다음 각 항의 업무를 수행한다.

- 1.개인·기관의 정보 보호 계획의 수립 및 시행
- 2.개인·기관의 정보 처리 실태 및 관행의 정기적인 조사 및 개선
- 3.개인정보 처리와 관련한 불만의 처리 및 피해 구제
- 4.개인·기관의 정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
- 5.개인·기관의 정보 보호 교육 계획의 수립 및 시행
- 6.개인·기관의 정보 자료의 보호 및 관리 감독
- 7.개인·기관의 정보 보호 관련 자료의 관리
- 8.처리 목적이 달성되거나 보유기간이 지난 개인·기관의 정보의 파기

제7조(개인정보보호관리자의 의무와 책임) 개인·기관의 정보보호관리자는 정보주체의 개인정보 보호를 위하여 다음 각 항의 업무를 수행한다.

- 1.개인·기관의 정보처리시스템을 이용하는 소관부서 직원에 대한 개인정보 보호업무의 지도·감독

- 2.개인 • 기관의 정보처리시스템의 사용자 권한설정에 관한 사항의 확인·감독
- 3.개인 • 기관의 정보 오·남용 사고의 예방
- 4.기타 소관분야별 개인정보 보호를 위해 필요한 사항 등

제8조(개인정보취급자의 의무와 책임) 개인 • 기관의 정보취급자는 정보보호와 관련하여 다음 각 항의 의무 및 책임이 있다.

- 1.개인 • 기관의 정보보호 활동 참여
- 2.개인 • 기관의 정보보호 업무처리 지침의 준수 및 이행
- 3.개인 • 기관의 정보의 기술적·관리적 보호조치 기준 이행
- 4.소관 부서 또는 사업기관의 개인정보 현황 파악
- 5.업무상 알게 된 개인정보를 제3자에게 제공하지 않음

제9조(접근권한 관리 및 인증) 1.개인정보처리 • 기관정보 시스템관리자는 개인 • 기관의 정보처리시스템에 대한 접근권한을 업무 수행에 필요한 최소한의 범위로 업무담당자에 따라 차등 부여한다.

- 2.개인 • 기관의 정보처리시스템관리자는 전보 또는 퇴직 등 인사이동이 발생하여 취급자가 변경되었을 경우 지체 없이 개인 • 기관의 정보처리시스템의 접근권한을 변경 또는 말소 하여야 한다.
- 3.개인 • 기관의 정보처리시스템관리자는 정보처리시스템에 접속할 수 있는 사용자 계정을 발급하는 경우 개인 • 기관의 정보취급자별로 한 개의 사용자 계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

제10조(비밀번호 관리) 1.개인 • 기관의 정보처리시스템의 비밀번호는 영문, 숫자, 특수기호 등을 조합하여 유추가 어렵도록 설정하고 주기적으로 변경하여야 한다.

- 2.비밀번호 작성원칙은 다음의 각 호와 같다.
 - ① 추측하기 어려운 비밀번호를 생성한다.
 - ② 비밀번호는 최소 6개월마다 변경한다.
 - ③ 동일 단어(문자) 또는 숫자를 반복하여 사용하지 않는다.
 - ④ 동일 비밀번호를 여러 사람이 공유하여 사용하지 않는다.

제11조(접근통제) 모든 직원은 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 하여야 한다.

제12조(보안프로그램 설치 및 운영) 1.모든 직원은 개인정보처리시스템 또는 업무용 컴퓨터에 악성 프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 한다.

2.모든 직원은 보안 프로그램의 자동 업데이트 기능을 사용하거나 일 1회 이상 업데이트를 적용하여야 한다.

3.모든 직원은 악성 프로그램관련 정보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우즉시 이에 따른 업데이트를 적용하여야 한다.

제13조(접근제한) 1.개인·기관의 정보보호관리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입을 통제 하여야 한다.

2.개인·기관의 정보보호관리자는 물리적 접근방지를 위한 별도의 보호시설에 출입하거나 개인정보를 열람하는 경우, 그 출입자에 대한 출입사실 및 열람 내용에 관한 관리대장을 작성하도록 하여야 한다.

3.모든 직원은 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.

제14조(정보보호 교육의 실시) 1.개인·기관의 정보보호책임자는 정보주체 정보보호에 대한 직원들의 인식제고를 위해 노력해야 하며, 개인정보의 오·남용 또는 유출 등을 적극 예방하기 위해 임·직원을 대상으로 매년 정기적으로 연1회 개인정보보호 교육을 실시한다.

2.개인·기관의 정보보호책임자는 교육 방법은 집체 교육뿐만 아니라, 인터넷 교육, 그룹웨어 교육 등 다양한 방법을 활용하여 실시하고, 필요한 경우 외부 전문기관이나 전문요원에 위탁하여 교육을 실시한다.

제15조(정보유출 징계) ①개인·기관의 정보 취급 및 사용을 직원이 고의적으로 그 정보를 유출 하거나 그 정보를 이용하여 직원 개인이 이익 취할 경

우 기관 인사위원회의 심의를 걸쳐 징계할 수 있다.

②정보유출에 대한 내용에 있어 손해 또는 규모가 클 경우 관련 규정에 따라 고발 조치하여야 한다.

제16조(사전 동의 및 공유금지) 기관은 개인정보수집에 있어 각호를 준수하여야 한다.

1. 정보수집의 목적과 사용범위 및 사용기간, 동의를 거부할 권리, 삭제, 삭제요청, 불이익이 있는 경우에는 그 불이익의 내용 등을 정보제공자에게 사전에 설명하고 동의를 얻어야 한다.
2. 수집 하고자 하는 정보는 최소한으로 하여야 한다.
3. 수집된 정보는 본 목적에만 사용 하여야 한다.
4. 수집된 정보는 직원 간에 공유 및 외부 유출을 원칙적으로 금지하되 공유필요시 최소한의 정보를 관리자 임회하에 공유 할 수 있다.

제17조(정보 유출 대응 및 통지) 1. 개인 • 기관의 정보보호관리자는 개인 • 기관의 정보가 유출되었음을 알게 되었을 때에는 보호책임자에게 개인정보 유출신고서를 작성하여 보고한다.

2. 개인 • 기관의 정보 보호책임자는 서면, 우편, 전화, 전자우편 등의 방법으로 5일 이내에 유출된 개인정보의 항목, 시점, 경위 등 법령에서 정하는 사항을 해당 정보주체에게 알린다.

3. 개인 • 기관의 정보 보호책임자는 개인정보가 유출된 경우 정보주체가 알 수 있도록 7일 이상 홈페이지에 게재한다.

제18조(권익침해 구제방법) 개인정보침해로 인한 구제를 받기 위하여 개인정보 분쟁조정위원회, 한국인터넷진흥원 개인정보침해신고센터 등에 분쟁해결이나 상담 등을 신청할 수 있다.

제19조(정보파기) ①정보관리자는 개인 • 기관의 정보보유기간종료, 사업종료 시에는 관련정보를 삭제 • 파세기로 파기 하여야 한다.

②개인, 팀, 기관의 정보 파기 요청시 불이익이 발생된다면 충분히 설명하고 그 정보를 기관장의 승인 하에 파기 한다.