강릉원주대학교

2019년 개인정보 내부 관리계획(안)

2019. 1.

강 릉 원 주 대 학 교

목 차

목 차

목 차

제1장 총칙

제1조(목적)

개인정보보호 내부관리계획(이하 '본 계획' 또는 '내부관리계획'이라 한다)은 개인정보의 안전성 확보조치 기준 제3조에 의거하여 제정된 것으로 강릉원주대학교(이하 '본교'라 한다)가 취급하는 개인정보를 체계적으로 관리하여 개인정보가 분실, 도난, 누출, 변조, 훼손, 오·남용 등이 되지 아니하도록 함을 목적으로 한다.

제2조(적용범위)

본 계획은 정보통신망을 통하여 수집, 이용, 제공 또는 관리되는 개인정보뿐만 아니라 서면 등 정보통신망 이외의 수단을 통해서 수집, 이용, 제공 또는 관리되는 개인정보 및 영상정보처리기기(CCTV)에 대해서도 적용되며, 이러한 개인정보를 취급하는 내부 교직원 및 외부업체 직원에 대해 적용된다.

제3조(용어의 정의)

이 계획에서 사용하는 용어의 뜻은 다음과 같다.

1. "개인정보"란 살아 있는 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 있는것을 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(이하 "보호책임자"이라 한다)"란 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 최종적으로 책임지는 자로서, 개인정보 보호법 시행령 제32조제2항에 해당하는 자를 말한다.

7. "개인정보 보호담당자(이하 "보호담당자"라 한다)"란 개인정보 보호책임자가 업무를 수행함에 있어 보조적인 역할을 하는 자를 말하며, 개인정보 보호책임자가 일정 요건의 자격을 갖춘 자를 지정한다.
8. "개인정보 분야별책임자(이하 "분야별책임자"이라 한다)"이란 개인정보 보호책임자가 개인정보보호 관련 업무의 효율적인 관리·운용을 위하여 지정한 부서장(처장,원장,관장,학부장,학과장 등)을 말한다.
9. "개인정보취급자"란 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 임직원, 파견근로자, 시간제근로자 등을 말한다.
10. "개인정보처리시스템"란 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템을 말한다.
11. "고유식별정보"란 개인을 고유하게 구별하기 위하여 부여된 식별정보를 말하며, 대통령령으로 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호 등을 정하고 있다.
12. "접속기록"이라 함은 개인정보취급자 등이 개인정보처리시스템에 접속한 사실을 알수 있는 계정, 접속일시, 접속자 정보, 수행업무 등을 전자적으로 기록한 것을 말한다. 이 경우, "접속"이란 개인정보처리시스템과 연결되어 데이터 송신 또는 수신이 가능한 상태를 말한다.
13. "정보통신망"이란 「전기통신기본법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말한다.
14. "내부망"이란 물리적 망분리, 접근 통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.
15. "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.
16. "바이오정보"란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.
17. "보조저장매체"란 이동형 하드디스크(HDD), 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. "위험도 분석"이란 개인정보 유출에 영향을 미칠 수 있는 다양한 위험요소를 식별·평가하고 해당 위험요소를 적절하게 통제할 수 있는 방안을 위해 종합적으로 분석하는 행위를 말한다.
19. "모바일 기기"라 함은 무선망을 이용할 수 있는 PDA, 스마트폰, 태블릿 PC 등 개인정보처리에 이용되는 휴대용 기기를 말한다.

20. “공개된 무선망”이라 함은 불특정 다수가 무선접속장치(AP)를 통하여 인터넷을 이용할 수 있는 망을 말한다.
21. “수탁자”란 개인정보 처리 업무를 위탁 받아 처리하는 자를 말한다.
22. “관리용 단말기”란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리시스템에 직접 접속하는 단말기를 말한다.

제2장 내부관리계획의 수립 및 시행

제4조(내부관리계획의 수립 및 승인)

1. 개인정보 보호담당자는 본교 개인정보보호를 위한 전반적인 사항을 포함하여 내부관리계획을 수립하여야 한다.
2. 개인정보 보호담당자는 개인정보보호를 위한 내부관리계획의 수립 시 개인정보보호와 관련한 법령 및 관련 규정을 준수하도록 내부관리계획을 수립하여야 한다.
3. 개인정보 보호책임자는 개인정보 보호담당자가 수립한 내부관리계획의 타당성을 검토하여 개인정보보호를 위한 내부관리계획을 승인하여야 한다.
4. 개인정보 보호담당자는 개인정보보호 관련 법령의 제.개정 사항 등을 반영하기 위하여 내부관리계획의 타당성과 개정 필요성을 검토하여야 한다.
5. 개인정보 보호담당자는 모든 항목의 타당성을 검토한 후 수정할 필요가 있다고 판단되는 경우 내부관리계획의 수정안을 작성하여 개인정보 보호책임자에게 보고하고 개인정보보호책임자의 승인을 받아야 한다.
6. 개인정보 보호책임자는 연 1회 이상으로 내부 관리계획의 이행 실태를 점검·관리하여야 한다.

제5조(내부관리계획의 공표)

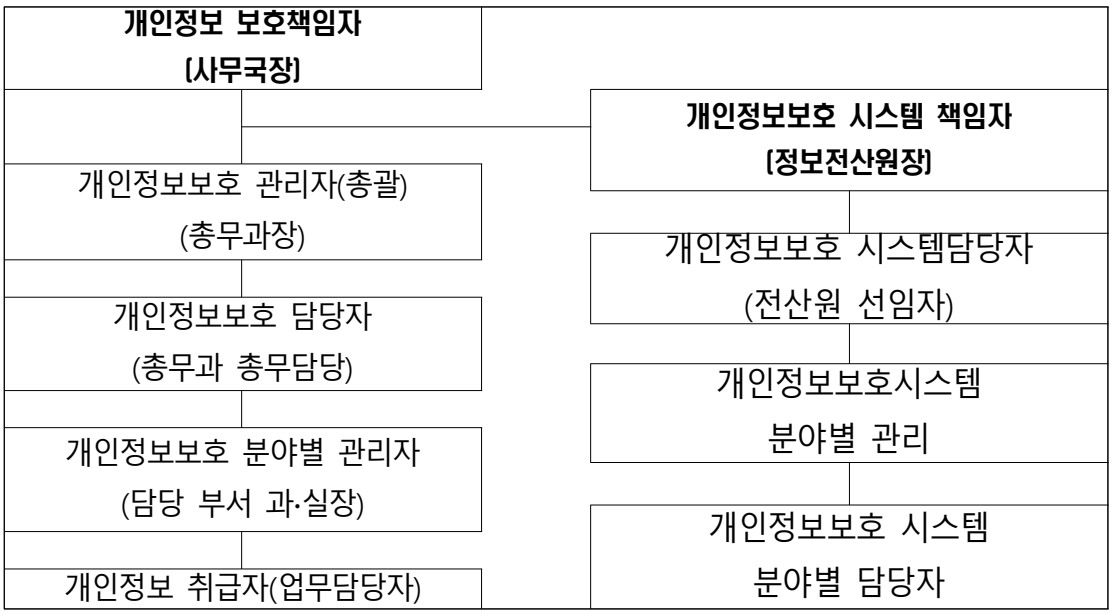
1. 개인정보 보호책임자는 승인한 내부관리계획을 전교직원에게 공표한다.
2. 내부관리계획은 교직원이 언제든지 열람할 수 있는 방법으로 비치하여야 하며, 변경사항이 있는 경우에는 이를 공지하여야 한다.

제3장 개인정보보호 관리 체계

제6조(개인정보 보호조직 구성과 개인정보 보호책임자의 지정)

본교의 개인정보 보호조직 구성은 아래와 같으며, 개인정보 보호법 시행령 제32조 제2항 제1호에 따라 해당하는 지위에 있는 사무국장을 개인정보 보호책임자(CPO : Chief Privacy Officer)로 지정한다.

개인정보 보호 조직도



제7조(개인정보 보호 조직별 역할과 책임)

직책	담당자	역할 및 책임
개인정보 보호 책임자	사무국장	- 개인정보 보호 계획의 수립 및 시행 - 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선 - 개인정보 처리와 관련한 불만의 처리 및 피해 구제 - 개인정보파일의 보호 및 관리·감독 - 개인정보보호 및 사용자에 대한 교육계획 수립 및 시행
개인정보보호 관리자/	- 총무과장(총괄) - 주요부서과 •	- 개인정보파일의 보호 및 관리·감독 - 개인정보취급자의 개인정보처리 이력

분야별관리자	실장 및 선임자	- 개인정보 처리와 관련된 불만 처리 - 부서 내 개인정보보호 업무 추진계획 수립 - 부서 내 개인정보보호 담당자와 취급자 지정 - 부서 내 개인정보보호 대책의 운영 관리 책임 - 부서 내 개인정보처리시스템 접근 권한 관리 - 개인정보보호 서약서 징구 - 부서 내 개인정보보호 관련 보안관리 활동 - 부서 내 개인정보 관리 현황 정기 점검 - 부서 내 개인정보취급자 명단 관리 - 부서 내 개인정보 침해사고 및 관리현황 보고 - 기타 개인 정보 보호 관리자가 요구하는 사항 처리
부서별 개인 정보보호 담당자	개인정보보호 관리자(책임자)가 지정하는 자	- 개인정보보호 관리자(책임자)를 보좌하여 개인정보 보호업무에 대한 실무
부서별 개인정보 취급자	서비스 운영자 및 개인정보에 접근 가능한 자	- 부서별 개인정보 처리 관련 업무 수행 - 개인정보보호 규정 준수 및 처리활동 수행 - 보유 개인정보 보호 · 관리
개인정보보호 시스템 책임자	정보전산원장	- 대학 내 운영되는 전산시스템의 정보보호 및 개인정보 보호 계획의 수립 및 시행 - 대학 내의 모든 전산시스템의 보호·및 관리감독 - 개인정보보호를 위한 시스템 도입 계획수립 및 시행
개인정보보호 시스템 담당자	정보전산원 주무 또는 선임자	- 개인정보보호시스템 책임자를 보좌하여 전산시스템의 정보보호와 개인정보보호의 업무를 수행 - 시스템운영과 관련된 자체계획의 수립 및 감독 - 대학 내 시스템으로 운영되는 홈페이지, 서버 등의 정보보호와 개인정보보호 업무의 지휘·감독 - 개인정보보호와 관련된 정책의 수립 및 집행
개인정보보호 시스템 분야별 관리자	운영부서장 또는 과·실장	- 부서에서 운영 중인 홈페이지 및 전산시스템의 정보 보호와 개인정보 보호를 위한 기본계획 수립 및 운영 - 소속부서 사용자 컴퓨터 개인정보보호에 관한 업무 - 소속부서 개인정보보호에 관련된 제반 업무
개인정보보호 시스템별 담당자	운영부서 선임자	- 개인정보보호 시스템 분야별 관리자를 보좌하여 개인정보 보호 및 정보보호에 관련된 업무 추진 - 운영 중인 홈페이지 및 전산시스템의 정보보호 및 개인정보보호와 관련된 업무의 수행

제4장 개인정보의 기술적 · 관리적 · 물리적 보호조치

제8조(개인정보 물리적 접근제한 및 관리)

1. 개인정보 보호책임자는 개인정보시스템, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 한다.
2. 분야별책임자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.
3. 분야별책임자는 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안대책을 마련하여야 한다.
4. 분야별책임자는 물리적 접근방지를 위한 별도의 보호시설에 출입하거나 개인정보를 열람하는 경우, 그 출입자에 대한 출입사실 및 열람 내용에 관한 관리대장을 작성하도록 하여야 한다.
5. 분야별책임자는 물리적 접근제한 관리대장의 출입 및 열람 내용을 주기적으로 검토하여 정당하지 않은 권한으로 출입하거나 열람하는 경우가 있는지를 점검하여 확인하여야 한다.

제9조(개인정보 출력 복사 시 보호조치)

1. 분야별책임자는 개인정보가 포함된 정보를 출력하거나 복사할 경우에 개인정보 유출사고를 방지하기 위한 보호조치를 취하여야 한다.
2. 분야별책임자는 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. 개인정보의 이용을 위하여 출력 및 복사한 개인정보의 이용 목적이 완료된 경우 분쇄기로 분쇄하거나 소각하는 등의 안전한 방법으로 파기하여야 한다.

제10조(개인정보취급자 접근권한 관리)

1. 개인정보처리시스템에 대한 접근 권한을 서비스 제공에 필요한 최소한의 인원에게만 부여한다.
2. 개인정보취급 업무를 담당하는 교직원의 담당업무에 따라 개인정보 취급권한을 부여 및

부서별/업무별에 따라 개인정보에 대한 접근권한을 차등 부여한다.

3. 개인정보취급자가 전보 또는 퇴직 등 인사이동으로 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소한다.
4. 개인정보 보호책임자는 제2항 내지 제3항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관한다.
5. 개인정보처리시스템에 접속할 수 있는 사용자 계정을 발급하는 경우, 개인정보취급자 별로 한 개의 사용자 계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

제11조(개인정보의 암호화)

1. 고유식별정보(주민등록번호, 여권번호, 운전면허번호, 외국인등록번호) 및 비밀번호, 바이오정보에 대해서는 안전한 암호 알고리즘으로 암호화하여 저장하도록 한다. 단, 비밀번호를 저장하는 경우에는 복호화되지 않도록 일방향 암호화하여 저장하여야 한다.

   가. 비밀번호 최소 길이: 구성 문자의 종류에 따라 10자리 또는 8자리이상으로 구성

   1) 최소 10자리 이상: 영대문자(A~Z, 26개), 영소문자(a~z, 26개), 숫자(0~9, 10개) 및 특수문자(32개)중 2종류 이상으로 구성한 경우

   2) 최소 8자리 이상: 영대문자(A~Z, 26개), 영소문자(a~z, 26개), 숫자(0~9, 10개) 및 특수문자(32개)중 3종류 이상으로 구성한 경우

   나. 추측하기 어려운 비밀번호 생성

   1) 생성한 비밀번호에 12345 등과 같은 일련번호, 전화번호 등 쉬운 문자열 포함금지

   2) love, happy 등과 같은 잘 알려진 단어, 키보드 상 나란히 있는 문자열 포함 금지

   다. 비밀번호 주기적 변경: 비밀번호 유효기간(3개월)설정, 장기간 사용 금지

   라. 동일한 비밀번호 사용 제한: 2개의 비밀번호 교대 사용 금지

   마. 국가정보보안 기본 지침 제39조(비밀번호관리) 및 개인정보안전성 확보조치 기준 제4조(접근권한의 관리) 준수

2. 제1항에 따른 개인정보를 정보통신망을 통하여 송·수신 하거나 보조저장매체등을 통하여 전달하는 경우에는 이를 암호화하여야 한다. 또한, 업무와 관련된 메일은 교내메일을 사용하여야 한다.
3. 개인정보취급자는 정보주체의 개인정보를 업무용 컴퓨터 또는 모바일 기기에 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화하여 저장해야 한다.
4. 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized

Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.

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

제12조(접근통제시스템의 설치 및 운영)

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

   가. 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol) 주소 등으로 제한하여 인가받지 않은 접근을 제한

   나. 개인정보처리시스템에 접속한 IP(Internet Protocol) 주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지 및 대응

2. 정보통신망을 통해 외부에서 개인정보처리시스템에 접속 하려는 경우에는 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단 또는 안전한 인증수단을 적용하여야 한다.

3. 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통해 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 업무용컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제에 관한 조치를 취하여야 한다.

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

5. 별도의 개인정보처리시스템을 이용하지 아니하고 업무용 컴퓨터 또는 모바일기기를 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.

6. 인터넷홈페이지에서 다른 법령에 근거하여 정보주체의 본인확인을 위해 성명, 주민등록번호를 사용할 수 있는 경우에도 정보주체의 추가적인 정보를 확인하여야 한다.

7. 고유식별정보를 처리하는 개인정보처리자는 인터넷홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점을 점검하여야 한다.

8. 개인정보처리자는 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.

제13조(비밀번호 관리)

1. 개인정보취급자가 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 한다.
2. 개인정보취급자 및 정보주체가 본교「정보보안 기본지침」제24조에 따라 비밀번호를 관리할 수 있도록 한다.

제14조(접속기록의 보관 및 점검)

1. 개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리하는 경우 처리일시, 처리내역 등 접속기록을 저장하도록 하여야 하며, 개인정보처리시스템에 접속한 기록을 최소 6개월 이상 보관·관리 하여야 한다.
2. 개인정보처리시스템의 접속기록이 위·변조 및 도난, 분실되지 않도록 안전하게 보관하여야 한다.
3. 개인정보책임자는 개인정보의 유출·변조·훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 반기별 1회 이상 점검하여야 한다.

제15조(악성프로그램 등 방지)

1. 개인용 컴퓨터(PC) 등을 이용하여 개인정보를 취급하는 경우 개인정보가 분실, 도난, 누출, 변조 또는 훼손되지 아니하도록 안전성 확보를 위한 백신 프로그램 등의 보안 프로그램을 설치.운영하여야 한다.
2. 보안 프로그램은 자동 업데이트 기능을 사용하거나 일 1회 이상 업데이트를 적용하여 항상 최신의 상태로 유지하며 정기적으로 PC 검사·치료 하여야 한다.
3. 악성 프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 즉시 이에 따른 업데이트를 실시하여야 하며 발견된 악성프로그램 등에 대해서는 삭제 대응 조치를 하여야 한다.

제16조(오프라인을 통한 개인정보 이용·제공시 안전성 확보)

1. 개인정보를 오프라인으로 제공시 보안 USB 등 보안성이 높은 저장매체를 활용하며 처리정보를 보호할 수 있도록 반드시 암호화하여 제공하여야 한다.
2. 처리정보를 안전하게 이동한 후 그 저장매체의 처리정보가 복구 될 수 없도록 파기 조치하여야 한다.

제17조(개인정보 비밀유지)

1. 업무 목적으로 개인정보를 취급하는 모든 개인정보 취급자를 대상으로 다음의 사항을 포함하여 "정보보호 서약서"를 징구한다.

   가. 업무 중 알게 된 개인정보에 대한 비밀 준수

   나. 개인정보보호를 위한 본교의 규정의 준수

   다. 정당한 절차 없이 개인정보를 무단으로 조회, 누출 금지

   라. 개인정보보호법 및 본교의 개인정보보호 규정의 숙지

   마. 위반 시 형사・민사의 책임

2. 본교의 개인정보 취급자 이외에도 개인정보의 취급 위탁 또는 제3자 제공 등의 경우에도 제1항의 개인정보에 관한 비밀유지 조항을 포함하여, 제3자 제공금지, 사고 시 손해배상 등 을 포함한 "개인정보 위탁 제공 계약서"를 작성하여야 한다.

제18조(관리용 단말기의 안전조치)

정보처리자는 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

제19조(재해·재난 대비 안전조치)

1. 개인정보 보호책임자는 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검하여야 한다.
2. 개인정보 보호책임자는 재해·재난 발생 시 개인정보처리시스템 백업 및 복구를 위한 계획을 마련하여야 한다.

제20조(위험도 분석 및 대응)

1. 개인정보처리시스템에서 처리되는 개인정보를 자산으로 관리하여야 한다.

   가. 개인정보를 구분하여 자산으로 식별하여 관리

   나. 개인정보 보호책임자는 개인정보 자산식별 및 분류가 적절히 관리되고 있는지 관리·감독

다. 개인정보 보호담당자는 개인정보 자산에 대하여 정기적으로 관리하여 최신화

2. 자산으로 분류된 개인정보는 위험도를 분석하고 대응방안을 수립하여 관리하여야 한다.

가. 개인정보 보호담당자는 관리하는 개인정보 자산에 대하여 주기적인 위험평가를 수행하여 위험요소를 최소화

나. 위험평가를 통해 발견된 위험요소를 최소화하기 위하여 개선방안을 마련하여 개선조치를 수행

다. 개인정보 보호담당자는 위험요소에 대한 개선조치가 잘되었는지 여부를 관리·감독

라. 개인정보영향평가 대상이 되는 개인정보처리시스템에 대하여는 개인정보영향평가를 통해 위험평가 및 관리

제5장 정기적인 자체점검

제21조(자체점검 주기 및 절차)

1. 개인정보관리책임자는 개인정보보호를 위한 내부관리 계획 및 관련 법령에서 정하는 개인정보보호 규정을 성실히 이행하는지를 주기적으로 점검하여야 한다.
2. 개인정보 자체점검을 위한 대상, 절차 및 방법 등 점검의 실시에 관하여 필요한 별도의 계획을 수립할 수 있다.
3. 개인정보보호 자체점검은 최소 년 1회 이상 실시한다.

제22조(자체점검 결과 반영)

1. 개인정보 보호를 위한 자체점검 실시 결과, 개인정보의 관리·운영상의 문제점을 발견하거나 관련 직원이 본 계획의 내용을 위반할 때에는 시정·개선 또는 인사발령 등 필요한 조치를 취하여야 한다.
2. 개인정보 위반사실에 대한 시정·개선 조치가 이행되지 않거나, 개인정보보호에 심각한 영향이 발생할 수 있는 우려가 되는 경우 개인정보 취급자 등에 대한 인사발령 등의 필요한 추가 조치를 취할 수 있다.

제6장 개인정보보호 교육

제23조(개인정보보호 교육 계획의 수립)

1. 다음 각 호의 사항을 포함하는 연간 개인정보보호 교육계획을 매년 3월말까지 수립한다.

   가. 교육목적 및 대상

   나. 교육내용

   다. 교육 일정 및 방법

2. 수립한 개인정보보호 교육 계획을 실시한 이후에 교육의 성과와 개선 필요성을 검토하여 차년도 교육계획 수립에 반영하여야 한다.

제24조(개인정보보호 교육의 실시)

1. 개인정보보호에 대한 교직원들의 인식제고를 위해 노력해야 하며, 개인정보의 오.남용 또는 유출 등을 적극 예방하기 위해 교직원을 대상으로 매년 정기적으로 개인정보보호 교육을 실시한다.
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, 개인정보관리책임자는 부서회의 등을 통해 수시 교육을 실시할 수 있다.
4. 개인정보보호 정책 수립 및 관리에 필요한 워크샵 및 컨퍼런스 등 1회 이상 개인정보보호 교육에 참석하여야 한다.
5. 개인정보관리담당자는 개인정보보호에 관한 교육을 이수한다.

제7장 개인정보보호 사무의 인수 · 인계

제25조(개인정보보호 사무의 인수 · 인계)

1. 개인정보관리책임관과 개인정보관리담당자의 변경시 다음 각 호를 인수·인계하여야 한다.

가. 개인정보보호에 관한 규정 및 지침

나. 개인정보보호 조직에 관한 사항

다. 개인정보처리시스템의 사용자 권한 설정

라. 대학의 개인정보 보유목록

마. 개인정보 유출사례를 포함한 자료

바. 기타 개인정보보호 업무 수행에 필요한 사항

2. 개인정보취급자의 변경 시 다음 각 호를 인수・인계하여야 한다.

가. 취급하는 개인정보 보유목록

나. 통상적으로 이용·제공하는 개인정보에 관한 사항

다. 기타 개인정보보호 업무 수행에 필요한 사항

제8장 개인정보 처리업무 위·수탁 시 조치

제26조(위탁 계약 및 위탁 사실 공개)

1. 개인정보처리자가 제3자에게 개인정보의 처리 업무를 위탁하는 경우 다음 각 호의 내용이 포함된 문서에 의하여야 한다.

가. 위탁업무의 목적 및 범위

나. 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항

다. 재위탁 제한에 관한 사항

라. 개인정보의 기술적 관리적 보호조치에 관한 사항

마. 개인정보에 대한 접근제한 등 안전성 확보 조치에 관한 사항

바. 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 점검 현황 점검 등 감독에 관한 사항

사. 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

2. 개인정보처리자는 위탁하는 업무의 내용과 수탁자를 정보주체가 언제든 쉽게 확인 할 수 있도록 홈페이지 등에 지속적으로 게재하여야 한다.

제27조(수탁자에 대한 교육 및 감독)

1. 위탁자는 정보주체의 개인정보가 분실, 도난, 유출, 변조 또는 훼손되지 않도록 수탁자를 교육하고, 수탁자가 개인정보를 안전하게 처리하는지 감독하여야 한다.
2. 위탁자는 수탁자에 대하여 정기적인 교육을 실시하는 외에 수탁자의 개인정보처리 현황 및 실태, 목적 외 이용, 안전성 확보조치 등을 정기적으로 점검하여야 한다.

제9장 개인정보 유·노출 및 침해 사고 대응 절차

제28조(개인정보침해사고 대응에 관한 역할)

1. (개인정보 보호책임자)
   가. 개인정보 보호책임자는 개인정보침해사고 예방, 처리 및 재발방지의 총괄 관리를 한다.
   나. 개인정보 보호책임자는 개인정보침해사건 발생 시 침해사고 처리책임자를 지정하고 개인정보침해사고 대응팀을 소집하여 운영한다.
2. (개인정보침해사고 대응팀) 개인정보보호 분야별책임자로 구성되며 개인정보보호책임자가 해당 침해사고 분석, 대응 및 복구에 필요한 관련자를 지정하여 소집한다. 필요시 업무담당자, 외부 전문가 등이 포함될 수 있다.
3. (침해사고 처리책임자) 해당 침해사고의 발생 부서의 장으로 지정되며 처리 및 재발방지에 대한 책임을 지고 개인정보침해사고 대응팀과 협력하여 사고를 해결한다.
4. (개인정보 보호담당자)
   가. 개인정보침해사고를 접수하고 본 지침 제29조의 기준에 따라 등급을 분류하여 침해사고 대응 절차를 개시한다.
   나. 개인정보침해사고 대응팀의 간사로서 대내외 비상연락망을 관리하고 팀 내 연락 및 조정을 담당한다.
   다. 개인정보침해기록을 관리하고 필요시 관련자 및 기관에 보고한다.
5. (정보보안담당자) 정보보안담당자는 침해사고 발생 시 기술적인 분석을 제공한다.
6. 대학의 내부 교직원(계약직 등 비정규직 포함)은 개인정보에 대한 침해가 발생한 것을 인지한 경우, 지체 없이 개인정보 보호담당자에게 신고하여야 한다.

제29조(침해사고의 분류)

1. (개인정보침해의 분류) 개인정보침해사고는 다음과 같이 3등급으로 분류한다.

침해등급	내용	예시
1등급	법적 근거, 규정 또는 본인의 동의 없이 개인정보가 대학 외부의 제3자에게 노출 또는 제공	• 해킹, DDOS, 내부자에 의한 개인정보 유출 • 본인 동의 없이 목적 외 이용 또는 제3자 제공 등
2등급	법적 근거, 규정 또는 본인의 동의 없이 개인정보를 수집, 접근, 분석, 이용, 내부자에게 제공, 저장, 파기	• 개인정보취급 권한이 없는 직원이 개인정보 취급.훼손 • 개인정보 취급자에 의한 개인정보 훼손.침해 • 이용자의 동의 없는 개인정보 수집/이용 • 과도한 개인정보 수집 등
3등급	안전하지 않은 상태로 개인정보를 저장하거나, 파기해야 할 정보를 파기하지 않는 등 세부지침의 규정 위반	• 주요 개인정보(고유식별번호 등) 암호화 미실시 • 개인정보에 대한 기술적.관리적 조치 미비 • 개인정보 수집 또는 제공받은 목적 달성 후 개인정보 미파기 등

제30조(개인정보침해 대응 절차)

1. (개인정보침해 예방 및 탐지)

   가. 개인정보보호담당자는 웹사이트를 통한 개인정보 유출을 예방하기 위하여 개인정보 유출차단 시스템을 운영·관리한다.

   나. 게시판 등에 자료를 게재할 때 개인정보 유출에 대하여 주의를 환기시키기 위한 경고를 제공하여야 한다.

   다. 개인정보보호담당자는 년 1회 웹사이트의 개인정보 노출 취약점 점검을 시행하고 개인정보보호책임자에게 결과를 보고한다.

2. (개인정보침해의 신고)

   가. 대학 내부직원(계약직 등 비정규직 포함)이 취급하는 개인정보에 대하여 본 지침 제29조에서 정의한 침해가 발생한 것을 인지한 경우 또는 그러한 침해의 발생이 의심되는 경우 지체 없이 개인정보보호담당자에게 신고하여야 한다.

   나. 개인정보침해사고 발생 시 고의적으로 신고를 누락 한 경우 개인정보보호책임자는 관련자에 대한 처분(징계 등)을 요청 할 수 있다.

3. (개인정보침해사고의 접수)

   가. 개인정보보호담당자는 개인정보침해사고를 접수한 경우 [제8호 서식] "개인정보 침해사고 관리대장" 에 사고 접수를 기록한다.

   나. 개인정보보호담당자는 접수 후 지체 없이 개인정보보호책임자에게 보고 한다.

4. (개인정보침해사고 대응팀 구성)

가. 개인정보보호책임자는 유출 또는 제공된 정보의 종류에 따라, 발생 부서의 분야별책임자를 침해사고 처리책임자로 지정하여 개인정보침해사고 대응팀을 구성한다.

나. 발생 부서를 적시할 수 없거나 담당 분야별책임자가 침해사고에 연루된 경우 개인정보보호책임자가 임의로 침해사고 처리책임자를 지정할 수 있다.

다. 개인정보침해사고 대응팀은 분야별책임자 중에서 사안에 따라 선정한다.

라. 2, 3등급 침해의 경우 개인정보보호책임자는 침해사고처리책임자와 협의하여 개인정보침해사고 대응팀을 구성하지 않을 수 있다.

마. 개인정보보호책임자는 필요시 외부 전문가에게 분석을 의뢰할 수 있다.

5. (침해사고의 분석)

가. 침해사고 처리책임자는 침해 사실 여부를 확인하고 사실로 확인될 경우 침해의 규모, 경위, 방법, 원인 및 관련자를 조사한다.

나. 침해사고 처리책임자는 필요한 경우 개인정보침해사고 대응팀 또는 개인정보보호책임자가 승인한 외부 전문가의 지원을 받아 증거자료를 수집한다.

6. (침해사고의 대응 및 복구)

가. 1등급의 경우 침해사고 처리책임자는 해당 개인정보를 파기 또는 회수하기 위한 조치를 취한다.

나. 2등급의 경우 침해사고 책임자는 해당 개인정보를 파기, 회수 또는 복구하기 위한 조치를 취하거나 정보주체의 사후 동의를 받아 근거를 마련한다.

다. 3등급의 경우 침해사고 처리책임자는 해당 개인정보를 적절히 보호하거나 파기하기 위한 조치를 취한다.

라. 침해사고 처리책임자는 즉각적 조치가 가능한 경우 재발방지 조치를 취한다.

7. (침해사고의 종료)

가. 침해사고 처리책임자는 [제10호서식] 개인정보침해사고 처리보고서를 작성하여 개인정보보호책임자에게 제출한다.

나. 개인정보보호책임자는 개인정보침해사고 처리보고서를 검토하고 승인한다.

8. (침해사고 사후분석)

가. 침해사고 처리책임자는 처리보고서 제출 후 30일 이내 근본원인 분석, 교훈 및 예방을 위한 개선대책을 마련하여 개인정보보호책임자에게 제출한다.

나. 개인정보보호책임자는 개선안을 검토하여 시행 및 변경 여부와 시기를 결정한다.

다. 개인정보보호책임자는 필요하다고 판단할 경우 사고의 교훈을 적절한 대상을 지정하

여 전파 및 교육을 할 수 있다.

라. 개인정보보호책임자는 개선안 시행, 교훈 전파 및 교육 후 그 성과를 검토한다.

제31조(개인정보침해사고의 관리)

1. (개인정보침해사고의 보고) 개인정보보호책임자는 1등급 사고의 경우 발생 즉시 및 수시로 그 진행 현황을 총장에게 보고한다.
2. (개인정보침해사고의 현황 관리) 개인정보보호책임자는 개인정보침해사고 현황을 분석하여 추가적인 개선대책이 필요한 경우 개선 대책을 마련하여 시행한다. 개선 대책에는 교육자료 활용 등을 포함할 수 있다.
3. (개인정보침해사고 교육훈련) 개인정보보호책임자는 전 직원에게 연1회 이상 개인정보침해사고의 유형과 보고 방법을 교육하여야 한다.

제32조(개인정보의 유출·침해 시 처리방안)

1. (개인정보유출 통지시기 및 항목)

   가. 개인정보보호 담당자는 실제로 유출 사고가 발생한 것으로 확인된 때에는 정당한 사유가 없는 한 5일 이내에 해당 정보주체에게 다음 각 호의 사항을 알려야 한다.

      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 피해구제절차

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

   나. 개인정보보호 담당자는 제1항 제2호의 경우 개인정보 유출 사고가 최초 발생한 시점과 알게 된 시점 사이에 시간적 차이가 있는 경우에는 이에 대한 과실유무를 입증하여야 한다.

   다. 개인정보보호담당자는 제1항 각 호의 조치를 취한 이후에는 정보주체에게 다음 각 호의 사실만을 일차적으로 알리고, 추후 확인되는 즉시 알릴 수 있다.

      1) 정보주체에게 유출이 발생한 사실

      2) 가항의 통지항목 중 확인된 사항

2. (개인정보유출 통지방법)

가. 개인정보보호담당자는 정보주체에게 제30조 제1항 각 호의 사항을 통지할 때에는 서면, 전자우편, 모사전송, 전화, 휴대전화 문자전송 또는 이와 유사한 방법을 통하여 5일 이내에 정보주체에게 알려야 한다.

나. 개인정보 보호담당자는 가항의 통지방법과 동시에, 홈페이지 등을 통하여 공개할 수 있다.

3. (개인정보 유출 보고 절차)

가. 개인정보보호담당자는 정보주체에 관한 개인정보 유출내용 및 조치결과를 5일 이내에 교육부(정보보호화과)에 보고하여야 한다. 다만 1천명 이상의 개인정보가 유출된 경우에는 행정안전부장관 또는 개인정보보호법 시행령 제39조제2항 각 호의 전문기관 중 어느 하나에 신고하여야 한다.

나. 가항에 따른 신고는 [별지 제5호 서식] 개인정보 유출신고서를 작성하여 공문으로 신고하여야 한다.

다. 개인정보 보호담당자는 전자우편, 모사전송 또는 인터넷 사이트를 통하여 유출 보고 또는 신고를 할 시간적 여유가 없거나 그 밖에 특별한 사정이 있는 때에는 먼저 전화를 통하여 신고한 후, [별지 제5호 서식] 개인정보 유출신고서를 제출할 수 있다.

[유출신고 기관 및 연락처]

○ 교육부(정보보호화과)
- 전화: 044-203-6504 / FAX 044-203-6185

○ 한국인터넷진흥원(privacy.kisa.or.kr)
- 전화: 118(ARS 내선 2번) / Fax: 02-405-4789 / 메일: privacy@kisa.or.kr
- 우편: 서울시 송파구 중대로 135 (가락동 78)
  IT벤처타워 개인정보침해신고센터/개인정보분쟁조정위원회
- 방문: (찾아오시는 길) 지하철 8호선 가락시장역 2번 출구 경찰병원 방향 400

4. 유출통지는 서면, 전자우편, 팩스, 전화, 문자전송 등의 방법으로 정보주체에게 개별 통지하여야 하며, 1천명 이상 개인정보 유출 시에는 개별 통지와 함께 홈페이지에 유출통지 내용(5개항목)을 7일 이상 게시하여야 합니다.

5. (개인정보침해 신고자의 보호)

가. 개인정보침해 신고자의 신분은 침해사고 대응에 반드시 필요한 경우 반드시 필요한 담당자 및 권한자에게만 제공되어야 하며 외부로 노출되어서는 아니 된다.

나. 개인정보침해 신고자는 어떠한 경우에도 신고로 인해 불이익을 당하는 경우가 없어야 한다.

6. (개인정보 침해신고에 대한 대응) 개인정보에 관한 권리 또는 이익을 침해받은 사람은 개인정보침해신고센터에 침해사실을 신고한 경우, 해당기관이 사실의 조사·확인을 통해 필요

한 조치를 취하므로 사실조사에 적극 협조하여야 한다.

7. (개인정보 침해구제 절차) 개인정보 침해구제 절차는 다음과 같습니다.

가. 개인정보 침해에 대한 신고(☏118, privacy.kisa.or.kr)

나. 개인정보침해신고센터의 사실조사(서면, 방문조사 등)

다. 사실조사 결과 통보 및 위법 사실 발견시 조치(수사의뢰, 과태료 등)

라. 손해배상, 침해행위 중지, 재발방지 등에 대한 분쟁조정 (☏118, privacy.kisa.or.kr)

※ 동일 피해를 입은 정보주체가 50명 이상인 경우 집단분쟁조정 신청 가능

마. 분쟁조정위원회 자료조사 및 조정안 작성

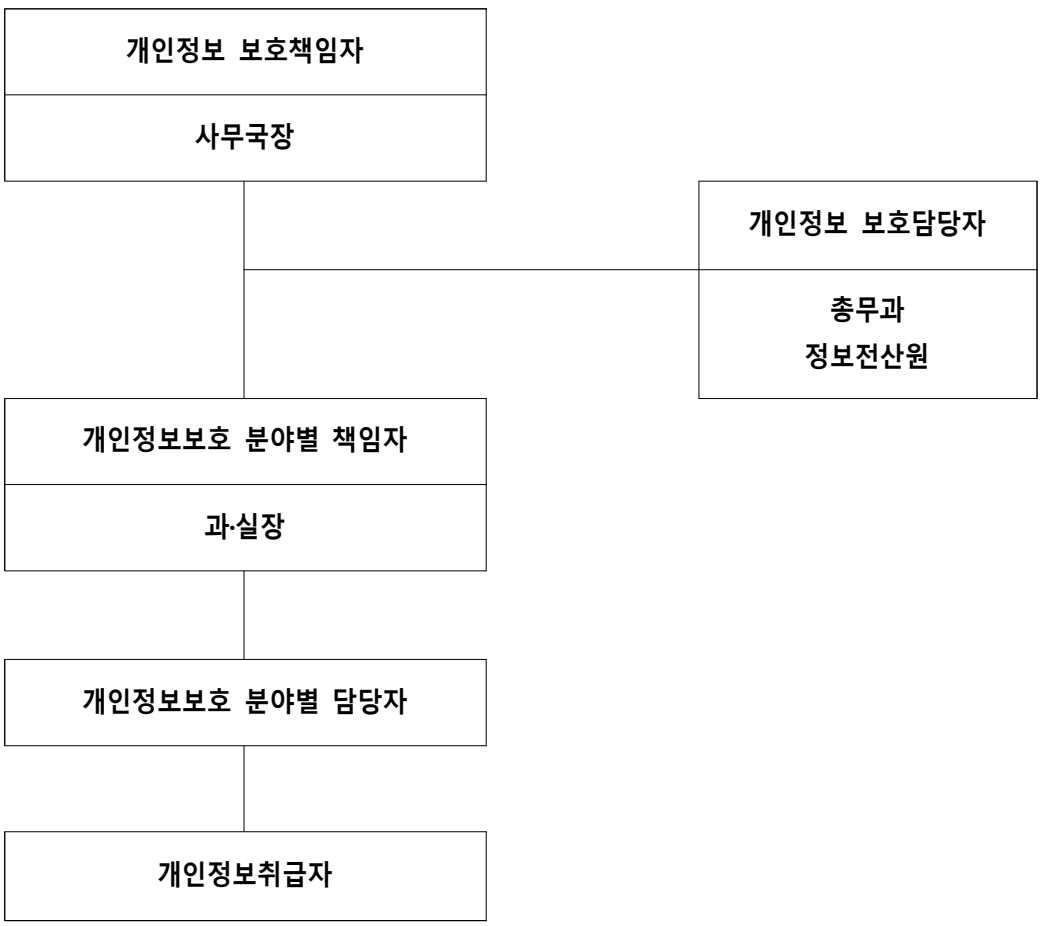
바. 조정안 제시(당사자들이 조정안 수용시 재판상 화해의 효력을 갖음)

사. 분쟁조정이 실패할 경우 민사소송 또는 단체소송 제기 가능(관할 지방법원)

※ 단체소송은 권리침해행위의 금지·중지를 구하는 소송

8. 유출사고 대응팀 조직 및 역할

가. 조직체계



나. 역할

조직별	담당자	역 할
개인정보 보호책임자	사무국장	- 개인정보 유출사고 대응 총괄 지휘
개인정보 유출사고 대응팀	개인정보보호담당자, 개인정보보호 분야별 책임자, 정보보안담당자, IT담당자, 기타 협조부서	- 개인정보 유출사고 인지·접수 - 개인정보 유출사고 대응 절차 수립 - 개인정보 유출사고 사실 확인조사 실시 - 정보주체에게 유출사실 통지 - 행정안전부 또는 전문기관에 유출통지 신고 - 외부요인에 의한 유출의 경우, 교육사이버안전센터, 행정안전부 등과 협조하여 사고 해결 - 사고내용 세부조사 및 사후 인사조치가 필요한 경우 유관부서와 협조
사고발생 부서	개인정보취급자	- 내부요인에 의한 침해.유출의 경우, 사고대응팀에 사고내용 신고 - 침해사고 대응팀과 협력하여 사고처리 적극 지원
사고신고자	정보주체	개인정보를 침해 받은 피해자

제10장 개인정보 목적 외 이용 및 제 3자 제공절차

제33조(제공기준 기본원칙)

1. (자료제공 판단기준) 목적의 정당성, 수단의 적정성, 피해의 최소성, 법익의 균형성에 대하여 종합적으로 검토한 후 필요한 최소한의 범위 내에서 제공한다.

   가. 목적의 정당성 : 구체적으로 어떠한 목적을 위하여 당해 개인정보가 필요한지

나. 수단의 적정성 : 당해 개인정보를 제공함으로써 당해 공익목적을 달성할 수 있는 것인지

다. 피해의 최소성 : 목적달성을 위하여 필요한 최소한의 정보는 어디까지인지

라. 법익의 균형성 : 제공에 따른 이익과 정보주체가 받을 수 있는 예상피해를 비교하여 전자가 우월하다고 할 수 있는지 여부 판단

2. (요청 기관의 적격 여부 확인)

가. 요청 기관의 개별법에 자료요청의 근거조항이 구체적으로 명시된 경우 제공 가능

나. 요청 기관의 자료요청에 대하여 근거법이 없는 경우 정보주체의 동의가 있었는지 여부 등 예외적 제공가능 사항에 해당되는지 확인한 후 제공여부 결정

3. (제공항목 판단)

가. 본교에서 수집한 정보여부 확인

1) 본교에서 직접 수집, 생산한 정보가 아닌 경우 자료제공 불가 : 단, 정보주체의 동의가 있는 경우 제공가능

2) 요청 목적에 부합하는 필수 항목만 제공(개인정보 최소 제공 원칙)

나. 민감정보는 법령(법률, 시행령, 시행규칙)에 민감정보의 처리를 요구(허용)하도록 규정되어 있는 경우 제공

4. (개인정보 제공기준)

가. 수집목적 범위 내에서 제공하는 경우(법 제17조)

1) 정보주체의 동의를 받은 경우

2) 법 제15조제1항 제2호,제3호 및 제5호에 따라 개인정보를 수집한 목적 범위에서 개인정보를 제공하는 경우

나. 수집목적 외의 용도로 제공하는 경우(법 제18조)

1) 개인정보처리자는 개인정보보호법 제18조(개인정보의 이용·제공 제한) 제1항에 따라 개인정보보호법 제17조(개인정보의 제공) 제1항(수집 목적 범위에서 제공) 및 제3항(국외의 제3자에게 제공)의 범위를 초과하여 제3자에게 제공하여서는 아니되나 개인정보보호법 제18조 제2항 각 호에 해당하는 다음의 경우는 예외적으로 제공 가능함

다만, 정보주체 또는 제3자의 권익을 부당하게 침해할 우려가 있다고 인정되는 때에는 제공 불가

① 정보주체(본인)로 부터 별도의 동의를 받은 경우 - 정보주체에게 법 제18조 제3항에 따라 개인정보를 제공받는 자 등을 알리고 동의를 받아야함 ② 다른 법률에 특별한 규정이 있는 경우 - 법률에서 개인정보의 제공을 구체적으로 요구하거나 허용하고 있는 경우 ③ 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전

동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 **급박한** 생명, 신체, 재산의 이익을 위해 필요하다고 인정되는 경우

④ 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 **특정 개인을 알아볼 수 없는 형태로** 개인정보를 제공하는 경우

⑤ 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 **'개인정보보호심의위원회'의 심의·의결**을 거친 경우

⑥ **조약, 그 밖의 국제협정의 이행을 위하여** 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우

⑦ 범죄의 **수사와 공소의 제기 및 유지**를 위하여 필요한 경우

⑧ 법원의 **재판업무 수행**을 위하여 필요한 경우

⑨ **형 및 감호, 보호처분의 집행**을 위하여 필요한 경우

다. 권한있는 기관의 본교에 대한 감사 또는 조사에 응하여야 하는 경우

라. 업무의 일부 또는 전부를 위탁하는 경우(법 제26조)

개인정보 처리업무를 위탁하는 경우 위탁업무의 목적 등이 포함된 문서에 의하여야 하며 위탁계약 사항에 구체적으로 표기된 범위 내에서 제공

※ 위탁자의 이익을 위해 처리하는 경우는 업무 위탁에 해당되며 개인정보를 제공 받는 제3자의 이익을 위해 처리하는 경우에는 제3자 제공에 해당됨

제34조(자료제공 업무처리 기준)

1. (자료 제공 여부 판단 등 업무처리절차)

문서 접수부서에서 자료제공 여부를 판단하여 처리함을 원칙으로 한다.

2. (자료제공 처리 기준)

가. 개인정보 자료제공은 부득이한 경우를 제외하고는 그룹웨어에 의한 문서회신을 원칙으로 한다.

나. 회신 문서에는 이용목적, 이용방법, 이용기간, 이용형태의 제한사항, 개인정보의 안전성 확보를 위해 필요한 구체적인 조치사항을 반드시 기재한다.

다. 자료제공 내역을 [별지 8호 서식] 개인정보의 목적 외 이용 및 제3자 제공 대장에 반드시 기록,관리하여야 함

※ 제공 건수가 없는 경우라도 개인정보의 목적 외 이용 및 제3자 제공 대장에 기록

라. 관련업무 처리 후 PC에 개인정보 자료가 저장된 경우 업무종료 후 즉시 삭제

3. (자료제공 방법)

가. 그룹웨어를 이용해 제공하는 경우

1) 개인정보를 엑셀, 한글 등 첨부파일 형태로 제공하되, 반드시 암호화 조치하여 송부하고 암호는 유선 등의 방법으로 별도 통보한다.

2) 문서 본문에 개인정보 및 비밀번호를 표기하여 제공하는 것은 불가하다.

나. 엑셀 등 문서 출력물에 의해 직접 전달하는 경우

1) 자료 제공시 요청 기관의 담당자 또는 직상급자에게 직접 전달

2) 수령자 인적사항 등을 반드시 확인하여 기록 관리

다. 보조기억매체(USB, CD, 디스켓 등)를 이용하여 제공하는 경우

1) 제공되는 개인정보 자료는 반드시 암호화 조치

2) 본교 직원이 직접 출장하여 제공하는 경우 요청 기관의 담당자 또는 직상급자에게 직접 전달하고 수령자 인적사항 등을 반드시 확인하여 기록 관리

3) 요청 기관 직원이 본교에 방문하여 제공하는 경우 반출된 보조기억매체는 요청 기관의 제공자료 확인 조치 후 즉시 회수하여 저장된 개인정보 삭제 처리

라. 기타의 방법에 의해 자료제공이 필요한 경우는 안전성 조치 등에 대해 개인정보보호 담당자와 협의를 거쳐 제공

제35조(개인정보의 목적 외 이용 또는 제 3자 제공의 공고)

1. (공고기간) 개인정보 자료를 목적 외의 용도로 외부기관 등에 제공한 부서는 제공한 날부터 5일 이내에 홈페이지에 게시하여야 한다.
2. (공고 방법 및 필수 기재사항)

   가. 그룹웨어 – 개인정보 업무위탁 및 제 3자 정보제공 작성 시 홈페이지에 게시

   나. (필수 기재사항) 제공한 날짜, 법적근거, 제공 목적, 제공한 개인정보 항목을 [별지 제8호 서식] 개인정보 제공내역으로 공지한다.

※ 개인정보(이름, 주민번호 등)는 제외

제36조(안전성 확보 조치)

1. 개인정보 자료 제공은 문서로 시행되어야 하며, 문서에 제공목적 이외의 이용금지, 사용목적 달성 후 폐기, 사후관리 실태 확인 등의 안전성 확보조치 문구를 표기하여 시행하여야 한다.
2. 제공받은 개인정보 자료는 제공받은 목적 외의 용도로 이용하거나 제3자에게 제공할 수 없음(개인정보보호법 제19조)

11장 개인정보의 처리

제37조(개인정보의 수집·이용)

1. 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다.

   가. 정보주체로부터 사전에 동의를 받은 경우

   나. 법률에서 구체적으로 명시하거나 허용하고 있는 경우

   다. 개인정보를 수집, 이용하지 않고는 법령 등에서 정하는 소관 업무의 수행이 불가능하거나 현저히 곤란한 경우

   라. 정보주체 또는 제3자의 생명, 신체, 재산에 대한 피해를 방지해야할 급박한 상황에서 정보주체 또는 법정대리인이 의사표시를 할 수 없는 상태에 있거나 연락을 취할 수 없어 사전 동의를 받을 수 없는 경우

   마. 업무부서 법령 또는 정보주체와의 계약에 따른 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 업무부서의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한 한다.

2. 정보주체의 동의를 받아 수집·이용하는 경우 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.

   가. 수집·이용 목적

   나. 수집 항목

   다. 해당정보의 보유 및 이용 기간

   라. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

3. 필요 최소한의 개인정보를 수집해야 하며, 수집 및 이용 목적의 범위를 초과한 이용은 불가 하다.

4. 개인정보의 보유 및 이용기간은 수집·이용 목적에 맞게 관련 법령에 근거하여 최소한으로 책정하며, 관련법령 근거가 없을 시 기관장이 승인하는 기간으로 한다.

5. 개인정보를 수집 시에는 필수정보, 고유식별정보, 선택정보, 민감정보 등을 분리구분해서 동의를 받아야 하며 각 정보의 수집거부에 따른 불이익을 명시해야 한다.

6. 개인정보처리자는 만14세 미만 아동의 개인정보를 처리하기 위하여 동의를 받아야 할 때에는 그 법정대리인의 동의를 받아야 한다.

7. 개인정보 위탁 및 제 3자 제공시에는 정보주체의 동의를 받아야 하며, 개인정보를 제공받는 자에게 이용 목적, 이용 방법, 그 밖에 필요한 사항에 대하여 제한을 하거나, 개인정보의 안전성 확보를 위하여 필요한 조치를 마련하도록 요청하여야 한다.
8. 개인정보를 수집 시에는 개인정보처리자는 정보주체가 선택적으로 동의할 수 있는 사항을 동의하지 아니하거나, 목적 외 제공에 대한 동의를 하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 아니 된다.

제38조(개인정보의 파기)

1. 개인정보처리자는 보유기간의 경과, 처리 목적 달성, 해당 서비스의 폐지 등 그 개인정보가 불필요하게 되었을 경우 5일 이내에 파기하여야 하며, 개인정보의 파기에 관한 사항을 기록·관리하여야 한다.
2. 개인정보보호담당자는 개인정보파일의 보유기간, 처리목적 등을 반영한 개인정보 파기 계획을 수립하여 시행·확인하여야 한다.
3. 복구 또는 재생되지 아니하도록 다음 각 호의 구분에 따른 방법으로 하여야 한다.

   가. 완전파괴(소각·파쇄 등)

   나. 전용 소자장비를 이용하여 삭제

   다. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행
4. 개인정보의 일부만을 파기하는 경우, 제3항의 방법으로 파기하는 것이 어려운 때에는 다음 각 호의 조치를 하여야 한다.

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

   나. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 해당 부분을 마스킹, 천공 등으로 삭제
5. 개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 해당 개인정보를 다른 개인정보와 분리하여서 저장·관리하여야 하며, 법령에 따라 해당 개인정보를 보존한다는 점을 분명히 표시하여야 한다.
6. 개인정보보호담당자는 개인정보의 보유 기간 만료 등에 따른 구체적 파기 시점·방법 등을 반영한 개인정보 파기계획을 수립·시행하고 파기계획은 개인정보처리방침에 포함하여 시행하여야 하며 개인정보의 파기 결과를 확인하여야 한다.

제39조(개인정보파일 대장 관리 및 공개)

1. 개인정보처리자는 1개의 개인정보파일에 대하여 1개의 개인정보파일 대장을 작성하여 관리하여야 한다.
2. 개인정보처리자는 개인정보종합지원시스템에 접속하여 개인정보파일대장을 등록 및 변경 신청하여야 한다.
3. 내부적 업무처리만을 위하여 사용되는 개인정보파일,「통계법」에 따라 수집되는 개인정보파일 등은 법령에 따라 등록 신청 대상에서 제외된다.

제40조(개인정보 처리방침의 수립 및 공개)

1. 개인정보 보호책임자는 개인정보처리방침을 수립하고 본 대학에서 운영하는 인터넷 홈페이지를 통해 인터넷 홈페이지 첫 화면 또는 첫 화면과의 연결화면에 지속적으로 게재하여야 한다.
2. 별도 업무용 홈페이지를 운영하는 분야별 보호책임자는 등록대상이 되는 개인정보파일에 대하여 개인정보처리방침을 정한다.
3. 개인정보처리방침을 게재하는 경우에는"개인정보처리방침"이라는 명칭을 사용하되, 글자 크기, 색상 등을 활용하여 다른 고지사항과 구분함으로써 정보주체가 쉽게 확인할 수 있도록 하여야 한다.
4. 개인정보처리방침에 반드시 포함되어야 할 사항은 다음 각 호와 같다.

   가. 개인정보의 처리 목적

   나. 개인정보의 처리 및 보유 기간

   다. 개인정보의 제3자 제공에 관한 사항

   라. 개인정보처리의 위탁에 관한 사항

   마. 정보주체의 권리·의무 및 그 행사방법에 관한 사항

   바. 처리하는 개인정보의 항목

   사. 개인정보의 파기에 관한 사항

   아. 개인정보 보호책임자에 관한 사항

   자. 개인정보처리방침의 변경에 관한 사항

   차. 개인정보의 안전성 확보조치에 관한 사항
5. 개인정보 보호책임자 또는 개인정보보호 분야별 책임자가 개인정보처리방침을 변경하는 경우에는 변경 및 시행의 시기, 변경된 내용을 인터넷 홈페이지 등에 지속적으로 공개하여야 하며, 변경된 내용은 정보주체가 쉽게 확인할 수 있도록 변경 전·후를 비교하여 공개하여야 한다.

제41조(개인정보영향평가)

개인정보처리자는 아래 각 호에 해당하는 경우 영향평가를 의무적으로 수행한 후 개인정보 보호책임자에게 그 결과를 제출하여야 한다.

1. 구축·운용 또는 변경하려는 개인정보파일로서 5만 명 이상의 정보주체에 관한 법 제23조에 따른 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일
2. 구축·운용하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서 구축·운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50만 명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일
3. 구축·운용 또는 변경하려는 개인정보파일로서 100만 명 이상의 정보주체에 관한 개인정보파일
4. 법 제33조제1항에 따른 개인정보 영향평가를 받은 후에 개인정보 검색 체계 등 개인정보파일의 운용체계를 변경하려는 경우 그 개인정보파일. 이 경우 영향평가 대상은 변경된 부분으로 한정

12장 정보주체의 권리보장

제42조(개인정보 열람,정정·삭제,처리정지 요구에 대한 조치)

1. 개인정보의 열람,정정·삭제,처리정지 요구의 접수는 각 개인정보를 처리하는 분야별 책임자 또는 담당자 및 취급자가 수행한다.
2. 개인정보처리자는 정보주체가 [별지 제6호 서식] 에 따른 서면, 전자우편, FAX 등을 통하여 개인정보의 열람,정정·삭제,처리정지를 요구하는 경우에는 본인 또는 대리인 여부를 확인하고 지체 없이 필요한 조치를 취하고 [별지 제7호 서식]에 따른 '결과통지서'를 통하여 해당 정보주체에게 알려야 한다.
3. 개인정보처리자는 정보주체가 홈페이지에서 열람,정정·삭제,처리정지 요구를 수행할 수 있도록 개인정보처리방침에 정보주체의 권리행사 방법을 명시하여야 한다.
4. 정보주체가 개인정보의 오류 등에 대한 정정 또는 삭제를 요구한 경우에는 정정 또는 삭제를 완료할 때까지 당해 개인정보를 이용하거나 제공하지 않는다.

5. 개인정보처리자는 다른 법률에 명시되어 있거나 타인의 이익을 부당하게 침해할 우려가 있는 경우 정보주체의 열람,정정·삭제,처리정지 요구를 거절할 수 있으며 그 권리가 제한 될 수 있습니다.
6. 정보주체가 열람,정정·삭제,처리정지 요구에 대한 거절조치에 이의를 제기할 경우, 개인정보처리자는 해당 사유를 서면, 전자우편, 유선전화 등을 통해 관련사항을 보다 상세하게 안내해야 한다.

첨부자료

별표/별지 서식

[별표 서식]

1. 내부점검 항목 관리현황
2. 내부점검 항목 기술적 보호조치
3. 개인정보파일 보유기간 책정 기준표
4. 개인정보 처리단계별 준수사항 및 위반시 벌칙사항

[별지 서식]

1. 개인정보파일보유사전협의서/개인정보파일대장
2. 개인정보파일 등록·변경등록 신청서
3. 개인정보파일 파기 요청서
4. 개인정보파일 파기 관리대장
5. 개인정보유출 신고서
6. 개인정보 열람·정정삭제·처리정지 청구서
7. 개인정보 정정삭제·처리정지 요구에 대한 결과 통지서
8. 개인정보의 목적외 이용 및 제3자 정보 제공대장
9. 개인정보 침해사고 관리대장
10. 개인정보 침해사고 처리보고서

■ 강릉원주대학교 [별표 1호]

내부점검 항목 관리현황

구분	감사 항목
개인정보수집	개인정보 수집 시 수집.이용 목적, 개인정보의 항목, 보유 및 이용 기간을 모두 고지하고 동의를 얻고 있는가?
	이용자의 동의를 받거나 근거 법률에 따라 사상, 신념 과거의 병력 등 개인의 권리.이익이나 사생활을 뚜렷하게 침해할 수 있는 개인정보를 수집하는가?
개인정보 이용 및 제공	수집한 이용자의 개인정보를 이용자로부터 동의 받은 목적 및 고지사항과 다른 목적으로 이용하고 있지 않은가?
	이용자의 개인정보를 제3자에게 제공 시 관련 모든 사항을 이용자에게 알리고 동의 받고 있는가?
	개인정보 취급 위탁 시 수탁자, 개인정보취급을 하는 업무의 내용에 대해 알리고 동의를 얻는가?
	개인정보에 대한 접근 권한이 과도하게 부여되진 않았는가?
	외부망에 의한 정보 유출 방지를 위한 관리적 조치를 취하는가?
	업무상 관계기관 및 부서에게 개인정보 자료 제공 시 모든 사항을 고지하는가?
	관계기관 및 부서에서 업무처리 상 개인정보자료 요구 시 정확한 법적 근거에 의하여 요구하였고 그에 준하여 제공 하였는가?
개인정보 파기	이용자의 개인정보를 사전에 고지한 보유기간 및 파기기간에 맞게 적절히 개인정보를 파기하는가?
	회원 탈퇴한 이용자의 개인정보를 별도 저장.관리하는가?
정보주체권리	이용자가 개인정보 수집.이용 제공 등의 철회할 수 있게 하고 있는가?
	이용자가 자신의 개인정보에 대한 열람이나 제공을 요구할 수 있고 오류가 있는 경우 정정을 할수 있게 하고 있는가?
	이용자가 개인정보에 수집.이용에 대한 동의를 철회하면 지체 없이 수집된 개인정보를 파기하는가?
개인정보취급(처리)방침	개인정보취급방침을 정하여 이용자가 쉽게 인식할 수 있도록 대통령령이 정하는 방법에 따라 공개하고 있는가?
	개인정보취급방침을 변경하는 경우 이용자가 그 이유 및 변경내용을 지체 없이 공지하고, 이용자가 쉽게 알아볼 수 있도록 하는가?
내부관리 계획수립시행	개인정보 내부관리계획의 수립 및 시행 개인정보보호책임자 의무와 책임 개인정보 처리단계별 기술적 관리적 안전조치 개인정보보호 교육 개인정보 침해대응 및 피해구제

■ 강릉원주대학교 [별표 2호]

내부점검 항목 기술적 보호조치

구분	점검항목
접근통제	개인정보처리시스템에 대한 접근권한을 서비스 제공을 위해 필요한 자에게만 부여하는가?
	관련업무 및 직제변경 시 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하는가?
	개인정보처리시스템의 접근 권한 부여,변경 또는 말소에 대한 내역을 기록하는가?
	개인정보처리시스템에 접속권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하는가?
	개인정보처리시스템에 접속한 IP등을 재분석하여 불법적인 개인정보 유출시도를 탐지하는가?
	개인정보취급자가 안전한 비밀번호를 이용할 수 있도록 비밀번호 작성규칙을 수립하고, 이행하는가?
	개인정보취급자의 비밀번호는 아래의 문자 종류 중 2종류 이상 최소 10자 이상 또는 3종류 이상 최소8자리로 구성되는가?
	개인정보취급자의 비밀번호는 연속적이 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보를 사용하지 못하도록 조치하였는가?
	개인정보취급자의 비밀번호는 식별자(ID)와 비슷한 비밀번호를 사용하지 못하도록 조치하였는가?
	개인정보취급자의 비밀번호는 유효기간 설정, 주기적(6개월)으로 변경하는가?
	개인정보취급자의 PC에서 P2P를 사용하지 못하도록 조치하였는가?
	개인정보취급자의 PC에서 고유설정을 한 경우 접근제어를 수행하는가?
	개인정보취급자가 비밀번호를 일정 횟수 이상 잘못 입력 시 접근을 제한하는가?
	개인정보취급자가 일정시간 이상 시스템을 사용하지 않을 경우 자동 접속 차단하는가?
접속기록 위변조방지	개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 처리 일시, 처리내역 등 접속 기록을 저장하는가?
	개인정보취급자의 접속기록에 대하여 반기 1회 이상 확인.감독을 수행하는가?
	개인정보취급자의 접속기록에 대하여 최소 6개월 이상 보관하고 있는가?
	보관하고 있는 개인정보취급자의 접속기록에 대하여 관리 방법을 보유하고 있는가?
	개인정보처리시스템의 접속기록을 별도 저장장치에 백업 보관하는가?
개인정보 암호화	비밀번호 또는 바이오 정보와 같은 본인임을 인증하는 정보를 저장할 때 암호화하여 저장하는가?
	개인정보처리시스템에 보관하는 이용자의 주민등록번호, 비밀번호에 대하여 암호화 저장하는가?
	개인정보를 정보통신망을 통해 전송하는 경우에 암호화하여 송.수신하는가?
	개인정보를 개인정보취급자의 PC에서 저장하는 경우에 암호화 설정을 하는가?
악성프로그램 방지	개인정보처리시스템에 백신 소프트웨어를 설치하여 운영하는가?
	개인정보취급자의 개인컴퓨터에 백신 소프트웨어를 설치하여 운영하고 있는가?
	백신 소프트웨어를 월 1회 이상 주기적으로 갱신.점검하고 있는가?
	개인정보처리시스템의 OS 보안패치는 최신 소프트웨어로 작용하고 있는가?
	개인정보취급자 PC의 OS 보안패치는 최신 소프트웨어로 작용하고 있는가?

■ 강릉원주대학교 [별표 3호]

개인정보파일 보유기간 책정 기준표

보유기간	대상 개인정보파일
영구	1. 국민의 지위, 신분, 재산을 증명하기 위해 운용하는 개인정보파일 중 영구보존이 필요한 개인정보파일 2. 국민의 건강증진과 관련된 업무를 수행하기 위해 운용하는 개인정보파일 중 영구보존이 필요한 개인정보파일
준영구	1. 국민의 신분, 재산을 증명하기 위해 운용하는 개인정보파일 중 개인이 사망, 폐지 그 밖의 사유로 소멸되기 때문에 영구 보존할 필요가 없는 개인정보파일 2. 국민의 신분증명 및 의무부과, 특정대상 관리 등을 위하여 행정기관이 구축하여 운영하는 행정정보시스템의 데이터 셋으로 구성된 개인정보파일
30년	1. 관계 법령에 따라 10년 이상 30년 미만의 기간 동안 민.형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일
10년	1. 관계 법령에 따라 5년 이상 10년 미만의 기간 동안 민.형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일
5년	1. 관계 법령에 따라 3년 이상 5년 미만의 기간 동안 민.형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일
3년	1. 행정업무의 참고 또는 사실 증명을 위하여 1년 이상 3년 미만의 기간 동안 보존할 필요가 있는 개인정보파일 2. 관계 법령에 따라 1년 이상 3년 미만의 기간 동안 민. 형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일 3. 각종 증명서 발급과 관련된 개인정보파일(단 다른 법령에서 증명서 발급 관련 보유기간이 별도로 규정된 경우 해당 법령에 따름)
1년	1. 상급기관(부서)의 요구에 따라 단순 보고를 위해 생성한 개인정보파일

■ 강릉원주대학교 [별표 4호]

개인정보 처리단계별 준수사항 및 위반시 벌칙사항

구분	주요내용	처벌 및 벌칙
수집·이용	민감정보(사상·신념·정당가입·건강 등) 처리기준 위반(제23조)	5년 이하 징역 또는 5천만원 이하 벌금
	고유식별정보(주민등록·여권·운전면허 번호 등) 처리기준 위반(제24조)	
	부당한 수단이나 방법에 의해 개인정보를 취득하거나 개인정보처리에 관한 동의를 얻는 행위를 한 자(제59조)	3년 이하 징역 또는 3천만원 이하 벌금
	개인정보의 수집기준 위반(제15조)	5천만원 이하 과태료
	만14세 미만 아동의 개인정보 수집시 법정대리인 동의획득여부 위반(제22조)	
	탈의실·목욕실 등 영상정보처리기기 설치 금지 위반(제25조)	
	최소한의 개인정보 외 정보의 미동의를 이유로 재화 또는 서비스 제공을 거부한 자(제16조, 제22조)	3천만원 이하 과태료
	주민등록번호를 제공하지 아니할 수 있는 방법 미제공(제21조)	
	동의획득방법 위반하여 동의받은 자(제22조)	1천만원 이하 과태료
제공·위탁	정보주체의 동의 없는 개인정보 제3자 제공(17조)	5년 이하 징역 또는 5천만원 이하 벌금
	개인정보의 목적 외 이용·제공(제18조, 제19조, 제26조)	
	개인정보 주체에게 알려야 할 사항을 알리지 아니한 자(제15조, 제17조, 제18조, 제26조)	3천만원 이하 과태료
	업무위탁 시 공개의무 위반(제26조)	1천만원 이하 과태료
개인정보 안전관리	개인정보의 누설 또는 타인 이용에 제공(제59조)	5년 이하 징역 또는 5천만원 이하 벌금
	개인정보의 훼손, 멸실, 변경, 위조, 유출(제59조)	
	영상정보처리기기 설치목적과 다른 목적으로 임의 조작하거나 다른곳을 비추는 자 또는 녹음기능을 사용한 자(제25조)	3년 이하 징역 또는 3천만원 이하 벌금
	직무상 알게 된 비밀을 누설하거나 직무상 목적 외 사용한 자(제60조)	
	안전성 확보에 필요한 보호조치를 취하지 않아 개인정보를 도난·유출·변조 또는 훼손당하거나 분실한 자(제24조, 제25조, 제29조)	2년 이하 징역 또는 1천만원 이하 벌금
	안전성 확보에 필요한 조치의무 불이행(제24조, 제25조, 제29조)	3천만원 이하 과태료
	영상정보처리기기 설치·운영기준 위반(제25조)	
	개인정보를 분리해서 저장·관리하지 아니한 자(제21조)	1천만원 이하 과태료
	개인정보처리방침 미공개(제30조)	
	개인정보관리책임자 미지정(제31조)	
	영상정보처리기기 안내판 설치 등 필요조치 불이행(제25조)	
정보주체 권익보호	개인정보의 정정·삭제요청에 대한 필요한 조치를 취하지 않고, 개인정보를 계속 이용하거나 제3자에게 제공한 자(제36조)	2년 이하 징역 또는 1천만원 이하 벌금
	개인정보의 처리정지 요구에 따라 처리를 중단하지 않고 계속 이용하거나 제3자에게 제공한 자(제37조)	
	개인정보 유출사실 미통지(제34조)	3천만원 이하 과태료
	정보주체의 열람 요구의 부당한 제한·거절(제35조)	1천만원 이하 과태료
	정보주체의 정정·삭제요구에 따라 필요 조치를 취하지 아니한 자(제36조)	
	처리정지된 개인정보에 대해 파기 등의 조치를 하지 않은 자(제37조)	
	시정명령 불이행(제64조)	
	정보주체의 열람, 정정·삭제, 처리정보 요구 거부 시 통지의무 불이행(제35조, 제36조, 제37조)	
	관계물품·서류 등의 미제출 또는 허위제출(제63조)	
	출입·검사를 거부·방해 또는 기피한 자(제63조)	
파기	개인정보 미파기(제21조)	3천만원 이하 과태료

강릉원주대학교 [별지 제1호서식] (앞면)

개인정보파일보유사전협의서/개인정보파일대장

① 기 관 명	00	② 연 번	1
③ 파 일 명	학교생활기록부		
④ 보 유 목 적	원활한 학사관리를 위하여 학생들의 필요 정보를 체계적 수집·관리 (성적증명, 졸업증명, 재학증명 등)		
⑤ 보 유 근 거	고등교육법 제 25조		
⑥ 수 집 방 법	서면에 의한 본인동의		
⑦ 대상개인범위	00 졸업생 및 재학생		
⑧ 대 상 인 원 수	119,522명 ('08.12월말 현재)	⑨ 보유기간	영구
⑩ 기 록 항 목 (항 목 수)	성명, 생년월일, 성적, 상벌, 적성, 활동 등		

210mm×297mm(인쇄용지(특급) 34g/㎡)

⑪ 사 용 부 서		00부, 00실
⑫ 열람예정일		수시
⑬ 열 람 청 구 부서 및 주소		00 학교 00부
⑭ 열 람 제 한	항 목	없음
	사 유	없음
⑮ 이용·제공기관명		국가기관, 상급학교 등
⑯ 이용·제공근거		고등 교육법 제 25조 공공기관의 개인정보보호에 관한 법률 제 10조 1항, 3항
⑰ 이용·제공항목		성명, 생년월일, 성적, 상벌, 적성, 활동 등

210mm×297mm(인쇄용지(특급) 34g/㎡)

■ 강릉원주대학교 [별지 제2호서식]

개인정보파일 ([ ] 등록 [ ] 변경등록) 신청서

기관명		부서명	

등록항목	등록정보	변경정보 및 변경사유
개인정보파일 명칭		
개인정보파일의 운영 근거 및 목적		
개인정보파일에 기록되는 개인정보의 항목		
개인정보의 처리방법		
개인정보의 보유기간		
개인정보를 통상적 또는 반복적으로 제공하는 경우 그 제공받는 자		
개인정보파일을 운용하는 기관명		
개인정보파일로 보유하고 있는 개인정보의 정보주체 수		
개인정보의 처리 관련 업무를 담당하는 부서		
개인정보의 열람 요구를 접수·처리하는 부서		
개인정보파일에서 열람을 제한하거나 거절할 수 있는 개인정보의 범위 및 그 사유		

「개인정보 보호법」 제32조제1항 및 같은 법 시행령 제34조제1항, 「개인정보 보호지침」 제14조제1항에 따라 위와 같이 개인정보파일 ([ ] 등록 [ ] 변경등록)을 신청합니다.

년 월 일

신청 부서 및 부서장

(서명 또는 인)

210㎜×297㎜[일반용지 70g/㎡(재활용품)]

■ 강릉원주대학교 [별지 제3호서식]

개인정보파일 파기 요청서

작성일		작성자	
파기 대상 개인정보파일			
생성일자		개인정보취급자	
주요 대상업무		현재 보관건수	
파기 사유			
파기 일정			
특기사항			
파기 승인일		승인자 (개인정보 보호책임자)	
파기 장소			
파기 방법			
파기 수행자		입회자	
폐기 확인 방법			
백업 조치 유무			
매체 폐기 여부			

210㎜×297㎜[일반용지 70g/㎡(재활용품)]

■ 강릉원주대학교 [별지 제4호서식]

개인정보파일 파기 관리대장

번호	개인정보 파일명	자료의 종류	생성일	폐기일	폐기사유	처리담당자	처리부서장

210㎜×297㎜[인쇄용지(특급) 34g/㎡]

■ 강릉원주대학교 [별지 제5호서식]

개인정보 유출 신고서

부서명					
정보주체에의 통지 여부					
유출된 개인정보의 항목 및 규모					
유출된 시점과 그 경위					
유출피해 최소화 대책·조치 및 결과					
정보주체가 할 수 있는 피해 최소화 방법 및 구제 절차					
담당부서·담당자 및 연락처		성명	부서	직위	연락처
	개인정보 보호책임자				
	개인정보 취급자				

유출신고접수기관	부서명	담당자명	연락처

210㎜×297㎜[신문용지 54g/㎡]

■ 강릉원주대학교 [별지 제6호서식]

(앞쪽)

개인정보(□열람□정정·삭제□처리정지) 청구서	처리기한
※ 아래 유의사항을 읽고 굵은 선 안쪽의 사항만 적어 주시기 바랍니다.	10일 이내

청 구 인	성 명		전 화 번 호	
	생년월일		정보주체와의 관계	
	주 소			
정보주체의 인적사항	성 명		전 화 번 호	
	생년월일			
	주 소			
청구내용 (구체적으로 요청하지 않으면 처리가 곤란할 수 있음)	개인정보파일명			
	열람	대상	□ 개인정보파일 기록 항목 : 전부,일부( ) □ 개인정보 제3자 제공현황 : 기간(~) □ 개인정보 처리에 대한 동의 현황	
		방법	**□ 열람 : 직접방문, 전자열람** **□ 사본.출력물 수령 : 우편, 모사종이** **□ 전자파일 수령 : 전자우편, 기타()**	
	정정.삭제	※정정.삭제하고자 하는 개인정보의 항목과 그 사유를 기재합니다.		
	처리정지	※개인정보의 처리정지를 원하는 대상.내용 및 그 사유를 기재합니다.		

「개인정보보호법」 제35조1항,제36조 1항 및 제37조 1항에 따라 위와 같이 개인정보의 열람,정정,삭제 또는 처리정지를 청구합니다.

년 월 일

청구인 (서명 또는 인)

강릉원주대학교 총장 귀하

담당자의 청구인에 대한 확인 서명	

■ 강릉원주대학교 [별지 제7호서식]

개인정보 ([ ] 정정·삭제, [ ] 처리정지) 요구에 대한 결과 통지서

수신자 (우편번호: , 주소:)

요구 내용	
□ 정정·삭제 □ 처리정지 조치 내용	
□ 정정·삭제 □ 처리정지 결정 사유	
이의제기방법	※ 개인정보처리자는 이의제기방법을 기재합니다.

「개인정보 보호법」 제36조제6항 및 같은 법 시행령 제43조제3항 또는 같은 법 제37조제5항 및 같은 법 시행령 제44조제2항에 따라 귀하의 요구에 대한 결과를 위와 같이 통지합니다.

년 월 일

발 신 명 의 직인

유의사항

개인정보의 정정·삭제 또는 처리정지 요구에 대한 결정을 통지받은 경우에는 개인정보처리자가 '이의제기방법'란에 적은 방법으로 이의제기를 할 수 있습니다.

210㎜×297㎜[신문용지 54g/㎡]

■ [강릉원주대학교 별지 제8호서식]

개인정보의 목적 외 이용 및 제3자 제공 대장

개인정보 또는 개인정보파일 명칭			
이용 또는 제공 구분	[ ] 목적외 이용 [ ] 제3자 제공		
목적 외 이용기관의 명칭 (목적 외 이용의 경우)		담당자	소 속 성 명 전화번호
제공받는 기관의 명칭 (제3자 제공의 경우)		담당자	성 명 소 속 전화번호
이용하거나 제공한 날짜, 주기 또는 기간			
이용하거나 제공한 형태			
이용 또는 제공의 법적 근거			
이용 목적 또는 제공받는 목적			
이용하거나 제공한 개인정보의 항목			
「개인정보 보호법」 제18조제5항에 따라 제한을 하거나 필요한 조치를 마련할 것을 요청한 경우에는 그 내용			

210㎜×297㎜[인쇄용지(특급) 34g/㎡]

■ [강릉원주대학교 별지 제9호서식]

개인정보침해사고 관리대장

접수		신고개요	등급	처리유형	종결일자	처리내용	비고
일시	신고자 유형						

■ [강릉원주대학교 별지 제10호서식]

개인정보침해사고 처리보고서

<table>
<tr><td>보고일자</td><td colspan="2"></td><td>문서번호</td><td></td></tr>
<tr><td colspan="5">침해 신고 / 접수 정보</td></tr>
<tr><td>침해등급</td><td colspan="2">☐ 1등급 ☐ 2등급 ☐ 3등급</td><td>침해대상정보</td><td>☐ 일반 개인정보
☐ 주민등록번호
☐ 계좌번호</td></tr>
<tr><td>접수일시</td><td colspan="2"></td><td>신고일자</td><td></td></tr>
<tr><td>침해사고
처리책임자</td><td colspan="2"></td><td>신고자 연락처</td><td></td></tr>
<tr><td>신고 내용</td><td colspan="4"></td></tr>
<tr><td rowspan="2">대응 과정</td><td>일시</td><td colspan="3">대응활동</td></tr>
<tr><td></td><td colspan="3"></td></tr>
<tr><td>침해 내용</td><td colspan="4">확인된 침해 정보의 세부사항, 규모 및 침해 방법(노출, 외부자 제공, 수집, 접근, 분석, 이용, 내부자 제공, 불법 저장, 불안전한 저장, 파기, 비파기 등 세부사항)</td></tr>
<tr><td>침해 발생 경위</td><td colspan="4"></td></tr>
<tr><td>관련자</td><td colspan="4"></td></tr>
<tr><td>침해 발생 원인</td><td colspan="4"></td></tr>
<tr><td>증거자료</td><td colspan="4"></td></tr>
<tr><td>복구 및
재발방지 조치</td><td colspan="4"></td></tr>
<tr><td>처분</td><td colspan="4"></td></tr>
</table>