[붙임5]

- 2021년 안산대학교 -

개인정보보호 내부관리 계획

2021. 04.

행정지원처

목 차

목 차

제1장 총칙

제1조(목적) 안산대학교(이하“본교”라 한다) 개인정보 내부관리계획(이하 ‘본 계획’ 또는 ‘내부관리계획’이라 한다.)은 개인정보 보호법 제29조 및 개인정보의 안전성 확보조치 기준 제4조에 따라 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(적용범위) 본 계획은 정보통신망을 통하여 수집, 이용, 제공 또는 관리되는 개인정보뿐만 아니라 서면 등 정보통신망 이외의 수단을 통해서 수집, 이용, 제공 또는 관리되는 개인정보에 대해서도 적용되며, 이러한 개인정보를 취급하는 내부 교직원 및 외부위탁업체에 대해 적용된다.

제3조(용어의 정의) 본 계획에서 사용하는 용어의 뜻은 다음과 같다.

1. “개인정보”라 함은 살아있는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명·주민등록번호·학력 및 사진·영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함)를 말한다.

> ▷ 고유식별정보 : 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호
> ▷ 민감정보 : 사상, 신념, 노동조합 · 정당의 가입 · 탈퇴, 정치적 견해, 건강, 성생활, 유전정보, 범죄경력 정보 등에 관한 정보와 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보

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 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. "개인정보보호책임자"란 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지는 자로서 영 제32조제2항에 해당하는 자를 말한다.
7. "개인정보보호담당자”란 개인정보보호책임자를 보좌하여 개인정보 보호업무에 대한 실무를 처리하는 자를 말한다.
8. "개인정보취급자"란 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무

를 담당하는 자로서 임직원, 파견근로자, 시간제근로자 등을 말한다.

9. "개인정보보호분야별책임자"란 개인정보취급자를 관리·감독하며, 개인정보보호업무에 대한 세부 업무를 총괄하고 관리하는 자를 말한다.
10. "개인정보처리시스템"이란 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템을 말한다.
11. "영상정보처리기기"란 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치를 말한다.
12. "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.
13. "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.
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. "공개된 무선망"이란 불특정 다수가 무선접속장치(AP)를 통하여 인터넷을 이용할 수 있는 망을 말한다.
16. "모바일 기기"란 무선망을 이용할 수 있는 PDA, 스마트폰, 태블릿PC 등 개인정보처리에 이용되는 휴대용 기기를 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"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.
19. "내부망"이란 물리적 망분리, 접근 통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.
20. "접속기록"이란 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무내역에 대하여 개인정보취급자 등의 계정, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 전자적으로 기록한 것을 말한다. 이 경우 "접속"이란 개인정보처리시스템과 연결되어 데이터 송신 또는 수신이 가능한 상태를 말한다.
21. "관리용 단말기"란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리시스템에 직접 접속하는 단말기를 말한다.

제2장 개인정보 내부관리계획의 수립 및 시행

제4조(내부관리계획의 수립 및 시행)

① 개인정보 보호책임자는 행정지원처장(문용국처장)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 보호책임자는 제1항, 제2항에 따라 내부 관리계획을 수립하거나 수정하는 경우에는 총장으로부터 내부결재 등의 승인을 받아야 하며, 그 이력을 보관·관리하여야 한다.

④ 개인정보처리자는 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(내부관리계획의 공표)

① 관리책임관은 승인한 내부관리계획을 학칙 또는 본교 규정에 정하지 않은 경우, 30일 이내, 교내 전 교직원 및 학생에게 공포한다.

② 내부관리계획은 교내 전 교직원 및 학생이 언제든지 열람(홈페이지 게시)할 수 있도록 하여야 하며, 변경사항이 있는 경우에는 즉시 공지하여야 한다.

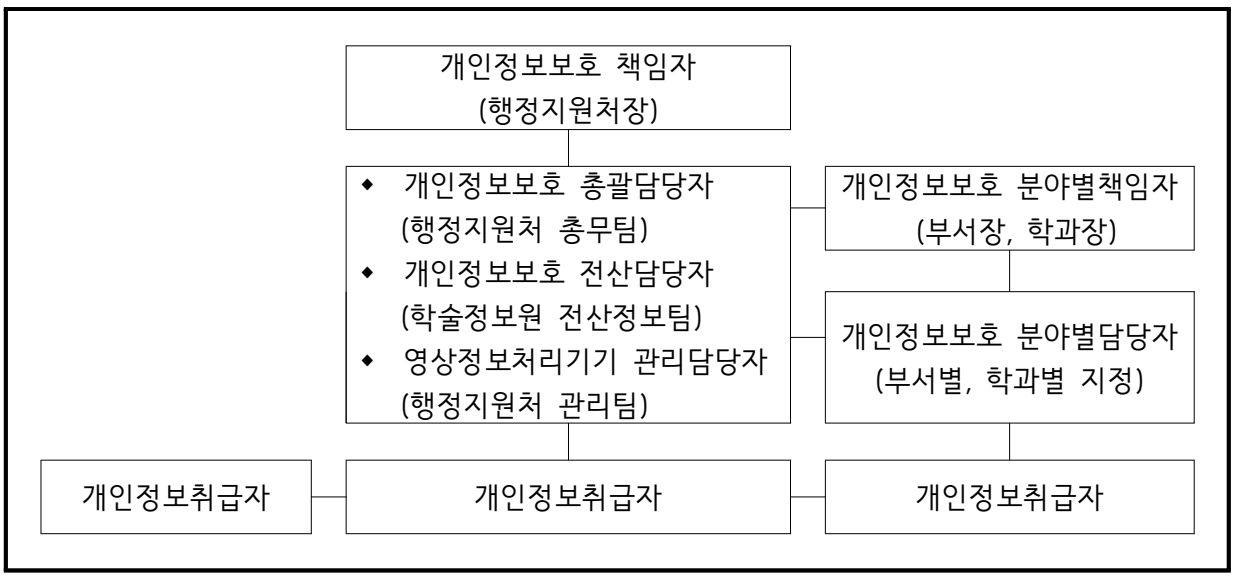
제3장 개인정보보호책임자의 의무와 책임

제6조(개인정보 보호조직 구성과 개인정보관리책임자의 지정)

본교의 개인정보 보호조직 구성은 아래와 같으며, 개인정보 보호법 시행령 제32조 제2항1호에 따라 해당하는 지위에 있는 행정지원처장을 개인정보관리책임자(CPO : Chief Privacy Officer)으로 지정한다.

1. 개인정보 보호관리 체계

2. 개인정보 보호관리 조직



제7조(개인정보보호책임자의 의무와 책임)

① 개인정보보호책임자는 개인정보보호를 위하여 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.「개인정보 보호법」 제30조에 따른 개인정보 처리방침의 수립·변경 및 시행
8. 개인정보 보호 관련 자료의 관리
9. 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기

② **개인정보 분야별책임자**은 다음 각 호의 업무를 수행한다.

1. 보유하고 있는 개인정보파일에 대한 안전성 확보
2. 개인정보취급자 교육 및 관리·감독
3. 개인정보보호 계획 및 방침 준수
4. 처리정보의 이용·제공에 대한 절차·기준 마련
5. 기타 개인정보보호와 관련된 사항
6. 개인정보분야별책임자는 개인정보분야별담당자를 지정하여 개인정보 보호업무를 담당하게 할 수 있다.

③ **개인정보보호담당자**는 다음 각 호의 업무를 수행한다.

1. 개인정보보호 정책 및 규정의 검토
2. 개인정보보호 교육계획 수립 및 시행
3. 상급기관 개인정보보호정책 적용 및 교육 참석
4. 개인정보 노출 점검 및 로그관리
5. 개인정보보호 관련 개인정보보호책임자의 업무 지원

제8조(개인정보취급자의 의무와 책임)

① 개인정보취급자는 개인정보보호와 관련하여 다음과 같은 역할 및 책임을 이행한다.

1. 개인정보보호 규정 및 내부관리계획 준수
2. 개인정보 처리결과에 대하여 분야별책임자에게 보고체계 유지
3. 개인정보 제공처리 등의 기록 유지 및 보고
4. 직원 또는 제3자에 의한 위법·부당한 개인정보 침해행위 점검 등
5. 열람청구, 정정·삭제, 처리정지 등 정보주체의 권리 보장
6. 기타 개인정보보호를 위해 필요한 사항의 이행 등

제4장 개인정보의 기술적·관리적·물리적 안전조치

제9조(접근권한의 관리)

① 분야별책임자는 개인정보처리시스템에 대한 접근권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.

② 분야별책임자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하여야 한다.

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

④ 분야별책임자는 개인정보처리시스템에 접속할 수 있는 사용자 계정을 발급하는 경우, 개인정보취급자 별로 한 개의 사용자 계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

제10조(비밀번호 관리)

① 개인정보처리자는 사용하는 아이디의 비밀번호는 분기 1회 이상 변경 하여야 한다.

② 관리책임자는 모든 사용자에게 비밀번호 변경에 대한 필요성과 의무를 고지하여야 하며, 필요시 비밀번호 변경을 강제하기 위하여 시스템 접근을 제한하거나 비밀번호 강제변경 프로그램 사용 등의 조치를 취할 수 있다.

③ 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.

④ 개인정보처리자는 비밀번호 설정 시 다음 각호의 사항을 반영하여 설정한다.

1. 사용자 계정과 동일하지 않은 것
2. 비밀번호는 구성하는 문자의 종류에 따라 최소 10자리 또는 9자리 이상의 길이로 구성하도록 한다
   최소 10자리 이상 : 영대문자, 영소문자, 숫자, 특수문자(32개)중 2종류 이상
   최소 9자리 이상 : 영대문자, 영소문자, 숫자, 특수문자(32개)중 3종류 이상
3. 개인 신상 및 부서명칭, 전화번호 등과 관계가 없는 것
4. 일반 사전에 등록된 단어 사용을 피할 것
   예) love, happy등과 같은 잘 알려진 단어
5. 동일 단어(문자) 또는 숫자를 반복하여 사용하지 말 것
6. 2개의 비밀번호를 교대로 사용하지 말 것
7. 규칙적인 문자·숫자열 등을 사용하지 말 것

제11조(접근통제시스템의 설치 및 운영)

① 관리책임자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 시스템을 설치·운영하여야 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 시도를 탐지

② 관리책임자는 정보통신망을 통해 외부에서 개인정보처리시스템에 접속 하려는 경우에는

가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단 또는 안전한 인증수단을 적용하여야 한다.

③ 관리책임자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 조치를 취하여야 한다.

④ 관리책임자는 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 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.

⑥ 개인정보처리자는 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 점검 하여야 한다.

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

제12조(개인정보의 암호화)

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

② 제1항에 따른 개인정보를 정보통신망을 통하여 송·수신하거나 보조저장매체 등을 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.

제13조(접속기록의 보관 및 점검)

① 관리책임자는 개인정보취급자가 개인정보처리시스템에 접속한 기록 1년 이상 보관·관리하여야 한다. 다만, 5만명 이상의 정보주체에 관하여 개인정보를 처리하거나, 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다.

② 관리책임자는 개인정보처리시스템의 접속기록이 위·변조 및 도난, 분실되지 않도록 안전하게 보관하여야 한다.

③ 분야별책임자는 개인정보의 분실·도난·유출·위조·변조·훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 특히 개인정보를 다운로드한 것이 발견되었을 경우에는 내부관리계획으로 정하는 바에 따라 그 사유를 반드시 확인하여야 한다.

제14조(보안프로그램의 설치 및 운영) 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 자동 업데이트 기능을 사용하거나, 또는 일 1회 이상 업데이트를 실시한다.
2. 악성 프로그램관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 실시한다.
3. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치한다.

제15조(관리용 단말기의 안전조치) 개인정보처리자는 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

제16조(물리적 접근제한 및 관리)

① 관리책임자는 행정지원처에서 행정관리를 진행하고 전산정보원에서 기술적(전산정보자료) 조치, 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 마련하

여야 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 열람내용을 주기적으로 검토하여 정당하지 않은 권한으로 출입하거나 열람하고 있는지 를 점검하여 확인하여야 한다.

제17조(출력 복사시의 보호조치)

① 분야별책임자는 개인정보가 포함된 정보를 출력하거나 복사할 경우에 개인정보 유출 사고를 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 적용하여야 한다.

③ 개인정보취급자는 개인정보의 이용을 위하여 출력 및 복사한 개인정보의 이용 목적이 완료된 경우 분쇄기로 분쇄하거나 소각하는 등의 안전한 방법으로 파기하여야 한다.

제18조(개인정보의 파기)

① 개인정보처리자는 개인정보를 파기할 경우 다음 각 호의 조치를 취하여야 한다

1. 완전파기(소각.파쇄 등)
2. 전용 소자장비를 이용하여 삭제
3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

② 개인정보처리자가 개인정보 일부만을 파기하는 경우, 제1항의 방법으로 파기하는 것이 어려울 때에는 다음 각 호의 조치를 하여야 한다.

1. 전자적 파일의 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

③ 개인정보를 파기하지 않고 보존해야 하는 경우 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여 저장·관리하여야 한다.

제19조(재해·재난 대비 안전조치)

① 개인정보관리책임자은 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템

보호를 위한 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검하여야 한다.

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

제20조(위험도 분석 및 대응) 개인정보 유출에 영향을 미칠 수 있는 다양한 위험요소를 사전에 식별·평가하고 해당 위험요소를 적절하게 통제할 수 있는 방안을 마련하기 위해 종합적으로 분석하는 등 위험도 분석 및 대응방안에 관한 사항을 마련하여야 한다.

제5장 개인정보 처리 실태조사·점검(감사)

제21조(실태조사 주기 및 절차)

① 본교의 개인정보보호에 대한 감사는 관련 법률 및 규정이 정한 사항을 확인하고 문제점 등을 보완하기 위하여 교내 모든 개인정보 관련 자원 및 전 구성원을 대상으로 실시한다.

② 개인정보보호 감사는 정기감사와 특별감사로 구분한다.

③ 관리책임자는 연 1회의 정기감사를 실시하되 학사일정 등 교내 상황을 고려하여 감사범위, 시기, 방법 등을 포함한 감사계획을 수립하여 사전에 공지하여야 한다.

④ 특별감사는 개인정보 유출사고나 위험요소 발견 등 중요한 사안 발생시 총장의 결재를 얻은 후 실시한다.

⑤ 관리책임자는 보호담당자를 포함한 감사조직을 구성하되 감사조직 구성이 여의치 않을 경우에는 외부 전문가에게 용역을 맡길 수 있다.

⑥ 관리책임자는 감사결과에 대하여 감사결과보고서를 기록·관리하고 총장에게 보고하여야 한다.

제6장 개인정보보호 교육

제22조(개인정보보호 교육의 실시)

① 관리책임자는 교내 전 교직원을 대상으로 개인정보보호에 관한 교육을 실시하여 개인정보보호정책 및 세부활동계획을 전달하고 개인정보보호에 대한 인식을 제고하여 부주의나 인식부족으로 인한 개인정보 침해사고가 발생하지 않도록 사전에 예방하여야 한다.

② 개인정보보호 교육은 년 2회 정기교육을 실시하고 필요에 따라 수시교육을 할 수 있다.

③ 관리책임자 및 보호담당자는 행정자치부장관이 주관하는 개인정보보호관련 교육 및 컨퍼런스에 반드시 참석하여야 하며, 교육이수내용을 개인정보정책 수립 및 개인정보보호 활동에 적극 활용하여야 한다.

제23조(개인정보보호 교육 계획의 수립)

① 관리책임자는 전 교직원을 대상으로 연2회의 연간 개인정보보호 교육계획을 수립하고 이를 사전 공지하여 본교 학사일정에 포함하여야 한다.

② 교육계획에는 내용·강사·방법·일시·장소·대상 등의 사항이 포함되어야 한다.

③ 교육 방법은 집체 교육뿐만 아니라, 사이버 교육, 그룹웨어 교육 등 다양한 방법을 활용하여 실시하고, 필요시 외부 전문가에게 위탁하여 교육을 실시할 수 있으며 이 경우에는 사전에 전문가를 선정하여 교육계획을 협의하여야 한다.

④ 교육 후 필요시 설문을 실시할 수 있으며 그 결과는 추후 개인정보보호 정책 수립 및 교육계획 등에 반영하도록 한다.

제7장 개인정보 침해대응 및 피해구제

제24조(개인정보 유출 등의 통지)

① 관리책임자는 개인정보가 유출되었음을 알게 되었을 때에는 지체없이 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. 본교의 대응조치 및 피해 구제절차
5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

제25조(개인정보 침해사고 신고)

① 본교에서 수집·처리·보유 중인 개인정보파일에 의해 개인정보의 권익을 침해받은 자는 개인정보침해사실신고서(별지 제13호 서식)를 작성하여 행정자치부장관에게 신고할 수 있다.

② 관리책임자는 행정자치부장관으로부터 개인정보 침해사고 사실을 통보 받은 경우 침

해사고 사실여부를 확인하고 그에 대한 사고조치를 수행한 후 개인정보 침해사고접수·처리결과보고서를 작성하고 총장의 결재를 득하여 행정자치부장관에게 보고하여야 한다.

③ 교내에서 개인정보 침해사고가 발견되거나 신고되었을 때에도 최초 발견 또는 신고받은 교직원은 보호담당자에게 신고하고, 보호담당자는 관리책임자에게 즉시 보고하여 사실여부를 확인하고 해당 개인정보에 대한 적절한 조치를 취한 후 결과보고서를 작성하여 행정자치부장관에게 보고하여야 한다.

④ 개인정보 침해신고를 접수하였을 때에는 접수한 날로부터 7일 이내에 관련 사실에 대한 기본조사 및 상담을 실시하고, 30일 이내에 세부조사 및 적절한 조치 및 결과보고를 완료하여야 한다.

⑤ 개인정보 침해사고 및 신고에 대한 처리가 완료된 후에는 관련 내용에 대하여 개인정보침해신고처리대장(별지 제14호 서식)을 기록하여 관리하여야 한다.

제26 조(권익침해 구제방법)

① 개인정보주체는 개인정보침해로 인한 구제를 받기 위하여 개인정보분쟁 조정위원회, 한국인터넷진흥원 개인정보침해신고센터 등에 분쟁해결이나 상담 등을 신청한다.

1. 개인정보 분쟁조정위원회 : 02-2100-2499(www.kopico.go.kr)
2. 개인정보 침해신고센터 : 국번없이 118번(privacy.kisa.or.kr)
3. 대검찰청 사이버범죄수사단 : 02-3480-3571
4. 경찰청 사이버안전국 : 국번없이 118번

제8장 개인정보의 목적 외 이용·제공 절차 및 유의사항

제27 조(개인정보의 목적 외 이용·제공시 절차)

① 목적 외 이용·제3자 제공이 가능한 경우에 해당하는지 법적근거 검토

② 법적근거가 없는 경우에는 정보주체로부터 별도의 동의를 받아야 한다

③ 개인정보의 목적 외 이용 및 제3자 제공대장을 기록·관리하여야 한다

④ 30일 이내에 관보 또는 인터넷 홈페이지에 게재

⑤ 제3자 제공시에는 이용목적, 이용방법, 이용기간, 이용형태 등을 제한 하거나, 개인정보의 안전성 확보를 위하여 필요한 조치를 마련하도록 문서로 요청

⑥ 안전한 확보조치 요청을 받은 자는 그에 따른 조치를 취한 후 결과를 개인정보를 제공한 개인정보처리자에게 문서를 알려야 한다

제28 조(개인정보의 목적 외 이용·제공시 유의사항)

① 개인정보보호법 제18조제2항 각 호(다른 법률에 특별한 규정이 있는 경우 등)에 해

당하는 경우에만 당초 수집 목적 외 이용·제공 가능

- 이에 해당하지 않는 경우에는 정보주체의 사전 동의를 받아야 한다

② 목적 외 이용·제공이 가능한 경우에도 필요 최소한 범위 이내로 제한

③ 개인정보를 제공하는 기관은 제공받는 기관에 이용 목적·범위 제한 및 안전조치 마련 등을 요청하고, 그 기관은 이에 따라야 한다

④ 목적 외 이용·제공 후 주요사항 공개 및 세부내역 대장 관리

- 주요사항 공개 : 법적 근거 등을 인터넷 등에 공개(본인 동의, 범죄수사 등의 경우 제외)

제29 조(제3자에 대한 개인정보 제공 중단 절차) 개인정보처리자는 개인정보를 이용하거나 제공받는 기관이 개인정보의 이용 및 제공의 제한을 이행하지 아니한 때에는 다음 각 호의 절차에 따라 개인정보의 이용을 중지시키거나 제공을 중지한다.

1. 개인정보처리자는 관리책임자 및 개인정보취급자에게 관련 사실을 알린다.
2. 개인정보처리자는‘개인정보의 이용 및 제공의 제한’의무 미이행 사항을 인지한 날부터 해당 기관에 개인정보 제공을 임시로 중지한다.
3. 개인정보를 제공받는 기관에게 ‘개인정보의 이용 및 제공의 제한’의무 미이행 사항에 대한 소명을 문서로 요청한다.
4. 해당 기관으로부터 소명받은 자료를 접수한 후 개인정보보호담당자는 조치방안을 수립하여 관리책임자의 승인을 받는다.
5. 관리책임자는 개인정보 제공 중지를 해당 기관에 통보한다. 동시에 해당기관에 개인정보 제공을 중지한다.

제9장 개인정보 처리업무 위탁 관리 및 감독

제30조 (위탁목적 등의 문서화) 개인정보의 처리업무를 위탁하는 경우 다음 각 호의 내용이 포함된 문서에 의하여야 한다.

1. 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
2. 개인정보의 기술적·관리적 보호조치에 관한 사항
3. 위탁업무의 목적 및 범위
4. 재위탁 제한에 관한 사항
5. 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
6. 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한

사항

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

제31조 (수탁자에 대한 교육 및 관리 감독)

① 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난· 유출·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.

② 위탁자는 수탁자가 개인정보처리자가 준수하여야 할 사항의 준수 여부를 확인·점검하여야한다.

③ 위탁자는 수탁자에 대하여 정기적인 교육을 실시하는 외에 수탁자의 개인정보처리 현황 및 실태, 목적외 이용·제공, 재위탁 여부, 안전성 확보조치 여부 등을 정기적으로 조사·점검하여야 한다.

[별지1]개인정보보호 서약서

개인정보보호 서약서

1. 본인은 안산대학교로부터 취득한 모든 개인정보를 업무에 한해 이용하며, 타 기관의 보호 대상 정보를 안산대학교 내에 보관하지 않겠습니다.
2. 본인은 직무상 알게 된 개인정보를 누설하지 않겠습니다.
3. 본인은 명백히 허가 받지 않은 개인정보나 시설에는 접근하지 않으며, 관련 업무 수행 시 안산대학교에서 지정한 데이터 처리 방법만을 이용하겠습니다.
4. 본인은 업무와 관련한 개인정보의 수집, 생성, 기록, 저장, 이용, 제공, 공개, 파기 및 그 밖에 이와 유사한 일체의 행위에 대하여 안산대학교의 규정과 통제절차를 준수하겠습니다.
5. 본인은 본인에게 할당된 사용자 ID, 패스워드, 출입증, 인증서, 개인정보처리시스템을 타인과 공동 사용하거나 관련정보를 누설하지 않겠습니다.
6. 본인은 안산대학교로부터 제공받은 정보자산(서류, 사진, 영상, 전자파일, 저장매체 등)을 무단변조, 복사, 훼손, 분실 등으로부터 안전하게 관리하겠으며 승인 받지 않은 프로그램, 정보저장 매체는 기관 내부에서 사용하지 않겠습니다.
7. 본인은 퇴직 시 안산대학교에서 제공받은 정보자산을 반드시 반납할 것이며, 퇴직 후에도 퇴직 전 알게 된 모든 개인정보와 업무상 비밀 등 각종 정보(서류포함)에 대하여는 일체 누설하지 않겠습니다.

개인정보 보호와 관련한 비밀의 준수와 개인정보보호를 위한 법적 준수기준인 “정보통신이용촉진 및 정보보호에 관한 법률”에 명시된 모든 조항과 “개인정보보법” 및 안산대학교의 개인정보보호 규정“과 ”안산대학교 개인정보 내부관리계획“등 관련된 모든 조항이 포함된다는 것을 충분히 설명 받고 숙지하였습니다.

만약, 이러한 서약에도 불구하고 업무상 알게 된 사항에 대하여 비밀을 누설하거나 정당한 사유 없이 조회, 유출, 오용할 경우, 형사상 민사상의 법률 조항에 의거하여 제재 및 안산대학교에 끼친 손해에 대해 지체 없이 변상·복구 할 수 있음을 통고 받았으며, 이러한 제재에 대하여 이의를 제기하지 않을 것을 본인의 자의로 서약합니다.

일 시 : 20 년 월 일

소 속:

성 명: (인)

안산대학교 총장 귀하

[별지2]개인정보처리위탁 계약서

개인정보처리위탁 계약서

안산대학교(이하 “갑”이라 한다)과 (이하 “을”이라 한다)는 “갑”의 개인정보 처리업무를 “을”에게 위탁함에 있어 다음과 같은 내용으로 본 업무위탁계약을 체결한다.

제1조 (목적) 이 계약은 “갑”이 개인정보처리업무를 “을”에게 위탁하고, “을”은 이를 승낙하여 “을”의 책임아래 성실하게 업무를 완성하도록 하는데 필요한 사항을 정함을 목적으로 한다.

제2조 (용어의 정의) 본 계약에서 별도로 정의되지 아니한 용어는 개인정보보호법, 동법 시행령 및 시행규칙, 「개인정보의 안전성 확보조치 기준」(행정안전부 고시 제2020-2호) 및 「표준 개인정보 보호지침」(행정안전부 고시 제2020-1호)에서 정의된 바에 따른다.

제3조 (위탁업무의 목적 및 범위) “을”은 계약이 정하는 바에 따라 ( ) 목적으로 다음과 같은 개인정보 처리 업무를 수행한다.[1)]
1. (시스템 및 업무명)
2. (시스템 및 업무명)

<신설> 제4조(위탁업무 기간) 이 계약서에 의한 개인정보 처리업무의 기간은 다음과 같다.
계약기간 : 20○○년 ○ 월 ○ 일 ~ 20○○년 ○ 월 ○ 일

제5조 (재위탁 제한) ① “을”은 “갑”의 사전 승낙을 얻은 경우를 제외하고 “갑”과의 계약상의 권리와 의무의 전부 또는 일부를 제3자에게 양도하거나 재위탁할 수 없다.
② “을”이 다른 제3의 회사와 수탁계약을 할 경우에는 “을”은 해당 사실을 계약 체결 7일 이전에 “갑”에게 통보하고 협의하여야 한다.

제6조 (개인정보의 안전성 확보조치) “을”은 「개인정보 보호법」 제23조제2항, 제24조제3항 및 제29조, 같은 법 시행령 제21조 및 제30조, 「개인정보의 안전성 확보조치 기준」(행정안전부 고시 제2020-2호)에 따라 개인정보의 안전성 확보에 필요한 관리적·기술적 조치를 취하여야 한다.

제7조 (개인정보의 처리제한) ① “을”은 계약기간은 물론 계약 종료 후에도 위탁업무 수행 목적 범위를 넘어 개인정보를 이용하거나 이를 제3자에게 제공 또는 누설하여서는 안 된다.
② “을”은 계약이 해지되거나 또는 계약기간이 만료된 경우 위탁업무와 관련하여 보유하고 있는 개인정보를 「개인정보보호법」 시행령 제16조 및「개인정보의 안전성 확보조치 기준」(행정안전부 고시 제2020-2호)에 따라 즉시 파기하거나 “갑”에게 반납하여야 한다.
③ 제2항에 따라 “을”이 개인정보를 파기한 경우 지체 없이 “갑”에게 그 결과를 통보

1) 각호의 업무 예시 : 고객만족도 조사 업무, 회원가입 및 운영 업무, 사은품 배송을 위한 이름, 주소, 연락처 처리 등

하여야 한다.

제8조 (수탁자에 대한 관리·감독 등) ① “갑”은 “을”에 대하여 다음 각 호의 사항을 관리하도록 요구할 수 있으며, “을”은 특별한 사유가 없는 한 이에 응하여야 한다.

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

② “갑”은 “을”에 대하여 제1항 각 호의 사항에 대한 실태를 점검하여 시정을 요구할 수 있으며, “을”은 특별한 사유가 없는 한 이행하여야 한다.

③ “갑”은 처리위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 1년에 1회 “을”을 교육할 수 있으며, “을”은 이에 응하여야 한다.[2)]

④ 제3항에 따른 교육의 시기와 방법 등에 대해서는 “갑”은 “을”과 협의하여 시행한다.

제9조 (손해배상) ① “을” 또는 “을”의 임직원 또는 기타 “을”의 수탁자가 이 계약에 의하여 위탁 또는 재위탁받은 업무를 수행함에 있어 이 계약에 따른 의무를 위반하거나 “을” 또는 “을”의 임직원 또는 기타 “을”의 수탁자의 귀책사유로 인하여 “갑” 또는 개인정보주체 또는 기타 제3자에게 손해가 발생한 경우 “을”은 그 손해를 배상하여야 한다.

② 제1항과 관련하여 개인정보주체 또는 기타 제3자에게 발생한 손해에 대하여 “갑”이 전부 또는 일부를 배상한 때에는 “갑”은 이를 “을”에게 구상할 수 있다.

제10조 (정보주체 권리보장) ① “을”은 정보주체의 개인정보 열람, 정정·삭제, 처리 정지 요청 등에 대응하기 위한 연락처 등 민원 창구를 마련해야 한다.

제11조 (개인정보의 파기) ① “을”은 제4조의 위탁업무기간이 종료되면 특별한 사유가 없는 한 지체 없이 개인정보를 파기하고 이를 “갑”에게 통보하고 확인받아야 한다.

본 계약의 내용을 증명하기 위하여 계약서 2부를 작성하고, “갑”과 “을”이 서명 또는 날인한 후 각 1부씩 보관한다.

20 년 월 일

“갑” :	**안산대학교**	**“을” :**	
사업자번호:	134-82-02670	사업자번호:	
사업장주소:	경기도 안산시 상록구 안산대학로 155(일동)	사업장주소:	
총 장:		대표자명:	

2) 「개인정보 안전성 확보조치 기준 고시」(개인정보 보호위원회 고시 제2020-2호) 및 「개인정보 보호법」 제26조에 따라 개인정보처리자 및 취급자는 개인정보보호에 관한 교육을 의무적으로 시행하여야 한다.

[별지3]개인정보 유출신고서

개인정보 유출신고서

기관명					
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 구제절차					
담당부서·담당자 및 연락처		성명	부서	직위	연락처
	개인정보 보호책임자				
	개인정보 취급자				

유출신고접수기관	기관명	담당자명	연락처

[별지4]개인정보 파기 요청서

개인정보파일 파기 요청서

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

[별지5]개인정보파일 파기 관리대장

개인정보파일 파기 관리대장

번호	개인정보 파일명	자료의 종류	생성일	폐기일	폐기사유	처리담당자	처리부서장

[별지6]개인정보의 목적 외 이용 및 제 3자 제공 대장

개인정보의 목적 외 이용 및 제3자 제공 대장

<table>
<tr><td>개인정보 또는
개인정보파일 명칭</td><td colspan="4"></td></tr>
<tr><td>이용 또는 제공 구분</td><td colspan="4">[ ] 목적외 이용 [ ] 제3자 제공</td></tr>
<tr><td rowspan="3">목적 외 이용기관의 명칭
(목적 외 이용의 경우)</td><td rowspan="3"></td><td rowspan="3">담당자</td><td>소 속</td><td></td></tr>
<tr><td>성 명</td><td></td></tr>
<tr><td>전화번호</td><td></td></tr>
<tr><td rowspan="3">제공받는 기관의 명칭
(제3자 제공의 경우)</td><td rowspan="3"></td><td rowspan="3">담당자</td><td>성 명</td><td></td></tr>
<tr><td>소 속</td><td></td></tr>
<tr><td>전화번호</td><td></td></tr>
<tr><td>이용하거나 제공한 날짜,
주기 또는 기간</td><td colspan="4"></td></tr>
<tr><td>이용하거나 제공한 형태</td><td colspan="4"></td></tr>
<tr><td>이용 또는 제공의 법적
근거</td><td colspan="4"></td></tr>
<tr><td>이용 목적 또는
제공받는 목적</td><td colspan="4"></td></tr>
<tr><td>이용하거나 제공한
개인정보의 항목</td><td colspan="4"></td></tr>
<tr><td>「개인정보 보호법」
제18조제5항에 따라
제한을 하거나 필요한
조치를 마련할 것을
요청한 경우에는 그 내용</td><td colspan="4">1. 비밀정보를 취급함에 있어 신의와 성실을 다하고 이를 별도로 구분하여 엄중히 관리하여야 하며, 업무의 수행과 관계없는 제3자에게 열람케 하거나 누설할 염려가 있는 일체의 행위를 하여서는 아니 된다.
2. 비밀정보와 관련 있는 사항을 위탁업무 목적 외에는 사용 할 수 없다. 이를 위반할 경우 민, 형사상의 손해배상 책임을 진다.
3. 비밀정보를 제3자가 사용하고 있음을 발견하게 된 때에는 지체 없이 그 사실을 대학에 통지하여야 하며, 상호간에 정한 거래목적 이외에 다른 용도나 영업상의 수단으로 사용 할 수 없으며, 타인에게 양도, 이전, 공개하여서는 아니 된다.
4. 대학으로부터 제공받은 비밀정보를 복사, 재생산, 제본 등의 행위를 하여서는 아니 된다.
5. 제공받은 비밀정보를 담당하는 자에게 개인정보에 관한 교육 및 관리.감독을 실시하여야 한다.
6. 위탁종료시 제공받은 일체의 자료(복사 등에 의한 자료 포함)를 대학의 요구에 따라 반납하거나 안전한 방법으로 파기하고 그 증빙을 대학에 공문서로 제출하여야 한다.</td></tr>
</table>

210㎜×297㎜[인쇄용지(특급) 34g/㎡]

[별지7] 개인정보 열람, 정정, 삭제처리청구서

(앞 쪽)

개인정보(□열람 □정정·삭제 □처리정지) 청구서 ※ 아래 유의사항을 읽고 굵은 선 안쪽의 사항만 적어 주시기 바랍니다.	처리기한 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	개인정보파일명				
	□ 열람	대상	□ 개인정보파일 기록항목 : 전부, 일부( ) □ 개인정보 제3자 제공 현황 : 기간(~) □ 개인정보 처리에 대한 동의 현황		
		방법	□ 열람 : 직접방문, 전자열람 □ 사본·출력물 수령 : 우편, 모사전송 □ 전자파일 수령 : 전자우편, 기타( )		
	□ 정정·삭제	※ 정정·삭제하고자 하는 개인정보의 항목과 그 사유를 기재합니다.			
	□ 처리정지	※ 개인정보의 처리정지를 원하는 대상·내용 및 그 사유를 기재합니다.			

「개인정보 보호법」 제35조제1항, 제36조제1항 및 제37조제1항에 따라 위와 같이 개인정보의 열람, 정정·삭제 또는 처리정지를 청구합니다.

년 월 일

청구인 (서명 또는 인)

○○○○ 귀하

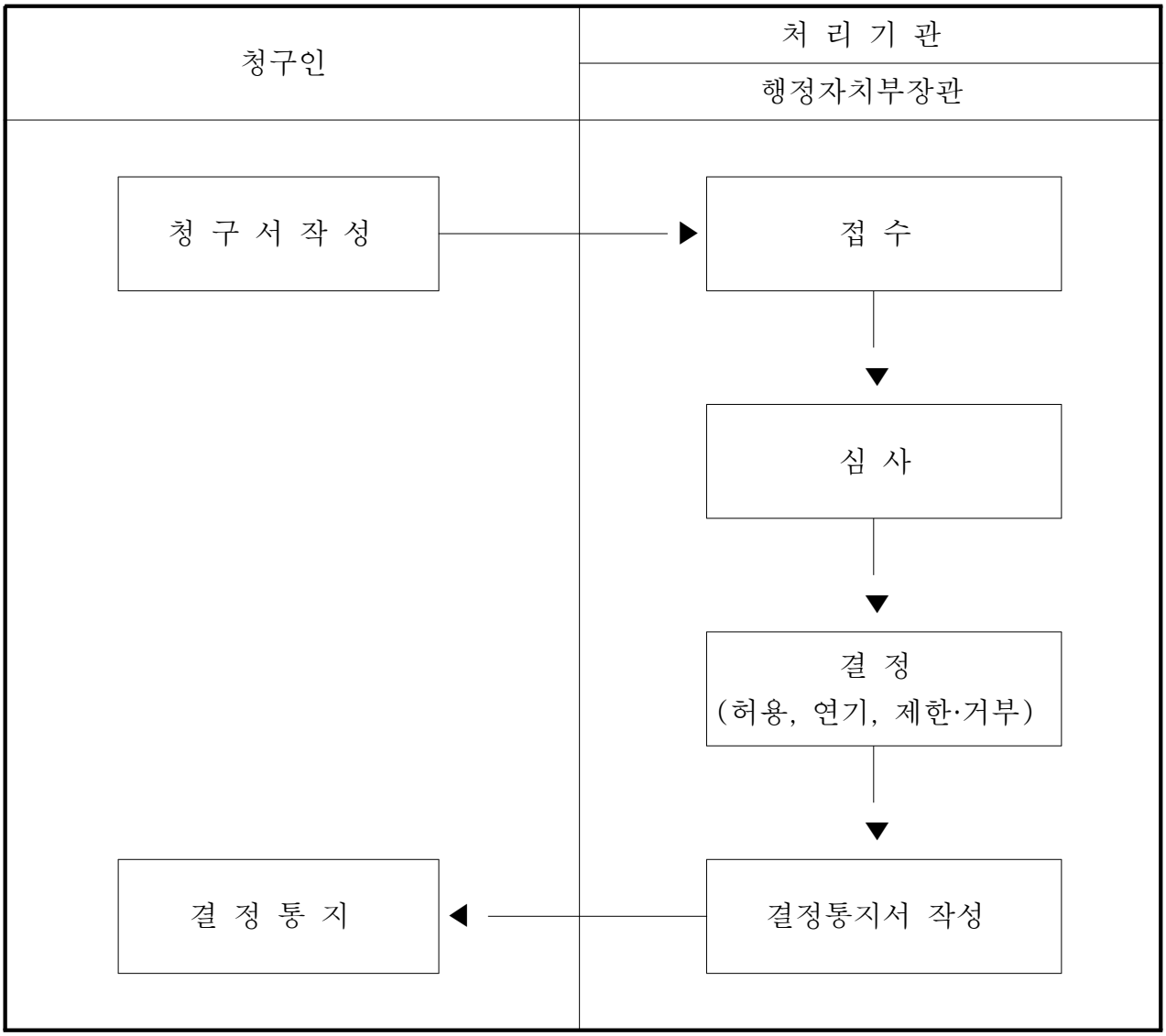
<유의사항>

1. '개인정보파일명' 란에는 「개인정보 보호법」 제32조제1항에 따라 등록·공개되는 개인정보파일의 명칭을 기재합니다.
2. 개인정보의 열람을 청구하고자 하는 경우에는 '열람' 란에 ☑ 표시를 하고 열람하고자 하는 대상과 방법을 선택하여 ☑ 표시를 합니다. 표시를 하지 않은 경우에는 '미포함'으로 처리됩니다.
3. 개인정보의 정정·삭제를 청구하고자 하는 경우에는 '정정·삭제' 란에 ☑ 표시를 하고 정정 또는 삭제하고자 하는 개인정보의 항목과 그 사유를 기재합니다.
4. 개인정보의 처리정지를 청구하고자 하는 경우에는 '처리정지' 란에 ☑ 표시를 하고 처리정지 청구의 대상·내용 및 그 사유를 기재합니다.

담당자의 청구인에 대한 확인 서명	

210mm×297mm(신문용지 54g/㎡)

이 청구서는 아래와 같이 처리됩니다. (뒤 쪽)



[별지8] 위임장

위 임 장

① 위임받는자	성 명		전 화 번 호	
	생년월일		정보주체와의 관계	
	주 소			
② 위임자	성 명		전 화 번 호	
	생년월일			
	주 소			

「개인정보 보호법」 제38조제1항에 따라 위와 같이 개인정보의 열람, 정정·삭제 또는 처리정지 청구를 위임합니다.

년 월 일

위임자 (서명 또는 인)

○○○○ 귀하

※ 유 의 사 항

정보주체로부터 위임을 받은 자(수임인)는 본 위임장과 정보주체의 인감증명서 또는 주민등록증·운전면허증·여권 등의 신분증명서 사본을 제출하여야 하며, 수임인의 주민등록증·운전면허증 또는 여권 등의 신분증명서를 제시하여야 합니다.

210mm×297mm(인쇄용지(특급) 34g/㎡)

[별지9] 개인정보침해사실 신고서

개인정보침해사실 신고서

① 신고인	성 명		
	생년월일		
	연락처	전화번호(핸드폰)	
		전자우편	
		주 소	
② 피신고기관	기 관 명		
	연락처	전화번호	
		주 소	
③ 신고내용			

「공공기관의 개인정보보호에 관한 법률」제18조의2 제1항에 따라 위와 같이 개인정보 침해사실을 신고합니다.

첨부 :

년 월 일

신고인 : (서명 또는 인)

[별지10] 개인정보 침해신고 처리대장

개인정보 침해신고 처리대장

접 수		신고개요	처리결과	비고
일시	신고인 인적사항			