개인정보보호 내부관리계획

2018. 3.

안산대학교
ANSAN UNIVERSITY

(행정지원처)

목 차

제5장 정기적인 자체감사

제6장 개인정보보호 교육

제7장 개인정보보호 침해대응 및 피해구제

제8장 개인정보보호 사무의 인수·인계

제9장 개인정보 처리업무 위탁 시 관리 · 감독사항

제10장 개인정보 관리에 관한 사항

부칙

첨부

별지서식

제1장 총칙

제1조(목적)

개인정보 내부관리계획(이하 '본 계획' 이라 한다)은 개인정보보호법(이하 "법" 이라 한다) 제29조와 같은 법 시행령(이하 "영" 이라 한다) 제30조에 따라 제정된 것으로 안산대학교(이하 '대학' 이라 한다)의 개인정보처리자가 개인정보를 처리함에 있어서 취급하는 개인정보를 체계적으로 관리하여 개인정보가 분실, 도난, 유출, 변조, 훼손, 오·남용 등이 되지 아니하도록 안전성을 확보하기 위함을 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 교·직원 및 외부업체직원에 대해 적용된다.

제3조(용어 정의)

본 계획에서 사용하는 용어의 정의는 다음 각 호와 같다.

1. "개인정보" 라 함은 생존하는 개인에 관한 정보로서 성명/주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호/문자/음성/음향 및 영상 등의 정보(해당 정보만으로 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)를 말한다.
2. "개인정보보호책임자" 라 함은 대학의 개인정보보호 업무 및 조직을 총괄하여 지휘하는 자를 말한다.
3. "개인정보보호담당자" 라 함은 개인정보보호책임자를 보좌하여 개인정보보호업무에 대한 실무를 총괄하고 관리하는 자를 말한다.
4. "개인정보취급자" 라 함은 사업장 내에서 고객의 개인정보를 수집, 보관, 처리,

이용, 제공, 관리 또는 파기 등의 업무를 하는 자를 말한다.

5. “개인정보처리시스템”이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다.

6. “개인정보보호 분야별 책임자”라 함은 개인정보를 취급하는 업무부서의 장을 말한다.(2017.4.12.)

제2장 내부관리계획의 수립 및 시행

제4조(내부관리계획의 수립 및 승인)

① 개인정보보호담당자는 대학의 개인정보보호를 위한 전반적인 사항을 포함하여 내부관리 계획을 수립하여야 한다.

② 개인정보보호담당자는 개인정보보호를 위한 내부관리계획의 수립 시 개인정보보호와 관련한 법령 및 관련 규정을 준수하도록 내부관리계획을 수립하여야 한다.

③ 개인정보보호책임자는 개인정보보호담당자가 수립한 내부관리계획의 타당성을 검토하여 개인정보보호를 위한 내부관리계획을 승인하여야 한다.

④ 개인정보보호담당자는 개인정보보호 관련 법령의 제·개정 사항 등을 반영하기 위하여 매년 1월말까지 내부관리계획의 타당성과 개정 필요성을 검토하여야 한다.

⑤ 개인정보보호담당자는 모든 항목의 타당성을 검토한 후 개정할 필요가 있다고 판단되는 경우 2월말까지 내부관리계획의 개정안을 작성하여 개인정보보호책임자에게 보고하고 승인을 받아야 한다.

제5조(내부관리계획의 공표)

① 개인정보보호책임자는 4조에 따라 승인한 내부관리계획을 매년 3월말까지 제2조 대학의 교·직원에게 공표한다.

② 내부관리계획은 교·직원이 언제든지 열람할 수 있는 방법으로 비치하여야 하며, 변경사항이 있는 경우에는 이를 공지하여야 한다.

제3장 개인정보보호책임자의 의무와 책임

제6조(개인정보보호책임자의 지정)

대학은 대학의 행정업무를 총괄하는 행정지원처장을 개인정보보호 책임자로 임명한다.

제7조(개인정보보호책임자의 의무와 책임)

① 개인정보보호책임자는 대학의 개인정보보호를 위하여 다음 각 호의 임무를 수행한다.

1. 개인정보취급자의 의무와 책임의 규정 및 총괄관리
2. 개인정보보호 계획 및 지침의 수립 · 시행
3. 개인정보의 기술적·관리적 보호조치 기준 이행 총괄
4. 개인정보 침해행위에 대한 점검, 대응, 사후조치 총괄
5. 민원인의 개인정보에 관한 고충이나 의견의 처리 및 감독 총괄
6. 교직원 및 개인정보취급업무 수탁자 등에 대한 교육 총괄
7. 개인정보보호와 관련된 제반 조치의 시행 총괄
8. 기타 개인정보보호에 필요한 사항.

② 개인정보보호 책임자는 개인정보 취급자를 최소한으로 제한하여 지정하고 수시로 관리 · 감독하여야 하며, 교 · 직원에 한 교육 및 보안서약 등을 통해 개인정보 침해사고를 사전에 예방한다.

③ 개인정보보호 책임자는 개인정보 관련 업무의 효율적 운영을 위하여 개인정보 관리 전담부서의 직원 중 1인 이상을 개인정보보호 담당자로 임명한다.

제8조(개인정보보호 분야별 책임자의 의무와 책임)(2017.4.11.) 신설

① 개인정보보호 책임자는 필요에 따라 각 업무부서의 장을 개인정보보호 분야별 책임자로 지정하여 업무를 담당하게 할 수 있다.

② 개인정보보호 분야별 책임자는 민원인의 개인정보를 위하여 다음 각 호의 임무를 수행한다.

1. 개인정보 취급자 지정 · 관리 · 감독 · 교육
2. 개인정보파일 지정 · 관리 · 보호 · 파기
3. 개인정보 파일 이용 · 제공에 대한 승인
4. 공개 대상 개인정보파일 등록 · 공개
5. 공개 대상 개인정보파일의 처리방침 수립 · 시행 및 공개
6. 영상정보처리기기 운영관리 방침 수립 · 시행
7. 개인정보보호 관련 자료 관리 및 제출
8. 개인정보 처리와 관련한 요구 처리 및 피해 구제
9. 개인정보 유출 통지 및 피해확산 방지
10. 개인정보 관련 개선 권고 및 시정 조치사항 이행 등
11. 개인정보보호 분야별 책임자는 개인정보보호 분야별 담당자를 지정하여 개인정보 보호업무를 담당하게 할 수 있다.

제9조(개인정보보호 담당자의 의무와 책임)

① 개인정보보호 담당자는 개인정보보호 책임자를 보좌하여 개인정보보호 업무에 대한 실무를 총괄하고 관리한다.

② 개인정보보호 담당자는 개인정보보호를 위하여 다음 각 호의 임무를 수행한다.

1. 개인정보보호 계획 수립 및 운영
2. 개인정보 관리 실태 점검
3. 개인정보 교육 계획 및 실시
4. 개인정보 파일 대장 유지 및 관리

5. 개인정보보호 방침 수립 및 유지 관리

6. 홈페이지상 개인정보 노출 현황 점검 및 공지

③ 개인정보보호 담당자는 개인정보보호 책임자의 부재 시 이를 대신하여 업무를 수행한다.

제10조(개인정보취급자의 범위 및 의무와 책임)

① 개인정보취급자의 범위는 대학 내에서 개인정보 수집, 보관, 처리, 이용 제공, 관리 또는 파기 등의 업무를 수행하는 자를 말하고, 정규직 이외의 임시직, 계약직 직원 조교도 포함될 수 있다.

② 개인정보취급자는 개인정보보호와 관련하여 다음과 같은 역할 및 책임을 이행한다.

1. 개인정보보호 활동 참여
2. 내부관리계획의 준수 및 이행
3. 교·직원 또는 제3자에 의한 위법·부당한 개인정보 침해행위에 대한 점검 등
4. 개인정보 처리단계별 일반사항 준수
5. 기타 개인정보보호를 위해 필요한 사항의 이행

③ 개인정보취급자는 법률에 근거하여 개인정보를 수집, 보관, 처리, 이용, 제공, 관리 또는 파기하여야 한다.

④ 개인정보취급자는 개인정보 수집 목적 이외의 제공 필요시 문서(전자문서포함)를 통하여 요청하여야 하며, 개인정보보호책임자의 결재를 득 한 후에 이용·제공해야 한다.

⑤ 개인정보취급자는 개인정보보호와 관련된 역할 책임사항 이행을 위해 개인정보보호서약서(별지1)를 제출 하여야 한다.

제4장 개인정보의 기술적·관리적 보호조치

제11조(개인정보의 안전한 처리를 위해 처리단계별 기술적 보호조치)

개인정보보호책임자는 아래와 같이 시스템에 대한 영역별 보안솔루션 도입 등의 조치를 취하여야 한다.

구 분	개인정보 유출 방지 솔루션.
악성코드예방 및 대응(PC단계)	웜·바이러스 대책, 스파이웨어 차단 등
사용자 인증(PC 단계)	인증서(GPKI, EPKI, NPKI 등) 도입 등
네트워크 접근통제	방화벽, 침입차단시스템 도입 등
서버, DB 접근통제	서버보안솔루션, DB접근제어 도입, 중요 정보 암호화 솔루션 도입 등
웹 App, 어플리케이션	웹 방화벽 도입, 보안서버 도입, 키보드 해킹방지 솔루션 도입, 게시판 필터링 솔루션 도입

제12조(물리적 접근제한)

① 개인정보보호책임자는 개인정보와 개인정보처리시스템의 안전한 보관을 위한 물리적 잠금장치 등의 물리적 접근방지를 위한 보호조치를 취하여야 한다.

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

③ 개인정보보호책임자는 물리적 접근제한 관리대장의 출입 및 열람 내용을 주기적으로 검토하여 정당하지 않은 권한으로 출입하거나 열람하는 경우가 있는지를 점검하여 확인하여야 한다.

제13조(출력 복사 시 보호조치)

① 개인정보보호책임자는 개인정보가 포함된 정보를 출력하거나 복사할 경우에 개인정

보 유출사고를 방지하기 위한 보호조치를 취하여야 한다.

② 개인정보보호책임자는 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 개인정보취급자는 개인정보의 이용을 위하여 출력 및 복사한 개인정보의 이용 목적이 완료된 경우 분쇄기로 분쇄하거나 소각하는 등의 안전한 방법으로 파기하여야 한다.

제14조(개인정보취급자 접근권한 관리 및 인증)

① 개인정보보호책임자는 개인정보처리시스템에 대한 접근 권한을 서비스 제공에 필요한 최소한의 인원에게만 부여한다.

② 개인정보보호책임자는 개인정보취급자의 담당업무에 따라 개인정보 취급권한을 부여하며, 개인정보취급자가 전보 또는 퇴직 등 인사이동으로 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소한다.

③ 개인정보보호책임자는 개인정보취급자가 정보통신망을 통하여 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 공인인증서 등 안전한 인증 수단을 적용하여야 한다.

④ 개인정보보호책임자는 제1항 내지 제3항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관한다.

제15조(개인정보의 암호화)

① 개인정보보호책임자는 주민등록번호 대해서는 안전한 암호 알고리즘으로 암호화하여 저장하여야 한다.

② 개인정보보호책임자는 비밀번호 및 바이오정보는 복호화 되지 아니하도록 일방향 암호화 하여 저장하는 방식을 고려할 수 있다.

③ 개인정보보호책임자는 정보통신망을 통해 고객의 개인정보 및 인증정보를 송수신 할

때에는 안전한 보안서버 구축 등의 조치를 통해 이를 암호화해야 한다. 보안서버는 다음 각 호 중 하나의 기능을 갖추어야 한다.

1. 웹서버에 SSL(Secure Socket Layer) 인증서를 설치하여 전송하는 정보를 암호화하여 송·수신하는 기능
2. 웹서버에 암호화 응용프로그램을 설치하여 전송하는 정보를 암호화하여 송·수신하는 기능

④ 개인정보취급자는 개인정보를 개인용 컴퓨터에 저장할 때 암호화해야 하며, 개인정보 이용이 끝나는 즉시 삭제하여야 한다. 개인정보 암호화 방법은 다음중 하나의 기능을 이용 할 수 있다.

1. 자료 유출방지나 문서암호화 전용시스템을 활용
2. Windows7 등의 OS 자체에서 지원하는 파일 암호화기능 사용
3. 개인정보의 저장형태가 어플리케이션 파일 형태일 경우 해당 어플리케이션에서 제공하는 암호설정기능 사용

제15조 의 2(암호화된 개인정보 보관)

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

(2018.03.01.개정).

제16조(접근통제)

① 개인정보보호책임자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해, 개인정보처리시스템에 대한 접속 권한을 IP 주소 등으로 제한하여 인가받지 않은 접근을 제한하는 기능을 설치 운영한다.

② 개인정보보호책임자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통해 열람권한이 없는 자에게 공개되지 않도록 개인정보처리시스템 및 개인정

보취급자의 컴퓨터에 조치를 취하여야 한다.

제17조(비밀번호)

① 개인정보보호책임자는 개인정보취급자의 패스워드는 암호화하여 안전하게 보관하고, 생일, 주민등록번호, 전화번호 등 추측하기 쉬운 숫자나 개인관련 정보를 패스워드로 이용하지 않도록 하여야 한다.

② 개인정보취급자는 정보보안담당관이 수립한 대학 정보보안 기본지침 제4장 4.2(별표1)를 준수하여야 한다.

제18조(접속 기록의 위변조 방지)

① 개인정보보호책임자는 접속 기록의 위변조 방지를 위해 개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리(입/출력, 수정, 등 DB접근)하는 경우에는 처리일시, 처리내역 등 접속기록을 저장한다.

② 개인정보보호책임자는 제1항의 접속기록에 대해 분기 1회 이상 정기적으로 확인·감독한다.

③ 개인정보보호책임자는 제1항의 접속기록에 대해 위·변조 방지를 위해 별도의 저장매체에 백업 보관하며, 보관기간은 최소 6개월 이상으로 한다.

제19조(보안프로그램의 설치 및 운영)

① 개인정보보호책임자는 개인용 컴퓨터(PC) 등을 이용하여 개인정보를 취급하는 경우 개인정보가 분실, 도난, 누출, 변조 또는 훼손되지 아니하도록 안전성 확보를 위한 PC개인정보보호 전용 솔루션, 백신 프로그램 등의 보안 프로그램을 설치·운영하여야 한다.

② 보안 프로그램은 항상 최신의 버전으로 업데이트를 적용하여야 한다.

③ 보안 프로그램의 최신 업데이트를 적용하기 위하여 자동 업데이트 설정 및 실시

간 감시 기능을 적용하여야 한다.

제20조(오프라인으로 처리정보 이용·제공시 안정성 확보)

① 개인정보를 오프라인으로 제공시 보안USB 등 보안성이 높은 저장매체를 활용하고, 처리정보를 보호할 수 있도록 반드시 암호화하여 제공하여야 한다.

② 처리정보를 안전하게 이동한 후 그 저장매체의 처리정보가 복구될 수 없도록 파기 조치하여야 한다.

제21조(개인정보 비밀유지)

① 개인정보보호책임자는 개인정보취급자 등 업무 목적으로 업무상 개인정보를 취급하는 모든 개인정보 취급자를 대상으로 다음의 사항을 포함하여 개인정보보호 서약서(별지1)를 징구한다.

1. 업무 중 알게 된 개인정보에 대한 비밀 준수
2. 개인정보보호를 위한 회사의 관리 규정의 준수
3. 적당한 절차 없이 개인정보를 무단으로 조회, 누출하는 것의 금지
4. 개인정보보호와 관련된 법률 및 대학의 개인정보보호 관리 규정의 숙지
5. 위반 시 형사·민사상의 책임

② 개인정보보호책임자는 대학의 개인정보 취급자 이외에도 개인정보의 취급 위탁 또는 제3자 제공 등의 경우에도 제1항의 개인정보에 관한 비밀유지 조항을 포함하여, 제3자 제공 금지, 사고시 손해배상 등 개인정보보호를 위하여 필요한 사항을 포함한 개인정보 위탁 제공 계약서(별지2)를 작성하여야 한다.

제22조(개인정보 표시제한 보호조치)

개인정보 업무처리를 목적으로 개인정보의 조회, 출력 등의 업무를 수행하는 과정에서 개인정보보호를 위하여 개인정보를 마스킹 하여 표시제한 조치를 취하는 경우에는 다음의

원칙으로 적용할 수 있다.

1. 성명 중 이름의 첫 번째 글자 이상
2. 주민번호의 경우 뒷자리 전체
3. 전화번호 또는 휴대폰 전화번호의 국번
4. 주소의 읍·면·동

제23조(개인정보파일의 파기)(2017. 4. 11.) 신설

① 대학은 개인정보파일의 보유기간 경과, 처리목적 달성 등 개인정보파일이 불필요하게 되었을 때에는 지체 없이 그 개인정보파일을 파기하여야 하나 업무의 처리의 효율성을 고려하여 분기마다 파기하도록 한다.

다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니한다.

② 개인정보취급자는 보유기간 경과, 처리목적 달성 등 파기 사유가 발생한 개인정보파일을 선정하고 “개인정보파일 파기요청서”에 파기 대상 개인정보파일의 명칭, 파기방법 등을 기재하여 개인정보보호 책임자의 승인을 받아 개인정보를 파기하여야 한다.

③ 개인정보보호 책임자는 개인정보 파기 시행 후 파기 결과를 확인하고 개인정보파일 파기 대장을 작성하고 홈페이지에 공지하여야 한다.

제24조(개인정보파일 등록 사실의 삭제) (2017. 4. 11.) 신설

① 개인정보취급자는 제 23조에 따라 개인정보파일을 파기한 경우, 개인정보파일 등록사실에 대한 삭제를 개인정보보호 책임자에게 요청해야 한다.

② 개인정보파일 등록의 삭제를 요청받은 개인정보보호책임자는 그 사실을 확인하고, 지체 없어 등록 사실을 삭제한 후 그 사실을 행정자치부(http://intra.privacy.go.kr/)에 통보한다.

제25조(재해 · 재난 대비 안전조치) (2017. 4. 11.) 신설

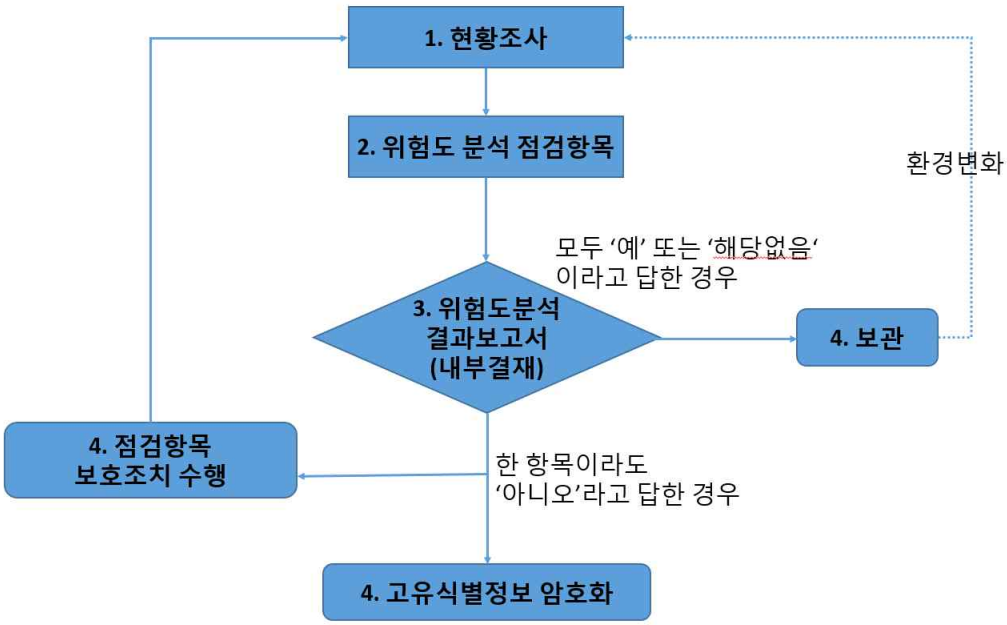
① 개인정보보호책임자는 화재, 홍수, 단전 등의 재난 · 재해 발생 시 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검하여야 한다.

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

제26조(위험도 분석 및 대응) (2017. 4. 11.) 신설

① 개인정보보호책임자는 개인정보처리시스템에 적용하고 있는 개인정보보호를 위한 수단과 유출 시 정보주체의 권리를 침해할 위협의 정도를 위험도 분석 절차를 통해 분석하여야 한다.

② 개인정보보호책임자는 최초 위험도 분석 이후에도 개인정보처리시스템을 증설하거나, 내 · 외부망과 연계하거나, 기타 운영환경이 변경된 경우에도 지속적으로 실시하여야 한다.



제5장 정기적인 자체감사

제27조(자체감사 주기 및 절차)

① 개인정보보호책임자는 개인정보보호를 위한 내부관리 계획 및 관련 법령에서 정하는 개인정보보호 규정을 성실히 이행하는지를 주기적으로 감사 또는 점검하여야 한다.

② 개인정보보호책임자는 개인정보 자체감사를 위한 감사대상, 감사절차 및 방법 등 감사의 실시에 관하여 필요한 별도의 계획을 수립할 수 있다.

③ 개인정보보호 자체감사는 년 1회 이상 실시한다.

제28조(자체검사 결과 반영)

① 개인정보보호책임자는 개인정보 보호를 위한 자체감사 실시 결과, 개인정보의 관리·운영상의 문제점을 발견하거나 관련 직원이 본 계획의 내용을 위반할 때에는 시정·개선 또는 인사발령 등 필요한 조치를 취하여야 한다.

② 개인정보보호책임자는 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

제29조(개인정보보호 교육 계획의 수립)

① 개인정보보호책임자는 다음 각 호의 사항을 포함하는 연간 개인정보보호 교육계획을 매년 2월말까지 수립한다.

1. 교육목적 및 대상
2. 교육내용

3. 교육 일정 및 방법

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

제30조(개인정보보호 교육의 실시)

① 개인정보보호책임자는 고객정보보호에 대한 교·직원들의 인식제고를 위해 노력해야 하며, 개인정보의 오·남용 또는 유출 등을 적극 예방하기 위해 교·직원을 대상으로 매년 정기적으로 연1회 이상의 개인정보보호 교육을 실시한다.

② 연1회의 정기교육을 실시한다.

③ 교육 방법은 집체 교육뿐만 아니라, 인터넷 교육, 그룹웨어 교육 등 다양한 방법을 활용하여 실시하고, 필요한 경우 외부 전문기관이나 전문요원에 위탁하여 교육을 실시할 수 있다.

④ 개인정보보호에 대한 중요한 전파 사례가 있거나 개인정보보호 업무와 관련하여 변경된 사항이 있는 경우, 개인정보보호책임자는 부서 회의 등을 통해 수시 교육을 실시할 수 있다.

제31조(개인정보보호 인력에 대한 교육 의무화)

① 개인정보보호책임자는 개인정보보호 정책 수립 및 관리에 필요한 워크샵 및 컨퍼런스 등 1회 이상 개인정보보호 교육에 참석하여야 한다.

② 개인정보보호실무자는 20시간 이상의 개인정보 보호에 관한 전문 교육과정을 이수하여야 한다.

제7장 개인정보 침해대응 및 피해구제

제32조(개인정보의 유출)

개인정보의 유출이라 함은 법령이나 개인정보취급자의 자유로운 의사에 의하지 않고, 정보주체의 개인정보에 대하여 개인정보취급자가 통제를 상실하거나 또는 권한 없는 자의 접근을 허용한 것으로서, 다음 각 호의 어느 하나에 해당하는 경우를 말한다.

1. 개인정보가 포함된 서면, 이동식 저장장치, 휴대용 컴퓨터 등을 분실하거나 도난당한 경우
2. 개인정보가 저장된 데이터베이스 등 개인정보처리시스템에 정상적인 권한이 없는 자가 접근한 경우
3. 개인정보처리자의 고의 또는 과실로 인해 개인정보가 포함된 파일 또는 종이문서, 기타 저장매체가 권한이 없는 자에게 잘못 전달된 경우
4. 기타 권한이 없는 자에게 개인정보가 전달되거나 개인정보처리시스템 등에 접근 가능하게 된 경우

제33조(통지시기 및 항목)

① 개인정보처리자는 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

② 개인정보처리자는 제1항 제2호의 경우 개인정보 유출 사고가 최초 발생한 시점과 알게 된 시점 사이에 시간적 차이가 있는 경우에는 이에 대한 과실유무를 입증하여야 한다.

③ 개인정보처리자는 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. 제33조 제1항의 통지항목 중 확인된 사항

제34조(통지방법)

① 개인정보처리자는 정보주체에게 제33조 제1항 각호의 사항을 통지할 때에는 서면, 전자우편, 모사전송, 전화, 휴대전화 문자전송 또는 이와 유사한 방법을 통하여 지체 없이 정보주체에게 알려야 한다.

② 개인정보처리자는 제1항의 통지방법과 동시에, 홈페이지 등을 통하여 제33조 제1항 각호의 사항을 공개할 수 있다.

제35조(개인정보 유출신고)

① 개인정보처리자는 1천명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 정보주체에 대한 통지 및 조치결과를 5일 이내에 행정안전부장관 또는 시행령 제39조제2항 각호의 전문기관 중 어느 하나에 신고하여야 한다.(2018.03.01.개정)

② 제1항에 따른 신고는 개인정보 유출신고서(별지3)를 통하여 하여야 한다.

③ 개인정보처리자는 전자우편, 팩스 또는 인터넷 사이트를 통하여 유출신고를 할 시간적 여유가 없거나 그밖에 특별한 사정이 있는 때에는 먼저 전화를 통하여 제33조 제1항의 사항을 신고한 후, 별지 제3호 서식에 따른 개인정보 유출신고서를 제출할 수 있다.

④ 개인정보처리자는 1만명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 제33조 제1항에 따른 통지와 함께 인터넷 홈페이지에 정보주체가 알아보기 쉽도록 제33조 제1항 각호의 사항을 7일 이상 게재하여야 한다.

제8장 개인정보보호 사무의 인수·인계

제36조(개인정보보호 사무의 인수·인계)

① 개인정보보호책임자와 개인정보담당자의 변경 시 다음 각 호를 인수·인계 하여야

한다.

1. 개인정보보호에 관한 규정 및 지침
2. 개인정보보호 조직에 관한사항
3. 개인정보처리시스템의 사용자 권한 설정 및 보호에 관한 사항
4. 대학의 개인정보 보유목록
5. 개인정보 유출사례를 포함한 교육교재
6. 기타 개인정보보호 업무 수행에 필요한 사항

② 개인정보취급자의 변경 시 다음 각 호를 인수•인계 하여야 한다.

1. 취급하는 개인정보 보유목록
2. 통상적으로 이용•제공하는 개인정보에 관한 사항
3. 기타 개인정보보호 업무 수행에 필요한 사항

제9장 개인정보 처리업무 위탁 시 관리 · 감독사항 (2017.4. 1.) 신설

제37조(수탁자의 선정 시 고려사항)

① 개인정보 처리 업무를 위탁하는 대학은 개인정보 처리 업무를 위탁받아 처리하는 자(이하 '수탁자' 라 한다)를 선정할 때에는 인력과 물적 시설, 재정 부담능력, 기술보유의 정도, 책임능력 등을 고려하여야 한다.

② 대학은 개인정보의 처리 업무를 위탁하는 때에는 수탁자의 처리 업무의 지연, 처리업무와 관련 없는 불필요한 개인정보의 요구, 처리기준의 불공정 등의 문제점을 검토하여 이를 방지하기 위한 필요한 조치를 마련하여야 한다.

제38조(개인정보 보호 등 조치의무)

① 수탁자는 위탁받은 대인정보를 통해서 안전하게 보호하기 위하여 기술적 · 관리적 · 물리적 조치를 하여야 하며 대학은 조치 여부를 확인하여야 한다.

② 대학은 수탁자가 개인정보를 안전하게 처리하는지에 대해 정기적으로 관리 · 감독

을 실시해야 된다. 위탁업무별 또는 위탁자별로 관리·감독해야 될 일반적인 점검항목은 다음과 같다.

1. 개인정보보호 책임자의 지정여부
2. 내부관리계획의 수립여부
3. 개인정보처리방침의 수립 및 공개 여부
4. 개인정보취급자의 개인정보보호 서약서 작성 여부
5. 개인정보취급자에 대한 개인정보보호 관련 교육 실시 여부
6. 개인정보의 암호화 보관 여부
7. 접근통제 솔루션의 도입 및 적용여부(침입차단시스템, 비인가 사이트 차단 등)
8. 개인정보처리시스템에 대한 보안프로그램 설치 및 정기적 업데이트 수행 여부
9. 물리적 접근방지(전산실, 문서고 등 출입통제 및 물리적 보안 조치)여부
10. 개인정보처리시스템에 대한 접근기록 보관 및 점검 여부
11. 개인정보처리시스템에 대한 접근권한 차등 부여 여부
12. 개인정보 수집 목적 달성 시 파기 여부(전자파일 및 종이문서)
13. 재 위탁(제3자 제공 포함) 금지 준수 여부
14. 위탁 업무에 대한 처리 목적 외 사용 여부
15. 개인정보 취급 업무용 PC의 안전성 확인 여부(패치, 백신 업데이트 등)
16. 위탁업무처리를 위해 제공된 개인정보의 유·노출 사실 여부
17. 침해사고 대응절차 수립 및 전파 여부
18. 기타 법령 또는 계약사항 위반 여부
19. 개인정보처리현황 및 실태 파악

③ 대학은 년 1회 이상 위탁자에게 ②항의 점검항목을 통보받아야 한다.

제39조(수탁기관 개인정보취급자 교육)

① 대학은 수탁기관 개인정보취급자에 대하여 개인정보가 분실, 도난, 유출, 변조 또는 훼손되지 않도록 다음 내용을 포함하여 정기적으로 교육을 실시해야 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 관련해 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항
7. 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등에 관한 사항

② 대학은 직접 수탁자를 불러 기관 내 개인정보보호 교육에 참석토록 해도 되고, 수탁자가 직접 온라인이나 오프라인 교육에 개인정보취급자가 참석토록 해 개인정보 취급에 따른 이해도 향상 및 개인정보의 중요성과 유출 시 위험성 등 법령사항들에 대해 숙지토록 해야 한다.

제40조(정보주체와 재위탁의 관계)

정보주체는 수탁자로부터 개인정보처리 업무를 재위탁 받아 처리하는 자(재수탁자)가 재위탁받은 개인정보 처리 업무를 수행하면서 발생하는 손해에 대한 배상을 청구할 수 있다.

제41조(위탁 완료 후 개인정보 파기 통보)

개인정보 처리 업무위탁이 종료된 경우 대학은 수탁자에게 해당 개인정보를 파기하고 그 결과를 통보받아야 하며, 대학은 파기결과를 확인하여야 한다.

제10장 개인정보의 관리에 관한 사항 (2017.4.11.) 신설

제42조(개인정보의 수집 · 이용)

① 개인정보취급자는 다음 각 호에 의한 경우에만 개인정보를 수집할 수 있으며, 그 수집 목적의 범위 내에서 이용할 수 있다.

1. 정보주체로부터 동의를 받은 경우
2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
3. 공공기관이 법령 등에서 정하는 소관업무의 수행을 위하여 불가피 한 경우 등
4. 기타(법 제15조제1항 제4호부터 제6호까지 해당)

② 개인정보취급자는 정보주체의 개인정보를 수집하는 경우, 적법하고 정당한 수단

에 의하여 업무에 필요한 성명, 연락처, 주소 등 최소한의 정보를 수집하여야 한다.
③ 개인정보취급자는 부서에서 개인정보를 수집하는 신청서식 등 수집에 대한 근거가 없는 경우 학칙, 규정, 지침 등에 근거를 반영하도록 개정하여야 한다.
④ 개인정보취급자는 부서에서 사용하는 민원서식 및 자체서식 등을 파악 후 불필요하게 사용하고 있는 주민등록번호 등 고유식별정보를 생년월일로 대체하여 법령 요구사항에 반영하도록 개선하여야 한다.
⑤ 개인정보취급자는 정보주체로부터 동의를 받는 경우에 개인정보의 수집·이용 목적, 수집하는 개인정보 항목, 보유 및 이용 기간, 동의를 거부할 권리가 있다는 사실, 동의거부에 따른 불이익 내용 등을 알려야 한다.
⑥ 다음호에 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다.
1. 법령에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우
2. 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우
3. 제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 행정자치부령으로 정하는 경우

제43조(개인정보의 이용·제공 제한)

① 개인정보취급자는 개인정보를 목적 외의 용도로 이용하거나 제3자에게 제공하면 아니 된다. 다만, 정보주체의 별도의 동의가 있거나 다른 법률에 특별한 규정이 있는 경우 등은 예외로 한다.
② 개인정보취급자는 제3자(외부기관 포함)에게 개인정보를 제공할 경우 개인정보보호법과 법령(법률, 시행령, 시행규칙) 등에 제공근거가 있는 지를 검토한 후 제공여부를 판단하여야 하며, 법률적 제공근거가 없는 경우 제공을 금지하거나, 정보주체의 동의를 받아 제공하여야 한다.
③ 개인정보를 목적 외의 용도로 이용하거나 제3자에게 제공하는 경우에는 개인정보의 목적 외 이용 및 제3자 제공대장에 기록·관리하여야 하며, 1개월 이내에 이용 또는 제공의 법적 근거, 목적 및 범위 등에 관한 사항을 홈페이지 등에 게재하여야 하고, 홈페이지에 게재할 때에는 10일 이상 게재하여야 한다.
④ 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우에는 개인정보를 제공하는

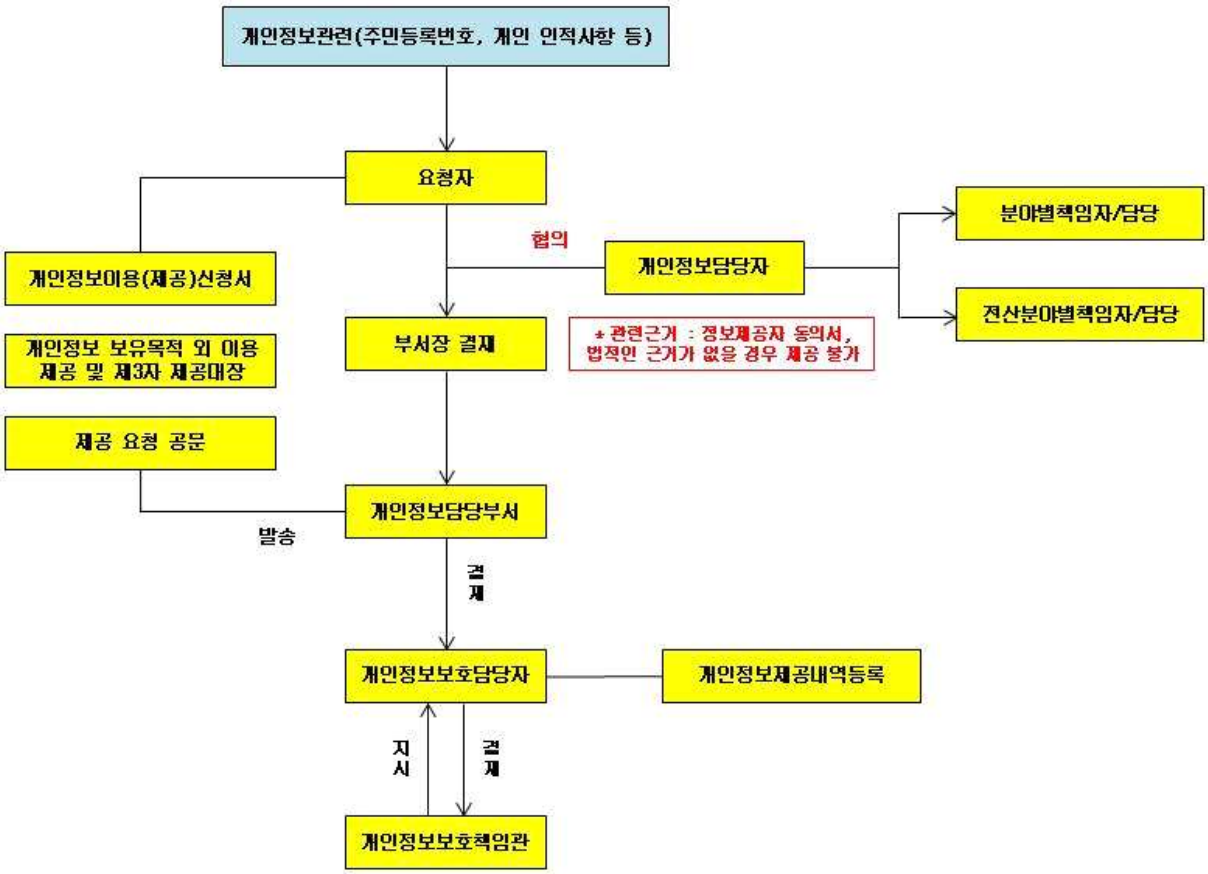
자와 개인정보를 제공받는 자는 개인정보의 안전성에 관한 책임관계를 명확히 하여야 한다.

⑤ 개인정보처리자가 정보주체에게 개인정보를 제공받는 자를 알리는 경우에는 그 성명(법인 또는 단체인 경우에는 그 명칭)과 연락처를 함께 알려야 한다.

⑥ 개인정보처리자가 개인정보를 제3자에게 제공하는 경우에는 다른 정보와 결합하여서도 특정 개인을 알아볼 수 없는 형태로 제공하여야 한다.

제44조(개인정보 목적 외 이용 및 제 3자 제공절차)

① 개인정보를 목적 외 이용 또는 제 3자에게 제공하고자 할 경우는 그룹웨어의 “개인정보 이용(제공) 신청서”를 통하여 다음 절차에 따라 이용·제공하여야 한다.



② 개인정보를 제 3자에게 제공시는 다음 절차를 준수하여야 한다.

1. 첨부 파일에 주민등록번호등 개인정보가 포함시 암호화하여 첨부 또는 전송
2. 제공 요청처에 별도의 문서나 전화로 문서 암호 송부(해당 문건에 암호 기입 금지)
3. 하단에 다음과 같은 문건 필히 입력하여 전송

> • 대학의 자료는 개인의 사생활과 밀접한 관련이 있는 개인정보이므로 개인정보 보호법령 등에 맞게 이용 및 관리하시기 바랍니다.(2017.4.11 개정)
>
> 1. 제공하는 자료의 보유기간은 ____년(개월)____입니다. 만약 법령이나 해당기관에서 별도로 보유기간이 정해진 경우 있는 경우는 해당 기간을 준수하시기 바랍니다.
> 2. 본교로부터 제공받은 자료를 요구 목적 외 사용 하거나 타 기관이나 부서에 제공하는 등의 행위를 하여서는 아니 됩니다.
> 3. 제공받은 정보를 담당하는 자에게 개인정보에 관한 교육 및 관리.감독을 실시하여야 합니다.
> 4. 제공하는 개인정보의 목적 달성시 또는 보유기간 경과시 제공받은 일체의 자료를 안전한 방법으로 파기하시기 바랍니다.
> 5. 관계 법률 등에 따라 대학이 제공한 내용은 신고사항 등에 기초한 자료이므로 향후 변동될 수 있습니다.(2017.4.11 신설)

③ 개인정보 제3자 제공시 홈페이지에 제공내역을 등록 하여야 하나, 민감정보, 의료정보, 수사자료 요청 등 개인 사생활 침해가 의심되는 경우나 학력조회등과 같이 개별적인 요청사항은 개인정보담당자의 판단으로 등록을 생략 할 수 있다.

제45조(고유식별정보 및 민감정보 처리의 제한)

① 분야별 책임자 또는 개인정보취급자는 정보주체의 별도 동의 또는 법령에서 구체적으로 고유식별정보의 처리를 요구하거나 허용하는 경우를 제외하고는 고유식별정보를 처리해서는 아니 된다.

② 분야별 책임자 또는 개인정보취급자는 사상, 신념, 노동조합, 건강, 정당의 가입, 정치적 견해 등에 관한 정보, 그밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 민감 정보를 처리해서는 아니 되며, 다음 각 호의 어느 하나에 해당하는 경우 그러하지 아니한다.

1. 다른 개인정보의 처리에 대한 동의와 별도의 동의를 받은 경우
2. 법령에서 민감정보의 처리를 요구하거나 허용하는 경우

(유전자검사 등의 결과로 얻어진 유전정보,「형의 실효 등에 관한 법률」제2조 제5호에 따른 범죄경력 자료에 해당하는 정보는 시행령 제18조에 의하여 제외)

③ 고유식별정보 및 민감정보 처리에 대한 동의를 받고자 할 경우에는 수집·이용 목적, 정보의 항목, 보유 및 이용 기간, 거부권리 및 불이익의 내용 등 정보주체에게 알리고 동의를 받아야 한다.

④ 홈페이지를 관리하는 분야별 책임자는 정보주체자가 회원으로 가입할 경우 주민등록번호를 사용하지 아니하고 회원으로 가입할 수 있는 방법으로 제공하여야 한다.

제46조(개인정보 열람, 정정 및 삭제, 처리정지)

① 분야별 책임자 또는 개인정보취급자는 정보주체가 자신의 개인정보 열람을 요구한 경우 시행령으로 정하는 기간 내에 열람할 수 있도록 하여야 한다. 다만, 열람제한 또는 거부 사유 발생 시 정보주체에게 통보하여야 한다.

② 개인정보를 열람한 정보주체가 개인정보취급자에게 그 개인정보의 정정 또는 삭제를 요구 하였을 때에는 다른 법령에 규정되어 있는 경우를 제외하고는 지체 없이 정정·삭제 등 필요한 조치를 한 후 그 결과를 정보주체에게 알려야 한다.

③ 분야별 책임자 또는 개인정보취급자는 정보주체로부터 개인정보 처리중지 요구를 받았을 때에는 지체 없이 개인정보 처리의 전부 또는 일부를 정지하여야 한다. 다만, 처리정지 거부에 대한 사유 발생 시 정보주체에게 통보하여야 한다.

제47조(제3자에 대한 개인정보 제공 중단 절차)

개인정보처리자는 개인정보를 이용 하거나 제공받는 기관이 개인정보의 이용 및 제공의 제한을 이행하지 아니하는 때에는 다음의 각호의 절차에 따라 개인정보의 이용을 중지시키거나 제공을 중지하여야 한다.

1. 개인정보처리자는 개인정보보호책임자 및 개인정보취급자에 관련 사실을 알린다.
2. 개인정보처리자는 '개인정보의 이용 및 제공의 제한' 의무 미 이행 사항을 인지한 날 부터 해당 기관에 개인정보 제공을 임시로 중지한다.
3. 개인정보를 제공받는 기관에게 '개인정보의 이용 및 제공의 제한' 의무 미 이행 사항에 대해 문서를 통한 소명을 요청한다.
4. 개인정보를 제공받는 기관에게 '개인정보의 이용 및 제공의 제한' 의무 미 이행 사항에 대해 문서를 통한 소명을 받는다.

5. 해당 기관으로 부터 소명 받은 자료를 접수한 후 개인정보보보 담당자는 '개인정보의 이용 및 제공의 제한' 의무를 위반한 제공받은 기관에 대한 조치방안을 수립하여 개인정보보호책임자의 승인을 득한다.

6. 개인정보보호책임자는 개인정보 제공 중지를 해당 기관에 통보한다. 동시에 해당 기관에 개인정보 제공을 중지한다.

부칙

1. 본 계획은 2012년 3월 8일부터 시행한다.
2. 본 계획은 2015년 4월 6일부터 시행한다.
3. 본 계획은 2017년 4월 11일부터 시행한다.
4. 본 계획은 2018년 3월 1일부터 시행한다.

[첨부 1] 비밀번호 규정

정보보안 기본지침 - 비밀번호 규정

4.2. 비밀번호 규정

4.2.1 보안 지침

⑴ 사용자는 안전한 패스워드를 설정하여 사용해야 합니다.

⑵ 초기 패스워드가 시스템에 의해 할당되는 경우, 사용자는 빠른 시간 내에 해당 패스워드를 새로운 패스워드로 변경해야 합니다.

⑶ 사용자는 패스워드를 주기적으로 변경해야 하며, 권장하는 패스워드 변경주기는 3개월입니다.

⑷ 패스워드 변경 시, 이전에 사용하지 않은 새로운 패스워드를 사용하고 변경된 패스워드는 이전 패스워드와 연관성이 없어야 합니다.

⑸ 자신의 패스워드가 제3자에게 노출되지 않도록 해야 합니다
패스워드를 메모지 등에 기록할 경우, 메모지는 항상 자신이 소유하고 있거나 안전한 장소에 보관함으로써 외부로 노출되지 않도록 해야 합니다.

⑹ 제3자에게 자신의 패스워드와 관련된 정보 및 힌트를 제공하지 않아야 합니다.

⑺ 자신의 패스워드가 제3자에게 노출되었을 경우, 즉시 새로운 패스워드로 변경해야 합니다.

4.2.2 안전한 패스워드

⑴ 문자열 구성

1) 세가지 종류 이상의 문자구성으로 8자리 이상의 길이로 구성된 문자열

2) 두가지 종류 이상의 문자구성으로 10자리 이상의 길이로 구성된 문자열

⑵ 3개월에 한번 정기적인 패스워드 변경

⑶ 기억하기 쉬운 패스워드 설정방법

1) 특정명칭을 선택하여 예측이 어렵도록 가공하여 패스워드 설정

① 특정명칭의 홀·짝수 번째의 문자를 구분하는 등의 가공방법을 통해 설정

② 국내 사용자는 한글 자판을 기준으로 특정명칭을 선택하고 가공하여 설정

예) '안산대학교전산정보원'의 경우, 홀수 번째 '안1학자산'이 'dks1gkrwktks'로, 짝수 번째 '산대전계소'를 'tkseowjsrPth'로 사용

2) 노래 제목이나 명언, 속담, 가훈 등을 이용·가공하여 패스워드 설정

예) 영문사용의 경우, 'This May Be One Way To Remember'를 'TmB1w2R'이나 'Tmb1w>r~'로 활용

한글사용의 경우, '백설공주와 일곱 난쟁이'를 '백설+7난장'로 구성하고 '빽썰+7난짱'등으로 활용

⑷ 예측이 어려운 문자구성의 패스워드 설정방법

1) 영문자(대·소문자), 숫자, 특수문자들을 혼합한 구성으로 패스워드 설정

예) '10H+20Min','I!Can&9it'등과 같은 구성

2) 패스워드 길이를 증가시키기 위해서는 알파벳 문자 앞뒤가 아닌 위치에 특수문자 및 숫자 등을 삽입하여 설정

예) 'Security1'이 아니라 'Securi2t&&y'와 같은 형태로 패스워드의 길이를 늘림

3) 알파벳 대·소문자를 구별할 수 있을 경우, 대·소문자를 혼합하여 설정

① 특정위치의 문자를 대문자로 변경하거나, 모음만을 대문자로 변경

예) 'gkswjdqhwlsdnjs'->'gKsWjDqHwLsDnJs', 'rnrqhghgmd'->'rNrQhGhGmD'

⑸ 사이트별 상이한 패스워드 설정 위한 방법

1) 자신의 기본 패스워드 문자열을 설정하고 사이트별로 특정 규칙을 적용하여 패스워드 설정

예) 패스워드 문자열을 '486*+'로 설정하고, 사이트 이름의 짝수 번째 문자 추가를 규칙으로 ansan.ac.kr는 '486*+nsn.a.k', ansan.kr는 '486*+aa.k'등으로 활용

4.2.3 안전하지 못한 패스워드

⑴ 7자리 이하 또는 두가지 종류 이하의 문자구성으로 8자리 이하 패스워드

⑵ 특정 패턴을 갖는 패스워드

1) 동일한 문자의 반복

2) 키보드 상에서 연속한 위치에 존재하는 문자들의 집합

3) 숫자가 제일 앞이나 제일 뒤에 오는 구성의 패스워드

⑶ 제3자가 쉽게 알 수 있는 개인정보를 바탕으로 구성된 패스워드

⑷ 사용자 ID를 이용한 패스워드

⑸ 한글, 영어 등을 포함한 사전적 단어로 구성된 패스워드

⑹ 특정 인물의 이름이나 널리 알려진 단어를 포함하는 패스워드

⑺ 숫자와 영문자를 비슷한 문자로 치환한 형태를 포함한 구성의 패스워드

⑻ 시스템에서 초기에 설정되어 있거나 예제로 제시되고 있는 패스워드

⑼ 한글의 발음을 영문으로, 영문단어의 발음을 한글로 변형한 형태의 패스워드

[첨부 2] 개인정보 암호화 방법

⑴ 자료 유출방지나 문서암호화 전용시스템을 활용

※ 국내에서 인증 받은 시스템에 대한 정보는 국가정보원 IT보안인증사무국 웹사이트(http://www.kecs.go.kr)에서 확인할 수 있다.

· 자료유출방지시스템 : 인증제품 - 자료유출방지(제품유형) 검색

· 문서암호화시스템 : 암호제품 - 문서 암호화(제품군) 검색

⑵ Windows XP 등의 OS 자체에서 지원하는 파일 암호화 기능 사용

※ http://support.microsoft.com/kb/307877/ko

파일을 암호화하는 방법(NTFS 만적용)

1. Windows 탐색기를 누릅니다.
2. 원하는 파일을 찾아서 마우스 오른쪽 단추로 누른 다음 속성을 누릅니다.
3. 일반 탭에서 고급을 누릅니다.
4. 압축 또는 암호화 특성에서 데이터 보호를 위해 내용을 암호화 확인란을 선택한 다음 확인.
5. 확인을 누릅니다. 파일이 암호화되지 않은 폴더에 있으면 암호화 경고 대화 상자가 나타납니다.
   다음 단계 중 하나를 사용합니다.
  5-1. 파일만 암호화하려면 파일만 암호화를 누른 다음 확인을 누릅니다.
  5-2. 파일과 파일이 들어 있는 폴더도 암호화하려면 파일 및 상위 폴더를 암호화를 누른 다음 확인

다른 사용자가 암호화된 파일을 열려고 하면 파일을 열 수 없습니다. 예를 들어 다른 사용자가 암호화된 Microsoft Word 문서를 열려고 하면 다음과 같은 내용의 오류 메시지가 나타납니다.

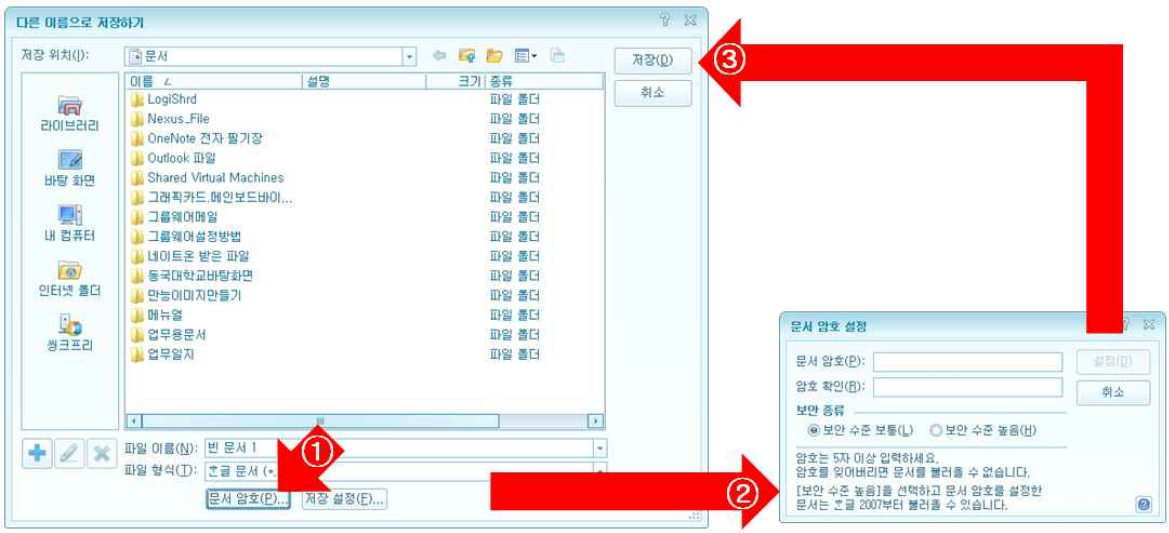
> 문서를 열 수 없습니다. username에게 액세스 권한이 없습니다

다른 사용자가 암호화된 문서를 하드 디스크 상의 다른 위치로 복사하거나 이동하려고 하면 다음과 같은 메시지가 나타납니다.

> 파일 또는 폴더 복사 오류
> filename을(를) 복사할 수 없습니다. 액세스가 거부되었습니다. 디스크가 꽉 찼거나 쓰기 금지되어 있는지, 해당 파일이 사용 중이 아닌지 확인하십시오.

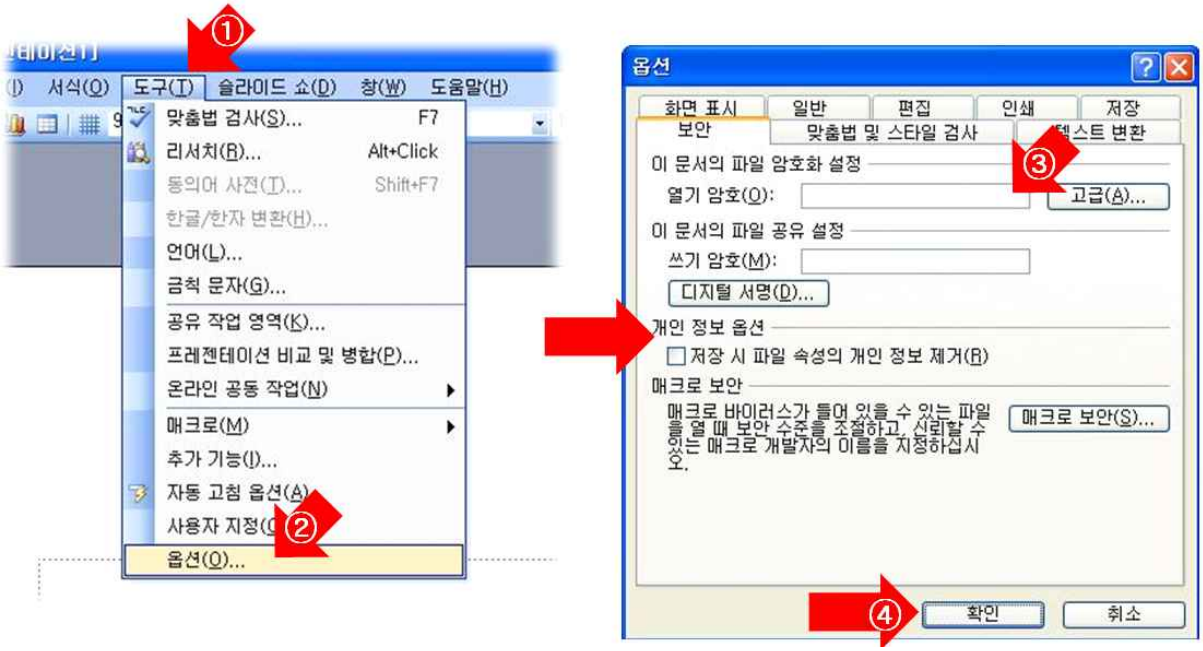
⑶ 개인정보의 저장형태가 어플리케이션 파일 형태일 경우 해당 어플리케이션에서 제공하는 방법을 통한 문서 암호화

(가) 한글 파일 암호화(**한글 2005,한글 2007,한글 2010 버전 공통**)

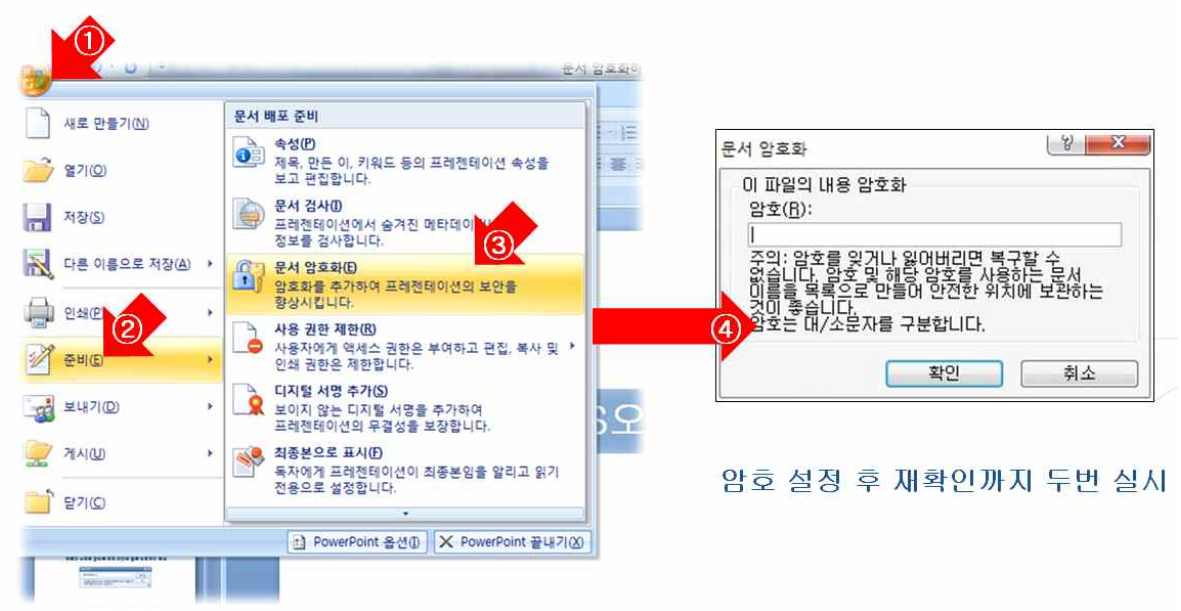


(나) MS-Office(PowerPoint, EXCEL)

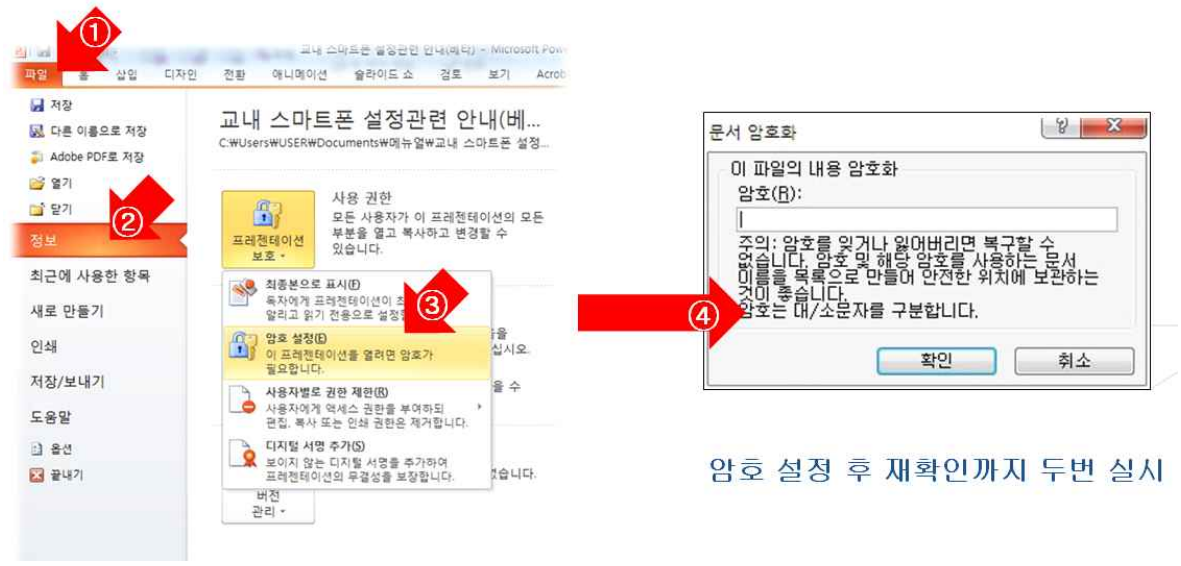
1) 2003버젼



2) 2007버전



3) 2010버전



[첨부 2] 개인정보 암호화 방법위험도 분석 점검항목

① (기관 기준) 점검 항목

※ 개인정보 파일이 포함되어 있는 개인정보처리시스템 환경에 관한 내용으로 기관 전체를 대상으로 합니다.

구 분	점 검 항 목	예	아니오	해당없음
정책기반	1. 개인정보 보호를 위한 책임자를 지정하여 운영하고 있습니까?			
	2. 개인정보 보호를 위한 정책 또는 관리계획(침해사고 대응계획 포함)을 수립·운영하고 있습니까?			
	3. 외주인력 보안관리를 위해 보안서약서 집행, 비밀번호 노출 예방 등 조치를 하고 있습니까?			
	4. DB 서버에 접속하는 장비(PC, 노트북 등)에서 불법 또는 비인가된 S/W 사용을 방지하고 정품 S/W만 사용하도록 하는 정책을 수립·운영하고 있습니까?			
	5. DB서버에 접근 가능한 자(내부직원, 위탁인력, 개발자 등) 대상으로 개인정보보호 관련 교육을 연2회 이상 실시하고 있습니까?			
네트워크 기반	6. 상시적으로 비인가 IP주소의 접근을 통제하고 있습니까?			
	7. 상시적으로 불필요한 서비스 포트 사용을 통제하고 있습니까?			
	8. 상시적으로 불법적인 해킹시도를 방지하고, 이에 대해 모니터링을 실시하고 있습니까?			
	9. 상시적으로 바이러스, 웜 등의 네트워크 유입을 차단하고 있습니까?			
	10. 주기적으로 네트워크 접속에 대한 로그를 관리하고, 분석하고 있습니까?			
	11. 네트워크 장비 및 정보보호시스템의 보안패치 발생시 지체없이 업데이트를 수행하고 있습니까?			

② (개인정보처리시스템 기준) 점검 항목

※ 개인정보파일이 운용되는 개인정보처리시스템의 보호조치에 관한 내용입니다.

구 분	점 검 항 목	예	아니오	해당없음
DB 및 Application 기반	12. 상시적으로 네트워크를 통한 비인가자의 DB 접근을 통제하고 있습니까?			
	13. DB서버내에 불필요한 서비스 포트를 차단하고 있습니까?			
	14. 상시적으로 DB 접속자 및 개인정보취급자의 접속기록을 남기고 있습니까?			
	15. DB 접속기록을 주기적으로 모니터링하여 통제하고 있습니까?			
	16. DB서버에 접속하는 관리자 PC가 인터넷 접속되는 내부망의 네트워크와 분리되어 있습니까?			
	17. 개인정보취급자의 역할에 따라 DB 접근권한을 차등화하여 부여하고 있습니까?			
	18. 개인정보취급자의 전보, 이직, 퇴사 등 인사 이동 발생시 지체없이 DB 접근권한을 변경하고 있습니까?			
	19. DB접속자 및 개인정보취급자의 DB 로그인 비밀번호를 최소 3개월마다 변경하고 있습니까?			
	20. DB접속자 및 개인정보취급자의 비밀번호 입력시 5회 이상 연속 입력오류가 발생한 경우 계정잠금 등 접근을 제한하고 있습니까?			
	21. DB 및 DB접속 어플리케이션 서버에 대한 물리적 접근을 인가된 자로 한정하고 있습니까?			
	22. DB 및 DB접속 어플리케이션 서버에서 보조기억매체(USB 등) 사용시 관리자 승인 후 사용하고 있습니까?			
	23. DB서버 및 DB접속 어플리케이션 서버에 접속하는 모든 개인정보취급자의 단말기(PC, 노트북 등)의 운영체제 보안패치를 제조사 공지 후 지체없이 수행하고 있습니까?			
	24. HDD등 DB 저장매체의 불용처리시(폐기, 양여, 교체 등) 저장매체에 저장된 개인정보는 모두 파기하고 있습니까?			
웹(Web) 기반 ※ 웹사이트를 운영하는 경우에만 해당	25. 신규 웹 취약점 및 알려진 주요 웹(Web) 취약점 진단/보완을 년1회 이상 실시하거나, 상시적으로 비인가자에 의한 웹서버 접근, 홈페이지 위·변조 등을 자동으로 차단할 수 있는 보호 조치를 하고 있습니까?			
	26. 웹서버 프로그램과 운영체제 보안패치를 제조사 공지 후 지체없이 수행하고 있습니까?			

[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, 「표준 개인정보 보호지침」(행정안전부 고시 제2014-1호)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)

제4조 (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 재 위탁받은 수탁회사를 선임하는 경우 “을”은 당해 재 위탁계약서와 함께 그 사실을 즉시 “갑”에 통보하여야 한다.

제5조 (개인정보의 안전성 확보조치) “을”은 개인정보보호법 제29조, 동법 시행령 제30조 및 개인정보의 안전성 확보조치 기준 고시(행정안전부 고시 제2011-43호)에 따라 개인정보의 안전성 확보에 필요한 관리적·기술적 조치를 취하여야 한다.

제6조 (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

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

보유하고 있는 개인정보를 「개인정보보호법」 시행령 제16조에 따라 즉시 파기하거나 “갑”에게 반납하여야 한다.

③ 제2항에 따라 “을”이 개인정보를 파기한 경우 지체 없이 “갑”에게 그 결과를 통보하여야 한다.

제7조 (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.

제8조 (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.

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

---

2) 「개인정보 안전성 확보조치 기준 고시」(행정안전부 고시 제2014-1호) 에 따라 개인정보처리자 및 취급자는 1년에 1회 이상 개인정보보호에 관한 교육을 의무적으로 시행하여야 한다.

20 년 월 일

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

[별지3]개인정보 유출신고서

개인정보 유출신고서

<table>
<tr><td>기관명</td><td colspan="5"></td></tr>
<tr><td>정보주체에의
통지 여부</td><td colspan="5"></td></tr>
<tr><td>유출된 개인정보의
항목 및 규모</td><td colspan="5"></td></tr>
<tr><td>유출된 시점과
그 경위</td><td colspan="5"></td></tr>
<tr><td>유출피해 최소화
대책·조치 및 결과</td><td colspan="5"></td></tr>
<tr><td>정보주체가 할 수
있는 피해 최소화
방법 및 구제절차</td><td colspan="5"></td></tr>
<tr><td rowspan="3">담당부서·담당자
및 연락처</td><td></td><td>성명</td><td>부서</td><td>직위</td><td>연락처</td></tr>
<tr><td>개인정보
보호책임자</td><td></td><td></td><td></td><td></td></tr>
<tr><td>개인정보
취급자</td><td></td><td></td><td></td><td></td></tr>
</table>

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>목적 외 이용기관의 명칭
(목적 외 이용의 경우)</td><td></td><td rowspan="3">담당자</td><td>소 속</td><td></td></tr>
<tr><td></td><td>성 명</td><td></td></tr>
<tr><td></td><td>전화번호</td><td></td></tr>
<tr><td>제공받는 기관의 명칭
(제3자 제공의 경우)</td><td></td><td rowspan="3">담당자</td><td>성 명</td><td></td></tr>
<tr><td></td><td>소 속</td><td></td></tr>
<tr><td></td><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 반납하거 안전한 방법으로 파기하고 그 증빙을 대학에 공문서로 제출하여야 한다.</td></tr>
</table>

210㎜×297㎜[인쇄용지(특급) 34g/㎡]

[별지7] 개인정보 열람, 정정, 삭제처리청구서

(앞 쪽)

<table>
<tr><td colspan="5">개인정보(□열람 □정정·삭제 □처리정지) 청구서
※ 아래 유의사항을 읽고 굵은 선 안쪽의 사항만 적어 주시기 바랍니다.</td><td>처리기한
10일 이내</td></tr>
<tr><td rowspan="3">청 구 인</td><td>성 명</td><td></td><td>전 화 번 호</td><td colspan="2"></td></tr>
<tr><td>생년월일</td><td></td><td>정보주체와의 관계</td><td colspan="2"></td></tr>
<tr><td>주 소</td><td colspan="4"></td></tr>
<tr><td rowspan="3">정보주체의
인적사항</td><td>성 명</td><td></td><td>전 화 번 호</td><td colspan="2"></td></tr>
<tr><td>생년월일</td><td colspan="4"></td></tr>
<tr><td>주 소</td><td colspan="4"></td></tr>
<tr><td rowspan="4">청구내용</td><td>개인정보파일명</td><td colspan="4"></td></tr>
<tr><td rowspan="2">□ 열람</td><td>대상</td><td colspan="3">□ 개인정보파일 기록항목 : 전부, 일부( )
□ 개인정보 제3자 제공 현황 : 기간(~)
□ 개인정보 처리에 대한 동의 현황</td></tr>
<tr><td>방법</td><td colspan="3">□ 열람 : 직접방문, 전자열람
□ 사본·출력물 수령 : 우편, 모사전송
□ 전자파일 수령 : 전자우편, 기타( )</td></tr>
<tr><td>□ 정정·삭제</td><td colspan="4">※ 정정·삭제하고자 하는 개인정보의 항목과 그 사유를 기재합니다.</td></tr>
<tr><td>□ 처리정지</td><td colspan="4">※ 개인정보의 처리정지를 원하는 대상·내용 및 그 사유를 기재합니다.</td></tr>
<tr><td colspan="6">「개인정보 보호법」 제35조제1항, 제36조제1항 및 제37조제1항에 따라 위와 같이 개인정보의 열람, 정정·삭제 또는 처리정지를 청구합니다.

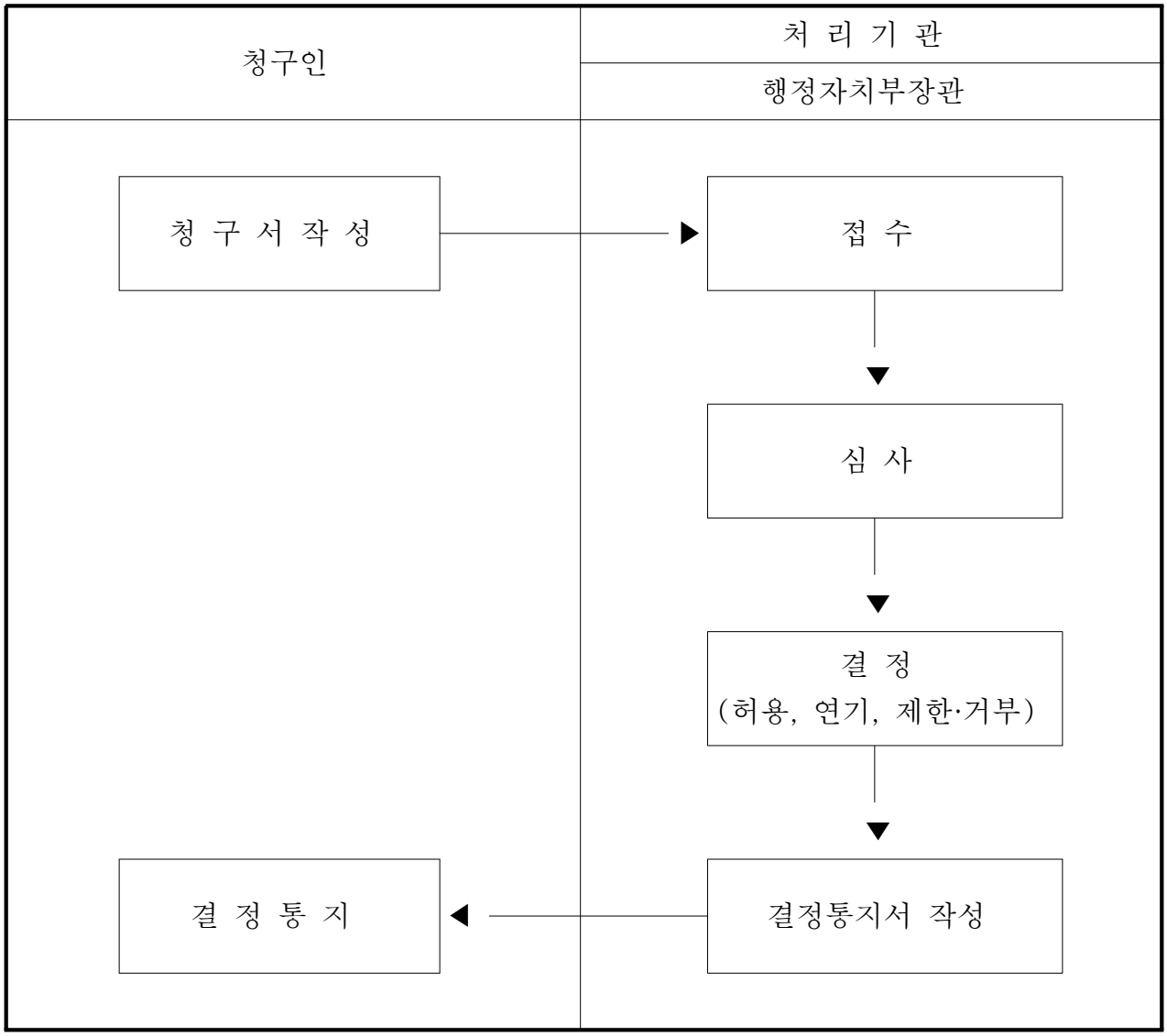
년 월 일

청구인 (서명 또는 인)

○○○○ 귀하</td></tr>
<tr><td colspan="6"><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.</td></tr>
<tr><td colspan="3">담당자의 청구인에 대한 확인 서명</td><td colspan="3"></td></tr>
</table>

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/㎡)

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 한자(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)	
	개인정보보호 책임자 미지정(제31조)	
	영상정보처리기기 안내판 설치 등 필요조치 불이행(제25조)	
정보주체 권익보호	개인정보의 정정·삭제요청에 대한 필요한 조치를 취하지 않고, 개인정보를 계속 이용하거나 제2자에게 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