개인정보보호 내부관리계획

2022. 8. 24

제 주 국 제 대 학 교

개 정 이 력

번호	개정일자	소 속	개인정보 보호담당자	개 정 내 용
1	2015.10.01	사무처 총무과	***	◦신규작성
2	2015.10.15	사무처 총무과	***	◦개인정보보호위원회 자문(문구수정)
3	2017.5.31	사무처 총무과	***	◦개인정보취급자 접근권한 관리 내용 추가 ◦개인정보의 암호화 내용 추가 ◦기술적 보호조치 및 물리적 보호조치 내용 추가
4	2018.1.19	사무처 총무팀	***	◦악성프로그램 등 방지 내용 추가 ◦위험도 분석 및 대응 내용 추가 ◦개인정보 처리업무 위탁 내용 추가
5	2020. 2. 27	사무처 총무팀	***	◦용어의 정의 ◦개인정보보호 조직
6	2021.7.30	사무처 총무팀	***	◦정기회의 일정 조정(3.1) ◦직책별 임무 내용 수정(3.2) ◦물리적 접근제한 및 관리 내용 수정(4.1) ◦개인정보취급자 접근권한 내용 수정(4.3) ◦개인정보의 암호화 내용 수정(4.4) ◦접근통제 내용 수정(4.5) ◦보안프로그램의 설치 및 운영 내용 수정(4.7) ◦기술적 보호조치 내용 수정(4.8) ◦개인정보 침해사실 신고처리 내용 수정(4.11) ◦개인정보보호 교육 계획의 수립 내용 수정(5.1) ◦개인정보보호 교육 계획서 내용 수정(5.1.1) ◦개인정보보호 교육의 실시 내용 수정(5.2) ◦사이버보안 진단의 날 내용 수정(6.1.1) ◦내부감사 기간 및 대상부서 내용 수정(6.2.2)

번호	개정일자	소 속	개인정보 보호담당자	개 정 내 용
7	2022.08.24	사무처 총무팀	***	◦개인정보보호 조직 수정(3.1) ◦직책별 임무 수정(3.2) ◦개인정보보호 교육 계획 수정(5.1.1) ◦연간 개인정보처리자 별 의무 교육이수시간 수정(5.1.2) ◦개인정보보호 교육의 실시 수정(5.2) ◦내부감사 기간 및 대상 부서 수정(6.2.2) ◦교육분야 가명·익명정보 처리 추가(10) ◦적용 범위 추가(10.1) ◦가명처리 목적 추가(10.2) ◦가명처리와 가명정보의 처리 전반 등 추가(10.3) ◦익명처리 개요 추가(10.4) ◦익명처리 원칙 추가(10.5) ◦익명처리 절차 개념도 등 추가(10.6)

목 차

1.총칙

1.1 목적

개인정보 내부관리계획(이하 “내부관리계획”이라 한다)은 개인정보의 안정성 확보조치 기준 제3조에 의거하여 제정된 것으로 제주국제대학교(이하 “본교”라 한다)가 취급하는 개인정보를 체계적으로 관리하여 개인정보가 분실, 도난, 누출, 변조, 훼손, 오남용 등이 되지 아니하도록 함을 목적으로 한다.

1.2 적용범위

내부관리계획은 정보통신망을 통하여 수집, 이용, 제공 또는 관리되는 개인정보뿐만 아니라 서면 등 정보통신망 이외의 수단을 통하여 수집, 이용, 제공 또는 관리되는 개인정보에 대해서도 적용되며, 이러한 개인정보를 취급하는 내부 교직원 및 외부업체 직원에 대해 적용한다.

1.3 용어정의

본 계획에서 사용하는 용어의 정의는 다음 각 호와 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 있는 것을 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”란 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지는 자로서 영 제32조제2항에 해당하는 자를 말한다.
7. “개인정보취급자”란 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 임직원, 파견근로자, 시간제근로자 등을 말한다.
8. “개인정보처리시스템”이란 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템을 말한다.
9. “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.

10. “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.
11. “정보통신망”이란 「전기통신기본법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말한다.
12. “공개된 무선망”이란 불특정 다수가 무선접속장치(AP)를 통하여 인터넷을 이용할 수 있는 망을 말한다.
13. “모바일 기기”란 무선망을 이용할 수 있는 PDA, 스마트폰, 태블릿PC 등 개인정보 처리에 이용되는 휴대용 기기를 말한다.
14. “바이오정보”란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.
15. “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.
16. “내부망”이란 물리적 망분리, 접근 통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.
17. “접속기록”이란 개인정보취급자 등이 개인정보처리시스템에 접속한 사실을 알 수 있는 계정, 접속일시, 접속자 정보, 수행업무 등을 전자적으로 기록한 것을 말한다. 이 경우 “접속”이란 개인정보처리시스템과 연결되어 데이터 송신 또는 수신이 가능한 상태를 말한다.
18. “관리용 단말기”란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리시스템에 직접 접속하는 단말기를 말한다.

2. 내부관리계획의 수립 및 시행

2.1 내부관리계획의 수립 및 승인

1) 개인정보보호책임자는 본교 개인정보보호를 위한 전반적인 사항을 포함하여 내부관리계획을 수립하여야 한다.
2) 개인정보보호책임자는 개인정보보호를 위한 내부관리계획의 수립 시 개인정보보호와 관련한 법령 및 관련 규정을 준수하도록 내부관리계획을 수립하여야 한다.
3) 개인정보보호책임자는 개인정보보호 관련 법령의 제·개정 사항 등을 반영하기 위하여 매년 내부관리계획의 타당성과 개정 필요성을 검토하여야 한다.
4) 개인정보보호책임자는 모든 항목의 타당성을 검토한 후 개정할 필요가 있다고 판단되는 경우 내부관리계획의 개정안을 작성하여 총장에게 보고하고, 승인을 받아야 한다.

2.2 내부관리계획의 공표

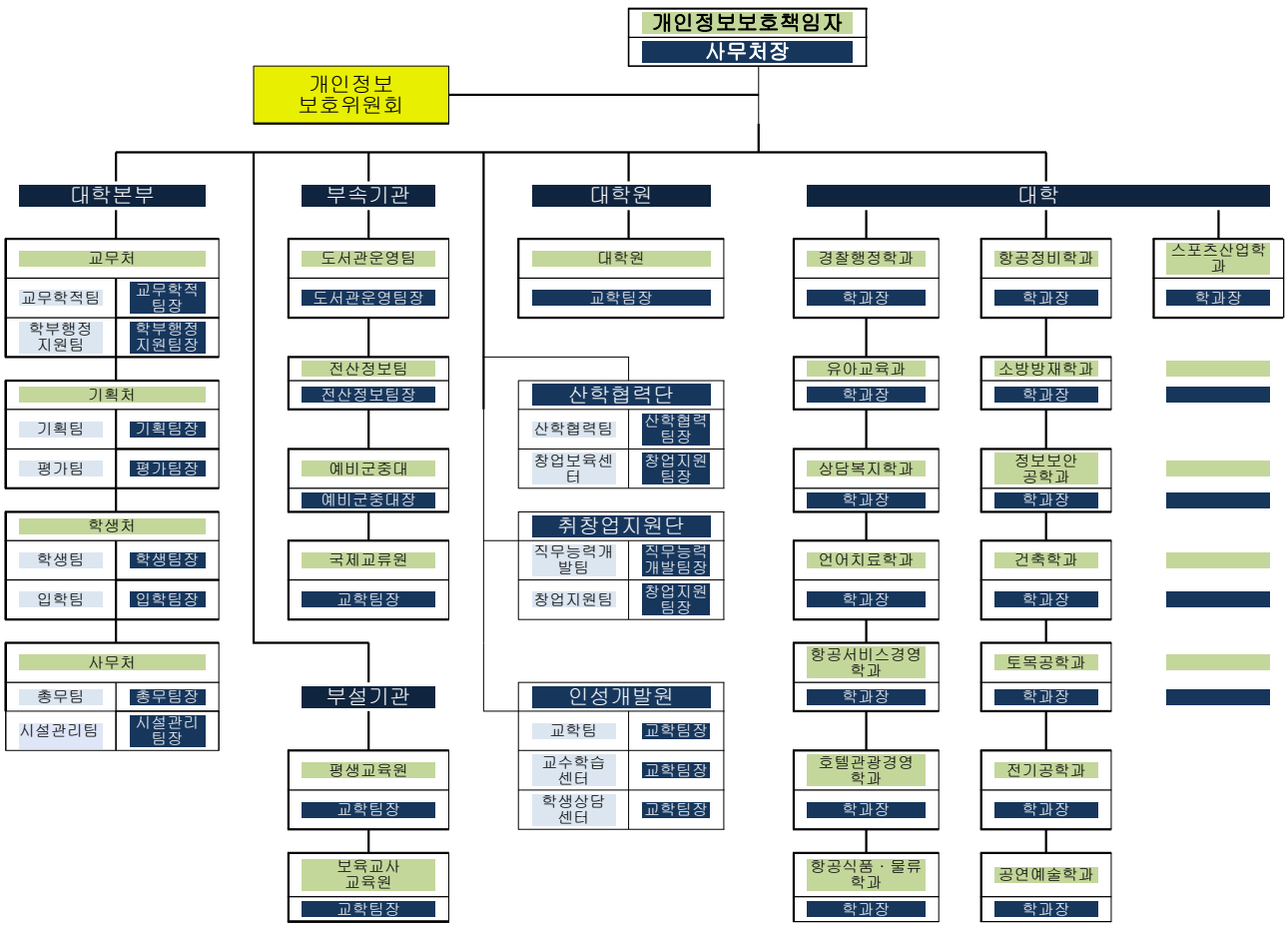
1) 개인정보보호책임자는 승인된 내부관리계획을 학칙 또는 본교 규정에 정하지 않는 경우, 30일 이내, 교내 전 교직원 및 학생에게 공표한다.
2) 내부관리계획은 교내 전 교직원 및 학생이 언제든지 열람(홈페이지 게제, 유인물 배포, E-mail발송 등)할 수 있도록 하여야 하며, 변경사항이 있는 경우에는 이를 즉시 공지하여야 한다.

3. 개인정보보호 조직 구성·운영

개인정보의 처리에 관한 업무를 총괄하는 개인정보보호책임자와 개인정보보호 업무를 수행할 개인정보보호담당자, 개인정보취급자를 지정하여 개인정보보호 조직을 구성하고, 각각의 역할과 책임을 정의한다.

3.1 개인정보보호 조직

1) 본교 개인정보보호정책을 수행하고 유사 시 신속하고 효율적인 대응을 도모할 개인정보보호 조직(개인정보보호책임자, 부서별 개인정보보호담당자, 개인정보취급자)은 다음과 같다.



2) 매년 1회(8월)에 정기회의를 통해 개인정보에 관한 사항 및 법률적 이슈를 검토하고, 개선 및 대응 방안을 강구한다.
3) 상기 회의에서 통해 도출된 사항들은 차기 내부관리계획에 반영하여 수행할 수 있도록 한다.

3.2 직책별 임무

구분	직책	임 무
개인정보보호 책임자	사무처장	- 개인정보보호의 총괄업무 - 개인정보보호 계획의 수립 및 시행 - 개인정보 처리와 관련된 불만 처리 - 오·남용 방지를 위한 내부통제시스템 구축 - 개인정보보호 교육 계획의 수립 및 시행 - 개인정보파일의 보호 및 관리 · 감독 - 개인정보처리방침의 수립 변경 및 시행
부서별 개인정보보호 담당자	교무학적팀장,학부행정지원팀장,기획팀장,학생팀장,입학팀장,직무능력개발팀장,총무팀장, 시설관리팀장교학팀장(대학원)도서관운영팀장,전산정보팀장,예비군중대장,교학팀장(국제교류원),교학팀장(평생교육원,보육교사교육원),직업능력개발팀장,창업지원팀장인성교육개발원팀장	- 부서내 개인정보보호 업무 추진계획 수립 - 부서내 개인정보 취급자 지정 및 관리 - 개인정보보호 대책의 운영 관리 책임 - 부서 내 개인정보처리시스템 접근 권한 관리 - 개인정보보호 관련 보안관리 활동 - 부서 내 개인정보 관리 현황 정기 점검 - 개인정보 침해사고 및 관리현황 보고 - 기타 개인정보보호책임자가 요구하는 사항처리 - 개인정보취급자의 개인정보처리이력 - 개인정보처리 시스템 및 자료 운영 관리 (전산정보팀장)
개인정보 취급자	부서의 업무 담당자 각 학과장	- 부서별 개인정보 처리 관련 업무 수행 - 개인정보보호 규정 준수 및 처리활동 수행 - 정보주체의 의견 수렴 및 불만사항 접수
개인정보 보호위원회	개인정보보호책임자 개인정보보호담당자 (총무, 전산정보) 학술정보원장 위촉 교직원	※ 개인정보보호위원회는 다음 사항을 심의한다. - 개인정보보호 내부계획의 수립 및 시행에 관한 사항 - 개인정보보호 주요 정책에 관한 사항 - 개인정보 침해사실 신고 처리에 관한 사항 - 개인정보보호 교육 계획 수립에 관한 사항 - 개인정보 점검 및 내부감사 실시에 관한 사항 - 기타 개인정보보호책임자가 요청한 사항

4. 개인정보의 기술적·관리적·물리적 보호조치

개인정보 관련 정책 및 법적 요구사항 만족과 본교 정보보안 강화를 위해 아래와 같이 개인정보 처리 보호조치를 수행한다.

4.1 물리적 접근제한 및 관리

1) 전산정보팀 개인정보보호담당자는 개인정보와 개인정보처리시스템의 안전한 보관을 위한 물리적 잠금장치 등의 물리적 접근방지를 위한 보호조치를 취하여야 한다.
2) 전산정보팀 개인정보보호담당자는 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.

4.2 출력 복사시의 보호조치

1) 부서별 개인정보보호담당자는 개인정보가 포함된 정보를 출력하거나 복사할 경우에 개인정보 유출사고를 방지하기 위한 보호조치를 취하여야 한다.
2) 부서별 개인정보보호담당자는 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) 부서별 개인정보취급자는 개인정보의 이용을 위하여 출력 및 복사한 개인정보의 이용목적이 완료된 경우 분쇄기로 분쇄하거나 소각하는 등의 안전한 방법으로 파기하여야 한다.

4.3 개인정보취급자 접근권한 관리

1) 전산정보팀 개인정보보호담당자는 개인정보처리시스템에 대한 접근 권한을 서비스 제공에 필요한 최소한의 인원에게만 부여한다.
2) 전산정보팀 개인정보보호담당자는 개인정보취급 업무를 담당하는 임직원의 담당업무에 따라 개인정보 취급권한을 부여하며, 부서별/직급별에 따라 개인정보에 대한 접근권한(읽기/쓰기/수정 및 삭제 권한)을 차등 부여한다.
3) 전산정보팀 개인정보보호담당자는 개인정보취급자가 전보 또는 퇴직 등 인사이동으로 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소한다.
4) 전산정보팀 개인정보보호담당자는 제1항 내지 제3항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 5년간 보관한다.
5) 전산정보팀 개인정보보호담당자는 개인정보취급자 및 정보주체가 안전한 비밀번호를 설정하여 이용할 수 있도록 다음의 조건에 맞는 비밀번호를 적용하여 이용하도록 한다.

가. 영 대문자, 영 소문자, 숫자 및 특수문자(32개) 중 2종류 이상으로 구성한 경우에는 최소 10자리 이상

나. 영 대문자, 영 소문자, 숫자 및 특수문자(32개) 중 3종류 이상으로 구성한 경우에는 최소 8자리 이상

다. 추측 하기 어려운 비밀번호의 생성

- 연속적인 숫자 금지
- 전화번호 금지
- 개인정보 포함 금지
- 아이디어 포함 금지

6) 전산정보팀 개인정보보호담당자는 매월 셋째주 수요일을 사이버보안 진단의 날로 지정하여 부서별 정기정검을 실시하도록 한다.

7) 전산정보팀 개인정보보호담당자는 사이버보안 진단의 날 정기점검을 실시하여 개인정보취급자가 개인정보처리시스템에 접속하여 처리한 기록과 시스템 이상 유무를 확인·검토하며, 결과를 시스템에 기록 관리한다.

8) 전산정보팀 개인정보보호담당자는 개인정보처리시스템에 접속할 수 있는 사용자 계정을 개인정보취급자별로 발급하고 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

9) 개인정보보호책임자는 재해·재난 발생시 개인정보의 손실 및 훼손등을 방지하고 개인정보 유출 사고 등을 예방하기 위한 대응책을 마련하여야 한다.(재해·재난 유형별 대응 매뉴얼)

4.4 개인정보의 암호화

1) 개인정보보호책임자는 주민등록번호, 신용카드 번호 및 계좌번호에 대해서는 안전한 암호 알고리즘으로 암호화하여 저장하도록 부서별 개인정보보호담당자에게 숙지시켜야 한다.

2) 개인정보관리책임자는 정보통신망을 통해 개인정보 및 인증정보가 송수신 될 때 안전을 보장하기 위하여 보안서버 등을 구축하도록 조치해야 한다.

3) 전산정보팀 개인정보보호담당자는 개인정보관리시스템 및 통신시스템 저장시스템 등을 관리, 운영함에 있어 정보암호화가 이루어질 수 있도록 개인정보관리책임자와 협의한다.

4) 개인정보취급자는 업무용 컴퓨터 또는 모바일 기기에 고유식별 정보를 저장하여 관리하는 경우에는 안전한 알고리즘이 탑재된 암호와 소프트웨어등을 이용하여 해당 파일을 암호화하여 불법적인 유·노출 및 접근 등으로부터 보호하여야 한다.

4.5 접근통제

1) 개인정보보호책임자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 시스템을 설치 및 운영하도록 관리 감독한다.

가. 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한

나. 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지

2) 전산정보팀 개인정보보호담당자는 개인정보취급자가 생일, 주민등록번호, 전화번호 등 추측하기 쉬운 숫자나 개인관련 정보를 패스워드로 이용하지 않도록 비밀번호 작성규칙을 수립하고, 이를 적용 및 운용하여야 한다. 개인정보취급자는 전산정보팀 개인정보보호담당자가 수립한 비밀번호 작성규칙을 준수하여야 한다.

3) 개인정보보호책임자는 전산정보팀 개인정보보호담당자와 함께 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통해 열람권한이 없는 자에게 공개되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터에 조치를 취하여야 하며, 또한 별도의 외부 저장매체(USB등)에 저장할 수 없도록 조치를 취해야 한다.

4.6 접속기록의 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 저장하도록 전산관련 개인정보보호담당자에게 지시한다.

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

3) 개인정보보호책임자는 제1학의 접속기록에 대해 위·변조 방지를 위해 별도의 저장매체에 백업 보관하며, 보관기간은 최소 6개월 이상하도록 조치한다.

4.7 보안프로그램의 설치 및 운영

1) 개인정보보호책임자는 교내 모든 컴퓨터(PC) 등을 이용하여 개인정보를 취급하는 경우 개인정보가 분실, 도난, 누출, 변조 또는 훼손되지 아니하도록 안전성 확보를 위한 백신 프로그램 등의 보안 프로그램을 설치/운영하도록 전산정보팀 개인정보보호담당자에게 지시해야 한다.

2) 보안프로그램은 항상 최신의 버전으로 업데이트를 적용하도록 해야 한다.

3) 보안프로그램의 최신 업데이트를 적용하기 위하여 자동 업데이트 설정 및 실시간 감시 기능이 있는 시스템을 설치 운영하도록 해야 하며, 개인이 직접 실시간 감시 Agent을 삭제할 수 없도록 해야 한다.

4.8 기술적 보호조치

1) 본교에서 보유하고 있는 개인정보관리의 안전성 확보를 위해 필요한 기술적 조치를 아래와 같이 계획하여 수행한다.

구분	보호조치	도입시기	점검시기	시행부서
접근통제 강화	DB 접근통제 솔루션 도입	도입	매년 10월	전산 정보팀
	네트워크 구성 일제 점검 및 취약점 파악	도입예정	매년 10월	
	보안시스템 일제 점검 및 취약점 파악	도입예정	매년 10월	
	DB 암호화 솔루션 도입	도입	매년 10월	
서버 보안강화	시스템 취약점 점검	도입예정	매년 10월	
컴퓨터 보안강화	백신서버 정책 점검 및 문제 컴퓨터 파악	도입	매년 10월	
웹사이트 보안강화	개인정보 노출 방지 취약점 점검	도입	매년 10월	
	Web방화벽 정책 점검 및 취약점 파악	도입	매년 10월	

2) 개인정보의 안전한 관리를 위해 항목별 현황파악과 저장 시 필요한 법적 기준을 적용한다.

암호화 대상항목	DB명	개인정보처리시스템	처리부서	관리부서
주민등록번호	학사DB	학사관리시스템	교무/학생/총무/대학원	전산 정보팀
	학사DB	입시관리시스템	입학	
	행정DB	일반행정관리시스템	교무/기획/총무/대학원	
	학사DB/행정DB	부속행정관리시스템	평생교육원/보육교사교육원	
외국인등록번호	학사DB	부속행정관리	국제교류원	
비밀번호	학사DB	학사관리시스템	교무/대학원	
	행정DB	일반행정관리시스템	교무/기획	
통장번호	학사DB	학사관리시스템	장학/총무/대학원	
	행정DB	일반행정관리시스템	교무/인사	
	행정DB	연구행정관리시스템	산학협력단	
	행정DB	부속행정관리시스템	평생교육원/보육교사교육원	

4.9 물리적 보호조치

1) 본교에서 보유하고 있는 개인정보관리의 안전성 확보를 위해 필요한 물리적 보호조치를 계획하여 수행한다(제주국제대학교 영상정보처리기기 운영ㆍ관리 방침)

4.10 기술적·관리적 보호조치 수행 및 점검시기

구분	항목	수행 및 점검시기	
		점검시기	내용
개인정보 관리체계 기반수립	개인정보보호 내부지침 및 가이드 제정	매년 10월	개인정보지침 수립/제작
	개인정보 보호조직 구성	매년 10월	조직 구성
	개인정보취급자 인식제고	매년 10월	개인정보 취급자 교육
	개인정보 취급방침 개선	매년 10월	취급방침 작성 적용
	개인정보 내부 감사 수행	매년 10월	내부감사
개인정보 기술적 보호조치 방안	개인정보처리시스템 접근통제 강화	매년 10월	DB접근통제 시스템 도입
	네트워크 구성 점검 및 취약점 파악	매년 10월	네트워크 시스템 전체 점검
	보안시스템 일제 점검 및 취약점 파악	연중	방화벽시스템 점검 및 취약점 파악
	개인정보 암호화 시스템 도입	매년 8월	적용계획 수립
		매년 8월	TEST 적용
		매년 8월	적용 및 운용
	서버 시스템 취약점 점검	매년 10월	전체시스템 취약점 파악
	백신 및 자동패치 프로그램 점검	연중	백신서버 및 자동패치서버 점검 사용자 컴퓨터 Agent 확인
	웹사이트 개인정보 노출방지 점검	매년 9월	전체 웹사이트 점검
개인정보 관리적 보호조치 방안	개인정보처리시스템 접근권한 검토	연중	개인정보취급자 권한에 따른 통제적용
	개인정보 파기 정책 및 절차 검토	매년 10월	관련 법률과 비교
		매년 10월	관련법 반영하여 정책 개선
	개인정보 포함서류 보관 안전성 강화	매년 10월	개인정보 지침 수립
		매년 10월	물리적 보안 장치 적용

4.11 개인정보 침해사실 신고처리

1) 침해신고 대상

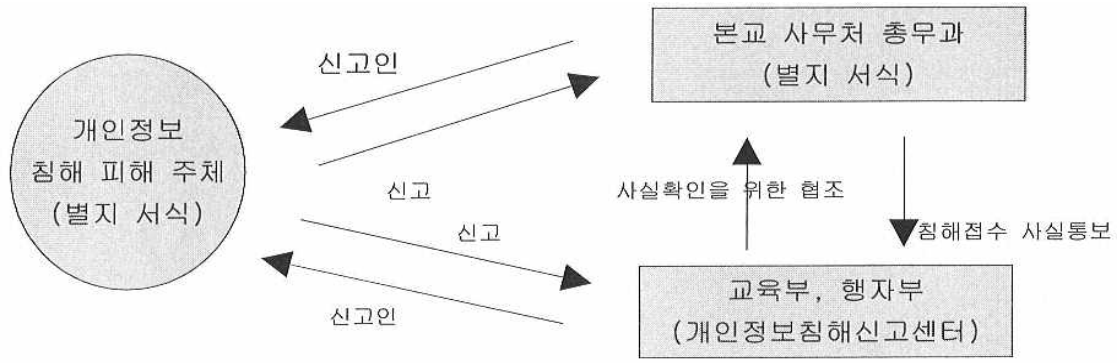
가. 개인정보를 수집, 처리 시 개인정보에 관한 권리 또는 이익의 침해를 받은 자

나. 개인정보파일을 보유함에 있어 개인정보에 관한 권리 또는 이익의 침해를 받은 자

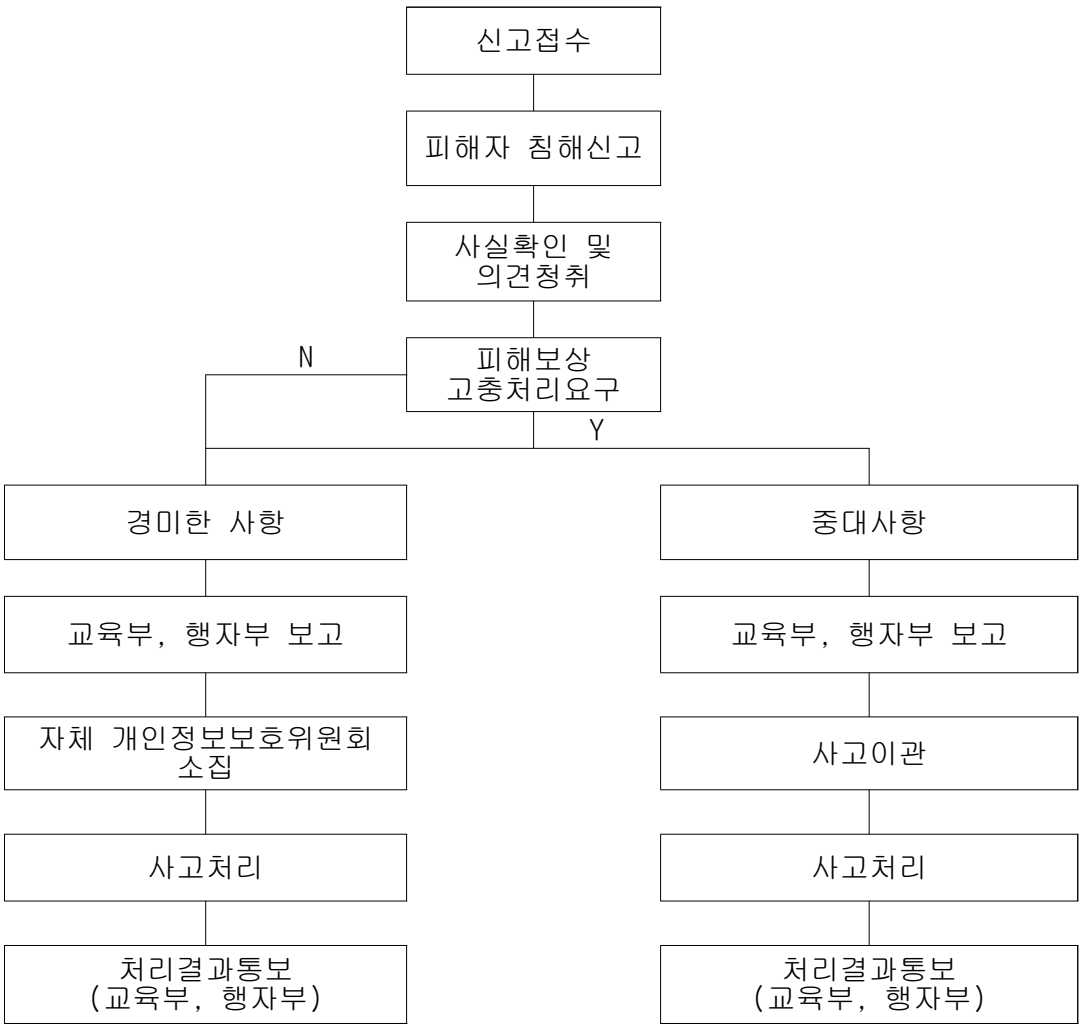
2) 침해신고 및 처리절차

가. 오프라인 : 총무팀 침해신고 창구(개인정보보호 담당자)

⇒ 민원 접수 후 개인정보 침해 사실에 대한 관련자 징계·고발, 안전성 확보 등 조치를 취한 후, 신고주체와 관련기관에 처리 결과 통보



3) 침해신고 처리방법



4) 국가기관 개인정보침해신고센터 상담방법

전화상담	(국번없이)118 (내선 2번)
팩스	02-2100-3008
인터넷	개인정보침해신고센터(privacy.kisa.or.kr)

5. 개인정보보호 교육 수행

개인정보취급자의 개인정보보호에 대한 인식제고와 정책 및 법률 준수사항 실천을 향상시키기 위한 개인정보보호 교육과 정기적인 점검을 실시한다.

5.1 개인정보보호 교육 계획의 수립

1) 개인정보보호책임자는 다음 각 호의 사항을 포함하는 연간 개인정보보호 교육계획을 매년 수립한다.
   가. 교육목적 및 대상
   나. 교육내용
   다. 교육일정 및 방법
2) 개인정보보호책임자는 수립한 개인정보보호 교육계획을 실시한 이후에 교육의 성과와 개선 필요성을 검토하여 차년도 교육계획 수립에 반영하여야 한다.

5.1.1 개인정보보호 교육 계획서

1) 본교 개인정보관련 업무를 수행하는 모든 교직원을 대상으로 다음과 같이 개인정보보호 교육을 실시한다.

교육과정명	개인정보보호교육
교육 대상	전임교원, 일반직원
교육자	전문강사 또는 온라인 교육
교육일시	연중
교육방법	교육자료 배포를 통한 강의, 온라인 교육, 그룹웨어 교육 등

5.1.2 연간 개인정보처리자 별 의무 교육이수시간

1) 본교 개인정보관련 업무를 수행하는 개인정보처리자의 연간 의무교육이수시간은 다음과 같다

구 분	직 위	의무이수 시간
개인정보보호 책임자	사무처장	3시간 이상
개인정보보호담당자	총무팀장	3시간 이상
부서별 개인정보보호담당자	교무학적팀장,학부행정지원팀장,기획팀장, 학생팀장,입학팀장,직무능력개발팀장, 총무팀장, 시설관리팀장,교학팀장(대학원) 도서관운영팀장, 전산정보팀장, 예비군중대장, 교학팀장(국제교육), 교학팀장(평생교육원, 보육교사교육원), 산학협력팀장, 창업지원팀장, 인성교육개발원팀장	1시간 이상
개인정보취급자 (외주업체 포함)	부서의 업무담당자 각 학과장	1시간 이상

5.2 개인정보보호 교육의 실시

1) 개인정보보호책임자는 정보보호에 대한 교직원들의 인식제고를 위해 노력해야 하며, 개인정보의 오·남용 또는 유출 등을 적극 예방하기 위해 교직원을 대상으로 매년 정기적으로 개인정보교육을 실시한다.
2) 정기 교육은 연중 실시한다.
3) 교육 방법은 집체 교육뿐만 아니라 온라인 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, 개인정보보호책임자 및 담당자는 부서 회의 등을 통해 수시 교육을 실시할 수 있다.
5) 개인정보보호책임자 및 담당자는 교육 전·후 교육 계획서 및 교육 결과서 작성 등 증빙자료를 첨부하여 개인정보보호 책임자 및 총장의 결재를 받아 보관한다.

6. 개인정보 보안점검 및 내부감사 실시

개인정보취급자가 개인정보보호정책을 숙지하여 이행할 수 있도록 정기점검을 실시하고 점검결과에 따라 대응 및 개선사항을 도출하여 업무에 반영한다.

6.1 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 최소 년1회 이상 실시한다.

6.1.1 사이버보안 진단의 날

“사이버보안 진단의 날”을 지정하여 개인정보취급자(전교직원)의 컴퓨터 안전성 정기점검, 비밀현황 확인 등 자체보안 점검을 실시한다.

1) 시행시기 : 매월 셋째 주 수요일
2) 주관부서 : 학술정보원 전산정보팀
3) 세부사항 : 매년 초 “사이버보안 진단의 날” 세부 추진계획서를 작성하여 시행한다.

6.2 내부감사

개인정보보호 정책에 대한 이행여부 점검으로 미흡한 사항을 조기 발견하여, 보안사고를 예방하여 효과적인 대책마련으로 대외적인 신뢰성 확보를 통해 본교 이미지 제고를 목적으로 한다.

6.2.1 개요

목 적	개인정보 처리 실태의 미비점 발견 및 보완
주 기	년 1회
주요내용	개인정보 관련 법 준수여부 점검 개인정보보호 지침 이행여부 점검 ※ 상세 항목은 별첨 참고

6.2.2 내부감사 기간 및 대상 부서

기 간	년 1회
주관부서	사무처 총무팀(협조 : 학술정보원 전산정보팀)
대상부서	교내 전부서
심사자	- 개인정보보호책임자(사무처장) - 정보보안책임자(학술정보원장) - 개인정보보호담당자(총무팀장) - 정보보호담당자(전산정보팀장)

6.3 자체감사 결과 반영

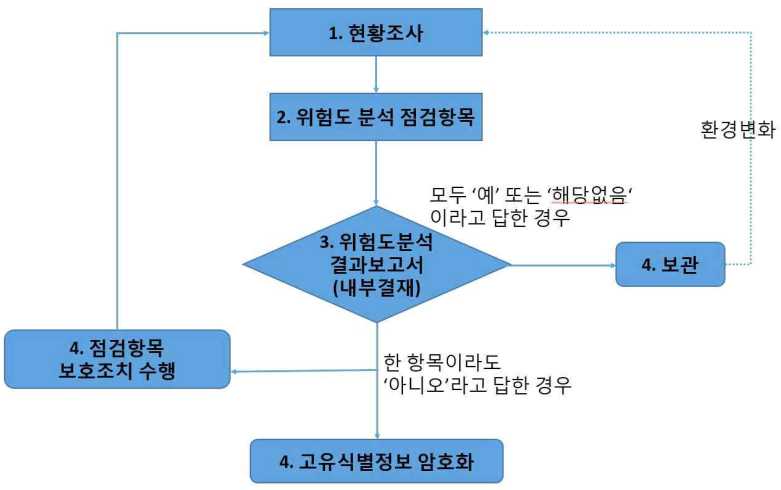
1) 개인정보보호책임자는 자체감사 실시 결과 현황을 취합 정리하여 총장에게 보고하여야 하며, 관련 자료는 문서화하여 보관한다.
2) 개인정보보호책임자는 개인정보 보호를 위한 자체감사 실시 결과, 개인정보의 관리운영상의 문제점을 발견하거나 관련 직원이 본 계획의 내용을 위반할 때에는 총장에게 보고 후 시정·개선 또는 인사발령 등 필요한 조치를 취해야 한다.
3) 개인정보책임자는 개인정보 위반사실에 대한 시정·개선 조치가 이행되지 않거나, 개인정보보호에 심각한 우려가 되는 경우 총장에게 보고 후 개인정보취급자 등에 대한 인사발령 등의 필요한 조치를 취할 수 있다.

7. 악성프로그램 등 방지(2018.1.19. 신설)

1) 개인정보시스템관리자는 개인정보처리시스템 또는 업무용 컴퓨터에 악성 프로그램 등을 방지 · 치료할 수 있는 백신 소프트웨어 등의 보안프로그램을 설치 · 운영하여야 한다.
2) 보안 프로그램의 자동 업데이트 기능을 사용하거나 또는 일 1회 이상 업데이트를 적용하여야 한다.
3) 악성 프로그램관련 경보가 발령된 경우 또는 사용 중인 응용프로그램이나 운영체제소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 적용하여야 한다.

8. 위험도 분석 및 대응(2018.1.19. 신설)

1) 개인정보책임자는 개인정보처리시스템에 적용하고 있는 개인정보보호를 위한 수단과 유출 시 정보주체의 권리를 침해할 위협의 정도를 위험도 분석 절차를 통해 분석하여야 한다.
2) 개인정보책임자는 최초 위험도 분석 이후에도 개인정보처리시스템을 증설하거나, 내 · 외부망과 연계하거나, 기타 운영환경이 변경된 경우에도 지속적으로 실시하여야 한다.



9. 개인정보 처리업무 위탁(2018.1.19. 신설)

9.1 개인정보 처리업무 위탁

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

9.2 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.

9.3 수탁자 선정 시 고려사항

1) 개인정보 처리 업무를 위탁하는 대학은 개인정보 처리 업무를 위탁받아 처리하는자(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.

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

가. 개인정보보호 책임자의 지정여부
나. 내부관리계획의 수립여부
다. 개인정보처리방침의 수립 및 공개 여부
라. 개인정보취급자의 개인정보보호 서약서 작성 여부
마. 개인정보취급자에 대한 개인정보보호 관련 교육 실시 여부
바. 개인정보의 암호화 보관 여부
사. 접근통제 솔루션의 도입 및 적용여부(침입차단시스템, 비인가 사이트 차단 등)
아. 개인정보처리시스템에 대한 보안프로그램 설치 및 정기적 업데이트 수행 여부
자. 물리적 접근방지(전산실, 문서고 등 출입통제 및 물리적 보안 조치)여부
차. 개인정보처리시스템에 대한 접근기록 보관 및 점검 여부
카. 개인정보처리시스템에 대한 접근권한 차등 부여 여부
타. 개인정보 수집 목적 달성 시 파기 여부(전자파일 및 종이문서)
파. 재 위탁(제3자 제공 포함) 금지 준수 여부
거. 위탁 업무에 대한 처리 목적 외 사용 여부
너. 개인정보 취급 업무용 PC의 안전성 확인 여부(패치, 백신 업데이트 등)
더. 위탁업무처리를 위해 제공된 개인정보의 유·노출 사실 여부
러. 침해사고 대응절차 수립 및 전파 여부
머. 기타 법령 또는 계약사항 위반 여부
버. 개인정보처리현황 및 실태 파악

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

9.5 수탁기관 개인정보취급자 교육

1) 대학은 수탁기관 개인정보취급자에 대하여 개인정보가 분실, 도난, 유출, 변조 또는 훼손되지 않도록 다음 내용을 포함하여 정기적으로 교육을 실시해야 한다.
가. 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
나. 개인정보의 기술적·관리적 보호조치에 관한 사항
다. 위탁업무의 목적 및 범위
라. 재위탁 제한에 관한 사항
마. 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
바. 위탁업무와 관련해 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항
사. 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 개인정보취급에 따른 이해도 향상 및 개인정보의 중요성과 유출 시 위험성 등 법령사항들에 대해 숙지토록 해야 한다.

9.6 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.

9.7 위탁 완료 후 개인정보 파기

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

10. 교육분야 가명·익명정보 처리(2022.00.00. 신설)

10.1 적용 범위

1) 우선순위 : 교육 분야의 개인정보 가명 익명처리 및 결합 등
   - 동 사항에 별도로 정하지 않은 사항은 개인정보보호위원회 「가명정보 처리 가이드 라인」준용
2) 적용대상 : 전 학과 및 전 행정부서
3) 적용범위
   - 가명처리 : 개인정보 보호법 제28조의2(가명정보의 처리 등)에 근거하여 통계 작성, 과학적 연구, 공익적 기록보존 등을 위한 가명처리에 적용
   - 익명처리 : 개인정보 보호법 제58조의2(적용 제외)에 근거하여 당사자가 누구인지 알아볼 수 없는 형태로 제공하는 경우에 적용

10.2 가명처리 목적

1) 통계작성 : 집단적 현상이나 수집된 자료의 내용에 관한 수량적인 정보를 작성하는 행위를 말함
2) 과학적 연구 : 기술 개발, 실증, 기초연구, 응용연구, 민간투자연구 등 과학적 방법을 적용하는 연구를 말함
3) 공익적 기록보존 : 공공의 이익을 위하여 지속적으로 열람할 가치가 있는 기록정보를 보존하는 것을 말함

10.3 가명처리와 가명정보의 처리 전반 등

- 교육분야 가명·익명정보 처리 가이드라인에 의함

10.4 익명처리 개요

- 익명정보는 더 이상 개인정보로 취급하지 않기 때문에 개인정보 보호법 등 관련 법령의 제한을 받지 않고 자유롭게 활용 가능

  ※ 단, 익명정보 활용을 위해서는 보다 명확하고 엄격한 처리와 객관적인 검증이 요구됨

10.5 익명처리 원칙

- 개인식별정보는 삭제하고, 개인식별가능정보는 원칙적으로 삭제하되 데이터 이용 목적상 꼭 필요한 경우에는 안전한 방식으로 익명처리 필요
- 익명처리 업무를 수행하는 자는 익명처리 대상 개인정보를 처리하는 업무 수행 금지. 다만, 불가피한 사유가 있을 경우 보완통제 대책을 수립하여 관리자의 승인하에 제한적으로 취급 가능
- 개인정보처리자는 익명정보 적정성 검토를 수행하는 경우 가명정보 적정성 검토 위원회와 동일한 절차로 구성하여 운영 가능 등

10.6 익명처리 절차 개념도 등

- 교육분야 가명 · 익명정보 처리 가이드라인에 의함

[별첨] 내부감사 항목

1. 내부감사 항목_관리현황

구분	감사 항목
개인정보 수집	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 않는가?
	이용자의 개인정보를 제3자에게 제공시 관련 모든 사항을 이용자에 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 대한 정보 유출방지를 위한 관리적 조치를 취하는가?
	업무상 관계기관 및 부서에게 개인정보 자료 제공 시 모든 사항을 고지하는가?
	관계기관 및 부서에서 업무처리상 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?
정보주체 권리	이용자가 개인정보 수집·이용 제공 등을 철회할 수 있게 하고 있는가?
	이용자가 자신의 개인정보에 대한 열람이나 제공을 요구할 수 있고 오류가 있는 경우 정정을 할 수 있게하고 있는가?
	이용자가 개인정보에 수집·이용에 대한 동의를 철회하면 지체없이 수집된 개인정보를 파기하는가?
개인정보 처리방침	개인정보취급방침을 정하여 이용자가 쉽게 인식할 수 있도록 대통령령이 정하는 방법에 따라 공개하고 있는가?
	개인정보취급방침을 변경하는 경우 그 이유 및 변경내용을 지체 없이 공지하고, 이용자가 쉽게 알아볼 수 있도록 하는가?
내부관리 계획수립 시행	□ 개인정보 내부관리계획의 수립 및 시행 □ 개인정보보호책임자의 의무와 책임 □ 개인정보 처리단계별 기술적 관리적 안전조치 □ 개인정보보호 교육 □ 개인정보 침해대응 및 피해구제

2. 내부감사 항목_기술적 보호조치

구분	감사 항목
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?
	외부망에서 개인정보처리시스템에 접속이 필요한 경우 공인인증서 또는 VPN등의 안전한 인증수단을 적용하는가?
	개인정보처리시스템에 대한 접속권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하는가?(침입차단)
	개인정보처리시스템에 접속한 IP등을 재분석하여 불법적인 개인정보 유출시도를 탐지하는가?
	개인정보취급자가 안전한 비밀번호를 이용할 수 있도록 비밀번호 작성규칙을 수립하고 이행하는가?
	개인정보취급자의 비밀번호는 아래의 문자종류 중 2종류 이상 최소 10자 이상 또는 3종류 이상 최소 8자 이상으로 구성하는가?
	개인정보취급자의 비밀번호는 연속적인 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 공유설정을 한 경우 접근제어를 수행하는가?
접속기록 위변조 방지	개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 처리 일시, 처리내역 등 접속 기록을 저장하는가?
	개인정보취급자의 접속기록에 대하여 월1회 이상 확인·감독을 수행하는가?
	개인정보취급자의 접속기록에 대하여 최소 2년 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 주민등록번호에 대해 암호화 저장하는가?
	개인정보처리시스템에 보관하는 이용자의 계좌정보에 대해 암호화 저장하는가?
	개인정보처리시스템에 보관하는 이용자의 신용카드번호에 대해 암호화 저장하는가?
	개인정보를 정보통신망을 통해 전송하는 경우에 암호화하여 송·수신 하는가?
	개인정보를 개인정보취급자의 PC에 저장하는 경우에 암호화 설정을 하는가?
악성 프로그램 방지	개인정보처리시스템에 백신 소프트웨어를 설치하여 운영하고 있는가?
	개인정보취급자의 PC에 백신 소프트웨어를 설치하여 운영하고 있는가?
	백신 소프트웨어를 월 1회 이상 주기적으로 갱신·점검하고 있는가?
	개인정보처리시스템의 OS보안패치는 최신 소프트웨어로 작용하고 있는가?
	개인정보취급자의 OS보안패치는 최신 소프트웨어로 작용하고 있는가?