개인정보보호 내부관리계획

2021. 03

문경대학교
MUN KYUNG COLLEGE

개정이력

버전	개정일자	소속	개인정보보호 관리자	개정내용
14.03	2014.03.24	사무처	정상학	개인정보보호관리업무이관 및 기술적, 관리적 보호조치, 개인정보보호교육계획
15.03	2015.03.27	사무처	김세환	개인정보보호관리업무이관 및 기술적, 관리적 보호조치, 개인정보보호교육계획
16.06	2015.03.28	사무처	김세환	개인정보보호관리업무이관 및 기술적, 관리적 보호조치, 개인정보보호교육계획
17.03	2017.03.15	사무처	홍재성	개인정보보호관리업무이관 및 기술적, 관리적 보호조치, 개인정보보호교육계획
18.03	2018.03.16	사무처	홍재성	개인정보보호 조직, 재해·재난대비 개인정보처리시스템의 물리적 안전조치 위험도 분석 및 대응방안
19.03	2019.03.21.	사무처	김세환	개인정보보호 조직, 재해·재난대비 개인정보처리시스템의 물리적 안전조치 위험도 분석 및 대응방안
20.04	2019.04.03.	사무처	이인복	개인정보보호 조직, 재해·재난대비 개인정보처리시스템의 물리적 안전조치 위험도 분석 및 대응방안
21.03	2021.03.15.	사무처	이인복	개인정보보호 조직, 재해·재난대비 개인정보처리시스템의 물리적 안전조치 위험도 분석 및 대응방안

목 차

5. 위험도 분석 및 대응방안 마련

5. 개인정보보호 교육 수행

7. 개인정보 보안점검 및 내부감사 실시

1. 총칙

1-1 목적

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

1-2 적용범위

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

1-3 용어의 정의

본 계획서에서 사용하는 용어의 정의는 다음과 같다.

1) "개인정보"라 함은 생존하는 개인에 관한 정보로서 성명/주민번호 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) "개인정보보호 책임자"라 함은 본교 개인정보보호 업무 및 조직을 총괄하여 지휘하는 자를 말한다.
3) "개인정보보호 관리자"라 함은 개인정보보호책임자를 보좌하여 개인정보보호업무에 대한 실무를 총괄하고 관리하는 자를 말한다.
4) "개인정보보호 취급자"라 함은 교내에서 교직원의 개인정보를 수집, 보관, 처리, 이용, 제공, 관리 또는 파기 등의 업무를 하는 자를 말한다.
5) "개인정보보호 시스템"이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다.

2. 내부관리계획의 수립 및 시행

2-1 내부관리계획의 수립 및 승인

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

2-2 내부관리계획의 공표

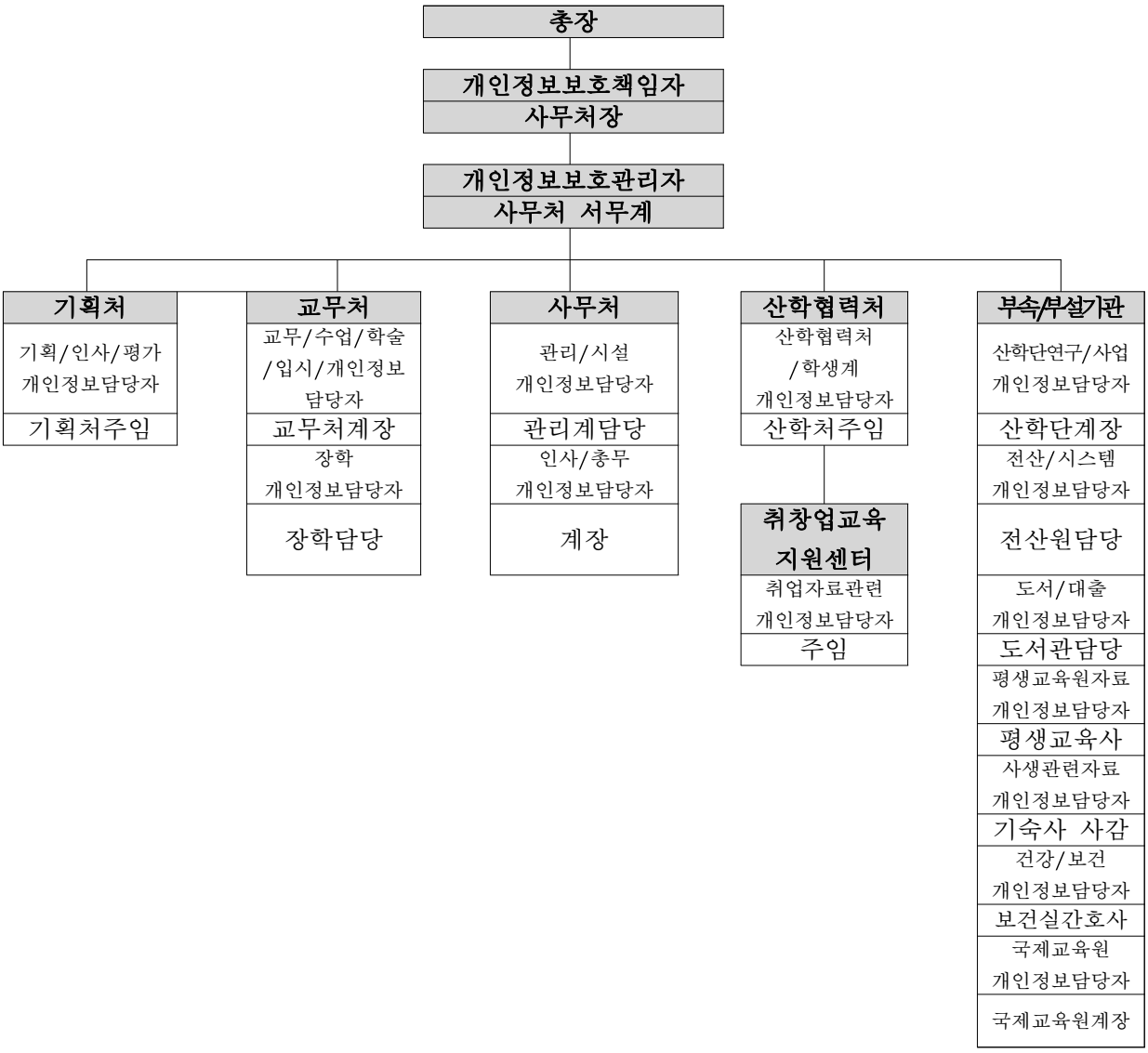
1) 개인정보보호책임자는 승인한 내부관리계획을 학칙 또는 본교 규정에 정하지 않은 경우, 30일 이내, 교내 전 교직원 및 학생에게 공표한다.
2) 내부관리계획은 교내 전 교직원 및 학생이 언제든지 열람(홈페이지게재, 유인물배포, E-mail발송 등)할 수 있도록 하여야 하며, 변경사항이 있을 경우에는 이를 즉시 공지하여야 한다.

3. 개인정보보호 조직 구성·운영

개인정보의 처리에 관한 업무를 총괄하는 개인정보보호책임자와 개인정보보호관리자와 개인정보업무를 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 개인정보보호조직은 다음과 같다.



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

3-2 역할별 임무

직책	담당자	임무
개인정보보호책임자	사무처장	- 개인정보보호 정책의 검토 · 승인 및 총괄업무
개인정보보호관리자	사무처 서무계 담당	- 개인정보보호 계획의 수립 및 시행 - 개인정보 처리와 관련된 불만처리 - 오 · 남용방지를 위한 내부통제시스템구축 - 개인정보보호교육 계획수립 및 시행 - 개인정보파일의 보호 및 관리 · 감독 - 개인정보취급자의 개인정보처리이력 - 보안진단의날 개인정보취급자의 보안실태 점검
부서별 개인정보보호 담당자	기획처주임, 교무처계장, 입학처주임, 관리계 담당, 서무계 담당, 산학협력처계장, 산학협력단계장, 정보전산원담당, 도서관담당, 평생교육사, 보건실간호사	- 부서 내 개인정보보호 업무 추진계획 수립 - 부서 내 개인정보취급자 지정 - 개인정보보호 대책의 운영 관리 책임 - 부서 내 개인정보취급자명단관리 - 부서 내 개인정보관리 현황 정기점검 - 개인정보 침해사고 및 관리현황 보고 - 기타 개인정보보호책임자가 요구하는 사항처리 - 개인정보처리 시스템 및 자료 운영 관리 책임 (정보전산원 담당)
부서별 개인정보보호 취급자	※ 개인정보보호책임자가 지정하는 자	- 부서별 개인정보 처리 관련 업무 수행 - 개인정보보호규정 준수 및 처리 활동 - 정보주체의 의견수렴 및 불만사항 접수

4. 개인정보보호 기술적 · 관리적 · 물리적 보호조치

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

4-1 물리적 접근제한 및 관리

1) 개인정보보호관리자는 개인정보와 개인정보처리시스템의 안전한 보관을 위한 물리적 잠금장치 등 물리적 접근방지를 위한 보호조치를 취하여야 한다.
2) 개인정보보호관리자는 물리적 접근방지를 위한 별도의 보호시설에 출입하거나 개인정보를 열람하는 경우, 그 출입자에 대한 출입사실 및 열람 내용에 관한 관리대장을 작성하도록 하여야 한다.
3) 개인정보보호관리자는 물리적 접근제한 관리대장의 출입 및 열람 내용을 주기적으로 검토하여 정당하지 않은 권한으로 출입하거나 열람하는 경우가 있는지를 점검하여 확인하여야 한다.

4-2 출력 복사 시의 보호조치

1) 부서별 개인정보보호담당자는 개인정보가 포함된 정보를 출력하거나 복사할 경우에 개인정보 유출사고를 방지하기 위한 보호조치를 취하여야 한다.
2) 부서별 개인정보보호담당자는 출력·복사자의 성명, 일시 등을 기재하여 개인정보 유출등에 대한 책임소재를 확인할 수 있는 강화된 보호조치를 추가로 적용하여야 한다.
3) 부서별 개인정보취급자는 개인정보의 이용을 위하여 출력 및 복사한 개인정보의 이용 목적이 완료된 경우 분쇄기로 분쇄하거나 소각하는 등의 안전한 방법으로 파기하여야 한다.

4-3 개인정보취급자 접근권한 관리

1) 개인정보보호관리자는 개인정보처리시스템에 대한 접근 권한을 서비스제공에 필요한 최소한의 인원에게만 부여한다.
2) 개인정보보호관리자는 개인정보취급 업무를 담당하는 교직원의 담당업무에 따라 개인정보 취급권한을 부여하며, 부서별/직급별에 따라 개인정보에 대한 접근권한(읽기/쓰기/수정 및 삭제권한)을 차등 부여한다.
3) 개인정보보호관리자는 개인정보보호취급자가 전보 또는 퇴직 등 인사이동으로 변경 되었을 경우 지체없이 개인정보처리시스템의 접근권한을 변경 또는 말소 한다.
4) 개인정보보호관리자는 제1항 내지 제3항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 5년간 보관한다.
5) 개인정보보호관리자는 개인정보취급자 및 정보주체가 안전한 비밀번호를 설정하여 이용할 수 있도록 다음의 조건에 만족하는 비밀번호를 적용하여 이용하도록 한다.
   가. 영 대문자, 영소문자, 숫자 및 특수문자(32개) 중 2종류 이상으로 구성한 경우에는 최소 10자리 이상
   나. 영 대문자, 영소문자, 숫자 및 특수문자(32개) 중 3종류 이상으로 구성한 경우에는 최소 8자리 이 이상
   다. 추측하기 어려운 비밀번호 생성
   - 사용자 계정(ID)과 동일하지 않은 것
   - 개인신상 및 부서 명칭 등과 관계
   - 일반 사전에 등록된 단어는 사용을 피할 것
   - 동일단어 또는 숫자를 반복하여 사용하지 말 것
   - 사용된 비밀번호는 재사용하지 말 것
   - 동일 비밀번호를 여러 사람이 공유하여 사용하지 말 것
   - 응용프로그램 등을 이용한 자동 비밀번호 입력기능 사용 금지
6) 개인정보보호관리자는 매월 셋째주 수요일 ‘사이버보안진단의 날’로 지정하여 부서별로 정기점검을 실시 하도록 한다.
7) 정보전산원 개인정보보호담당자는 사이버보안 진단의 날 정기점검을 실시하여 개인정보취급자가 개인정보처리시스템에 접속하여 처리한 기록과 시스템 이상 유무를 확인·검토하여, 결과를 시스템에 기록 관리한다.

4-4 개인정보의 암호화

1) 개인정보보호관리자는 주민등록번호, 신용카드번호 및 계좌번호에 대해서는 안전한 암호 알고리즘으로 암호화하여 저장하도록 부서별 개인정보보호담당자에게 숙지시켜야 한다.
2) 개인정보보호책임자는 정보통신망을 통하여 개인정보 및 인증정보가 송수신 될 때 안전을 보장하기 위하여 보안서버 등을 구축하도록 조치해야 한다.
3) 정보전산원 개인정보보호담당자는 개인정보관리시스템 및 통신시스템, 저장시스템 등을 관리, 운영함에 있어 정보암호화가 이루어 질 수 있도록 개인정보보호책임자와 협의한다.
4) 개인정보취급자는 개인정보를 개인용 컴퓨터(PC)에 저장하지 않도록 해야한다.

4-5 접근통제

1) 개인정보보호관리자는 정보통신망을 이용한 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 개인정보유출 시도 탐지
2) 개인정보보호관리자는 개인정보취급자가 생일, 주민등록번호, 전화번호 등 추측하기 쉬운 숫자나 개인관련 정보를 패스워드로 이용하지 않도록 비밀번호 작성규칙을 수립하고, 이를 적용 및 운용하여야 한다.
3) 개인정보보호취급자는 개인정보보호관리자가 수립한 비밀번호 작성규칙을 준수 하여야 한다.
4) 개인정보보호관리자는 정보전산원 개인정보보호담당자와 함께 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통해 열람권한이 없는 자에게 공개되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터에 조치를 취하여야한다.
5) 개인정보보호관리자는 개인정보취급 업무를 담당하는 교직원의 담당업무에 따라 개인정보 취급권한을 부여하며, 부서별/직급별에 따라 개인정보에 대한 접근권한(읽기/쓰기/수정 및 삭제권한)을 차등 부여한다.

4-6 접속기록의 위변조 방지

1) 개인정보보호책임자는 접속기록의 위 변조 방지를 위해 개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리(입/출력, 수정 등 DB접근)하는 경우에는 처리일시, 처리내역 등 접속기록을 저장하도록 정보전산원 개인정보보호담당자에게 지시한다.
2) 개인정보보호책임자는 제1항의 접속기록에 대해 월1회 이상 정기적으로 확인, 감독한다.
3) 개인정보보호책임자는 제1항의 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 안정성 확보를 위한 백신 프로그램 등의 보안 프로그램을 설치/운영하도록 해야 한다.
2) 보안 프로그램은 항상 최신의 버전으로 업데이트를 적용하도록 해야 한다.
3) 보안 프로그램의 최신 업데이트를 적용하기 위하여 자동 업데이트 설정 및 실시간 감지 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 안정성 확보를 위해 필요한 기술적 조치를 아래와 같이 계획하여 수행한다.

구분	보호조치	추진일정	시행부서
접근통제 강화	네트워크 구성 일제 점검 및 취약점 파악	2021년 06월	사무처 및 정보전산원
	보안시스템 일제 점검 및 취약점 파악	2021년 06월	
서버보안 강화	시스템 취약점 점검	2021년 06월	
컴퓨터보안 강화	백신서버 정책 점검 및 문제 컴퓨터 파악	2021년 07월	
	내PC지키미 사용현황 집중점검	2021년 04월	
웹사이트 보안강화	개인정보 노출방지 취약점 점검	2021년 07월	
	Web방화벽 정책 점검 및 취약점 파악	2021년 07월	

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

암호화 대상항목	DB명	개인정보 처리시스템	처리부서	관리부서
주민등록번호	입시/학사/행정DB	종합정보시스템	기획처/교무처/입학처 /정보전산원	정보전산원
비밀번호	입시/학사/행정DB	종합정보시스템		
계좌번호	입시/학사/행정DB	종합정보시스템		

4-9 기술적·관리적 보호조치 수행계획

구분	항목	2017년	
		추진 월	내용
개인정보 관리체계 기반수립	개인정보보호 내부관리계획 보고	04월	
	개인정보 보호조직 구성	04월	
	개인정보취급자 인식제고	07월	개인정보 취급자 교육
	개인정보 취급방법 개선	08월	
	개인정보 내부 감사 수행	익년 1월	내부감사 실시
개인정보 기술적 보안조치 방안	네트워크 구성 점검 및 취약점 파악	08월	네트워크시스템 전체점검
	보안시스템 일제 점검 및 취약점 파악	08월	방화벽시스템 정책점검 및 취약점 개선
	서버 시스템 취약점 점검	08월	전체시스템 취약점 파악
	백신 및 자동패치 프로그램 점검	08월	백신서버 및 자동패치서버점검 및 사용자 컴퓨터 Agent 확인
	웹사이트 개인정보 노출 방지 점검	08월	전체 웹사이트점검
개인정보 관리적	개인정보처리시스템 접근권한 검토	06월	개인정보취급자 권한에 따른 통제적용
	개인정보 파기 정책 및 절차 검토	08월	관련법률과 비교, 검토

보호조치 방안			관련법 반영하여 정책 개선
	개인정보 포함서류 보관 안정성 강화	06월	개인정보 지침 수립
		06월	물리적 보안 장치 적용

4-10 재해 · 재난 대비 개인정보처리시스템의 물리적 안전조치

1) 화재, 홍수 등 재해 · 재난 발생 시 개인정보처리시스템 보호를 위한 대응절차를 마련하고 정기적 점검을 하여야 한다.

2) 재해 · 재난 상황을 대비한 대응 매뉴얼을 문경대학교 안전관리 계획에 의하여 행동하도록 한다.

4-11 개인정보 침해사실 신고처리

1) 침해신고 대상

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

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

다. 침해신고 및 처리절차 : '보안사고 대응지침 및 대응절차'에 따른다.

목적	- 개인정보를 수집 · 처리하거나 개인정보파일을 보유 함에 있어서 개인정보에 관한 권리 또는 이익의 침해를 받은 자는 그 침해사실을 신고할 수 있다.
신고	- 본교 사무처 침해신고 창구(개인정보보호담당자) - 【개인정보침해신고처리대장】에 의한 침해신고 접수 · 처리 - 개인정보침해신고의 처리 절차는 민원사무처리 관계법령을 준용하여 신속하게 처리
절차	- 개인정보 침해신고는 "개인정보침해신고처리대장"에 의거 개인정보보호담당자가 속한 사무처에 접수 · 처리 ※ 타 부서에서 접수를 받은 때에는 사무처로 송부 - 민원접수 후 개인정보 침해 사실에 대한 관련자 징계, 고발, 안전성 확보등 조치를 취한 후, 신고주체와 개인정보보호책임자에게 처리결과 통보
안내도	**신고접수** (유출 · 침해사고 접수) → **사실조사** (유출침해여부 확인 및 시연조사) → **처리** (관련자 징계/고발 안전성 확보조치) → **결과통보** (신고인 및 행안부 통보)

3) 개인정보침해신고센터 상담방법

전화상담	국번없이 118, 내선 2번
인터넷	http://privacy.kisa.or.kr
우편 · 방문	전남 나주시 진흥길 9(빗가람동 301-2 3층) 개인정보침해신고센터(우편번호: 58324)
팩스	061)820-2619
[전화상담 가능시간] - 월 ~ 금 : 09:00 ~ 18:00(12:00 ~ 13:00, 점심시간 제외) - 휴무일 : 토 · 일 · 법정 공휴일 ※ 인터넷을 통한 상담 · 신고는 연중 1일 24시간 가능	

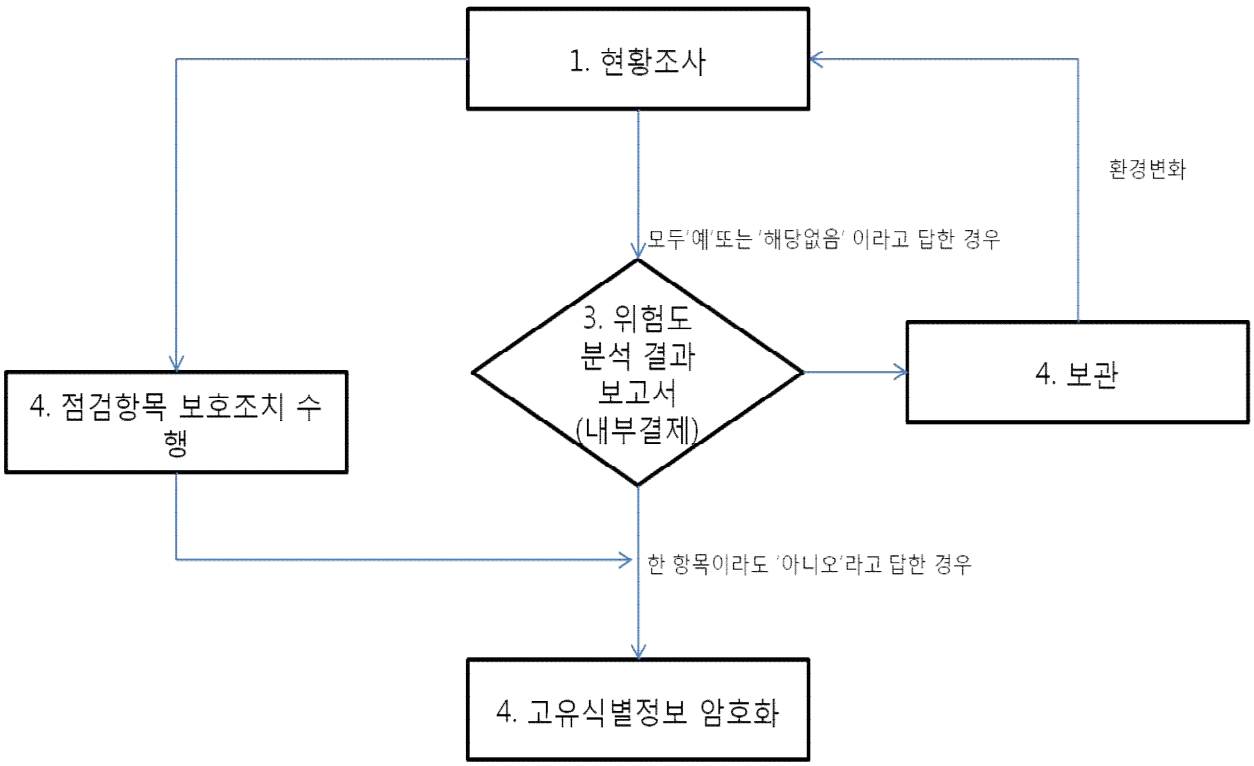
5.위험도 분석 및 대응방안

개인정보처리시스템의 운영에 발생할 수 있는 위험요소를 사전에 발견 및 대응하기 위하여 아래와 같이 위험도 분석 및 대응반안을 수행한다.

5-1 위험도 분석 및 대응

1) 개인정보처리시스템에 작용하고 있는 개인정보보호를 위한 수단과 유출 시 정보주체의 권리를 침해할 위협의 정도를 위험도 분석 절차를 통해 분석한다.
2) 최초 위험도 분석 후 개인정보처리시스템 증설 또는 내·외부망과 연계하거나, 기타 운영 환경이 변경된 경우에도 위험도 분석을 실시한다.
3) 위험도 분석 및 대응 시행 시 정보전산원에 협조 요청하여 기술적인 부분에 대한 분석을 실시
4) 위험도 분석 및 대응은 내부감사 시 동시에 실시할 수 있다.

5-2 위험도 분석 및 대응 절차



6. 개인정보보호 교육 수행

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

6-1 개인정보보호 교육 계획 수립

1) 개인정보보호관리자는 다음 각 호의 사항을 포함하는 연간 개인정보보호 교육 계획을 매년 2월 말까지 수립한다.
   가. 교육목적 및 대상
   나. 교육내용
   다. 교육 일정 및 방법
2) 개인정보보호관리자는 수립한 개인정보보호 교육 계획을 실시한 이후에 교육의 성과와 개선 필요성을 검토하여 차년도 교육계획 수립에 반영하여야 한다.

6-2 개인정보보호 교육 계획서

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

교육과정명	개인정보보호법 개정 및 관련사항
교육대상	개인정보보호취급자
교육자	개인정보보호책임자, 개인정보보호관리자
교육일시	방학기간 실시(하계 또는 동계)
교육방법	온라인 교육
교육내용	개인정보보호법 및 관련사항 설명

6-3 연간 개인정보차리자 별 의무 교육이수시간

1) 본교 개인정보관련 업무를 수행하는 개인정보처리자의 연간 의무교육이수시간은 다음과 같다.

직책	담당자	의무이수 시간
개인정보보호책임자	사무처장	2시간
개인정보보호관리자 및 개인정보보호담당자(부서별)	기획처주임, 교무처계장, 입학처주임, 사무처관리담당, 사무처 서무계, 산학협력처계장, 산학혁력단계장, 정보전산원담당, 도서관담당, 평생교육사	2시간
개인정보 취급자 (외부업체 포함)	※ 개인정보책임자가 지정하는 자 및 업무담당자	2시간

6-4 개인정보보호 교육의 실시

1) 개인정보보호책임자는 정보보호에 대한 교직원들의 인식제고를 위해 노력해야하며, 개인정보의 오·남용 또는 유출 등을 적극 예방하기 위해 교·직원을 대상으로 매년 정기적으로 연1회 이상의 개인정보보호 교육을 실시한다.
2) 연 1회의 정기 교육은 방학기간 중에 1회 실시한다.
3) 교육방법은 집체 교육뿐아니라, 인터넷교육, 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, 개인정보보호관리자는 부서 회의 등을 통해 수시교육을 실시할 수 있다.
5) 개인정보보호관리자는 교육 전·후 교육계획서 및 교육 결과서 작성 등 증빙자료를 첨부하여 개인정보보호책임자의 결재를 받아 보관한다.

7. 개인정보 보안점검 및 내부감사 실시

개인정보취급자가 개인정보보호정책을 숙지하여 이행할 수 있도록 정기점검을 실시하고, 점검 결과에 따라 개선사항을 도출하여 업무에 반영한다.

7-1 자체감사 주기 및 절차

1) 개인정보보호책임자는 개인정보보호를 위한 내부관리 계획 및 관련 법령에서 정하는 개인정보보호규정을 성실히 이해하는 지를 주기적으로 감사 또는 점검하여야 한다.
2) 개인정보보호책임자는 개인정보 자체감사를 위한 감사대상, 감사절차 및 방법 등 감사의 실시에 관하여 별도의 계획을 수립할 수 있다.
3) 개인정보보호 자체감사는 최소 년1회 이상 실시한다.

7-2 사이버보안 진단의 날

‘사이버 보안진단의 날’ 을 지정하여 개인정보취급자(전 교직원)의 컴퓨터 안정성 정기점검, 비밀현황 확인 등 자체보안점검을 실시 한다.

1) 시행시기 : 매월 셋째주 수요일
2) 주관부서 : 정보전산원
3) 세부사항 : 매년 초 ‘사이버보안 진단의 날’ 세부 추진 계획서를 작성하여 시행 한다.

7-3 내부감사

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

1) 개요

목 적	개인정보 처리 실태의 미비점 발견 및 보완
주 기	년 1회

주요내용	- 개인정보 관련 법 준수 여부 점검 - 개인정보보호 지침 이행 여부 점검 ※ 상세항목은 별첨자료 참조

2) 내부감사 기간 및 대상 부서

기 간	익년 2월
주관부서	사무처, 정보전산원
대상부서	학내 전체부서
주요내용	- 개인정보보호책임자(사무처장) - 보안담당관(사무처장) - 개인정보보호관리자(사무처 서무계) - 개인정보보호담당자(정보전산원 담당)

7-4 자체검사 결과 반영

1) 개인정보보호관리자는 자체감사 실시 결과 현황을 취합 정리하여 개인정보보호책임자에게 보고하여야 하며, 관련 자료는 문서화하여 보관한다.
2) 개인정보보호책임자는 개인정보보호를 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 취하여야 한다.
3) 개인정보보호책임자는 개인정보 위반사실에 대한 시정·개선 조치가 이행되지 않거나, 개인정보보호에 심각한 영향이 발생할 수 있는 우려가 되는 경우 총장에게 보고 후 개인정보취급자 등에 대한 인사발령 등의 필요한 추가 조치를 취할 수 있다.

[별첨1] 내부감사 항목

1. 내부감사 항목 관리현황

구분	감사항목
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 수집 하는가?
	수집한 이용자의 개인정보를 이용자로부터 동의 받은 목적 및 고지사항과 다른 목적으로 이용하고 있지 않은가?
	이용자의 개인정보를 제3자에게 제공 시 관련 모든 사항을 이용자에게 알리고 동의를 얻는가?
	개인정보 취급 위탁시 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 부서에서 개인정보 자료 제공 시 모든 사항을 고지하는가?
	관계기관 및 부서에서 업무처리 상 개인정보자료 요구 시 정확한 법적 근거에 의하여 요구하였고 그에 준하여 제공 하였는가?
개인정보파기	이용자의 개인정보를 사전에 고지한 보유기간 및 파기기간에 맞게 적절히 개인정보를 파기하는가?
	회원 탈퇴를 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 지체없이 공지하고, 이용자가 쉽게 알아볼 수 있도록 하는가?
내부관리계획 수립 시행	개인정보 내부관리계획의 수립 및 시행 개인정보보호책임자 의무와 책임 개인정보 처리단계별 기술적 관리적 안전조치 개인정보보호 교육 개인정보 침해대응 및 피해구제

2. 내부감사 항목 기술적 보호조치

구분	감사항목
접근통제	개인정보처리시스템에 대한 접근권한을 서비스 제공을 위해 필요한 자에게만 부여하는가?
	관련업무 및 직제변경시 지체없이 개인정보처리시스템의 접근권한을 변경 또는 말소하는가?
	개인정보처리시스템의 접근 권한 부여, 변경 또는 말소에 대한 내역을 기록하는가?
	외부망에서 개인정보처리시스템에 접속이 필요한 경우에 공인인증서 또는 VPN 등의 안전한 인증수단을 적용하는가?
	개인정보처리시스템에 접속권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하는가?
	개인정보처리시스템에 접속한 IP망등을 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 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 비밀번호에는 유효기간 설정, 주기적(6개월)으로 변경하는가?
	개인정보취급자의 PC에서 P2P를 사용하지 못하도록 조치하였는가?
	개인정보취급자의 PC에서 고유설정을 한 경우 접근제어를 수행하는가?
접속기록 위변조방지	개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 처리 일시, 처리내역 등 접속 기록을 저장하는가?
	개인정보취급자의 접속기록에 대하여 월1회 이상 확인 · 감독을 수행하는가?
	개인정보취급자의 접속기록에 대하여 최소2년이상 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, 계좌번호, 비밀번호에 대하여 암호화하여 저장하는가?
	개인정보를 정보통신망을 통해 전송하는 경우에 암호화하여 송 · 수신하는가?
	개인정보를 개인정보취급자의 PC에서 저장하는 경우에 암호화 설정을 하는가?
악성방지 프로그램	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?

[별지 1]

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		
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		

[개인정보보호법] 제32조제1항 및 같은 법 시행령 제34조제1항에 따라 위와 같이 개인정보파일 ([ ] 등록 [ ] 변경등록)을 신청합니다.

년 월 일

신청부서 및 부서장

[별지 2]

개인정보파일 파기 요청서

작성일		작성자	
파기대상 개인정보파일			
생성일자		개인정보취급자	
주요 대상업무		현재 보관건수	
파기 사유			
파기 일정			
특기사항			
파기 승인일		승인자 (개인정보 보호책임자)	
파기장소			
파기방법			
파기수행자		입회자	
폐기확인 방법			
백업 조치 유무			
매체 폐기 여부			

[별지 3]

개인정보파일 파기 관리대장

번호	개인정보 파일명	자료의 종류	생성일	폐기일	폐기사유	처리 담당자	처리 부서장

[별지 4]

개인정보 유출 신고서

부서명					
정보주체에 통지여부					
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
	개인정보보호 책임자				
	개인정보 취급자				

유출신고접수기관	부서명	담당자명	연락처

[별지 5]

<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">청구인</td><td>성명</td><td></td><td>전화번호</td><td></td></tr>
<tr><td>생년월일</td><td></td><td>정보주체와의 관계</td><td></td></tr>
<tr><td>주소</td><td></td><td>전화번호</td><td></td></tr>
<tr><td rowspan="3">정보주체의
인적사항</td><td>성명</td><td></td><td>전화번호</td><td></td></tr>
<tr><td>생년월일</td><td colspan="3"></td></tr>
<tr><td>주소</td><td colspan="3"></td></tr>
<tr><td rowspan="4">청구내용(구체적으로 요청하지 않으면 처리가 곤란할 수 있음)</td><td>개인정보파일명</td><td colspan="3"></td></tr>
<tr><td rowspan="2">열람</td><td>대상</td><td colspan="2">□ 개인정보파일 기록 항목 : 전부, 일부( )
□ 개인정보 제3자 제공현황 : 기간(~)
□ 개인정보 처리에 대한 동의 현황</td></tr>
<tr><td>방법</td><td colspan="2">□ 열람 : 직접방문, 전자열람
□ 사본, 출력물 수령 : 우편, 모사종이
□ 전자파일 수령 : 전자우편, 기타( )</td></tr>
<tr><td>정정, 삭제</td><td colspan="3">※ 정정 · 삭제하고자 하는 개인정의 항목과 그 사유를 기재합니다.</td></tr>
<tr><td>처리정지</td><td colspan="3">※ 개인정보의 처리정지를 원하는 대상, 내용 및 그 사유를 기재 합니다.</td></tr>
<tr><td colspan="6">『개인정보보호법』 제35조1항, 제36조1항 및 제37조1항에 따라 위와 같이 개인정보의 열람, 정정, 삭제 또는 처리정지를 청구합니다.

년 월 일
청구인 (서명 또는 인)

문경대학교 총장 귀하</td></tr>
<tr><td colspan="2">담당자의 청구인에 대한 확인 서명</td><td colspan="4"></td></tr>
</table>