개인정보보호 내부관리계획(안)

2023. 10. 10.

동남보건대학교
DONGNAM HEALTH UNIVERSITY

제 · 개정 이력

구분	제 · 개정일자	소속	개인정보보호책임자	제 · 개정내용
1	2013.04.01	사무처	사무처장	내부관리계획 제정
2	2015.12.01	사무처	사무처장	내부관리계획 부분개정
3	2017.11.01	사무처	사무처장	내부관리계획 전면개정
4	2018.12.12	사무처	사무처장	내부관리계획 부분개정
5	2020.03.25	사무처	사무처장	내부관리계획 부분개정
6	2021.06.23	사무처	사무처장	내부관리계획 부분개정
7	2022.09.16	사무처	사무처장	내부관리계획 부분개정
8	2023.10.10	사무처	사무처장	내부관리계획 전면개정
			- 이 하 여 백-	

목 차

Ⅰ 총칙

1 목적

「개인정보 보호법」 제29조와 동법 시행령 제30조에 따라 개인정보 처리자가 개인정보를 처리함에 있어서 개인정보가 분실·도난·유출·변조·훼손되지 아니하도록 안전성을 확보하기 위한 기술적·관리적·물리적 조치 계획을 수립하는 것을 목적으로 한다.

2 근거

○ 「개인정보보호법」 제29조(안전조치의무)

○ 「개인정보 보호법」 시행령 제30조(개인정보의 안전성 확보조치)의 제1호

○ 개인정보의 안전성 확보조치 기준(개인정보보호위원회 고시 제2021-2호, 2021.09.15)

○ 표준 개인정보 보호지침(행정안전부 고시 제~~2016-21~~호, 2023.09.15)

○ 교육부 개인정보 보호지침(교육부훈령 제355호, 2020.12.11)

3 적용범위

○ 본 계획은 정보통신망을 통하여 수집·이용· 제공 또는 관리되는 개인정보뿐만 아니라, 서면 등 정보통신망 이외의 수단을 통해서 수집·이용·제공 또는 관리되는 개인정보 및 영상정보기기(CCTV등)에 대해서도 적용되며, 이러한 개인정보를 취급하는 내부 직원 및 외부위탁업체에 대해서도 적용된다.

○ 필요시 처리기준, 절차, 양식 등은 『교육부 개인정보 보호지침』에 의거하여 시행한다.

4 용어 정의

○ “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.

> ▸ 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

○ “정보주체”란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서, 개인정보 보호법에 의해 보호대상이 되는 정보의주체가 되는 사람을 말한다.

○ “개인정보파일”이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.

○ “개인정보 처리자”란 업무를 목적으로 개인정보파일을 운용(수집·이용·저장·제공·파기 등)하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 모든 공공기관, 법인, 단체 및 개인 등 을 말한다.

○ “개인정보 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.

○ “개인정보 보호책임자”란 개인정보 처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지거나 업무처리를 최종적으로 결정하는 자로서, 법 제31조에 따른 지위에 해당하는 자를 말한다.

○ “개인정보 보호담당자”란 실질적인 개인정보 보호업무를 담당하는 자로 개인정보 처리자가 지정한 자를 말한다.

○ “개인정보보호 분야별 책임자”(이하 “분야별 책임자”라 한다)란 업무를 위하여 개인정보파일을 처리하는 부서의 장으로 본교 내 각 부서의 개인정보 업무를 지휘 · 감독하는 자를 말한다.

○ “개인정보 취급자”란 개인정보 처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 직접 개인정보에 관한 업무를 담당하는 자와 그 밖에 업무상 필요에 의해 개인정보에 접근하여 처리하는 모든 자를 말한다.

○ “개인정보처리시스템”이라 함은 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 응용시스템을 말한다.

○ “접속기록”이란 개인정보취급자 등이 개인정보처리시스템에 접속한 사실을 알 수 있는 계정, 접속일시, 접속자 정보(접속한 자의 PC, 모바일기기 등 단말기 정보 또는 서버의 IP주소 등), 수행업무(수집, 생성, 연계, 연동, 기록, 저장, 보유 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기 등) 등을 전자적으로 기록한 것을 말한다.

○ “바이오정보”란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 생성되거나 가공된 정보를 말한다.

○ “보조저장매체”란 이동형 하드디스크, USB 메모리, CD, DVD 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 용이하게 분리할 수 있는 저장매체를 말한다.

○ “고정형 영상정보처리기기”란 일정한 공간에 지속적으로 설치되어 지속적으로 또는 주기적으로 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 영 제3조제1항에 따른 폐쇄회로 텔레비전 및 네트워크 카메라를 말한다.

○ “이동형 영상정보처리기기”란 사람이 신체에 착용 또는 휴대하거나 이동 가능한 물체에 부착 또는 거치(据置)하여 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 영 제3조제2항에 따른 착용형, 휴대형, 부착·거치형, 그 밖에 이와 유사한 기능을 가지는 장치를 말한다.

○ “개인영상정보”라 함은 법 제2조제1호에 따른 개인정보 중 고정형 또는 이동형 영상정보처리기기에 의하여 촬영·처리되는 영상 형태의 개인정보 중 개인의 초상, 행동 등과 관련된 영상으로서 해당 개인을 식별할 수 있는 정보를 말한다.

○ “고정형영상정보처리기기운영자”란 법 제25조제1항 각 호에 따라 고정형 영상정보처리기기를 설치·운영하는 자를 말한다.

○ "이동형영상정보처리기기운영자"란 법 제25조의2제1항 각 호에 따라 업무를 목적으로 이동형 영상정보처리기기를 운영하는 자를 말한다.

○ "관리용 단말기"란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리시스템에 직접 접속하는 단말기를 말한다.

II 내부관리계획의 수립 및 시행

1 내부관리계획의 수립 및 승인

○ 개인정보 보호책임자는 본교의 개인정보보호를 위한 전반적인 사항을 포함하여 내부관리계획을 수립하여야 한다.

○ 개인정보 보호책임자는 개인정보보호를 위한 내부관리계획의 수립 시 개인정보보호와 관련한 법령 및 관련 규정을 준수하도록 내부관리계획을 수립하여야 한다.

○ 개인정보 보호책임자는 개인정보 보호담당자가 수립한 내부관리계획의 타당성을 검토하여 개인정보보호를 위한 내부관리계획을

개정하여야 한다.

2 내부관리계획의 공표

○ 개인정보 보호책임자는 내부관리계획을 매년 본교의 전 교직원에게 공표한다.

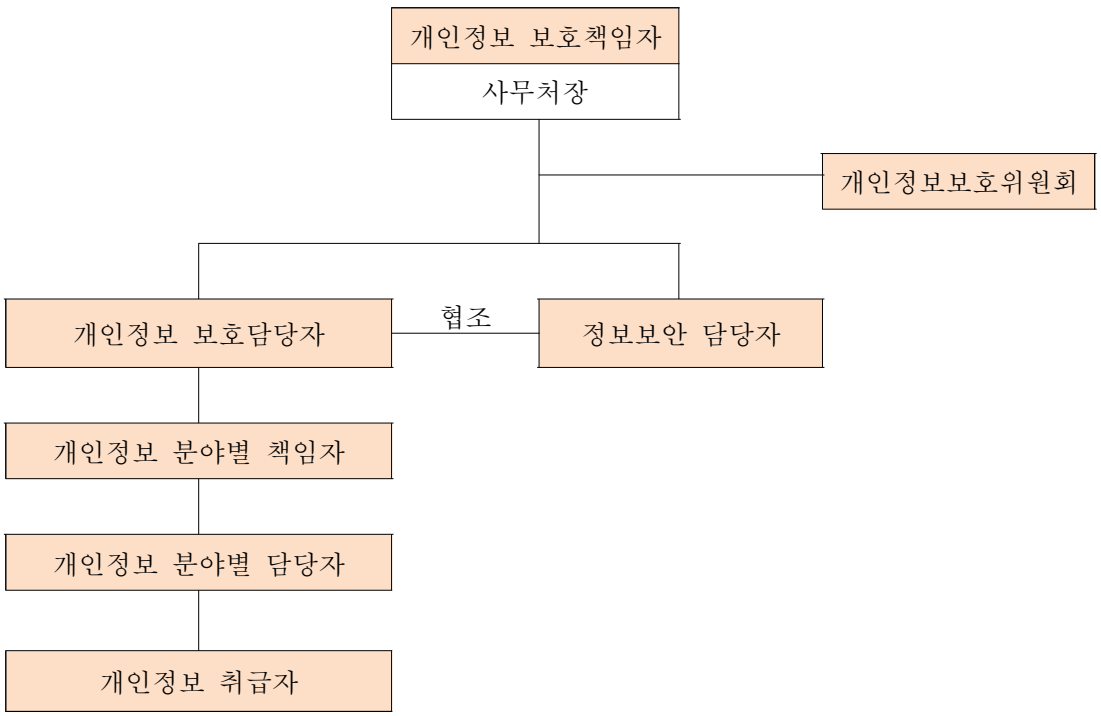
○ 내부관리계획은 교내 전 교직원이 언제든지 열람(홈페이지 게재, 유인물 배포, E-mail발송 등)할 수 있는 방법으로 비치하여야 하며, 변경사항이 있는 경우에는 이를 공지하여야 한다.

III 개인정보 보호조직 구성 및 운영

1 개인정보 보호책임자의 지정

○ 본교는 개인정보보호법 시행령 제32조제2항제1호사목에 따라 사무처장을 개인정보 보호책임자로 지정한다. (법 시행령 제2조제5호에 따른 각급 학교: 해당 학교의 행정사무를 총괄하는 사람)

2 개인정보 보호조직 구성 및 역할



구분	담당자	역할
개인정보 보호책임자	교무위원에 해당하는 행정사무 총괄하는 자 (사무처장)	-개인정보 보호 계획의 수립 및 시행 -개인정보 처리 실태 및 관행의 정기적인 조사 및 개선 -개인정보 처리와 관련한 불만의 처리 및 피해 구제 -개인정보 유출 및 오용 남용 방지를 위한 내부통제시스템의 구축 -개인정보 보호 교육 계획의 수립 및 시행 -개인정보파일의 보호 및 관리 감독 -개인정보 처리방침의 수립.변경 및 시행 -개인정보 보호 관련 자료의 관리 -처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기 등
개인정보 보호담당자	개인정보보호 책임자가 지정한 자	-개인정보보호의 계획 수립 및 운영 -개인정보 관리 실태 점검 -개인정보 교육 계획 및 실시 -개인정보 파일 대장 유지 및 관리 -개인정보보호 방침 수립 및 유지 관리 -기타 개인정보보호를 위해 필요한 사항

구분	담당자	역할
개인정보보호 분야별 책임자	개인정보를 취급하는 부서의 팀장(선임자)	-개인정보 처리 실태의 정기적인 조사 및 개선 -개인정보 처리와 관련한 불만의 처리 및 피해구제 -개인정보파일의 보호 및 관리·감독 -개인정보 처리방침의 수립·변경 및 시행 -개인정보 보호 관련 자료의 관리 -처리목적이 달성되거나 보유기간이 지난 개인정보의 파기 -그 밖에 해당부서의 개인정보 보호를 위해 필요한 사항
개인정보보호 분야별 담당자	개인정보보호 분야별 책임자가 지정한 자	-개인정보보호 기술적·관리적 보호, 법정 서식 및 대장 작성·유지 -개인정보보호 실태에 대한 자체 점검표 취합.통보
개인정보취급자	서비스 운영자 및 개인정보 접근 가능자	-개인정보보호 활동 참여 -내부관리계획의 준수 및 이행 -개인정보의 기술적·관리적 보호조치 기준 이행 -소속 직원 또는 제3자에 의한 위법.부당한 개인정보 침해행위에 대한 점검 등

Ⅳ 개인정보의 처리 및 관리

1 개인정보 보호 원칙

① 개인정보처리자는 개인정보 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.

② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활

용하여서는 아니 된다.

③ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성과 최신성을 유지하도록 하여야 하고, 개인정보를 처리하는 과정에서 고의 또는 과실로 부당하게 변경 또는 훼손되지 않도록 하여야 한다.

④ 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 그에 상응하는 적절한 관리적·기술적 및 물리적 보호조치를 통하여 개인정보를 안전하게 관리하여야 한다.

⑤ 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리가 보장될 수 있도록 합리적인 절차와 방법 등을 마련하여야 한다.

⑥ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적법하게 개인정보를 처리하는 경우에도 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.

⑦ 개인정보처리자는 개인정보를 적법하게 수집한 경우에도 익명에 의하여 업무 목적을 달성할 수 있으면 개인정보를 익명에 의하여 처리될 수 있도록 하여야 한다.

⑧ 개인정보처리자는 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다.

2 개인정보의 수집·이용

○ 개인정보는 다음의 경우에만 수집할 수 있으며, 그 수집 목적의 범위에서 이용할 수 있다.

1. 정보주체로부터 사전에 동의를 받은 경우
2. 법률에서 개인정보를 수집·이용할 수 있음을 구체적으로 명시

하거나 허용하고 있는 경우

3. 법령에서 개인정보처리자에게 구체적인 의무를 부과하고 있고, 개인정보처리자가 개인정보를 수집·이용하지 않고는 그 의무를 이행하는 것이 불가능하거나 현저히 곤란한 경우

4. 공공기관이 개인정보를 수집·이용하지 않고는 법령 등에서 정한 소관 업무를 수행하는 것이 불가능하거나 현저히 곤란한 경우

5. 개인정보를 수집·이용하지 않고는 정보주체와 체결한 계약을 이행하거나 계약을 체결하는 과정에서 정보주체의 요청에 따른 조치를 이행하기 곤란한 경우

6. 명백히 정보주체 또는 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자(정보주체를 제외한 그 밖의 모든 자를 말한다)의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우

7. 개인정보처리자가 법령 또는 정보주체와의 계약 등에 따른 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 다만, 이 경우 개인정보의 수집·이용은 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니한 경우에 한한다.

8. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우

○ 개인정보의 수집을 위하여 정보주체로부터 동의를 받는 경우 다음의 사항을 반드시 고지하여야 한다.

- 개인정보의 수집. 이용 목적
- 수집하는 개인정보의 항목
- 수집한 개인정보의 보유 및 이용 기간

- 동의를 거부할 권리가 있다는 사실
- 동의 거부에 따른 불이익이 있는 경우 그 내용

③ 개인정보파일의 등록 및 공개

○ 개인정보파일을 운용하는 기관의 분야별 담당자는 파일을 운용. 변경한 날로부터 60일 이내에 개인정보파일을 행정자치부(개인정보보호 종합지원시스템 : intra.privacy.go.kr)에 등록하고 개인정보 보호책임자 및 교육부의 승인을 받아야 한다.

○ 개인정보파일을 운용하는 기관은 등록.변경한 개인정보파일 1개에 대하여 1개의 개인정보파일대장을 작성. 관리하여야 한다

④ 개인정보의 목적 외 이용 및 제3자 제공

○ 개인정보취급자는 수집한 개인정보를 목적 외의 용도로 이용하거나 제3자에게 제공할 수 없다. 다만, 정보주체로부터 별도의 동의를 받거나 다른 법률에 특별한 규정이 있는 경우 등은 예외로 한다.

※ 제3자의 범위 : 정보주체 또는 그의 법정대리인으로부터 개인정보를 수집. 보유한 해당기관을 제외한 모든 자

○ 정보주체로부터 별도의 동의를 받아야 하는 경우 필수 고지사항
- 제공받는 자의 성명과 연락처
- 제공받는 자의 개인정보 이용 목적, 제공하는 개인정보 항목
- 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간
- 동의를 거부할 권리가 있다는 사실 및 동의 거부에 다른 불이익이 있는 경우에는 그 불이익의 내용

※ 동의를 받는 시점은 특별한 제한이 없음. 최초 수집시 미리 동의를 받아도 가능하나, 제3자 제공 및 목적 외 이용에 대한 동의를 받는 경우에는 수집. 이용에 대한 동의와 구분하여 별도의 동의를 받아야 함.

○ 개인정보를 목적 외로 이용하거나 제3자에게 제공한 기관은 반

드시 개인정보의 목적 외 이용 및 제3자 제공 대장에 기록. 관리하여야 한다.

5 개인정보 처리 위탁

○ 개인정보의 처리 업무를 위탁하는 개인정보 처리자(이하 "위탁자"라 한다)가 개인정보 처리 업무를 위탁받아 처리하는 자(이하 "수탁자"라 한다)를 선정할 때에는 인력과 물적 시설, 재정 부담능력, 기술 보유의 정도, 책임능력 등을 종합적으로 고려하여야 한다.

○ 개인정보 처리자가 개인정보의 처리 업무를 위탁하는 경우 다음의 내용이 포함된 문서에 의하여야 한다.

- 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
- 개인정보의 기술적·관리적 보호조치에 관한 사항
- 위탁업무의 목적 및 범위
- 재위탁 제한에 관한 사항
- 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
- 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항
- 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

○ 수탁자는 위탁받은 개인정보를 보호하기 위하여 행정자치부장관이 고시하는 「개인정보의 안전성 확보조치 기준」에 따른 기술적·관리적·물리적 조치를 하여야 한다.

○ 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리 현황 점검 등 수탁자가 개인정보를 안전하게 처리하는지를 관리·감독 하여야 한다.

○ 정보주체는 수탁자로부터 개인정보 처리 업무를 재위탁 받아 처리하는 자(이하 "재수탁자"라 한다)가 재위탁 받은 개인정보 처리 업무를 수행하면서 발생하는 손해에 대한 배상을 청구할 수 있다.

○ 개인정보 처리 업무의 재위탁에 대해서는 법 제26조를 준용한다.
○ 대학은 수탁기관 개인정보취급자에 대하여 개인정보가 분실, 도난, 유출, 변조 또는 훼손되지 않도록 정기적으로 교육을 실시해야 한다.
○ 개인정보 처리 업무위탁이 종료된 경우 대학은 수탁자에게 해당 개인정보를 파기하고 그 결과를 통보받아야 하며, 대학은 파기결과를 확인하여야 한다.

6 개인정보의 파기

○ 개인정보 처리자는 개인정보의 보유기간이 경과된 경우에는 정당한 사유가 없는 한 보유기간의 종료일로부터 5일 이내에, 개인정보를 파기하도록 하여야 한다.
○ 개인정보 처리자는 개인정보를 파기할 경우 다음 중 어느 하나의 조치를 하여야 한다.
- 완전파괴(소각·파쇄 등)
- 전용 소자장비를 이용하여 삭제
- 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

○ 개인정보 처리자가 개인정보의 일부만을 파기하는 경우, 완전파괴 또는 전용 소자장비를 이용하는 방법으로 파기하는 것이 어려운 때에는 다음의 조치를 하여야 한다.
- 전자적 파일 형태인 경우 : 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독
- 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 해당 부분을 마스킹, 천공 등으로 삭제

○ 개인정보 처리자는 개인정보의 파기에 관한 사항을 기록·관리하여야 한다.
○ 개인정보 파기의 시행 및 확인은 개인정보 보호책임자의 책임하에 수행되어야 하며, 개인정보 보호책임자는 개인정보 파기 시행 후 파기 결과를 확인하여야 한다. 단 분야별책임자를 지정한

경우에는 분야별책임자가 개인정보 보호책임자의 승인을 득한 후 이를 수행할 수 있다.

Ⅴ 개인정보의 기술적, 관리적 및 물리적 안전조치

1 접근권한의 관리

○ 개인정보 처리자는 개인정보처리시스템에 대한 접근권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.

○ 개인정보 처리자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하여야 한다.

○ 개인정보 처리자는 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.

○ 개인정보 처리자는 개인정보처리시스템에 접속할 수 있는 사용자 계정을 발급하는 경우 개인정보취급자 별로 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

○ 개인정보 처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다.

○ 개인정보 처리자는 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.

2 접근통제

○ 개인정보 처리자는 정보통신망을 통한 불법적인 접근 및 침해사

고 방지를 위해 다음의 기능을 포함한 조치를 하여야 한다.

- 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol) 주소 등으로 제한하여 인가받지 않은 접근을 제한
- 개인정보처리시스템에 접속한 IP(Internet Protocol)주소 등을 분석하여 불법적인 개인정보 유출 시도 탐지 및 대응

○ 개인정보 처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다.

○ 개인정보 처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치를 하여야 한다.

○ 고유식별정보를 처리하는 개인정보 처리자는 인터넷 홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점을 점검하고 필요한 보완 조치를 하여야 한다.

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

○ 개인정보 처리자가 별도의 개인정보처리시스템을 이용하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 업무용 컴퓨터 또는 모바일 기기의 운영체제(OS : Operating System)나 보안프로그램 등에서 제공하는 접근통제 기능을 이용할 수 있다.

○ 개인정보 처리자는 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.

3 개인정보의 암호화

○ 개인정보 처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

○ 개인정보 처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

○ 개인정보 처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.

○ 개인정보 처리자가 내부망에 고유식별정보를 저장하는 경우에는 다음 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.

- 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과
- 암호화 미적용시 위험도 분석에 따른 결과

○ 개인정보 처리자는 위 사항에 따라 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.

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

○ 개인정보 처리자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

4 접속기록의 보관 및 점검

○ 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 보관·관리하여야 한다. 다만, 5만명 이상의 정보주체에 관하여 개인정보를 처리하거나, 고유식별정보 또는

민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관 · 관리하여야 한다.

○ 개인정보 처리자는 개인정보의 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다.

○ 개인정보 처리자는 개인정보취급자의 접속기록이 위 · 변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.

5 악성프로그램 등 방지

○ 개인정보 처리자는 악성프로그램 등을 방지 · 치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치 · 운영하여야 하며, 다음의 사항을 준수하여야 한다.

- 보안 프로그램의 자동 업데이트 기능을 사용하거나, 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지
- 악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 즉시 이에 따른 업데이트를 실시
- 발견된 악성프로그램 등에 대해 삭제 등 대응 조치

6 관리용 단말기의 안전조치

○ 개인정보 처리자는 개인정보 유출 등 개인정보 침해사고 방지를 위하여 관리용 단말기에 대해 다음의 안전조치를 하여야 한다.

- 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치
- 본래 목적 외로 사용되지 않도록 조치
- 악성프로그램 감염 방지 등을 위한 보안

7 물리적 안전조치

○ 개인정보 처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 한다.

○ 개인정보 처리자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.

○ 개인정보 처리자는 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안대책을 마련하여야 한다. 다만, 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 이를 적용하지 아니할 수 있다.

8 재해·재난 대비 안전조치

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

○ 개인정보 처리자는 재해·재난 발생 시 개인정보처리시스템 백업 및 복구를 위한 계획을 마련하여야 한다.

9 비밀번호 관리

○ 비밀번호는 다음 사항을 반영하여 숫자와 문자, 특수문자 등을 혼합하여 9자리 이상으로 정하고, 분기 1회 이상 주기적으로 변경 사용하여야 한다.

- 사용자계정(ID)과 동일하지 않은 것
- 개인 신상 및 부서 명칭 등과 관계가 없는 것
- 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

○ 서버에 등록된 비밀번호는 암호화하여 저장하여야 한다.

○ 개인정보 처리자는 비밀번호에 적정한 기간의 유효기간(반기별 1회 이상)을 설정하여야 한다.

10 위험도 분석 및 대응

○ 개인정보 보호책임자는 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.

○ 개인정보 보호책임자는 최초 위험도 분석 이후에도 개인정보처리시스템을 증설하거나 기타 운영환경이 변경된 경우에도 지속적으로 실시하여야 한다.

Ⅵ 개인정보 침해 예방

1 개인정보 유·노출 모니터링

○ 개인정보 처리자는 교내 운영 중인 홈페이지 등에 대해 다음의 방법을 통해 개인정보 모니터링 및 노출 방지 조치를 취해야 한다.

- 직접점검, 구글 검색, 홈페이지 개인정보 노출점검 시스템 등을 활용한 개인정보 노출 상시 모니터링

- 웹 방화벽을 이용한 개인정보 노출 탐지 및 차단

○ 정보보안 담당자는 매달 '사이버·보안 진단의 날'에 본교에서 운영 중인 홈페이지 내 개인정보 노출 여부를 자체 점검(홈페이지 개인정보 노출점검 시스템, 구글 검색 이용) 하여야 한다.

2 권익침해 구제방법

○ 개인정보주체는 개인정보침해로 인한 구제를 받기 위하여 개인정보분쟁조정위원회, 한국인터넷진흥원 개인정보침해신고센터 등에 분쟁해결이나 상담 등을 신청한다. 이 밖에 기타 개인정보 침해의 신고 및 상담에 대하여는 아래의 기관에 문의한다.

- 개인정보보호 포털 : (국번없이)118
- 개인정보침해 신고센터 : (국번없이)118
- 개인정보분쟁조정위원회 : (국번없이)1833-6972
- 경찰청 사이버수사국 : (국번없이)182

VII 개인정보 유출사고 대응

1 개인정보 유출 신속 대응팀 구성

○ 본교 개인정보 유출 사고 대응 매뉴얼 - “침해사고 대응지침” (표준 개인정보 보호지침 제29조((개인정보 유출 사고 대응 매뉴얼 등))

○ 개인정보 유출 사실을 알게 된 즉시 개인정보 보호책임자는 총장에게 보고하고 개인정보 유출 신속 대응팀을 구성하여 추가유출 및 이용자 피해발생 방지를 위한 조치를 강구 하여야 한다.

2 유출 원인파악 및 유출 방지조치

○ 개인정보 유출원인을 파악한 후 추가 유출 방지를 위해 유출 원인 별 보호조치를 시행하여야 한다.

○ 해킹에 의한 사고일 경우 시스템 일시정지, 비밀번호 변경 등의 긴급조치를 시행하여야 한다.

3 개인정보 유출 신고 및 통지

○ 개인정보 유출 사실을 알게 된 즉시 교육부 사이버안전센터

(cyber.ecsc.go.kr)에 등 관계기관에 개인정보 유출 신고를 한다.

○ 정보유출 피해자에게 유출 사실을 통지하여 추가 피해가 발생하지 않도록 한다.

○ 유출 통시시기 및 항목, 유출 통지방법, 개인정보 유출신고 등은 표준 개인정보 보호지침 제26조, 제27조, 제28조에 따른다.

4 피해자 구제 및 재발방지 대책 마련

○ 유사 피해를 방지하고 유출사실을 확인 할 수 있는 전화, 이메일, SNS 등 다양한 창구를 마련하여야 한다.

○ 사고 재발방지를 위한 대책을 마련하고 정보보호 교육을 실시하여야 한다.

Ⅷ 개인정보보호 교육

1 교육목적

○ 안전하게 개인정보가 관리될 수 있도록 개인정보 보호책임자, 담당자, 취급자 각 급별 개인정보보호에 대한 인식을 제고시키고 개인정보보호 대책의 필요성을 이해시키기 위한 교육을 실시한다.

2 교육대상 : 개인정보 보호책임자, 개인정보 보호담당자, 개인정보취급자 등

3 교육실시

○ 개인정보 보호책임자는 개인정보보호에 대한 교직원들의 인식제고를 위해 노력해야 하며, 개인정보의 오·남용 또는 유출 등을 적극 예방하기 위해 교직원을 대상으로 매년 정기적으로 개인정보보호 교육을 실시한다.

○ 교육 방법은 집체 교육뿐만 아니라, 인터넷 교육, 그룹웨어 교육

등 다양한 방법을 활용하여 실시하고, 필요한 경우 외부 전문기관이나 전문요원에 위탁하여 교육을 실시한다.

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

4 개인정보보호 인력에 대한 교육 의무화

○ 개인정보 보호책임자는 개인정보 관련 전문기관 교육 및 기술 세미나 참석을 장려하는 등 개인정보 보호담당자의 업무 전문성을 제고하기 위하여 노력하여야 한다.

IX 개인정보 보호 감사(실태점검)

1 자체감사 주기 및 절차

○ 개인정보 보호책임자는 개인정보보호를 위한 내부관리계획 및 관련 법령에서 정하는 개인정보보호 규정을 성실히 이해하는지를 정기적으로 감사 또는 점검하여야 한다.

○ 개인정보 보호책임자는 개인정보 자체감사를 위한 감사대상, 감사절차 및 방법 등 감사의 실시에 필요한 별도의 계획을 수립하여 매년 1회 이상 실시할 수 있다.

2 자체감사 결과 반영

○ 개인정보 보호책임자는 개인정보보호를 위한 자체감사 실시결과 개인정보의 관리·운영상의 문제점을 발견하거나 개인정보취급자가 본 계획의 내용을 위반할 때에는 시정·개선 등 필요한 조치를 취하여야 한다.

○ 개인정보 보호책임자는 개인정보 위반사실에 대한 시정·개선 조치가 이행되지 않거나, 개인정보보호에 심각한 영향이 발생할 수 있는 우려가 되는 경우 개인정보취급자 등에 대하여 인사위원회 심의 요구 등 필요한 추가 조치를 취할 수 있다.

X 개인정보 보호 업무 추진계획

1 개인정보 보호 관련 규정 개정

○ 개인정보 내부관리계획 개정 : 개인정보보호법 및 교육부 개인정보 보호지침 개정시 변경사항 반영 및 미비점 보완

○ 개인정보 처리방침 개정 : 개인정보 처리방침에 포함되어 있는 개인정보파일, 개인정보 제3자 제공 현황, 개인정보 처리 위탁 현황 점검 결과 반영

○ 개인정보보호에 관한 규정 : 교육부 개인정보 보호지침 개정시 개정사항 반영

2 개인정보 보호 감사(실태점검)

○ 감사일정 : 연 1회 이상

○ 감사대상 : 전체 학과 및 행정부서 전수조사

○ 감사분야 : 개인정보보호, 정보보안, 일반보안 점검

※ 보안감사포함 시행

○ 감사 종료 후 결과 보고 및 보완사항 조치

3 개인정보파일 일제정비

○ 일정 : 연 1회 이상

※ 개인정보보호법 제32조(개인정보파일의 등록 및 공개) 또는 교

육부 개인정보파일 일제정비 시행 공문을 근거로 자체 진행(수시 점검)

○ 기관별 보유하고 있는 개인정파일 정보를 '개인정보종합시스템'에 등록

○ 개인정보 감사 시 개인정보파일 운영 부서 변경, 신규 등록 사항 점검 진행

4 개인정보 처리업무 위탁 시 관리·감독

○ 일정 : 매년 하반기

○ 개인정보보호법에 근거하여 매년 하반기 중 개인정보 처리업무 위탁 수탁자에 대한 관리·감독 진행

○ 개인정보 감사 시 각 부서별 위탁현황 점검(개인정보 처리위탁 계약서 확인 등)

○ 수탁자에 대한 자체 점검 후 필요시 방문 점검

5 개인정보 보호 교육

○ 추진계획

교육명	교육대상	실시주기	비고
정보보호 수준진단 지표 설명회	개인정보 보호담당자 정보보안 담당자	연 1회	
개인정보보호 교육	개인정보 보호책임자	연 1회	교육부 개인정보보호 교육(집합)
	개인정보 보호담당자	연 1회	교육부 개인정보보호 교육(집합)
	개인정보취급자(담당자)	연 1회	온라인교육
	개인정보취급자(전 교직원)	연 1회	온라인교육
정보보안 정기교육	교수, 조교, 직원	연 1회	온라인교육
정보보안 수시교육	신규 교직원	임용후 5일이내	자체 교육
정보보안 수시교육	비밀.암호자재 취급인가예정자	인사발령 시	자체 교육 총장, 사무처장, 총무팀장, 보안담당직원

6 개인정보 침해 예방

○ 추진계획

실적명	내 용	점검주기
사이버·보안 진단의 날 운영	내PC지키미'를 통해 업무용 PC의 취약점을 제거하여 개인정보보호	매월
매체제어 및 문서보안시스템 (PC FILTER)점검	이동식 매체 접근제어 및 업무용PC의 개인정보 파일을 암호화 현황 모니터링을 통해 개인정보보호	매월
개인정보 접속기록시스템 점검	개인정보 유출 방지를 위해 개인정보 접속기록 시스템 모니터링 및 개인정보 다운로드 기록 점검	매월
DB접근제어시스템 점검	데이터 유출 방지를 위해 DB접근기록을 모니터링 및 총 점검	분기 1회
DB암호화시스템 점검	DB를 암호화하여 저장된 개인정보를 보호하는 시스템 총 점검	연 1회
보안서버 구축	기간만료 인증서 갱신	연 1회
웹 방화벽 시스템점검	웹기반 시스템의 개인정보 침해 방지 시스템 총 점검	연 1회
웹필터 점검	홈페이지 등 게시판에 개인정보가 업로드되지 않는 방지시스템 총 점검	연 1회
홈페이지 보안점검	홈페이지 보안 취약점 점검 및 취약점 제거	연 1회

[별첨 1호 서식]

개인정보파일대장

기관 명칭	주소	등록부서	전화번호

등록항목	등록정보
① 개인정보파일 명칭	
② 개인정보파일의 운영 근거 및 목적	
③ 개인정보파일에 기록되는 개인정보의 항목	
④ 개인정보의 처리방법	
⑤ 개인정보의 보유기간	
⑥ 개인정보를 통상적 또는 반복적으로 제공하는 경우 그 제공받는 자	
⑦ 개인정보파일을 운용하는 기관의 명칭	
⑧ 개인정보파일로 보유하고 있는 개인정보의 정보주체 수	
⑨ 해당기관에서 개인정보 처리 관련업무를 담당하는 부서	
⑩ 개인정보의 열람 요구를 접수·처리하는 부서	
⑪ 개인정보파일에서 열람을 제한하거나 거절할 수 있는 개인정보의 범위 및 그 사유	

[별첨 제2호 서식]

개인정보의 목적 외 이용 및 제3자 제공 대장

<table>
<tr><td>개인정보 또는
개인정보파일 명칭</td><td colspan="3"></td></tr>
<tr><td>이용 또는 제공 구분</td><td colspan="3">[ ] 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
성 명
전화번호</td></tr>
<tr><td>제공받는 기관의 명칭
(제3자 제공의 경우)</td><td></td><td>성 명
소 속
전화번호</td></tr>
<tr><td>이용하거나 제공한
날짜, 주기 또는 기간</td><td colspan="3"></td></tr>
<tr><td>이용하거나 제공한
형태</td><td colspan="3"></td></tr>
<tr><td>이용 또는 제공의 법적
근거</td><td colspan="3"></td></tr>
<tr><td>이용 목적 또는
제공받는 목적</td><td colspan="3"></td></tr>
<tr><td>이용하거나 제공한
개인정보의 항목</td><td colspan="3"></td></tr>
<tr><td>「개인정보 보호법」
제18조제5항에 따라
제한을 하거나 필요한
조치를 마련할 것을
요청한 경우에는 그
내용</td><td colspan="3"></td></tr>
</table>

표준 개인정보처리위탁 계약서

표준 개인정보처리위탁 계약서(행정안전부 개인정보보호지침 별지 제 13호서식)

[별첨 제4호 서식]

개인정보파일 파기 요청서

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

[별첨 제5호 서식]

개인정보파일 파기 관리대장

번호	개인정보 파일명	자료의 종류	생성일	파기일	파기사유	처리담당자	처리부서장

[별첨 제6호 서식]

개인정보 수집·이용 동의서

[개인정보 수집•이용에 대한 동의][필수]

수집하는 개인정보 항목	*민감정보, 고유식별정보는 글씨크기 9pt 이상 다른 내용보다 20% 크게, 색깔/굵기/밑줄로 명확히 표시
개인정보의 수집 및 이용목적	
개인정보의 보유 및 이용기간	*글씨크기 9pt 이상 다른 내용보다 20% 크게, 색깔/굵기/밑줄로 명확히 표시
※ 귀하는 이에 대한 동의를 거부할 수 있으며, 다만, 동의가 없을 경우 ○○○ 진행이 불가능할 수 있음을 알려드립니다.	
개인정보 수집·이용에 동의하십니까? (해당란에 √표시)	동의함 □ 동의하지 않음 □

[고유식별정보 처리에 대한 동의][필수]

수집하는 고유식별정보 항목	
고유식별정보의 수집 및 이용목적	
고유식별정보의 보유 및 이용기간	
※ 귀하는 이에 대한 동의를 거부할 수 있으며, 다만, 동의가 없을 경우 ○○○ 진행이 불가능할 수 있음을 알려드립니다.	
고유식별정보 수집·이용에 동의하십니까? (해당란에 √표시)	동의함 □ 동의하지 않음 □

[개인정보 제3자 제공에 대한 동의][필수]

제공받는자	*글씨크기 9pt 이상 다른 내용보다 20% 크게, 색깔/굵기/밑줄로 명확히 표시
제공받는 자의 이용 목적	*글씨크기 9pt 이상 다른 내용보다 20% 크게, 색깔/굵기/밑줄로 명확히 표시
제공하는 개인정보 항목	*글씨크기 9pt 이상 다른 내용보다 20% 크게, 색깔/굵기/밑줄로 명확히 표시
제공받는 자의 보유 및 이용기간	
※ 귀하는 이에 대한 동의를 거부할 수 있으며, 다만, 동의가 없을 경우 ○○○ 진행이 불가능할 수 있음을 알려드립니다.	
개인정보 제3자 제공에 동의하십니까? (해당란에 √표시)	동의함 □ 동의하지 않음 □

※ 개인정보 제공자가 동의한 내용외의 다른 목적으로 활용하지 않으며, 제공된 개인정보를 변경하고자 할 때에는 개인정보 보호책임자를 통해 열람, 정정을 요구할 수 있음.

「개인정보보호법」 등 관련 법규에 의거하여 상기 본인은 위와 같이 개인정보 수집 및 활용에 동의함.

20 년 월 일

서 명

성 명 :

동 남 보 건 대 학 교 총 장 귀하