개인정보 내부관리계획

2020. 7

한국항공대학교
KOREA AEROSPACE UNIVERSITY

[제·개정 이력]

순 번	구 분	시행 일자	제정 · 개정 주요내용
1	제정	2018. 6. 1.	1. 내부관리계획의 목적 및 적용범위 2. 내부관리계획의 수립, 승인, 공표 3. 개인정보보호 조직의 구성과 책임자 지정 4. 개인정보보호 책임자, 분야별 책임자, 담당자, 취급자의 의무와 책임 5. 개인정보의 수집·이용 방법 및 이용·제공 제한 6. 개인정보의 기술적·관리적·물리적 안전조치 사항 7. 개인정보 처리 실태조사 및 점검 8. 개인정보보호 교육 계획의 수립 및 실시 9. 개인정보 침해 대응 방안 및 피해 구제 방법 10. 개인정보 처리업무 위탁 시 관리·감독 사항 11. 개인정보보호 사무의 인수·인계 방법
2	일부개정	2020. 7. 10.	1. 제3조의 2 : 개인정보의 처리에 생성, 연계, 연동, 기록 용어 추가 2. 제3조의 23~24 : '위험도 분석' 및 '관리용 단말기' 내용 신설 3. 제4조의 1항~3항 : 내부관리계획의 수립, 승인에 대한 최종 결재권자 총장으로 변경 4. 제6조의 2항 : 개인정보보호 조직의 설치, 변경, 폐지에 대한 최종 결재권자 총장으로 변경 5. 제7조의 3항~4항 : 개인정보보호 총괄책임관의 업무수행 및 개선조치 사항의 총장 보고 추가 6. 제20조의 3항 : 분야별 책임자의 보조저장매체의 보안대책 내용 중 예외사항 추가 7. 제37조의 4항 : 개인정보 수탁자에 대한 점검 기록 및 필요 시 보안조치 사항 추가 8. 제39조의 1항~2항 : 재해 및 재난 대비 안전조치 사항 신설

목 차

목 차

제1장 총칙

제1조(목적)

한국항공대학교 개인정보 내부관리계획은 개인정보보호법 제29조(안전조치의무) 및 같은법 시행령 제30조(개인정보의 안전성 확보 조치)에 따라 개인정보를 처리함에 있어서 개인정보가 분실, 도난, 유출, 위조, 변조, 훼손되지 아니하도록 안전성 확보에 필요한 기술적, 관리적, 물리적 안전조치에 관한 사항을 정하는 것을 목적으로 한다.

제2조(적용범위)

내부관리계획은 정보통신망을 통하여 수집, 이용, 제공 또는 관리되는 개인정보뿐 아니라 서면 등 정보통신망 이외의 수단을 통하여 수집, 이용, 제공 또는 관리되는 개인정보에 대해서도 적용되며, 이러한 개인정보를 취급하는 내부 교직원 및 개인정보 처리 업무를 위탁받아 처리하는 수탁자에게도 적용된다.

제3조(용어의 정의)

본 내부관리계획에서 사용하는 용어의 정의는 다음과 같다.

1. "개인정보"라 함은 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 개인정보를 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.<2020. 7. 10. 개정>
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. "개인정보보호 총괄책임관"이란 개인정보 처리에 관한 업무를 총괄하거나 업무처리를 최종적으로 결정하는 자로서, 개인정보 보호법 시행령 제32조 제2항에 해당하는 자를 말한다.
7. "개인정보보호 총괄담당관"이란 개인정보보호 총괄책임관을 보좌하여 개인정보보호 업무에 대한 실무를 총괄하고 관리하는 자를 말한다.
8. "개인정보보호 분야별책임자"이란 개인정보보호 관련 업무의 효율적인 관리·운용을 위한 부서의 팀, 실장을 말한다.
9. "개인정보보호 전산담당관"이란 전산책임관을 보좌하여 개인정보처리시스템에 관한 업무를 처리하는 부서의 팀장을 말한다.
10. "개인정보보호 담당자"(이하 "보호담당자"라 한다)"란 총괄담당관 및 전산담당관을 보좌하여 개인정보보호 업무에 대한 실무를 담당하는 자를 말한다.
11. "개인정보취급자"란 개인정보를 처리하는 업무를 담당하는 자로서 직접 개인정보에 관한 업무를 담당하는 자와 그 밖에 업무상 필요에 의해 개인정보에 접근하여 처리하는 모든 자를 말한다.
12. "개인정보처리시스템"란 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스 시스템을 말한다.
13. "고유식별정보"란 개인을 고유하게 구별하기 위하여 부여된 식별정보를 말하며, 대통령령으로 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호 등을 정하고 있다.
14. "접속기록"이라 함은 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무 내역에 대하여 식별자, 접속일시, 접속지를 알 수 있는 정보, 수행업무 등 접속한 사실을 전자적으로 기록한 것을 말한다.
15. "정보통신망"이란「전기통신기본법」제2조 제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집•가공•저장•검색•송신 또는 수신하는 정보통신체계를 말한다.
16. "내부망"이라 함은 물리적 망분리, 접근통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.
17. "비밀번호"라 함은 정보주체 또는 개인정보취급자 등이 개인정보

처리 시스템, 업무용컴퓨터 또는 정보통신망에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.

18. "바이오정보"라 함은 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.
19. "보조저장매체"라 함은 이동형 하드디스크(HDD), 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.
20. "모바일 기기"라 함은 무선망을 이용할 수 있는 PDA, 스마트폰, 태블릿 PC 등 개인정보처리에 이용되는 휴대용 기기를 말한다.
21. "공개된 무선망"이라 함은 불특정 다수가 무선접속장치(AP)를 통하여 인터넷을 이용할 수 있는 망을 말한다.
22. "제3자"란 정보주체와 정보주체에 관한 개인정보를 수집•보유하고 있는 개인정보처리자를 제외한 모든 자를 의미하며, 정보주체의 대리인(명백히 대리의 범위 내에 있는 것에 한함)과 법 제26조 제2항에 따른 수탁자는 제외 한다.
23. "위험도 분석"이란 개인정보 유출에 영향을 미칠수 있는 다양한 위험요소를 식별•평가하고 해당 위험요소를 적절하게 통제할 수 있는 방안 마련을 위한 종합적으로 분석하는 행위를 말한다.
    <2020. 7. 10. 개정>
24. "관리용 단말기"란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리시스템에 직접 접속하는 단말기를 말한다.
    <2020. 7. 10. 개정>

제2장 내부관리계획의 수립 및 시행

제4조(내부관리계획의 수립 및 승인)

① 개인정보보호 총괄 책임관은 한국항공대학교의 개인정보보호와 관련

한 법령 및 규정 등을 준수할 수 있도록 내부 의사결정 절차를 통하여 내부 관리계획을 수립하여야 한다.

② 개인정보보호 총괄 책임관은 내부 관리계획의 각 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부 관리계획을 수정하여야 한다.

③ 개인정보보호 총괄책임관은 제1항, 제2항에 따라 내부 관리계획을 수립하거나 수정하는 경우에는 총장으로부터 내부결재 등의 승인을 받아야 하며, 그 이력을 보관, 관리하여야 한다.<2020. 7. 10. 개정>

④ 개인정보보호 총괄책임관은 내부 관리계획의 세부 이행을 위한 각종 지침 등을 마련하여 시행할 수 있다.

⑤ 개인정보보호 총괄책임관은 연 1회 이상으로 내부 관리계획의 이행 실태를 점검•관리하고 그 결과에 따라 적절한 조치를 취하여야 한다.

제5조(내부관리계획의 공표)

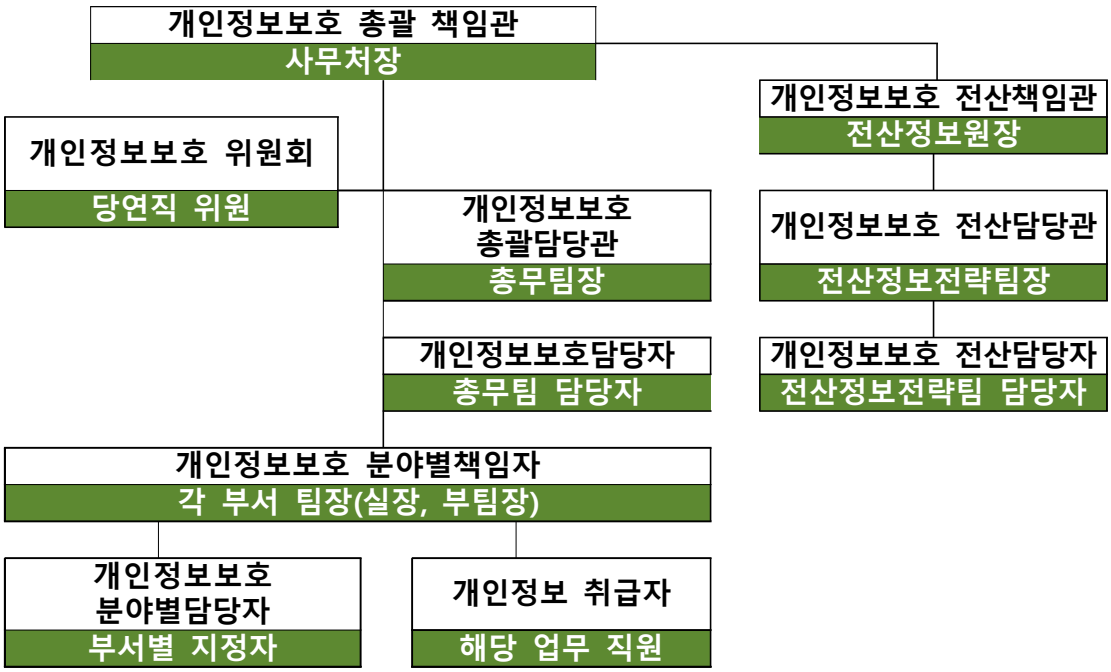
① 개인정보보호 총괄책임관은 제4조에 따라 승인된 내부관리계획을 30일 이내, 홈페이지 등을 통해 전 구성원에게 공표한다.

② 내부관리계획은 교내 전 구성원이 언제든지 열람(홈페이지 게제)할 수 있도록 하여야 하며, 변경사항이 있는 경우에는 즉시 공지하여야 한다.

제3장 개인정보보호책임자의 역할 및 책임

제6조(개인정보 보호조직 구성과 개인정보관리책임자의 지정)

① 본교의 개인정보 보호조직 구성은 아래와 같으며, 개인정보 보호법 시행령 제32조 제2항1호에 따라 해당하는 지위에 있는 사무처장을 개인정보총괄책임관(CPO : Chief Privacy Officer)으로 지정한다.



② 개인정보 보호조직의 설치, 변경 및 폐지는 총장으로부터 승인을 받아 정한다.<2020. 7. 10. 개정>

제7조(개인정보보호 책임자의 역할 및 책임)

① **개인정보보호 총괄책임관**은 개인정보보호를 위하여 다음 각 호의 업무를 수행한다.

1. 개인정보보호 계획 및 방침의 수립.시행
2. 개인정보처리실태의 점검 및 개선
3. 개인정보처리와 관련한 불만의 처리 및 피해 구제
4. 개인정보보호 교육 계획의 수립 및 시행
5. 개인정보처리방침의 수립, 변경 및 시행
6. 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기
7. 기타 정보주체의 개인정보보호를 위해 필요한 사항 등

② **개인정보보호 전산책임관**은 개인정보보호를 위하여 다음 각 호의 업무를 수행한다.

1. 개인정보 유출 및 오남용 방지를 위한 내부통제시스템 구축
2. 시스템 내 개인정보파일의 보호 및 관리 감독
3. 그 밖의 전산 관련 개인정보보호를 위하여 필요한 업무

③ 개인정보보호 총괄책임관은 제1항, 제2항의 업무를 수행함에 있어서 필요한 경우 개인정보의 처리 현황, 처리 체계 등에 대하여 수시로 조사하거나 관계

당사자로부터 보고를 받을 수 있다.<2020. 7. 10. 개정>

④ 개인정보보호 총괄책임관은 개인정보보호와 관련하여 이 법 및 다른 관계 법령의 위반 사실을 알게 된 경우에는 즉시 개선조치를 하여야 하며, 필요한 경우 총장에게 개선조치를 보고하여야 한다.<2020. 7. 10. 개정>

제8조(개인정보보호 분야별 책임자의 역할과 책임)

① **개인정보 분야별책임자**는 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. 개인정보 분야별 담당자를 지정
6. 기타 개인정보보호와 관련된 사항

제9조(개인정보보호 담당자의 역할과 책임)

① **개인정보보호담당자**는 다음 각 호의 업무를 수행한다.

1. 개인정보보호 정책 및 규정의 주기적 검토
2. 개인정보보호 교육계획 수립 및 시행
3. 상급기관 개인정보보호정책 적용 및 교육 참석
4. 개인정보 관리 실태 점검
5. 기타 개인정보보호 관련 업무 지원

제10조(개인정보취급자의 범위 및 역할과 책임)

① 개인정보취급자의 범위는 한국항공대학교 내에서 정보주체의 개인정보를 수집, 보관, 처리, 이용, 제공, 관리 또는 파기 등의 업무를 수행하는 자를 말하며 정규직 이외에 임시직, 계약직, 파견근로자를 포함한다.

② 개인정보취급자는 정보주체의 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 제3자에게 위법•부당한 개인정보 침해행위에 대한 점검
5. 열람청구, 정정•삭제, 처리정지 등 정보주체의 권리 보장
6. 기타 개인정보보호를 위해 필요한 사항의 이행 등

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

제4장 개인정보의 처리

제11조(개인정보의 수집·이용)

① 개인정보처리자는 다음 각 호의 경우에 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다.
1. 정보주체의 동의를 받은 경우
2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
3. 공공기관이 법령에서 정하는 소관업무의 수행을 위하여 불가피한 경우
4. 정보주체와의 계약의 체결 및 이행을 위하여 불가피한 경우
5. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태이거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우 (합리적 범위를 초과하지 아니하는 범위로 한정)

② 개인정보취급자는 정보주체의 개인정보를 수집하는 경우 적법하고 정당한 수단에 의하여 업무에 필요한 성명, 연락처, 주소 등 최소한의 정보를 수집하여야 한다.

③ 개인정보취급자는 개인정보 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•이용목적, 수집하는 개인정보의 항목, 보유 및 이용 기간, 동의를

거부할 권리가 있다는 사실, 동의 거부에 따른 불이익 내용 등을 알려야 한다.

제12조(개인정보의 이용·제공 제한)

① 개인정보취급자는 개인정보를 목적 외의 용도로 이용하거나 제3자에게 제공하면 아니 된다. 다만, 정보주체의 별도 동의【개인정보 관리규정 별지 제12호 서식 참조】가 있거나 다른 법률에 특별한 규정이 있는 경우 등은 예외로 한다.

② 개인정보취급자는 제3자에게 개인정보를 제공할 경우 개인정보보호법과 관련 법령 등에 제공 근거가 있는지를 검토한 후 제공여부를 판단하여야 하며, 법률적 제공 근거가 없는 경우 제공을 금지하거나 정보주체의 동의를 받아 제공하여야 한다.

③ 개인정보를 목적 외의 용도로 이용하거나 제3자에게 제공하는 경우에는 개인정보의 목적 외 이용 및 제3자 제공 대장에 기록•관리하여야 하며 30일 이내에 이용 또는 제공의 법적 근거, 목적 및 범위 등에 관한 사항을 홈페이지에 10일 이상 게재하여야 한다.

④ 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우에는 개인정보를 제공하는 자와 개인정보를 제공받는 자의 개인정보 안정성에 관한 책임관계를 명확히 하여야 한다.

⑤ 목적 외 이용 및 제3자 제공 절차

절 차	주요 내용	담당자	비 고
①	■ 개인정보의 제공 요청 접수 - 공문 등 문서로 접수 - 내용에 목적, 근거, 제공 받는 항목 등 포함 확인	개인정보 취급자	
②	■ 법률 근거 및 별도 동의 여부 확인 - 별도 동의 시 개인정보 관리규정 별표 3호를 참조하여 작성	개인정보 취급자	
③	■ 개인정보 제공 - 안전한 방법으로 최소한의 정보 제공 * 전자적 형태 : 암호 설정 등 * 종이 문서 : 정보유출이 되지 않도록 전달 - 제공받는 자에게 이용 목적, 방법, 기간, 형태 등을 제한하거나 개인정보 안전성 확보조치를 마련하도록 문서로 요청	개인정보 분야별 책임자 개인정보 취급자	
④	■ 목적 외 이용 및 제3자 제공 대장 작성 및 홈페이지에 게시(30일 이내) ※ 홈페이지 주소 (http://www.kau.ac.kr/page/privacy_protection/third_parties_available_list.jsp)	개인정보 취급자	

제5장 개인정보의 기술적·관리적·물리적 안전조치

제13조(접근권한의 관리)

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

② 전산책임관은 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 전산책임관은 개인정보처리시스템에 접속할 수 있는 사용자 계정을 발급하는 경우, 개인정보취급자 별로 한 개의 사용자 계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

제14조(비밀번호 관리)

① 개인정보처리자는 사용하는 아이디의 비밀번호를 반기별 1회 이상 변경하여야 한다.

② 전산책임관은 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 전산책임관은 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. 영문, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성
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

제15조(접근통제시스템의 설치 및 운영)

① 전산책임관은 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 시도 탐지 및 대응

② 전산책임관은 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단 또는 안전한 인증수단을 적용하여야 한다.

③ 전산책임관은 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 전산책임관은 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.(공인인증서, 휴대전화 등)

⑦ 고유식별정보를 처리하는 개인정보처리자는 인터넷홈페이지를 통해 고유식별정보가 유출•변조•훼손되지 않도록 연 1회 이상 취약점을 점검하여야 한다.

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

제16조(개인정보의 암호화)

① 전산책임관은 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 암호화

하여야 한다.

제17조(접속기록의 위·변조 방지)

① 전산책임관은 개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리하는 경우 처리일시, 처리내역 등 접속기록을 저장하도록 하여야 하며, 개인정보처리시스템에 접속한 기록을 최소 6개월 이상 보관•관리 하여야 한다.

② 전산책임관은 개인정보처리시스템의 접속기록이 위•변조 및 도난, 분실되지 않도록 안전하게 보관하여야 한다.

③ 전산책임관은 개인정보의 유출•변조•훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 반기별 1회 이상 점검하여야 한다.

제18조(보안프로그램의 설치 및 운영)

전산책임관은 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.

제19조(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

제20조(물리적 접근제한 및 관리)

① 개인정보처리자는 전산실, 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 마련하여야 한다. 다만, 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 이를 적용하지 아니할 수 있다.<2020. 7. 10. 개정>

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 있는지를 점검하여 확인하여야 한다.

제21조(출력 복사시의 보호조치)

① 분야별책임자는 개인정보가 포함된 정보를 출력하거나 복사할 경우에 개인정보 유출사고를 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 책임소재를 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.

제22조(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 3회 이상 수행

② 개인정보취급자는 보유기간 경과, 처리목적 달성 등 파기 사유가 발생한 개인정보파일을 선정하고 전자결재 또는 "개인정보파일 파기요청서"에 파기 대상 개인정보파일의 명칭, 파기방법 등을 기재하여, 개인정보보호 총괄 책임관의 승인을 받아 개인정보를 파기하여야 한다.

③ 개인정보처리자가 개인정보의 일부만을 파기하는 경우, 제1항의 방법으로 파기하는 것이 어려울 때에는 다음 각 호의 조치를 하여야 한다.

1. 전자적 파일 형태인 경우 개인정보를 삭제 후 복구 및 재생되지 않도록 관리 및 감독
2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 해당 부분을 마스킹, 천공 등으로 삭제

④ 다른 법령에 따라 개인정보를 파기하지 않고 보존해야 하는 경우 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여 저장·관리하여야 한다.

⑤ 개인정보 파기 절차

절 차	주요내용	담당자	비 고
①	■ 전자결재 또는 개인정보 파기요청서 제출 ※ 개인정보 관리규정 별지 제10호 서식 참조	개인정보 취급자	
②	■ 파기 요청 검토 및 승인•반려	개인정보보호 총괄 책임관 개인정보보호 담당자	
③	■ 승인 시 개인정보 파일 파기 실시 ■ 개인정보파일 파기 관리대장 작성 ※ 개인정보 관리규정 별지 제11호 서식 참조 ■ 개인정보파일 파기 결과 보고	개인정보 취급자	
④	■ 개인정보파일 파기 결과 확인	개인정보보호 총괄 책임관 개인정보보호 담당자	담당부서
⑤	■ 개인정보보호 종합지원시스템 등록 파일 삭제 ■ 개인정보처리방침에 공개된 개인정보파일 삭제	개인정보보호 전산 책임관	담당부서

제23조(개인정보파일 등록 사실의 삭제)

① 개인정보취급자는 제18조에 따라 개인정보파일을 파기한 경우, 개인정보파일 등록 사실에 대한 삭제를 개인정보보호 전산책임관에게 요청하여야 한다.

② 개인정보파일 등록의 삭제를 요청받은 개인정보보호 전산책임관은 그 사실을 확인하고, 지체 없이 개인정보파일을 삭제 후 그 사실을 행정안전부에 통보하여야 한다.

제24조(개인정보의 표시제한 보호조치)

개인정보 업무처리를 목적으로 개인정보의 조회, 출력 등의 업무를 수행하는 과정에서 개인정보보호를 위하여 다음과 같이 마스킹 등 표시제한 조치를 취하여야 한다.

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

제25조(개인정보의 비밀유지)

① 개인정보보호 총괄책임관은 업무 목적으로 개인정보를 취급하는 개인정보취급자를 대상으로 다음의 사항을 포함하여 개인정보보호 서약서를 작성하도록 하여야 한다.

1. 업무 중 알게 된 개인정보에 대한 비밀 준수
2. 개인정보보호를 위한 관련 법안 및 대학의 관련 규정 준수
3. 적법한 절차 없이 개인정보를 무단으로 조회, 누출하는 것의 금지
4. 위반 시 민•형사상의 책임

② 개인정보보호 총괄책임관은 대학의 개인정보취급자 이외에 개인정보의 취급 위탁 또는 제3자 제공 등의 경우에도 제1항의 개인정보에 관한 비밀유지 조항을 포함하여, 제3자 제공 금지, 사고 시 손해배상 등 개인정보보호를 위하여 필요한 사항을 포함한 개인정보처리 위탁 계약서를 작성하도록 하여야 한다.

제6장 개인정보 처리 실태조사·점검(감사)

제26조(실태조사 주기 및 절차)

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

② 실태조사는 정기 실태조사와 특별 실태조사(감사)로 구분한다.

③ 개인정보보호 총괄책임관은 연 1회의 정기 실태조사를 실시하되 학사일정 등 교내 상황을 고려하여 실태조사 범위, 시기, 방법 등을 포함한 실태조사 계획을 수립하여 사전에 공지하여야 한다.

④ 특별 실태조사는 개인정보 유출사고나 위험요소 발견 등 중요한 사안 발생 시 총장의 결재를 얻은 후 실시한다.

⑤ 개인정보보호 총괄책임관은 개인정보보호 담당자를 포함한 실태조사 조직을 구성하되 조직 구성이 여의치 않을 경우에는 외부 전문가에게 용역을 맡길 수 있다.

⑥ 개인정보보호 총괄책임관은 실태조사 결과에 대하여 결과보고서를 기록•관리하고 총장에게 보고하여야 한다.

제27조(실태조사 결과 반영)

① 개인정보보호 총괄책임관은 개인정보보호를 위한 실태조사 실시 결과 개인정보의 관리, 운영상의 문제점을 발견하거나 관련 직원이 본 계획의 내용을 위반한 때에는 시정, 개선 등의 필요한 조치를 취하여야 한다.

② 개인정보보호 총괄책임관은 개인정보보호 위반사실에 대한 시정, 개선 조치가 이행되지 않거나, 개인정보보호에 심각한 영향이 발생할 수 있는 우려가 있는 경우 총장에게 인사상의 필요한 조치를 건의할 수 있다.

제7장 개인정보보호 교육

제28조(개인정보보호 교육 계획의 수립)

① 개인정보보호 총괄책임관은 다음 각 호의 사항을 포함하는 연간 개인정보보호 교육계획을 수립하여야 한다.

1. 교육 목적 및 대상

2. 교육 내용
3. 교육 일정 및 방법

② 개인정보보호 총괄책임관은 수립한 개인정보보호 교육을 실시한 이후에 교육의 성과와 개선 필요성을 검토하여 차 년도 교육계획 수립에 반영하여야 한다.

제29조(개인정보보호 교육의 실시)

① 개인정보보호 총괄책임관은 개인정보 취급자를 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 1회 정기교육을 실시하고 필요에 따라 수시로 교육을 할 수 있다.

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

④ 개인정보보호에 중요한 전파 사례가 있거나 개인정보보호 업무와 관련하여 변경된 사항이 있는 경우, 개인정보보호 총괄책임관은 수시 교육을 실시할 수 있다.

제8장 개인정보 침해대응 및 피해구제

제30조(개인정보 유출)

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

1. 개인정보가 포함된 서면, 이동식 저장장치, 휴대용 컴퓨터를 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, 그 밖에 저장매체가 권한이 없는 자에게 잘못 전달된 경우

4. 그 밖에 권한이 없는 자에게 개인정보가 전달된 경우

제31조(통지시기 및 항목)

① 개인정보보호 총괄책임관은 개인정보가 유출되었음을 알게 되었을 때에는 정당한 사유가 없는 한 5일 이내에 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

② 개인정보보호 총괄책임관은 정보주체에게 제1항 각 호의 사항을 모두 확인하기 어려운 경우에는 정보주체에게 다음 각 호의 사실만을 우선 알리고 추후 확인되는 즉시 알릴 수 있다.

1. 정보주체에게 유출이 발생한 사실
2. 제1항의 통지항목 중 확인된 사항

③ 개인정보보호 총괄책임관은 개인정보 유출 사고의 미 인지로 인해 해당 정보주체에게 개인정보 유출통지를 하지 아니한 경우에는 실제 유출사고를 알게 된 시점을 입증하여야 한다.

제32조(통지방법)

① 개인정보보호 총괄책임관은 정보주체에게 제31조 제1항을 통지할 때에는 서면, 전자우편, 모사전송, 전화, 휴대전화 문자전송 또는 이와 유사한 방법을 통하여 5일 이내에 정보주체에게 알려야 한다.

② 개인정보보호 총괄책임관은 제1항의 통지방법과 동시에 홈페이지 등을 통하여 제31조 제1항 각호의 사항을 공개할 수 있다.

제33조(개인정보 유출신고)

① 개인정보처리자는 1명이라도 정보주체에 관한 개인정보가 유출된 경우에는 유출내용 및 조치결과를 5일 이내에 상급기관을 경유하여 교육부에 보고하여야 한다. 다만 1천명 이상의 개인정보가 유출된 경우에는 행정안전부장관 또는 한국인터넷진흥원 등 법 시행령 제39조 제2항의 전문기관으로 신고하여야 한다.

② 제1항에 따른 신고는 개인정보 유출신고서를 통하여 하여야 한다.

③ 개인정보처리자는 전자우편, 모사전송 또는 인터넷사이트를 통하여 유출 신고를 할 시간적 여유가 없거나 그 밖에 특별한 사정이 있는 때에는 먼저 전화를 통하여 제31조 제1항 각 호의 사항을 신고한 후 개인정보 유출신고서를 제출할 수 있다.

④ 개인정보처리자는 1천명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 제51조 따른 통지와 함께 인터넷 홈페이지에 정보주체가 알아보기 쉽도록 제51조 제1항 각 호의 사항을 7일 이상 게재하여야 한다.

제34조(권익침해 구제방법)

① 개인정보주체는 개인정보침해로 인한 구제를 받기 위하여 개인정보분쟁조정위원회, 한국인터넷진흥원 개인정보침해신고센터 등에 분쟁해결이나 상담 등을 신청할 수 있다.

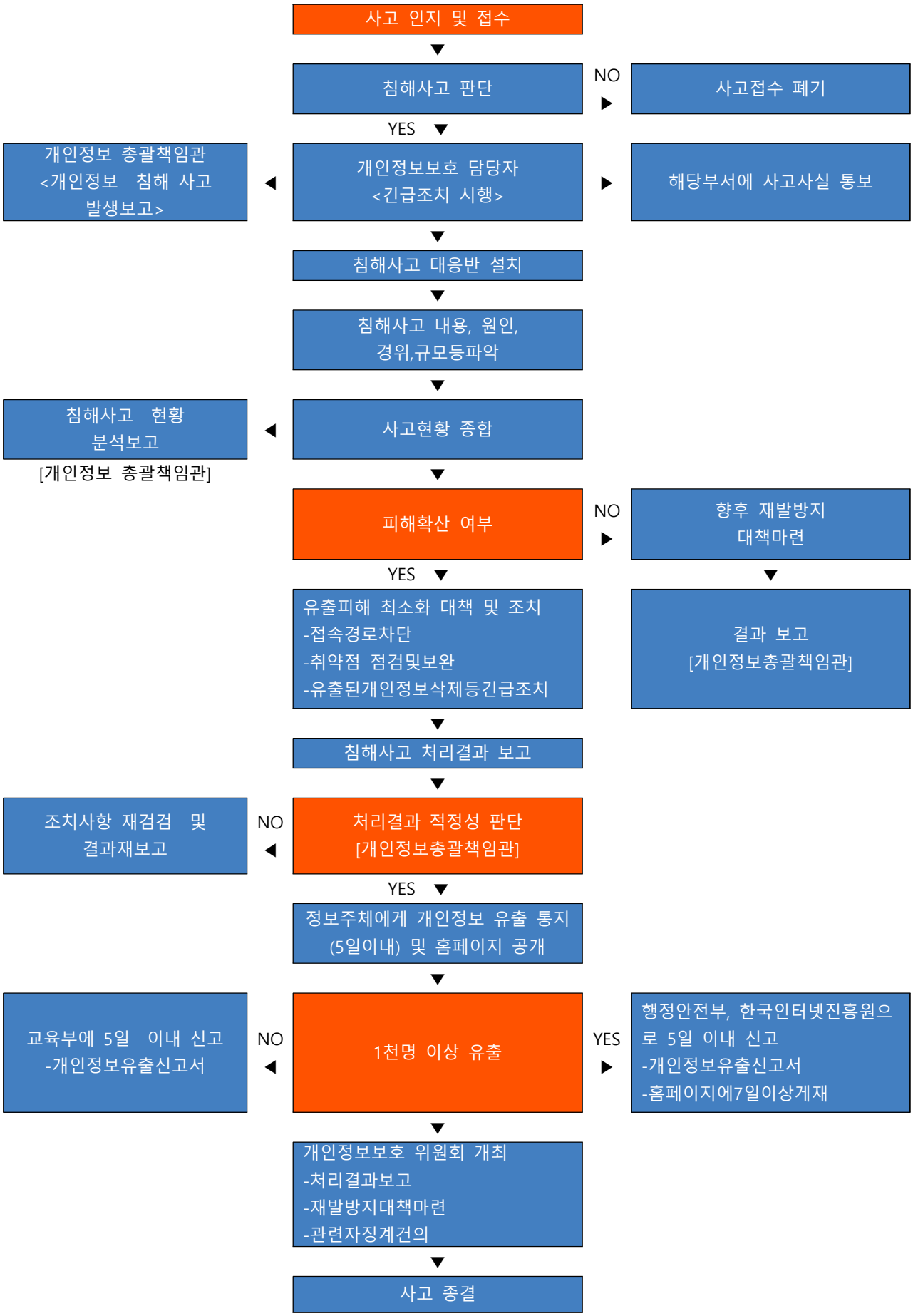
1. 개인정보분쟁 조정위원회 : 국번없이 1833-6972(www.kopico.go.kr)
2. 개인정보침해신고센터 : 국번없이 118번(privacy.kisa.or.kr)
3. 대검찰청 사이버범죄수사단 : 02-3480-3573(http://www.spo.go.kr)
4. 경찰청 사이버안전국 : 182(http://cyberbureau.police.go.kr)

제35조(위험도 분석 및 대응)

① 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 위험도 분석을 수행하고 필요한 보안조치 적용 등 대응방안을 마련하여야 한다.

② 제1항에 따른 위험도 분석은 개인정보 위험도 분석 기준을 활용하거나 위험요소를 식별 및 평가하는 등의 방법으로 수행할 수 있다.

■ 개인정보 침해사고 대응 절차



제9장 개인정보 처리업무 위탁 시 관리·감독 사항

제36조(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, 기술 보유의 정도, 책임능력 등을 고려하여야 한다.

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

제37조(위탁에 따른 개인정보 보호 조치의무)

① 개인정보처리자가 개인정보의 처리 업무를 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

② 수탁자는 위탁받은 개인정보를 보호하기 위하여 행정안전부 장관이 고시하는 "개인정보의 안전성 확보조치 기준"에 따른 기술적·관리적·물리적 조치를 하여야 한다.

③ 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·감독하여야 한다.

④ 제3항에 따른 결과에 대한 기록을 남기고 문제점이 발견된 경우에는 필요한 보안조치를 하여야 한다.<2020. 7. 10. 개정>

제38조(재 위탁에 따른 손해배상)

① 정보주체는 수탁자의 개인정보 처리 업무 및 수탁자로부터 개인정보 처리 업무를 재 위탁 받아 처리하는 자가 개인정보 처리 업무를 수행하면서 발생하는 손해에 대한 배상을 청구할 수 있다.

② 개인정보 처리 업무의 재 위탁에 대해서는 개인정보보호법 제26조를 준용한다.

제39조(재해 및 재난 대비 안전조치)

① 개인정보보호 전산책임관은 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검하여야 한다.<2020. 7. 10. 개정>

② 개인정보보호 전산책임관은 재해·재난 발생 시 개인정보처리시스템 백업 및 복구를 위한 계획을 마련하여야 한다.<2020. 7. 10. 개정>

제10장 개인정보보호 사무의 인수·인계

제40조(개인정보보호 사무의 인수·인계)

① 개인정보보호 총괄책임관 및 총괄담당관, 개인정보보호담당자의 변경 시 다음 각 호를 인수·인계 하여야 한다.

1. 개인정보보호에 관한 규정 및 지침
2. 개인정보보호 조직에 관한 사항
3. 개인정보처리시스템의 사용자 권한 설정 및 보호에 관한 사항
4. 대학의 개인정보보호 목록
5. 개인정보 내부관리계획 수립, 시행에 관한 사항
6. 기타 개인정보보호 업무에 필요한 사항

② 개인정보취급자의 변경 시 다음 각 호를 인수·인계 하여야 한다.

1. 취급하는 개인정보의 보유 목록
2. 통상적으로 이용·제공하는 개인정보에 관한 사항
3. 기타 개인정보보호 업무에 필요한 사항