김 해 대 학 교
개인정보 내부 관리계획

2024. 03.

개정 이력

버전	개정일자	소속	개인정보관리 실무자	개정내용
1.0	2012.6.20	학술정보원	문종익	신규작성(개인정보보호 계획)
2.0	2013.2.21	학술정보원	문종익	일부수정(일부항목 수정)
3.0	2014.5.19	학술정보원	문종익	일부수정(일부항목 수정)
3.1	2015.6.16	학술정보원	황명진	일부수정(일부항목 추가)
3.2	2016.4.25	교학3처	황명진	일부수정(일부항목 추가)
4.1	2018.4.05	행정지원처	김민규	일부수정(일부항목 추가)
5.0	2019.4.01	행정지원처	황보승봉	일부수정(일부항목 추가)
5.1	2019.11.26	행정지원처	황보승봉	일부수정(일부항목 추가)
6.0	2020.04.01	행정지원처	황보승봉	일부수정 1. 1의2. “가명처리” 내용 삽입 2. 일부항목 추가 3. 제19조 ~ 제28조 내용 삽입
7.0	2023.04.01	행정지원처	황보승봉	일부수정 1. 제2조 문구 수정 2. 제3조 20호, 20의2호 신규 삽입 3. 제19조(위험도 분석 및 대응 추가)
8.0	2024.02.20	행정지원처	조홍인	일부수정 1. 제10조 신규 채용자 및 전입자, 보호담당자의 교육 내용 삽입 2. 제12조 접근제한 내용 삭제 3. 제17조 문구 수정 및 부서구성 내용 삽입 4. 제18조 개인정보 유출 사고 대응 세부 내용 삽입

목 차

제1장 총칙
제1조(목적)
제2조(적용범위)
제3조(용어 정의)

제2장 내부관리계획의 수립 및 시행
제4조(내부관리계획의 수립 및 승인)
제5조(내부관리계획의 공표)

제3장 개인정보보호책임자의 의무와 책임
제6조(개인정보보호책임자의 지정)
제7조(개인정보보호책임자의 의무와 책임)
제8조(개인정보취급자의 범위 및 의무와 책임)

제4장 개인정보 보호 교육
제9조(개인정보 보호책임자의 교육)
제10조(개인정보취급자의 교육)

제5장 기술적 안전조치
제11조(접근 권한의 관리)
제12조(접근 통제)
제13조(개인정보의 암호화)
제14조(접속기록의 보관 및 점검)
제15조(악성프로그램 등 방지)
제16조(관리용 단말기의 안전조치)

제6장 관리적 안전조치
제17조(개인정보 보호조직 구성 및 운영)
제18조(개인정보 유출 사고 대응)
제19조(위험도 분석 및 대응)
제20조(수탁자에 대한 관리 및 감독)

제7장 물리적 안전조치
제21조(물리적 안전조치)
제22조(개인정보의 파기)

제8장 영상정보처리기기의 설치 및 운영·관리
제23조(영상정보처리기기 관리책임자 지정)
제24조(영상정보처리기기 운영·관리 방침)
제25조(사전의견 수렴)
제26조(안내판 설치)
제27조(개인영상정보 보호 조치)
제28조(영상정보처리기기 설치·운영 점검)

제9장 그 밖에 개인정보 보호를 위하여 필요한 사항
제29조(개인정보 목적 외 이용·제공)

제1장 총칙

제1조(목적)

김해대학교 개인정보보호 내부관리계획은 「개인정보 보호법」 제29조와 같은 법 시행령 제30조 그리고 '개인정보의 안전성 확보조치 기준'(제2020-2호)에 따라 개인정보를 처리함에 있어서 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 및 물리적 안전조치에 관한 사항을 정하는 것을 목적으로 한다.

제2조(적용범위)

김해대학교가 개인정보를 처리하거나 김해대학교의 개인정보 처리 업무를 위탁받아 처리하는 수탁자에게는 본 개인정보 내부관리계획이 적용된다.

제3조(용어 정의)

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.

1의2. "가명처리"란 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것을 말한다.

2. "처리"란 개인정보의 수집, 생성, 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 책임지거나 업무처리를 최종적으로 결정하는 자로서, 영 제32조제2항에 해당하는 자를 말한다.
7. "개인정보 보호담당자"란 개인정보책임자가 업무를 수행함에 있어 보조적인 역할을 하는 자를 말하며 개인정보보호 책임자가 일정 요건의 자격을 갖춘 이를 지정한다.
8. "개인정보취급자"란 개인정보처리자의 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.
9. "개인정보처리시스템"이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다.
10. "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.
11. "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 않

는 정보를 말한다.

12. “정보통신망”이란 「전기통신기본법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말한다.
13. “공개된 무선망”이란 불특정 다수가 무선접속장치(AP)를 통하여 인터넷을 이용할 수 있는 망을 말한다.
14. “모바일 기기”란 무선망을 이용할 수 있는 PDA, 스마트폰, 태블릿PC 등 개인정보 처리에 이용되는 휴대용 기기를 말한다.
15. “바이오정보”란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.
16. “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.
17. “내부망”이란 물리적 망분리, 접근 통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.
18. “접속기록”이란 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무내역에 대하여 개인정보취급자 등의 계정, 접속일시, 접속지 정보(접속한 자의 PC, 모바일기기 등 단말기 정보 또는 서버의 IP주소 등), 처리한 정보주체 정보, 수행업무(수집, 생성, 연계, 연동, 기록, 저장, 보유 가공, 편집, 검색 출력, 정정, 복구, 이용, 제공, 공개, 파기 등) 등을 전자적으로 기록한 것을 말한다. 이 경우 “접속”이란 개인정보처리시스템과 연결되어 데이터 송신 또는 수신이 가능한 상태를 말한다.
19. “관리용 단말기”란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리시스템에 직접 접속하는 단말기를 말한다.
20. “고정형 영상정보처리기기”란 일정한 공간에 설치되어 지속적 또는 주기적으로 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치를 말한다.

20의2. “이동형 영상정보처리기기”란 사람이 신체에 착용 또는 휴대하거나 이동 가능한 물체에 부착 또는 거치하여 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치를 말한다.

제2장(내부관리계획의 수립 및 시행)

제4조(내부관리계획의 수립 및 승인)

① 개인정보 보호책임자는 김해대학교가 개인정보 보호와 관련한 법령 및 규정 등을 준수할 수 있도록 내부 의사결정 절차를 통하여 내부 관리계획을 수립하여야 한다.

② 개인정보 보호책임자는 내부 관리계획의 각 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부 관리계획을 수정하여야 한다.

③ 개인정보 보호책임자는 제1항, 제2항에 따라 내부 관리계획을 수립하거나 수정하는 경우에는 총장으로부터 내부결재 등의 승인을 받아야 하며, 그 이력을 보관·관리하여야 한다.

④ 개인정보 처리자는 내부 관리계획의 세부 이행을 위한 각종 지침 등을 마련하여 시행할 수 있다.

⑤ 개인정보 보호책임자는 연 1회 이상으로 내부 관리계획의 이행 실태를 점검·관리 하고 그 결과에 따라 적절한 조치를 취하여야 한다.

제5조(내부관리계획의 공표)

① 개인정보보호책임자는 전조에 따라 승인한 내부관리계획을 모든 임직원 및 관련자에게 알림으로써 이를 준수하도록 하여야 한다.

② 내부관리계획은 임직원이 언제든지 열람할 수 있는 방법으로 비치하거나 제공하여야 한다.

제3장 개인정보보호책임자의 의무와 책임

제6조(개인정보보호책임자의 지정)

김해대학교는 「개인정보 보호법」제31조와 같은 법 시행령 제32조에 따라 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자를 행정지원처장으로 정한다.

제7조(개인정보보호책임자의 의무와 책임)

① 개인정보보호책임자는 정보주체의 개인정보 보호를 위하여 다음 각 호의 업무를 수행한다.

1. 개인정보 보호 계획의 수립 및 시행
2. 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
3. 개인정보 처리와 관련한 불만의 처리 및 피해 구제
4. 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
5. 개인정보 보호 교육 계획의 수립 및 시행
6. 개인정보파일의 보호 및 관리 감독
7. 법 제30조에 따른 개인정보 처리방침의 수립·변경 및 시행
8. 개인정보 보호 관련 자료의 관리
9. 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기

② 개인정보 보호책임자는 제1항의 업무를 수행함에 있어서 필요한 경우 개인정보의 처리 현황, 처리 체계 등에 대하여 수시로 조사하거나 관계 당사자로부터 보고를 받을 수 있다.

③ 개인정보 보호책임자는 개인정보 보호와 관련하여 이 법 및 다른 관계 법령의 위반 사실을 알게 된 경우에는 즉시 개선조치를 하여야 하며, 필요하면 총장에게 개선조치를 보고하여야 한다.

제8조(개인정보취급자의 범위 및 의무와 책임)

① 개인정보취급자는 김해대학교 내에서 다음 각 호의 업무를 수행하는 자를 말하며, 정규직 이외에 임시직, 파견근로자, 시간제근로자 등 포함될 수 있다.

1. 개인정보 처리
2. 개인정보 보호책임자가 위임한 개인정보보호와 관련된 업무

3. 개인정보 보호책임자에게 개인정보 파일 등록 신청
4. 개인정보(파일) 파기
5. 개인정보(파일) 파기 시 개인정보(파일)의 등록사실에 대한 삭제를 개인정보 보호책임자에게 요청
6. 개인정보보호 활동 참여
7. 내부관리계획의 준수 및 이행
8. 개인정보의 기술적·관리적 보호조치 기준 이행
9. 소속 직원 또는 제3자에 의한 위법·부당한 개인정보 침해행위에 대한 점검 등

② 개인정보취급자는 개인정보를 처리함에 있어서 개인정보가 안전하게 관리될 수 있도록 동 계획은 물론, 개인정보 보호와 관련한 법령 및 규정 등을 준수하여야 한다.

제4장 개인정보 보호 교육

제9조(개인정보 보호책임자의 교육) ① 김해대학교는 개인정보 보호책임자를 대상으로 연 1회 이상 개인정보 보호와 관련된 교육을 실시한다.

제10조(개인정보취급자의 교육) ① 개인정보 보호책임자는 개인정보의 적정한 취급을 보장하기 위하여 다음 각 호의 사항을 정하여 개인정보취급자에게 필요한 개인정보 보호 교육 계획을 수립하고 실시하여야 한다.

1. 교육 목적 및 대상
2. 교육 내용
3. 교육 일정 및 방법

② 개인정보 보호책임자는 제4장에 따라 개인정보 보호 교육을 실시한 결과 또는 이를 입증할 수 있는 관련 자료 등을 기록·보관하여야 한다.

③ 개인정보 보호책임자는 신규 채용자, 전입자에게 개인정보 보호 교육을 하여야 한다.

④ 개인정보 보호책임자는 개인정보 관련 전문기관 교육 및 기술 세미나 참석을 장려하고 신규로 지정된 개인정보 보호담당자가 신규 발령일로부터 1년 이내에 15시간 이상의 개인정보 보호 교육(정보보안 교육을 포함하되 5시간을 초과할 수 없다)을 받도록 노력하여야 한다.

제5장 기술적 안전조치

제11조(접근 권한의 관리) ① 김해대학교는 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.

② 김해대학교는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하여야 한다.

③ 김해대학교는 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.

④ 김해대학교는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자 별로 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

⑤ 김해대학교는 개인정보처리시스템, 인터넷 홈페이지 등에 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 다음 각 호의 사항을 적용하여야 한다.

1. 영대문자, 영소문자, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성
2. 연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않도록 노력
3. 비밀번호에 유효기간을 설정하여 분기별 1회 이상 변경

⑥ 김해대학교는 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.

제12조(접근통제) ① 김해대학교는 정보통신망을 통한 인가되지 않은 내·외부자의 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 조치를 하여야 한다.

1. 개인정보처리시스템에 접속한 IP(Internet Protocol)주소 등을 분석하여 불법적인 개인정보 유출 시도 탐지 및 대응

② 김해대학교는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다.

③ 김해대학교는 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.

④ 김해대학교는 고유식별정보를 처리하는 인터넷 홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연 2회 이상 취약점을 점검하고 필요한 보완 조치를 하여야 한다.

⑤ 김해대학교는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 하여야 한다.

⑥ 김해대학교에서 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 접근 통제 기능을 이용할 수 있다.

⑦ 김해대학교는 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.

제13조(개인정보의 암호화) ① 김해대학교는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

② 김해대학교는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 않도록 일방향 암호화(해쉬함수)하여 저장하여야 한다.

③ 김해대학교는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.

④ 김해대학교가 내부망에 고유식별정보를 저장하는 경우에는 암호화 하여야 한다.

⑤ 김해대학교는 제1항, 제2항, 제3항, 또는 제4항에 따라 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.

⑥ 김해대학교는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다.

⑦ 김해대학교는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

제14조(접속기록의 보관 및 점검) ① 김해대학교는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 보관·관리하여야 한다.

② 김해대학교는 개인정보의 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다.

③ 김해대학교는 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.

제15조(악성프로그램 등 방지) ① 김해대학교는 악성프로그램 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, 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지
2. 악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 즉시 이에 따른 업데이트를 실시
3. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치

제16조(관리용 단말기의 안전조치) ① 김해대학교는 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

제6장 관리적 안전조치

제17조(개인정보 보호조직 구성 및 운영) ① 김해대학교는 개인정보의 안전한 처리를 위하여 다음 각 호의 사항을 포함하는 부서를 구성하고 운영하여야 한다.

1. 개인정보 보호책임자의 지정
2. 개인정보 보호책임자의 지휘·감독 하에 개인정보 보호책임자의 업무를 지원하는 담당자의 지정
3. 개인정보를 처리하는 개인정보취급부서의 지정

② 개인정보취급부서에서는 행정지원처와 충분히 협의, 조정하여 개인정보를 처리하여야 한다.

③ 행정지원처는 제7조에 따른 업무를 수행하여야 하며, 그 밖에 개인정보의 안전성 확보를 위하여 김해대학교가 필요하다고 판단되는 사항을 수행할 수 있다.

④ 개인정보를 처리하는 부서의 구성은 다음과 같다.

구분	부서	직위	성명	내선	비고
개인정보보호 책임자	행정지원처	처장	양승철	621	CPO
개인정보보호 담당자	행정지원처	계장	황보승봉	623	
개인정보보호 담당자	행정지원처	담당	조홍인	630	
개인정보보호 취급자	전 부서 및 학과	부서장 및 학과장			

제18조(개인정보 유출 사고 대응) ① 김해대학교는 1명이라도 정보주체에 관한 개인정보의 유출등이 발생한 것을 알게 되었을 때에는 유출등 내용 및 조치결과를 72시간 내에 교육부에 신고하여야 한다. 다만 다음 각 호의 어느 하나에 해당하는 경우에는 72시간 내에 교육부 신고와 동시에 개인정보 보호위원회(이하 “보호위원회”라 한다) 또는 시행령 제40조제3항의 전문기관에 신고하여야 한다.

1. 1천명 이상의 정보주체에 관한 개인정보가 유출등이 된 경우
2. 민감정보, 고유식별정보가 유출등이 된 경우
3. 외부로부터의 불법적인 접근에 의해 개인정보가 유출등이 된 경우

② 제1항에 따른 개인정보 유출 사고 대응 계획에는 긴급조치, 유출 통지·조회 및 신고 절차, 고객 민원 대응조치, 현장 혼잡 최소화 조치, 고객불안 해소조치, 피해자 구제조치 등을 포함하여야 한다.

③ 김해대학교는 개인정보 유출에 따른 피해복구 조치 등을 수행함에 있어 정보주체의 불편과 경제적 부담을 최소화할 수 있도록 노력하여야 한다.

제19조(위험도 분석 및 대응) ① 김해대학교는 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.

제20조(수탁자에 대한 관리 및 감독) ① 김해대학교는 제3자에게 개인정보의 처리 업무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서에 의한다.

1. 위탁업무의 목적 및 범위
2. 위탁업무 기간
3. 재위탁 제한에 관한 사항
4. 위탁업무 수행 목적 외 개인정보 처리 금지에 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 김해대학교는 개인정보의 처리 업무를 위탁하는 경우 인터넷 홈페이지에 위탁하는 업무의 내용과 수탁자를 지속적으로 공개하여야 한다.

③ 김해대학교는 개인정보의 처리 업무를 위탁하는 경우 다음 각 호의 사항을 정하여 수탁자를 교육하고 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.

1. 교육 및 감독 대상
2. 교육 및 감독 내용
3. 교육 및 감독 일정, 방법

④ 김해대학교는 제3항에 따라 수탁자를 교육하고 감독한 결과에 대한 기록을 남기고 문제점이 발견된 경우에는 필요한 보안조치를 하여야 한다.

제7장 물리적 안전조치

제21조(물리적 안전조치) ① 김해대학교는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 한다.

② 김해대학교는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.

③ 김해대학교는 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안대책을 마련한다. 다만, 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 이를 적용하지 아니할 수 있다.

제22조(개인정보의 파기) ① 김해대학교는 개인정보의 보유기간 경과, 처리목적의 달성 등 보유중인 개인정보가 불필요하게 되었을 때에는 정당한 사유가 없는 한 5일 이내에 그 개인정보를 파기하며, 다음 각 호 중 어느 하나의 조치를 한다. 단,『공공기록물 관리에 관한 법률』등 다른 법령에서 보존해야 하는 경우에는 예외로 하며, 해당 개인정보는 다른 개인정보와 분리하여 관리하여야 한다.

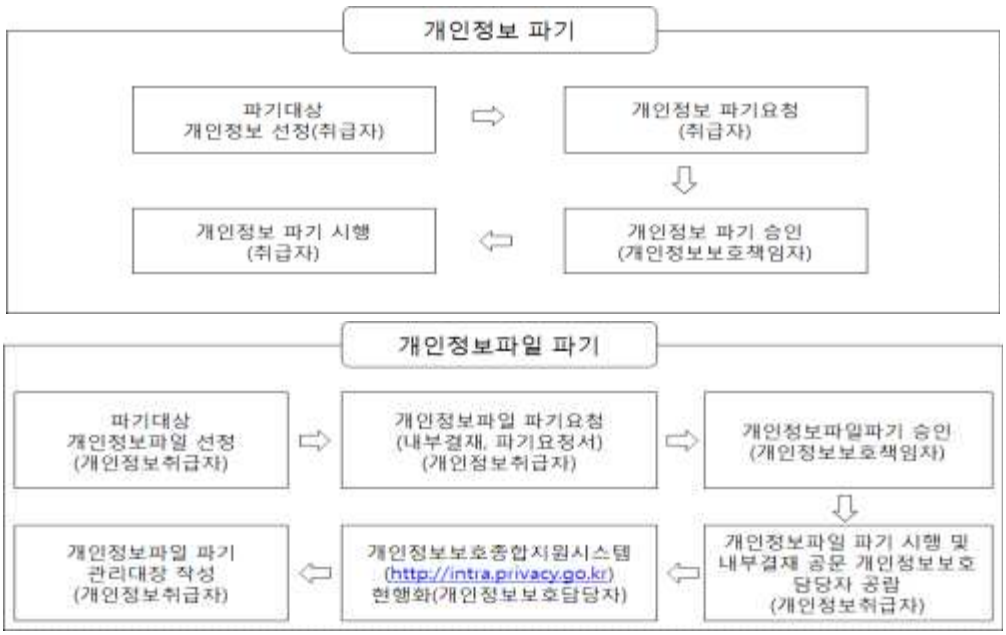
1. 완전파괴(소각·파쇄 등)
2. 전용 소자장비를 이용하여 삭제
3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

② 김해대학교는 개인정보의 일부만을 파기하는 경우, 제1항의 방법으로 파기하는 것이 어려울 때에는 다음 각 호의 조치를 하여야 한다.

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

③ 김해대학교는 개인정보 파기에 관한 사항을 기록·관리하며, 파기의 시행 및 확인은 개인정보 보호책임자의 책임하에 수행하여야 한다.

④ 개인정보(파일) 파기 절차



제8장 영상정보처리기기의 설치 및 운영·관리

제23조(영상정보처리기기 관리책임자 지정) ① 김해대학교는 교육부 개인정보 보호지침 제67조에 따라 행정지원처장을 개인영상정보 보호책임자로 지정한다.

② 제1항의 관리책임자는 법 제31조 제2항에 따른 개인정보 보호책임자의 업무에 준하여 다음 각 호의 업무를 수행하여야 한다.

1. 개인영상정보 보호 계획의 수립 및 시행
2. 개인영상정보 처리 실태 및 관행의 정기적인 조사 및 개선
3. 개인영상정보 처리와 관련한 불만의 처리 및 피해구제
4. 개인영상정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
5. 개인영상정보 보호 교육 계획 수립 및 시행
6. 개인영상정보 파일의 보호 및 파기에 대한 관리·감독
7. 그 밖에 개인영상정보의 보호를 위하여 필요한 업무

제24조(영상정보처리기기 운영·관리 방침) ① 개인영상정보 보호책임자는 영상정보처리기기 운영·관리방침을 수립하여 홈페이지 등에 공개하며, 변경하는 경우에는 정보주체가 쉽게 확인할 수 있도록 공개하여야 한다.

② 영상정보처리기기 운영 관리 방침은 법 제30조에 따라 개인정보 처리방침에 포함하여 정할 수 있다.

③ 개인영상정보 보유목적의 달성을 위한 최소한의 기간을 설정하기 곤란한 때에는 보관기간을 개인영상정보 수집 후 30일 이내로 하여야 한다.

제25조(사전의견 수렴) ① 영상정보처리기기의 설치 목적 변경에 따른 추가 설치 등의 경우에도 시행령 제23조제1항에 따라 관계 전문가 및 이해관계인의 의견을 수렴하여야 한다.

② 의견 수렴은 본교 운영위원회 등을 통해 할 수 있다.

제26조(안내판 설치) ① 개인영상정보 보호책임자는 정보주체가 영상정보처리기기가 설치·운영 중임을 쉽게 알아볼 수 있도록 다음 각 호의 사항을 기재한 안내판을 설치하여야 한다.

1. 설치목적 및 장소
2. 촬영범위 및 시간
3. 개인영상정보 관리책임자의 성명 또는 직책 및 연락처
4. 영상정보처리기기 설치·운영에 따른 사무를 위탁하는 경우 수탁자의 명칭 및 연락처

제27조(개인영상정보 보호 조치) ① 영상정보처리기기 운영자는 개인영상정보가 분실·도난·유출·변조 또는 훼손되지 않도록 다음 각 호의 조치를 취한다.

1. 영상정보처리기기의 설치 목적과 다른 목적으로 임의 조작하거나 다른 곳을 비추는 행위 금지, 녹음기능 사용 금지
2. 개인영상정보 접근통제 및 접근권한의 제한 조치
3. 개인영상정보를 안전하게 저장·전송할 수 있는 기술 적용(네트워크 카메라의 경우 암호화 전송, 개인정보영상파일의 비밀번호 설정 등)
4. 처리 기록의 보관 및 위·변조 방지를 위한 조치(개인영상정보의 이용·열람·제공·파기 시 개인영상정보 관리대장 작성 등)
5. 안전한 물리적 보관을 위한 보관시설 마련 또는 잠금장치 설치

제28조(영상정보처리기기 설치·운영 점검) ① 개인영상정보 보호책임자는 본 계획의 준수 여부에 대하여 다음 각 호의 자체점검을 실시하여야 한다.

1. 영상정보처리기기의 운영·관리 방침 내용
2. 관리책임자의 업무 수행, 위탁 및 수탁자에 대한 관리·감독 현황
3. 영상정보처리기기의 설치·운영 및 기술적·관리적·물리적 조치
4. 개인영상정보 수집 및 이용·제공·파기, 정보주체 권리행사 조치
5. 영상정보처리기기 설치·운영의 필요성 지속 여부 등

② 개인영상정보 보호책임자는 영상정보처리기기 운영 현황을 매년 개인정보보호종합지원 시스템(intra.privacy.go.kr)에 등록 · 관리하여야 한다.

제9장 그 밖에 개인정보 보호를 위하여 필요한 사항

제29조(개인정보의 목적 외 이용·제공) ① 김해대학교는 원칙적으로 개인정보를 당초 수집 목적의 범위를 초과하여 이용하거나 제공하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당되는 경우에는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다.

1. 정보주체의 별도 동의를 받은 경우
2. 다른 법률의 특별한 규정
3. 명백히 정보주체 또는 제3자의 생명, 신체, 재산의 이익에필요한경우
4. 개인정보를 목적 외 로 이용하거나 제3자에게 제공하지 않으면 다른 법률에서 정하는 소관업무 수행 불가한 경우로 보호위원회의심의·의결을 거친 경우
5. 조약, 국제협정 이행을 위해 외국 정부 등 제공에 필요한 경우
6. 범죄수사와 공소의 제기 및 유지를 위하여 필요한 경우
7. 법원의 재판업무 수행을 위하여 필요한 경우
8. 형(刑)및 감호, 보호처분의 집행을 위하여 필요한 경우

② 목적 외 이용·제3자 제공 시 절차

<table>
<tr><th>절 차</th><th>담당</th><th>주 요 내 용</th></tr>
<tr><td>1. 제공요청 접수</td><td>취급자(담당자)</td><td>- 개인정보 제공 요청은 문서로 접수</td></tr>
<tr><td>⇩</td><td></td><td></td></tr>
<tr><td>2. 법적근거 검토</td><td>취급자(담당자)</td><td>- 목적 외 이용·제3자 제공이 가능한 경우에 해당하는지 법적근거 검토</td></tr>
<tr><td>⇩</td><td></td><td></td></tr>
<tr><td>3. 동의절차 이행</td><td>취급자(담당자)</td><td>- 법적 근거가 없는 경우에는 정보주체로부터 별도의 동의를 받아야 함</td></tr>
<tr><td>⇩</td><td></td><td></td></tr>
<tr><td>4. 대장 기록·관리</td><td>취급자(담당자)</td><td>- 개인정보의 목적 외 이용 및 제3자 제공 대장(개인정보 보호법 시행규칙 [별지 제1호 서식])을 기록 · 관리하여야 함</td></tr>
<tr><td>⇩</td><td></td><td></td></tr>
<tr><td>5. 개인정보 보호 책임자 승인</td><td>개인정보 보호 책임자</td><td>- 개인정보보호 담당자 검토 후 개인정보 보호 책임자 승인 획득</td></tr>
<tr><td>⇩</td><td></td><td></td></tr>
<tr><td>6. 목적 외 이용·제공</td><td>취급자(담당자)</td><td>- 개인정보 보호 책임자 승인 후 개인정보 목적 외 이용·제3자 제공 처리
- 개인정보 보호 책임자 미승인 시 요청자에게 제공 불가 사유 통보</td></tr>
<tr><td>⇩</td><td></td><td></td></tr>
<tr><td>7. 보호조치 요구</td><td>취급자(담당자)</td><td>- 제3자 제공 시에는 이용목적, 이용방법, 이용기간, 이용형태 등을 제한하거나, 개인정보의 안전성 확보를 위하여 필요한 조치를 마련하도록 문서로 요청</td></tr>
<tr><td>⇩</td><td></td><td></td></tr>
<tr><td>8. 조치결과 제출</td><td>개인정보제공 요청자</td><td>- 안전성 확보조치 요청을 받은 자는 그에 따른 조치를 취한 후, 그 결과를 개인정보를 제공한 개인정보취급자(담당자)에게 문서로 알려야 함</td></tr>
<tr><td>⇩</td><td></td><td></td></tr>
<tr><td>9. 주요 내용 공개</td><td>취급자(담당자)</td><td>- <u>30일 이내</u>에 홈페이지 해당 게시판(또는 개인정보처리방침)에 <u>10일 이상</u> 게재
<table>
<tr><th>제공 받는자</th><th>개인정보 파일명</th><th>제공 근거</th><th>제공 항목</th><th>제공 목적</th><th>보유 기간</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>
※ 정보주체의 동의를 받았거나, 범죄의 수사와 공소의 제기 및 유지를 위하여 제공한 경우는 공개하지 않음</td></tr>
</table>