예수대학교
개인정보 내부 관리계획

2023. 05. 25.

[제·개정이력]

순 번	구 분	시행 일자	제정 · 개정 주요내용
1	제정	2012. 04. 04.	개인정보내부관리계획 제정
2	부분개정	2013. 04. 04.	개인정보내부관리계획 부분 개정
3	부분개정	2014. 03. 07.	개인정보내부관리계획 부분 개정
4	부분개정	2015. 03. 18.	개인정보내부관리계획 부분 개정
5	부분개정	2016. 04. 05.	개인정보내부관리계획 부분 개정
6	부분개정	2017. 04. 03.	개인정보내부관리계획 부분 개정
7	부분개정	2018. 03. 31.	개인정보내부관리계획 부분 개정
8	부분개정	2019. 04. 02.	개인정보내부관리계획 부분 개정
9	부분개정	2020. 04. 07.	개인정보내부관리계획 부분 개정
10	부분개정	2021. 05. 24.	개인정보내부관리계획 부분 개정
11	부분개정	2022. 05. 17.	개인정보내부관리계획 부분 개정
12	전부개정	2023. 05. 25.	개인정보내부관리계획 전부 개정

목 차

제1장 총 칙

예수대학교 개인정보에 관한 일반적인 사항은 본 내부관리계획으로 관리하며, 그 외 사항은 교육부 ‘개인정보 보호지침’을 준용한다.

제1조(목적) 예수대학교 개인정보 내부 관리계획은 「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 최소한의 기준을 정하는 것을 목적으로 한다.

제2조(용어 정의) 개인정보 내부 관리계획에서 사용하는 용어의 뜻은 다음과 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.

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, 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. “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.
10. “정보통신망”이란 「전기통신기본법」제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집・가공・

저장・검색・송신 또는 수신하는 정보통신체계를 말한다.

11. “공개된 무선망”이란 불특정 다수가 무선접속장치(AP)를 통하여 인터넷을 이용할 수 있는 망을 말한다.
12. “모바일 기기”란 무선망을 이용할 수 있는 PDA, 스마트폰, 태블릿PC 등 개인정보처리에 이용되는 휴대용 기기를 말한다.
13. “바이오정보”란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.
14. “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.
15. “내부망”이란 물리적 망분리, 접근 통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.
16. “접속기록”이란 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무내역에 대하여 개인정보 취급자 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.
17. “관리용 단말기”란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리시스템에 직접 접속하는 단말기를 말한다.

제3조(적용 범위) 예수대학교가 개인정보를 처리하거나 예수대학교의 개인정보 처리 업무를 위탁받아 처리하는 수탁자에게는 본 개인정보 내부 관리계획이 적용된다.

제2장 내부 관리계획의 수립 및 시행

제4조(내부 관리계획의 수립 및 승인) ① 개인정보 보호책임자는 개인정보 보호와 관련한 법령 및 규정 등을 준수할 수 있도록 내부 의사결정 절차를 통하여 내부 관리계획을 수립한다.

1. 개인정보보호책임자의 지정에 관한 사항
2. 개인정보보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항
3. 개인정보취급자에 대한 교육에 관한 사항
4. 접근권한의 관리에 관한 사항
5. 접근통제에 관한 사항
6. 개인정보의 암호화 조치에 관한 사항
7. 접속기록 보관 및 점검에 관한 사항

8. 악성프로그램 등 방지에 관한 사항

9. 물리적 안전조치에 관한 사항

10. 개인정보 보호조직에 관한 구성 및 운영에 관한 사항

11. 개인정보 유출사고 대응 계획 수립·시행에 관한 사항

12. 위험도 분석 및 대응방안 마련에 관한 사항

13. 재해 및 재난 대비 개인정보처리시스템의 물리적 안전조치에 관한 사항

14. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항

15. 그 밖에 개인정보 보호를 위하여 필요한 사항

② 개인정보 보호책임자는 내부 관리계획의 각 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부 관리계획을 수정하여야 하며, 그 이력을 보관·관리한다.

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

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

⑤ 개인정보 보호책임자는 연 1회 이상으로 내부 관리계획의 이행 실태를 점검·관리하고 그 결과에 따라 적절한 조치를 취한다.

⑥ [붙임1]의 유형1에 해당하는 개인정보보호책임자는 제1항에 따라 내부관리계획을 수립하지 아니할 수 있고, [붙임1]의 유형2에 해당하는 개인정보보호책임자는 제1항 제12호부터 제14호까지를 내부관리계획에 포함하지 아니할 수 있다.

⑦ 개인정보보호책임자는 예수대학교의 개인정보보호를 위한 전반적인 사항을 포함하여 내부관리계획을 수립하여야 한다.

⑧ 개인정보보호책임자는 개인정보보호를 위한 내부관리계획의 수립 시 개인정보 보호와 관련한 법령 및 관련 규정을 준수하도록 내부관리계획을 수립하여야 한다.

제5조(내부 관리계획의 공표) ① 개인정보보호책임자는 제4조에 따라 승인된 내부 관리계획을 모든 교직원 및 관련자에게 알림으로써 이를 준수하도록 한다.

② 내부 관리계획은 전 교직원 등이 언제든지 열람할 수 있는 방법으로 공개하며, 변경사항이 있는 경우에는 이를 공지한다.

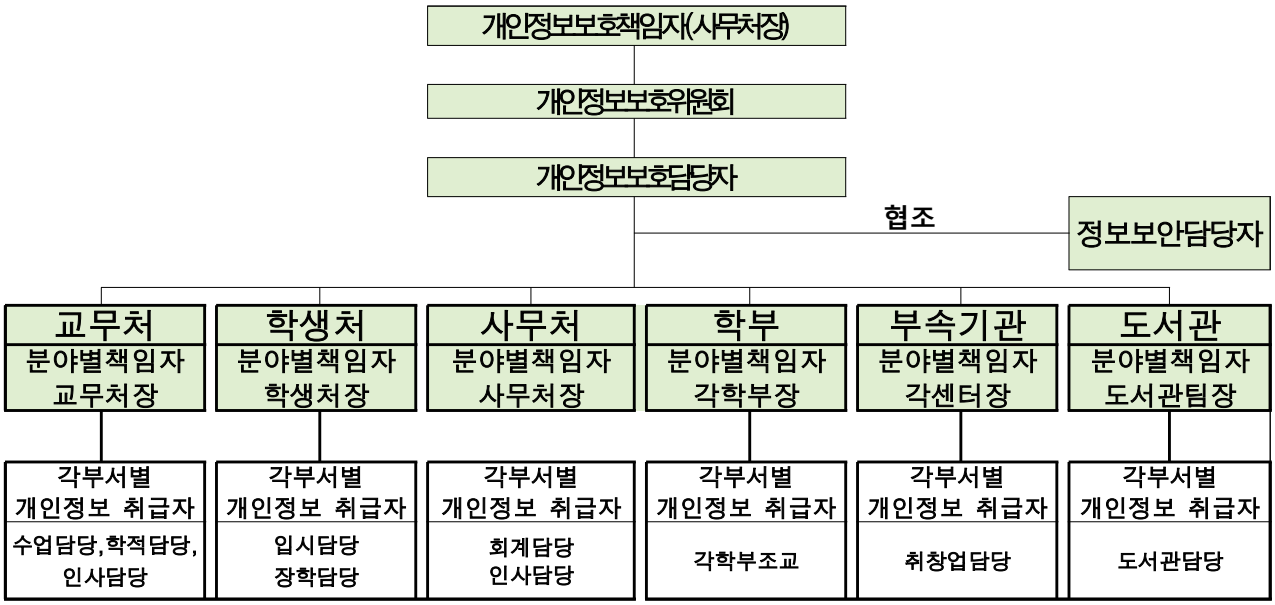
제3장 개인정보 보호책임자의 역할 및 책임

제6조 (개인정보 보호조직 구성)

① 개인정보책임자는 개인정보보호를 위하여 조직을 구성 운영한다.

② 개인정보 보호조직 구성은 아래와 같이 구성・운영 한다.

<개인정보보호 조직 구성>



제7조(개인정보보호책임자의 지정) ① 예수대학교는 「개인정보 보호법」제31조와 같은 법 시행령 제32조 및 교육부 개인정보보호지침(이하 “지침”) 제21조에 따라 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보보호책임자를 해당하는 지위에 있는 자로 정한다.

1. 해당 학교의 행정사무를 총괄하는 사람
2. 개인정보와 관련하여 고객의 고충처리를 담당하는 부서의 장

제8조(개인정보 보호책임자의 역할 및 책임) ① 개인정보보호책임자는 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. 「개인정보 보호법」제30조에 따른 개인정보 처리방침의 수립・변경 및 시행
8. 개인정보 보호 관련 자료의 관리
9. 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기

10. 그 밖에 개인정보의 적절한 처리를 위하여 대통령령으로 정한 업무

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 개선조치 한다.

④ 개인정보 보호책임자는 제3항 각 호의 업무를 수행함에 있어서 필요한 경우 개인정보의 처리 현황, 처리 체계 등에 대하여 수시로 조사하거나 관계 당사자로부터 보고를 받을 수 있다.

⑤ 개인정보 보호책임자는 개인정보 보호와 관련하여 이 법 및 다른 관계 법령의 위반 사실을 알게 된 경우에는 즉시 개선조치를 하여야 하며, 필요하면 소속 기관 또는 단체의 장에게 개선조치를 보고하여야 한다.

⑥ 개인정보처리자는 개인정보 보호책임자가 제3항 각 호의 업무를 수행함에 있어서 정당한 이유 없이 불이익을 주거나 받게 하여서는 아니 되며, 개인정보 보호책임자가 업무를 독립적으로 수행할 수 있도록 보장하여야 한다.

⑦ 개인정보처리자는 개인정보의 안전한 처리 및 보호, 정보의 교류, 그 밖에 대통령령으로 정하는 공동의 사업을 수행하기 위하여 제1항에 따른 개인정보 보호책임자를 구성원으로 하는 개인정보 보호책임자 협의회를 구성 · 운영할 수 있다.

⑧ 개인정보보호위원회는 제7항에 따른 개인정보 보호책임자 협의회의 활동에 필요한 지원을 할 수 있다.

⑨ 개인정보보호책임자는 개인정보취급자를 최소한으로 제한하여 지정하고 수시로 관리·감독하여야 하며, 직원(계약직 등 포함), 외부업체직원에 대한 교육 및 보안서약 등을 통해 개인정보 침해사고를 사전에 예방한다.

⑩ 개인정보보호책임자는 개인정보 관련 업무의 효율적 운영을 위하여 직원 중 1인 이상을 개인정보보호담당자로 임명한다.

⑪ 개인정보보호책임자는 개인정보관리에 대하여 개인정보 분야별책임자를 지정하여 관리할 수 있다.

제9조(개인정보보호담당자의 역할와 책임) ① 개인정보보호담당자는 개인정보보호책임자를 보좌하여 개인정보보호 업무에 대한 실무를 총괄하고 관리한다.

② 개인정보보호담당자는 개인정보보호를 위하여 다음 각 호의 임무를 수행한다.

1. 개인정보의 계획 수립 및 운영
2. 개인정보 관리 실태 점검
3. 개인정보 교육 계획 및 실시
4. 개인정보 파일 대장 유지 및 관리
5. 개인정보보호방침 수립 및 유지 관리

③ 개인정보보호담당자는 개인정보보호책임자의 부재 시 이를 대신하여 업무를 수행한다.

제10조(개인정보분야별책임자의 역할과 책임) ① 개인정보분야별책임자는 예수대학교 각 부서의 장 또는 이와 동등한 자격을 갖춘 자로 각부서의 장 또는 학부장을 포함하며, 부속·부설기관은 센터장이 될 수 있다.

② 개인정보분야별책임자는 정보주체의 개인정보보호와 관련하여 다음과 같은 역할 및 책임을 이행한다.

1. 개인정보파일의 보호 및 관리 · 감독
2. 개인정보취급자의 개인정보처리이력
3. 부서내 개인정보보호 취급자 지정
4. 부서 내 개인정보처리시스템 접근 권한 관리
5. 개인정보보호 서약서 청구
6. 개인정보보호 관련 보안관리 활동
7. 기타 개인정보보호책임자가 요구하는 사항처리

③ 개인정보분야별책임자는 개인정보책임자를 지원하며 각 부서의 개인정보취급자의 개인정보 업무를 관리·감독해야 한다.

제11조(개인정보취급자의 역할 및 책임) ① 개인정보취급자는 예수대학교의 지휘·감독을 받아 다음 각 호의 업무를 처리하는 자로서 모든 교직원, 계약직, 파견근로자 및 계약에 의한 개인정보 처리 위탁 외부 용역 업체 직원 등을 말한다.

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 개인정보보호책임자에게 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 준수한다.

제4장 개인정보 보호 교육

제12조(개인정보 보호책임자의 교육) ① 예수대학교는 개인정보보호책임자를 대상으로 연 1회 이상 개인정보보호와 관련된 교육을 실시한다.

제13조(개인정보취급자의 교육) ① 개인정보보호책임자는 개인정보의 적정한 취급을

보장하기 위하여 다음 각 호의 사항을 정하여 개인정보취급자에게 필요한 개인정보 보호 교육 계획을 수립하고 실시한다.

1. 교육 목적 및 대상
2. 교육 내용
3. 교육 일정 및 방법

② 개인정보 보호책임자는 제4장에 따라 개인정보 보호 교육을 실시한 결과(참석률 포함) 또는 이를 입증할 수 있는 관련 자료 등을 기록·보관한다.

제14조 (개인정보보호 교육 계획의 수립) ① 예수대학교는 개인정보보호책임자 및 개인정보취급자 를 대상으로 매년 정기적으로 개인정보보호 교육을 실시하여야 한다. 특히, 개인정보취급자가 정보주체의 개인정보를 훼손·침해·누설할 경우에는 중벌에 처해지므로, 교육 시 이러한 점을 개인정보취급자에게 인식시키기 위해 노력해야 한다.

② 개인정보보호 교육의 구체적인 사항에는 교육을 하는 목적, 교육 대상, 교육 내용 (프로그램 등 포함), 교육 일정 및 방법 등을 포함하며, 매년 교육계획은 아래와 같다.

번호	교육내용	일정	교육대상	목적
1	· 본교 개인정보처리 대응방안 · 개인정보 침해사고 대응절차 · 개인정보 유출 및 침해사고 대응 · 개인정보처리시스템 재해재난 대응 · 엑셀 취약점 등 · 개인정보 취급자의 임무 및 역할 등 · 개인정보 수집 시 주의사항 등 · 개인정보의 유노출 및 오남용 사례	동계	전 직원 (개인정보 취급자 포함)	개인정보보호
2	· 개인정보보호 워크샵 및 컨퍼런스 등	해당일	개인정보담당자	
3	· 개인정보보호 CPO 워크샵 및 컨퍼런스 등	해당일	개인정보보호책임자	

※ 일정, 장소, 내용 등은 변경 가능

제15조 (개인정보보호 교육의 실시) ① 개인정보보호책임자는 연 1회 이상 개인정보보호 교육에 참석하고, 개인정보보호담당자, 취급자 등 교육에 단순 참가하는 경우는 인정하지 않는다.

② 개인정보의 오·남용 또는 유출 등을 적극 예방하기 위해 개인정보취급자 등을 대상으로 매년 1회 이상의 개인정보보호 교육을 실시한다.

③ 교육 방법은 집합교육 뿐 아니라 조직의 환경을 고려하여 인터넷 교육, 그룹웨어 교육 등 다양한 방법을 활용하여 실시하도록 하고, 필요한 경우 외부 전문기관이나 전문요원에 위탁하여 교육을 실시할 수도 있다.

④ 개인정보보호에 대한 중요한 전파 사례가 있거나 개인정보보호 업무와 관련하여 변경된 사항이 있는 경우, 분야별책임자는 부서 회의 등을 통해 교육을 수시로 실시할 수 있다.

제5장 기술적 안전조치

제16조(접근 권한의 관리) ① 예수대학교는 개인정보처리시스템에 대한 접근권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여한다.

② 예수대학교는 개인정보처리 업무를 담당하는 구성원의 담당업무에 따라 개인정보처리권한을 부여하며, 부서별/직급별에 따라 개인정보에 대한 접근권한을 차등 부여한다.

③ 예수대학교는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근 권한을 변경 또는 말소 한다.

④ 예수대학교는 제1항 및 제2항 및 3항 및 4항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관한다.

⑤ 예수대학교는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자 별로 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 한다.

⑥ 예수대학교는 개인정보취급자가 정보통신망을 통하여 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 접속수단이나 인증수단을 적용하여야한다.

⑦ 예수대학교는 개인정보처리시스템, 인터넷 홈페이지 등에 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 다음 각 호의 사항을 적용한다.

1. 문자, 숫자의 조합·구성에 따라 최소 8자리 또는 10자리 이상의 길이로 구성

- 최소 8자리 이상 : 두 종류 이상의 문자를 이용하여 구성한 경우

※ 문자 종류 : 알파벳 대문자와 소문자, 특수문자, 숫자

- 최소 10자리 이상 : 하나의 문자종류로 구성한 경우

※ 단, 숫자로만 구성할 경우 취약할 수 있음

2. 비밀번호는 추측하거나 유추하기 어렵도록 설정

- 동일한 문자 반복(aaabbb, 123123 등), 키보드 상에서 나란히 있는 문자열(qwer 등), 일련번호(12345678 등), 가족이름, 생일, 전화번호 등은 사용하지 않음

3. 비밀번호가 제3자에게 노출되었을 경우 지체 없이 새로운비밀번호로 변경해야 함

⑧ 예수대학교는 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 한다.

제17조(접근통제) ① 예수대학교는 정보통신망을 통한 인가되지 않은 내·외부자의 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 조치를 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

3. 고유식별정보를 처리할 경우 인터넷 홈페이지를 통하여 고유식별정보 분실・도난・유출・위조・변조・훼손되지 않도록 연 1회 이상 취약점을 점검하고 취약점 발견 시 보완 조치 이행

4. 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템접속 차단 조치

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

③ 예수대학교는 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 접근통제 등에 관한 조치를 한다.

④ 예수대학교는 고유식별정보를 처리하는 인터넷 홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점을 점검하고 필요한 보완 조치를 한다.

⑤ 예수대학교는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 한다.

⑥ 예수대학교는 개인정보취급자가 생일, 주민등록번호, 전화번호 등 추측하기 쉬운 숫자나 개인관련 정보를 패스워드로 이용하지 않도록 비밀번호 작성규칙을 수립하고, 이를 적용 및 운용하여야 한다. 개인정보취급자는 예수대학교가 수립한 비밀번호 작성규칙을 준수하여야 한다.

⑦ 예수대학교에서 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.

⑧ 예수대학교는 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 한다.

제18조(개인정보의 암호화) ① 예수대학교는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체등을 통하여 전달하는 경우에는 이를 암호화한다.

② 예수대학교는 비밀번호 및 바이오정보는 암호화하여 저장한다. 다만,

비밀번호를 저장하는 경우에는 복호화되지 않도록 일방향 암호화(해쉬함수)하여

저장한다.

③ 예수대학교는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ :

Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화 한다.

④ 예수대학교가 내부망에 고유식별정보를 저장하는 경우에는 암호화 한다.

⑤ 예수대학교는 제1항, 제2항, 제3항, 또는 제4항에 따라 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장한다.

⑥ 예수대학교는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장한다.

⑦ 예수대하교는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립・시행하여야 한다.

제19조(접속기록의 보관 및 점검) ① 예수대학교는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 다음 각 호의 항목을 포함하여 최소 1년 이상 보관・관리한다. 다만, 5만명 이상의 정보주체에 관하여 개인정보를 처리하거나, 고유식별정보 또는 민감정보를 처리하는 개인정보시스템의 경우에는 2년 이상 보관·관리한다.

② 예수대학교는 개인정보의 분실・도난・유출・위조・변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검한다. 특히, 개인정보를 다운로드한 것이 발견되었을 경우에는 그 사유를 반드시 확인한다.

③ 예수대학교는 개인정보취급자의 접속기록이 위・변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관한다.

④ 예수대학교는 접속 기록의 위변조 방지를 위해 개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리(입/출력, 수정, 등 DB접근)하는 경우에는 처리일시, 처리내역 등 접속 기록을 저장한다.

제20조(악성프로그램 등 방지) ① 예수대학교는 개인용 컴퓨터(PC) 등을 이용하여 개인정보를 처리하는 경우 개인정보가 분실, 도난, 누출, 변조 또는 훼손되지 아니하도록 안전성 확보를 위한 백신 프로그램 등의 보안 프로그램을 설치·운영하여야 한다.
② 보안 프로그램은 항상 최신의 버전으로 업데이트를 적용하여야 한다.
③ 보안 프로그램의 최신 업데이트를 적용하기 위하여 자동 업데이트 설정 및 실시간 감시 기능을 적용하여야 한다.

④ 개인정보취급자는 악성 프로그램으로부터 정보주체의 개인정보가 손상·유출이 되지 않도록 업무용 컴퓨터에 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 하며, 다음 사항을 준수한다.

1. 자동 업데이트 기능을 사용하여 업데이트 실시로 최신의 상태 유지
2. 악성 프로그램 관련 경보 발령 시 또는 사용 중인 응용 프로그램이나 운영체제에 대한 보안 업데이트 공지 시 즉시 이에 따른 업데이트 실시하여야 한다.
3. 개인정보취급자는 악성프로그램 발견 시 즉시 삭제 등 대응 조치 실시하여야 한다.

제6장 관리적 안전조치

제21조(개인정보 보호조직 구성 및 운영) ① 예수대학교는 개인정보의 안전한 처리를 위하여 다음과 같이 개인정보보호 조직을 구성하고 운영한다.

<개인정보보호 조직 구성>

② 개인정보보호 조직의 설치, 변경 및 폐지는 총장으로부터 승인을 받아 정한다.

③ 개인정보취급부서에서는 개인정보보호 조직과 충분히 협의, 조정하여 개인정보를 처리한다.

④ 개인정보보호 조직은 제3장에 따른 업무를 수행하며, 그 밖에 개인정보의 안전성 확보를 위하여 필요하다고 판단되는 사항을 수행할 수 있다.

제22조(개인정보 유출 사고 대응) ① 예수대학교는 1천명 이상의 개인정보가 유출된 경우에는 법 제34조(개인정보 유출 통지 등) 제3항에 따라 행정안전부장관 또는 시행령 제39조(개인정보 유출 신고의 범위 및 기관) 제2항에 따른 한국인터넷진흥원에 신고한다. 이 경우 행정안전부장관 또는 대통령령으로 정하는 전문기관은 피해 확산 방지, 피해 복구 등을 위한 기술을 지원할 수 있다.

② 예수대학교는 개인정보의 유출 사고 발생 시 신속한 대응을 통해 피해 발생

을 최소화하기 위해 개인정보 유출 사고 대응 계획을 수립하고 시행하여야 한다.
개인정보 유출에 따른 통지의 시기, 방법 및 절차 등에 관하여 필요한 사항은 아래와 같다.
③ 또한 유출되었음을 알게 된 때에는 정당한 사유가 없는 한 5일 이내에 해당 정보주체에게 다음 각 호의 사항을 알린다. 다만, 유출된 개인정보의 확산 및 추가 유출 방지를 위한 긴급한 조치(접속경로의 차단, 취약점 점검・보완, 유출된 개인정보의 삭제 등) 필요 시 조치 후 5일 이내에 알릴 수 있다.(①유출된 개인정보의 항목, ②유출된 시점과 그 경위, ③유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보, ④본교의 대응조치 및 피해 구제절차, ⑤정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처)

④ 본교는 구체적인 유출 내용(시점 및 경위)을 확인하지 못한 경우에는 먼저 개인정보가 유출된 사실과 유출이 확인된 사항만을 서면 등의 방법으로 먼저 알리고 나중에 확인되는 사항을 추가로 알릴 수 있다.

⑤ 1천명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 서면 등의 방법과 함께 인터넷 홈페이지에 정보주체가 알아보기 쉽도록 정보를(①유출된 개인정보의 항목, ②유출된 시점과 그 경위, ③유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보, ④본교의 대응조치 및 피해 구제절차, ⑤정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처) 7일 이상 게재하여야 한다.

제7장 물리적 안전조치

제23조(물리적 안전조치) ① 예수대학교는 개인정보와 개인정보처리시스템의 안전한 보관을 위한 물리적 잠금장치 등의 물리적 접근방지를 위한 보호조치를 취하여야 한다. 예수대학교는 물리적 접근방지를 위한 별도의 보호시설에 출입하거나 개인정보를 열람하는 경우, 그 출입자에 대한 출입사실 및 열람 내용에 관한 관리대장을 작성하도록 하여야 한다.

② 예수대학교는 물리적 접근제한 관리대장의 출입 및 열람 내용을 주기적으로 검토하여 정당하지 않은 권한으로 출입하거나 열람하는 경우가 있는지를 점검하여 확인하여야 한다.

③ 예수대학교는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립・운영하여야 한다.

④ 예수대학교는 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.

제24조(관리용 단말기의 안전조치) ① 예수대학교는 개인정보 유출 등 개인정보 침해사고 방지를 위하여 관리용 단말기에 대해 다음 각 호의 안전조치를 한다.

1. 인가 받지 않은사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치
2. 본래 목적 외로 사용되지 않도록 조치
3. 악성프로그램 감염 방지 등을 위한 보안조치 적용
4. 관리용 단말기에 개인정보 저장금지 및 방치 금지

제25조(개인정보의 파기) ① 개인정보취급자는 개인정보의 보유기간 경과, 처리목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체없이 해당 개인정보를 파기하여야한다. 다만, 다른 법률에 따라 보존하여야 하는 경우에는 관련법에 따라 처리한다.

제26조(파기절차) ① 개인정보취급자는 보유기간 경과 및 처리목적을 달성한 개인정보파일은 [개인정보 파일 파기요청서(표준 개인정보 보호지침(행안부) 서식 4)] 서식에 기재하여 개인정보 보호담당자 및 개인정보보호 책임자의 승인을 받아 개인정보를 파기하고, 개인정보 파일 관리대장(표준 개인정보 보호지침(행안부) 서식 5)] 서식에 기록 관리하여야 한다. 세부적인 파기 절차는 아래에 의한다.

<개인정보 파일 파기 절차>

절차	주요내용	담당자	비고
1	– 개인정보 파일 파기 요청서 작성 및 제출 ☞ 개인정보 파일 파기 요청서” 작성 후 결재	개인정보취급자	
2	– 파기 요청 검토 및 승인 · 반려	개인정보 보호 책임자 개인정보 보호 담당자	
3	– 승인 시, 개인정보 파일 파기 실시(접속로그 기록 확인) – 개인정보파일 파기 관리대장 작성(업무 분야별 작성) ☞ “개인정보 파기 관리대장” 작성 후 결재 – 개인정보파일 파기 결과 보고	개인정보취급자	
4	– 개인정보파일 파기 결과 확인	개인정보보호 책임자 개인정보보호 담당자	담당 부서
5	– 개인정보보호위원 개인정보보호 종합 포털 파일 삭제 – 개인정보처리방침에 공개된 개인정보파일 삭제	개인정보 보호책임자	담당 부서

제27조(파기기한) ① 개인정보는 개인정보의 보유기간이 경과된 경우 그리고 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 정당한 사유가 없는 날로부터 지체없이(5일 이내)에 개인정보를 파기한다.

제28조(파기방법) ① 개인정보취급자는 종이에 출력된 개인정보는 분쇄기로 분쇄하거나 소각을 통하여 파기하고 전자적 파일 형태의 정보는 기록을 재생할 수 없는 기술적 방법을 사용하여 파기하여야 한다. 세부적인 파기 방법은 아래에 따른다.

<정보시스템 저장매체 및 자료별 파기방법>

저장매체 \ 저장자료	공개자료	민감자료 (개인정보 등)	비밀자료 (대외비 포함)
광디스크(CD, DVD 등)	㉮	㉮	㉮
자기 테이프	㉮ · ㉯중 택일	㉮ · ㉯중 택일	㉮
SSD, USB 등	㉮	㉮	㉮
하드디스크	㉰	㉮ · ㉯ · ㉰중 택일	㉮ · ㉯중 택일

㉮ 완전파괴(소각・파쇄・용해)

㉯ 전용 소자(소자)장비 이용 저장자료 삭제

㉰ 완전포맷 3회 수행

㉱ 완전포맷 1회 수행

② 개인정보취급자가 개인정보의 일부만을 파기하는 경우, 제1항의 방법으로 파기하는 것이 어려울 때에는 다음 각 호의 조치를 취한다.

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

제9장 그 밖에 개인정보 보호를 위하여 필요한 사항

제29조(개인정보의 위탁)

① 위탁과 제3자 제공의 구분

구분	개인정보처리위탁	제3자 제공
관련조항	법 제26조	법 제17조
이전목적	위탁자의 이익을 위하여 처리(수탁업무 처리)	제3자의 이익을 위하여 처리
예측가능성	정보주체가 사전 예측 가능	정보주체가 사전 예측 곤란
이전 방법	■ 원칙 : 위탁사실 공개 ■ 예외 : 위탁사실 고지	■ 원칙 : 제공목적 등 고지 후 정보주체 동의획득
관리・감독책임	위탁자 책임(사용자 책임)	제공받는 자 책임
손해배상책임	위탁자 부담(사용자 책임)	제공받는 자 부담

② 개인정보 처리업무 위탁 시 의무사항

1. 문서(계약서)로 작성하며 하단의 내용들이 포함되어야 함

- 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
- 개인정보의 관리적·기술적·물리적 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

※ '표준 개인정보처리위탁 계약서' 양식 (별지 제1호 서식) 작성으로 갈음 할 수 있음

2. 해당 사실에 대하여 정보주체가 확인하기 쉽도록 공개
   - 위반 시 3천만 원 이하 과태료
   - 알려야 할 내용

위탁하는 업무의 내용, 개인정보 처리업무를 위탁받은 처리자

   - 관보 또는 인터넷 홈페이지에 게재하거나 그 밖에 이와 유사한 방법으로 공개하여야 함.
3. 재화 또는 서비스를 홍보하거나 판매를 권유할 목적으로 위탁하는 경우, 정보주체에게 개별고지
4. 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하기 위한 수탁자 교육, 처리현황 점검 등 개인정보의 안전한 처리 에 대한 감독 실시
   - 수탁업체의 대표자와 직원들에게 보안서약서 징구

   ※ '보안 서약서(업체 대표용)', '보안 서약서' 양식 (별지 제2,3호 서식) 참고
   - 개인정보의 안전 관리에 관하여 수탁자 교육('개인정보보호 종합포털(privacy.go.kr) > 배움터 > 사이버 교육'에서 제공하는 모든 교육 수강하고 수료증 스캔본 징구)
   - 수탁자가 개인정보를 안전하게 처리하는지 감독(개인정보의 처리현황, 개인정보파일 접근대상자 및 접속 현황 등에 관한 사항을 기록·관리토록하고 실태점검 하여야 함 - 향후 세부 기준 고시)
5. 위탁받은 개인정보 처리 업무 범위를 초과한 개인정보의 이용 또는 제3자 제공의 금지(위반 시 5년 이하 징역 또는 5천만원이하 벌금)

제30조(개인정보 수집 및 이용.제공) ① 개인정보 수집 시 법적 근거 또는 정보주체의 동의를 받아야 하며, 정보주체에게 문서 또는 홈페이지 등을 통하여 다음의 내용을 알려야 함.

개인정보의 수집 · 이용 목적, 수집하려는 개인정보의 항목, 개인정보 보유 및 이용기간, 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익 내용

② 수집한 개인정보는 수집 목적의 범위에서 이용할 수 있음.

③ 개인정보의 목적 외 이용 혹은 제3자 제공이 가능한 경우

1. 정보주체의 별도 동의를 받은 경우
2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피 한 경우
3. 공공기관이 법령 등에서 정하는 소관 업무를 수행하기 위하여 불가피 한 경우
4. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우

④ 정보주체의 동의를 받는 경우, 정보주체에게 반드시 알려야 할 사항

(위반할 때 3천만 원 이하 과태료)

1. 개인정보를 제공 받는 자
2. 개인정보를 제공 받는 자의 이용 목적
3. 제공하는 개인정보의 항목
4. 개인정보를 제공받은 자의 개인정보 보유 및 이용기간
5. 동의를 거부할 권리가 있다는 사실 및 동의거부에 따른 불이익 내용

⑤ 개인정보의 처리 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 하고 각종 서식에 대해서 개인정보 기재항목이 반드시 필요한지 검토하고 업무 수행에 필요없는 개인정보는 다른정보로 변경하거나 삭제하여야 한다.

⑥ 개인정보의 보유 및 이용기간은 수집 · 이용 목적에 맞게 관련 법령에 근거하여 최소한으로 책정하며, 관련법령 근거가 없을 시 기관장이 승인하는 기간으로 한다.

⑦ 개인정보를 수집 시에는 필수정보, 고유식별정보, 선택정보, 민감정보 등을 분리 구분해서 동의를 받아야 하며 각 정보의 수집거부에 따른 불이익을 명시해야 한다.

⑧ 분야별 보호책임자는 만14세 미만 아동의 개인정보를 처리하기 위하여 동의를 받아야할 때에는 그 법정대리인의 동의를 받아야 한다.

⑨ 개인정보 위탁 및 제 3자 제공시에는 정보주체의 동의를 받아야 하며, 개인정보를 제공받는 자에게 이용 목적, 이용 방법, 그 밖에 필요한 사항에 대하여 제한을 하거나, 개인정보의 안전성 확보를 위하여 필요한 조치를 마련하도록 요청하여야 한다.

⑩ 개인정보를 수집 시에는 개인정보처리자는 정보주체가 선택적으로 동의할 수 있는 사항을 동의하지 아니하거나, 목적 외 제공에 대한 동의를 하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 아니 된다.

⑪ 개인정보처리자가 정보주체로부터 법 제18조 제2항 제1호 및 제22조 제4항에 따른 동의를 받거나 법 제22조 제3항에 따라 선택적으로 동의할 수 있는 사항에 대한 동의를 받으려는 때에는 정보주체가 동의 여부를 선택할 수 있다는 사실을 명확하게

확인할 수 있도록 선택적으로 동의할 수 있는 사항 외의 사항과 구분하여 표시하여야 한다.

⑫ 개인정보처리자는 제1항의 동의를 서면(「전자문서 및 전자거래 기본법」 제2조제1호에따른 전자문서를 포함한다)으로 받을 때에는 다음 각 호에서 정하는 중요한 내용에 대하여 정하는 방법에 따라 명확히 표시하여 알아보기 쉽게 하여야 한다.

1. 개인정보의 수집·이용 목적 중 재화나 서비스의 홍보 또는 판매 권유 등을 위하여 해당 개인정보를 이용하여 정보주체에게 연락할 수 있다는 사실
2. 처리하려는 개인정보의 항목 중 다음 각 목의 사항
   가. 시행령 제18조에 따른 민감정보
   나. 시행령 제19조제2호부터 제4호까지의 규정에 따른 여권번호, 운전면허의 면허번호 및 외국인등록번호
3. 개인정보의 보유 및 이용 기간(제공 시에는 제공받는 자의 보유 및 이용 기간)
4. 개인정보를 제공받는 자 및 개인정보를 제공받는 자의 개인정보 이용 목적

⑬ 개인정보처리자는 서면 동의 시 중요한 내용의 표시 방법은 다음 각 호의 방법을 말한다.

1. 글씨의 크기는 최소한 9포인트 이상으로서 다른 내용보다 20퍼센트 이상 크게 하여 알아보기 쉽게 할 것
2. 글씨의 색깔, 굵기 또는 밑줄 등을 통하여 그 내용이 명확히 표시되도록 할 것
3. 동의 사항이 많아 중요한 내용이 명확히 구분되기 어려운 경우에는 중요한 내용이 쉽게 확인될 수 있도록 그 밖의 내용과 별도로 구분하여 표시할 것

⑭ 개인정보의 목적 외 이용 혹은 제3자 제공 시 의무사항

1. 분야별 보호책임자는 다음 각 호중 어느 하나에 해당되는 경우에는 정보주체의 개인정보를 제3자에게 제공할 수 있다.
   가. 정보주체로부터 사전에 별도의 동의를 받은 경우
   나. 법률에서 구체적으로 명시하거나 허용하고 있는 경우
   다. 개인정보를 수집, 이용하지 않고는 법령 등에서 정한 소관업무 수행이 불가능하거나 현저히 곤란한 경우
   라. 정보주체 또는 제3자의 생명, 신체, 재산에 대한 피해를 방지해야할 급박한 상황에서 정보주체 또는 법정대리인이 의사표시를 할 수 없는 상태에 있거나 연락을 취할 수 없어 사전 동의를 받을 수 없는 경우
2. 수집한 개인정보를 제3자에게 제공하고자 할 때는 경우 각 호에 맞게 처리해야 한다.
   가. 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우에는 개인정보를 제공받는 자에게 이용 목적, 이용 방법, 이용 기간, 이용 형태 등을 제한하거나, 개인정보의 안전성 확보를 위하여 필요한 구체적인 조치를 마련하도록 문서(전자문서를 포함한다. 이하 같다)로 요청하여야 한다. 이 경우 요청을 받은 제3자는 그에 따른 조치를 취하고 그 사실을 개인정보를 제공한 소속기관에

문서로 알려야 한다.

나. 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우, 개인정보를 제공하는 소속기관과 개인정보를 제공받는 자는 개인정보의 안전성에 관한 책임 관계를 명확히 정하여야 한다.

다. 개인정보를 목적 외의 용도로 이용하거나 목적 외의 용도로 제3자에게 제공하는 경우에는 다음 각 호의 사항을 '별지 4호서식 개인정보의 목적 외 이용 및 제3자 제공 대장' 에 기록하고 관리하여야 한다.

3. 정보주체의 동의 없이 개인정보를 목적 외의 용도로 이용하거나 목적 외의 용도로 제3자에게 제공하는 경우에는, 다음 각 호의 사항을 목적 외 이용 등을 한 날부터 30일 이내에 인터넷 홈페이지에 10일 이상 계속 게재하여야 한다.

가. 이용 또는 제공의 일자

나. 이용 또는 제공의 법적 근거

다. 이용 또는 제공의 목적

라. 이용 또는 제공하는 개인정보의 항목

제31조(고유식별정보의 처리 제한) ① 개인정보처리자는 개인정보 고유식별정보를 법 제24조에 따라 개인정보파일별로 처리현황을 파악하여 년1회 이상 조사하고 개인정보보호책임자에게 보고한다.

② 고유식별정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 암호화 등 안전성확보에 필요한 조치를 한다.

제32조(자체감사 주기 및 절차) ① 개인정보보호책임자는 개인정보보호를 위한 내부관리 계획 및 관련 법령에서 정하는 개인정보보호 규정을 성실히 이행하는지를 정기적으로 감사 또는 점검하여야 한다.

② 개인정보보호책임자는 개인정보 자체감사를 위한 감사대상, 감사절차 및 방법 등 감사 실시에 관하여 필요한 별도의 계획을 수립할 수 있다.

③ 개인정보보호 자체감사는 최소 년 1회 이상 실시한다.

제33조(자체감사 결과 반영) ① 개인정보보호책임자는 개인정보 보호를 위한 자체감사 실시 결과, 개인정보의 관리·운영상의 문제점을 발견하거나 관련 직원이 본 계획의 내용을 위반할 때에는 시정·개선 등 필요한 조치를 취하여야 한다.

② 개인정보보호책임자는 개인정보 위반사실에 대한 시정·개선 조치가 이행되지 않거나, 개인정보보호에 심각한 영향이 발생할 수 있는 우려가 되는 경우 개인정보 취급자 등에 대한 인사발령 등의 필요한 추가 조치를 취할 수 있다.

[붙임1]

개인정보처리자 유형 및 개인정보 보유량에 따른 안전조치 기준

유형	적용 대상	안전성 확보 조치 기준	교육부 개인정보보호 지침
유형2 (표준)	.100만명 미만의 정보주체에 관한 개인정보를 보유한 중소기업 .10만명 미만의 정보주체에 관한 개인정보를 보유한 대기업, 중견기업, 공공기관 .1만명 이상의 정보주체에 관한 개인정보를 보유한 소상공인, 단체, 개인	· 제4조 : 제1항제1호부터 제11호까지 및 제 15호, 제3항부터 제4항까지 · 제5조 · 제6조 : 제1항부터 제7항까지 · 제7조 : 제1항부터 제5항까지, 제7항 · 제8조 · 제9조 · 제10조 · 제11조 · 제13조	· 제35조 : 제1항제1호부터 제11호 및 제15호, 제3항부터 제4항까지 · 제37조~제38조 · 제39조 : 제1항부터 제7항까지 · 제40조 : 제1항부터 제5항까지, 제7항 · 제41조 · 제42조 · 제39조 : 8항 · 제43조 · 제10조 : 제2항, 제3항
유형3 (강화)	.10만명 이상의 정보주체에 관한 개인정보를 보유한 대기업, 중견기업, 공공기관 .100만명 이상의 정보주체에 관한 개인정보를 보유한 중소기업, 단체	· 제4조 · 제5조 · 제6조 · 제7조 · 제8조 · 제9조 · 제10조 · 제11조 · 제12조 · 제13조	· 제35조 · 제37조~제38조 · 제39조 : 제1항부터 제7항까지 · 제40조 · 제41조 · 제42조 · 제39조 : 제8항 · 제43조 · 제31조 : 제2항, 제3항, 제4항 · 제10조 : 제2항, 제3항

[붙임2]

개인정보 처리단계별 준수사항 및 위반 시 벌칙사항

구분	주요내용	처벌 및 벌칙
수집·이용	민감정보(사상·신념·정당가입·건강 등) 처리기준 위반(제23조)	5년 이하 징역 또는 5천만원 이하 벌금
	고유식별정보(주민등록·여권·운전면허 번호 등) 처리기준 위반(제24조)	
	부당한 수단이나 방법에 의해 개인정보를 취득하거나 개인정보처리에 관한 동의를 얻는 행위를 한자(제59조)	3년 이하 징역 또는 3천만원 이하 벌금
	개인정보의 수집기준 위반(제15조)	5천만원 이하 과태료
	만14세 미만 아동의 개인정보 수집시 법정대리인 동의획득여부 위반(제22조)	
	탈의실·목욕실 등 영상정보처리기기 설치 금지 위반(제25조)	
	최소한의 개인정보 외 정보의 미동의를 이유로 재화 또는 서비스 제공을 거부한 자(제16조, 제22조)	3천만원 이하 과태료
	주민등록번호를 제공하지 아니할 수 있는 방법 미제공(제21조)	
	동의획득방법 위반하여 동의받은 자(제22조)	1천만원 이하 과태료
제공·위탁	정보주체의 동의 없는 개인정보 제3자 제공(17조)	5년 이하 징역 또는 5천만원 이하 벌금
	개인정보의 목적 외 이용·제공(제18조, 제19조, 제26조)	
	개인정보 주체에게 알려야 할 사항을 알리지 아니한 자(제15조, 제17조, 제18조, 제26조)	3천만원 이하 과태료
	업무위탁 시 공개의무 위반(제26조)	1천만원 이하 과태료
개인정보 안전관리	개인정보의 누설 또는 타인 이용에 제공(제59조)	5년 이하 징역 또는 5천만원 이하 벌금
	개인정보의 훼손, 멸실, 변경, 위조, 유출(제59조)	
	영상정보처리기기 설치목적과 다른 목적으로 임의 조작하거나 다른곳을 비추는 자 또는 녹음기능을 사용한 자(제25조)	3년 이하 징역 또는 3천만원 이하 벌금
	직무상 알게 된 비밀을 누설하거나 직무상 목적 외 사용한 자(제60조)	
	안전성 확보에 필요한 보호조치를 취하지 않아 개인정보를 도난·유출·변조 또는 훼손당하거나 분실한 자(제24조, 제25조, 제29조)	2년 이하 징역 또는 1천만원 이하 벌금
	안전성 확보에 필요한 조치의무 불이행(제24조, 제25조, 제29조)	3천만원 이하 과태료
	영상정보처리기기 설치·운영기준 위반(제25조)	
	개인정보를 분리해서 저장·관리하지 아니한 자(제21조)	1천만원 이하 과태료
	개인정보처리방침 미공개(제30조)	
	개인정보관리책임자 미지정(제31조)	
	영상정보처리기기 안내판 설치 등 필요조치 불이행(제25조)	
정보주체 권익보호	개인정보의 정정·삭제요청에 대한 필요한 조치를 취하지 않고, 개인정보를 계속 이용하거나 제2자에게 제공한 자(제36조)	2년 이하 징역 또는 1천만원 이하 벌금
	개인정보의 처리정지 요구에 따라 처리를 중단하지 않고 계속 이용하거나 제3자에게 제공한 자(제37조)	
	개인정보 유출사실 미통지(제34조)	3천만원 이하 과태료
	정보주체의 열람 요구의 부당한 제한·거절(제35조)	1천만원 이하 과태료
	정보주체의 정정·삭제요구에 따라 필요 조치를 취하지 아니한 자(제36조)	
	처리정지된 개인정보에 대해 파기 등의 조치를 하지 않은 자(제37조)	
	시정명령 불이행(제64조)	
	정보주체의 열람, 정정·삭제, 처리정보 요구 거부 시 통지의무 불이행(제35조, 제36조, 제37조)	
	관계물품·서류 등의 미제출 또는 허위제출(제63조)	
	출입·검사를 거부·방해 또는 기피한 자(제63조)	
파기	개인정보 미파기(제21조)	3천만원 이하 과태료

■ 별지 제1호 서식

본 표준 개인정보처리위탁 계약서는 「개인정보 보호법」 제26조제1항에 따라 위탁계약에 있어 개인정보 처리에 관하여 문서로 정하여야 하는 최소한의 사항을 표준적으로 제시한 것으로서, 위탁계약이나 위탁업무의 내용 등에 따라 세부적인 내용은 달라질 수 있습니다.

개인정보처리업무를 위탁하거나 위탁업무에 개인정보 처리가 포함된 경우에는 본 표준 개인정보처리위탁 계약서의 내용을 위탁계약서에 첨부하거나 반영하여 사용하실 수 있습니다.

표준 개인정보처리위탁 계약서(안)

예수대학교(이하 "위탁자"이라 한다)과 △△△(이하 "수탁자"이라 한다)는 "위탁자"의 개인정보 처리업무를 "수탁자"에게 위탁함에 있어 다음과 같은 내용으로 본 업무위탁계약을 체결한다.

제1조 (목적) 이 계약은 "위탁자"가 개인정보처리업무를 "수탁자"에게 위탁하고, "수탁자"는 이를 승낙하여 "수탁자"의 책임아래 성실하게 업무를 완성하도록 하는데 필요한 사항을 정함을 목적으로 한다.

제2조 (용어의 정의) 본 계약에서 별도로 정의되지 아니한 용어는「개인정보 보호법」, 같은 법 시행령 및 고시,「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시 제2021-2호) 및「표준 개인정보 보호지침」(개인정보보호위원회 고시 제2020-1호)에서 정의된 바에 따른다.

제3조 (위탁업무의 목적 및 범위) "수탁자"는 계약이 정하는 바에 따라 (_____) 목적으로 다음과 같은 개인정보 처리 업무를 수행한다.[1)]

1.
2.
3.

제4조 (위탁업무 기간) 이 계약서에 의한 개인정보 처리업무의 기간은 다음과 같다.

계약 기간 : 년 월 일 ~ 년 월 일

제5조 (재위탁 제한) ① "수탁자"는 "위탁자"의 사전 승낙을 얻은 경우를 제외하고 "위탁자"와의 계약상의 권리와 의무의 전부 또는 일부를 제3자에게 양도하거나 재위탁할 수 없다.

② "수탁자"가 다른 제3의 회사와 수탁계약을 할 경우에는 "수탁자"는 해당 사실을 계약 체결 7일 이전에 "위탁자"에게 통보하고 협의하여야 한다.

제6조 (개인정보의 안전성 확보조치) "수탁자"는「개인정보 보호법」제23조제2항 및 제24

1) 각호의 업무 예시 : 고객만족도 조사 업무, 회원가입 및 운영 업무, 사은품 배송을 위한 이름, 주소, 연락처 처리 등

조제3항 및 제29조, 같은 법 시행령 제21조 및 제30조, 「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시 제2021-2호)에 따라 개인정보의 안전성 확보에 필요한 관리적.기술적 조치를 취하여야 한다.

제7조 (개인정보의 처리제한) ① "수탁자"는 계약기간은 물론 계약 종료 후에도 위탁업무 수행 목적 범위를 넘어 개인정보를 이용하거나 이를 제3자에게 제공 또는 누설하여서는 안 된다.

② "수탁자"는 계약이 해지되거나 또는 계약기간이 만료된 경우 위탁업무와 관련하여 보유하고 있는 개인정보를 「개인정보 보호법」시행령 제16조 및「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시 제2021-2호)에 따라 즉시 파기하거나 "위탁자"에게 반납하여야 한다.

③ 제2항에 따라 "수탁자"가 개인정보를 파기한 경우 지체없이 "위탁자"에게 그 결과를 통보하여야 한다.

제8조 (수탁자에 대한 관리·감독 등) ① "위탁자"는 "수탁자"에 대하여 다음 각 호의 사항을 감독할 수 있으며, "수탁자"는 특별한 사유가 없는 한 이에 응하여야 한다.

1. 개인정보의 처리 현황
2. 개인정보의 접근 또는 접속현황
3. 개인정보 접근 또는 접속 대상자
4. 목적외 이용.제공 및 재위탁 금지 준수여부
5. 암호화 등 안전성 확보조치 이행여부
6. 그 밖에 개인정보의 보호를 위하여 필요한 사항

② "위탁자"는 "수탁자"에 대하여 제1항 각 호의 사항에 대한 실태를 점검하여 시정을 요구할 수 있으며, "수탁자"는 특별한 사유가 없는 한 이행하여야 한다.

③ "위탁자"는 처리위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 1년에 (__)회 "수탁자"를 교육할 수 있으며, "수탁자"는 이에 응하여야 한다.[2)]

④ 제1항에 따른 교육의 시기와 방법 등에 대해서는 "위탁자"는 "수탁자"와 협의하여 시행한다.

제9조 (정보주체 권리보장) ① "수탁자"는 정보주체의 개인정보 열람, 정정·삭제, 처리정지 요청 등에 대응하기 위한 연락처 등 민원 창구를 마련해야 한다.

제10조 (개인정보의 파기) ① "수탁자"는 제4조의 위탁업무기간이 종료되면 특별한 사유가 없는 한 지체 없이 개인정보를 파기하고 이를 "위탁자"에게 확인받아야 한다.

제11조 (손해배상) ① "수탁자" 또는 "수탁자"의 임직원 기타 "수탁자"의 수탁자가 이 계약에 의하여 위탁 또는 재위탁 받은 업무를 수행함에 있어 이 계약에 따른 의무를 위반하거나 "수탁자" 또는 "수탁자"의 임직원 기타 "수탁자"의 수탁자의 귀책사유로

---

2) 「개인정보 안전성 확보조치 기준 고시」(개인정보보호위원회 고시 제2021-2호) 및 「개인정보 보호법」 제26조에 따라 개인정보처리자 및 취급자는 개인정보보호에 관한 교육을 의무적으로 시행하여야 한다.

인하여 이 계약이 해지되어 “위탁자” 또는 개인정보주체 기타 제3자에게 손해가 발생한 경우 “수탁자”는 그 손해를 배상하여야 한다.

② 제1항과 관련하여 개인정보주체 기타 제3자에게 발생한 손해에 대하여 “위탁자”가 전부 또는 일부를 배상한 때에는 “위탁자”는 이를 “수탁자”에게 구상할 수 있다.

본 계약의 내용을 증명하기 위하여 계약서 2부를 작성하고, “위탁자”와 “수탁자”가 서명 또는 날인한 후 각 1부씩 보관한다.

20 . . .

위탁자	수탁자
주 소 :	주 소 :
기관(회사)명 :	기관(회사)명 :
대표자 성명 : (인)	대표자 성명 : (인)

보안 서약서(업체 대표용)

본인은 _____년 ____월 ____일부로 _____관련 용역사업(업무)을 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 본인은 _____관련 업무 중 알게 될 일체의 내용이 직무상 기밀사항임을 인정한다.
2. 본인은 이 기밀을 누설함이 예수대학교에 위해가 될 수 있음을 인식하여 업무수행 중 지득한 제반 기밀사항을 일체 누설하거나 공개하지 아니한다.
3. 본인이 이 기밀을 누설하거나 관계 규정을 위반한 때에는 관련 법령 및 계약에 따라 어떠한 처벌 및 불이익도 감수한다.
4. 본인은 하도급업체를 통한 사업 수행 시 하도급업체로 인해 발생하는 위반사항에 대하여 모든 책임을 부담한다.

년 월 일

서약자 (업체대표)

업 체 명 :
직 위 :
성 명 : (서명)

예수대학교 귀중

■ 별지 제3호 서식

보안 서약서

본인은 _____년 ____월 ____일부로 _____관련 용역사업(업무)을 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 본인은 _____관련 업무 중 알게 될 일체의 내용이 직무상 기밀사항임을 인정한다.
2. 본인은 이 기밀을 누설함이 예수대학교에 위해가 될 수 있음을 인식하여 업무수행 중 지득한 제반 기밀사항을 일체 누설하거나 공개하지 아니한다.
3. 본인이 이 기밀을 누설하거나 관계 규정을 위반한 때에는 관련 법령 및 계약에 따라 어떠한 처벌 및 불이익도 감수한다.

년 월 일

서약자 업 체 명 :
직 위 :
성 명 : (서명)

예수대학교 귀중

■ 별지 제4호 서식

개인정보의 목적 외 이용 및 제3자 제공 대장

개인정보 또는 개인정보파일 명칭			
이용 또는 제공 구분	[ ] 목적외 이용 [ ] 제3자 제공		
목적 외 이용기관의 명칭 (목적 외 이용의 경우)		담당자	소 속
			성 명
			전화번호
제공받는 기관의 명칭 (제3자 제공의 경우)		담당자	성 명
			소 속
			전화번호
이용하거나 제공한 날짜, 주기 또는 기간			
이용하거나 제공한 형태			
이용 또는 제공의 법적 근거			
이용 목적 또는 제공받는 목적			
이용하거나 제공한 개인정보의 항목			
「개인정보 보호법」 제18조제5항에 따라 제한을 하거나 필요한 조치를 마련할 것을 요청한 경우에는 그 내용			