

개인정보 내부관리계획 규정 개정이력 현황표

[illegible]

개인정보 내부 관리계획 규정

제 정 : 2020. 9. 24

제1장 총 칙

제1조(목적) 이 계획은 「개인정보 보호법」 제23조제2항, 제24조제3항 및 제29조와 같은법 시행령 제21조 및 제30조에 따라 금강대학교(이하 “대학교”라 한다.)가 개인정보를 처리함에 있어서 개인정보가 분실·도난·유출·변조·훼손되지 아니하도록 안전성을 확보하기 위한 기술적·관리적 및 물리적 계획을 수립하는 것을 목적으로 한다.

제2조(용어정의) 이 계획 규정에서 사용하는 용어의 정의는 다음 각 호와 같다.

1. “개인정보”란 살아있는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명·주민등록번호·학력 및 사진·영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함)를 말한다.
2. 고유식별정보 : 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호
3. 민감정보 : 사상, 신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활, 유전정보, 범죄경력 정보 등에 관한 정보와 그 밖에 정보주체의 사생활을 현저히 침해할 우려가있는 개인정보
4. “정보주체”란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서, 「개인정보 보호법」에 의해 보호대상이 되는 정보의 주체가 되는 사람을 말한다.
5. “개인정보파일”이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물을 말한다.
6. “개인정보처리자”란 업무를 목적으로 개인정보파일을 운용(수집·이용·저장·제공·파기 등)하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인을 말한다.
7. “개인정보의 처리”란 개인정보를 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 연계, 연동 그 밖에 이와 유사한 행위를 말한다.
8. “개인정보 보호책임자”라 함은 개인정보의 처리에 관한 업무를 총괄해서 책임지는 자를 말한다.
9. “개인정보보호 분야별 책임자”(이하 “분야별 책임자”라 한다)라 함은 업무를 위하여 개인정보파일을 처리하는 부서의 장으로 개인정보 보호책임자가 지정한 자를 말한다.
10. “개인정보보호 담당자”란 실질적인 개인정보 보호업무를 담당하는 자로 개인정보처리자가 지정한 자를 말한다.
11. “개인정보취급자”라 함은 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는

- 업무를 담당하는 자로서 직접 개인정보에 관한 업무를 담당하는 자와 그 밖의 업무상 필요에 의해 개인정보에 접근하여 처리하는 모든 자를 말한다.
12. “개인정보처리시스템”이란 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템을 말한다.
 13. “개인정보처리시스템 책임자”라 함은 해당 재해·재난 사고로 인해 위기가 발생한 시스템을 관리하는 분야별 책임자 또는 개인정보보호 책임자가 지정하는 자로, 해당 사고에 대한 분석, 대응, 복구 등의 처리에 대한 책임을 지는 자를 말한다.
 14. “접속기록”이란 개인정보취급자 등이 개인정보처리시스템에 접속한 사실을 알 수 있는 계정, 접속일시, 접속자 정보, 수행업무 등을 전자적으로 기록한 것을 말한다. 이 경우 “접속”이란 개인정보처리시스템과 연결되어 데이터 송신 또는 수신이 가능한 상태를 말한다.
 15. “바이오정보”란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 생성되거나 가공된 정보를 포함한다.
 16. “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.
 17. “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.
 18. “재해·재난”이란 태풍, 홍수, 지진, 낙뢰 등 이상적인 자연현상 또는 붕괴, 폭발 등으로 사회적 혼란을 유발할 수 있는 사고를 말한다.
 19. “백업”이란 잘못되거나 부주의한 조작으로 인하여 데이터가 손실될 것에 대비하여 미리 남겨둔 복사본을 말한다.
 20. “개인정보 유출”이란 ①개인정보가 포함된 서면, 이동식 저장장치, 휴대용 컴퓨터 등을 분실하거나 도난당한 경우 ②개인정보가 저장된 데이터베이스 등 개인정보처리시스템에 정상적인 권한이 없는 자가 접근한 경우 ③개인정보처리자의 고의 또는 과실로 인해 개인정보가 포함된 파일 또는 종이문서, 기타 저장매체가 권한이 없는 자에게 잘못 전달된 경우 ④기타 권한이 없는 자가 개인정보를 전달받거나 개인정보처리시스템 등에 접근 가능하게 된 경우를 말한다.
 21. “개인정보침해”라 함은 법적 근거, 규정 또는 본인 동의에 의하지 않고 이루어지는 개인정보의 수집, 저장, 이용 및 제공, 파기행위 일체를 말한다.

제2장 내부 관리계획의 수립 및 시행

제3조 (내부관리계획의 수립 및 시행) ① 개인정보 보호책임자는 대학교의 개인정보보호를 위한 전반적인 사항을 포함하여 내부관리계획을 수립하여야 한다.

② 개인정보 보호책임자는 개인정보보호를 위한 내부관리계획의 수립 시 개인정보보호와 관련

한 법령 및 관련 규정을 준수하도록 내부관리계획을 수립하여야 한다.

③ 개인정보 보호책임자는 개인정보 보호 운영책임자가 수립한 내부관리계획의 타당성을 검토하여 개인정보보호를 위한 내부관리계획을 승인하여야 한다.

④ 개인정보 보호 운영책임자는 개인정보보호 관련 법령의 제·개정 사항 등을 반영하기 위하여 매년 정기적으로 1회 이상 내부계획의 타당성과 개정 필요성을 검토하여야 한다.

⑤ 개인정보 보호 운영책임자는 모든 항목의 타당성을 검토한 후 개정할 필요가 있다고 판단되는 경우 12월말까지 내부관리계획의 개정안을 작성하여 개인정보 보호책임자에게 보고하고 개인정보 보호책임자의 승인을 받아야 한다.

제3장 개인정보 보호책임자의 역할과 책임

제4조 (개인정보 보호책임자 및 분야별 책임자의 지정) 대학교는 개인정보보호법 제31조제1항 및 동법 시행령 제32조제2항에 따라 소관 개인정보의 보호와 관리를 위하여 개인정보 보호책임자 및 분야별 책임자를 다음과 같이 지정·운영한다.

① 개인정보 보호책임자 : 금강대학교 총장

② 분야별 책임자 : 개인정보를 보유·처리하는 각 부서장, 각 학부의 장, 대학원의 원장, 각 부속 기관장, 각 부설 연구원(소)장

③ 개인정보 보호책임자 및 분야별 책임자는 인사발령에 따라 보직을 받은 날로부터 지정되는 당연직을 원칙으로 한다.

제5조 (개인정보 보호책임자의 역할과 책임) ① 개인정보 보호책임자는 정보주체의 개인정보 보호를 위하여 다음 각 호의 업무를 수행한다.

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

② 개인정보 보호책임자는 제1항 각 호의 업무를 수행함에 있어서 필요한 경우 개인정보의 처리 현황, 처리 체계 등에 대하여 수시로 조사하거나 관계 당사자로부터 보고를 받을 수 있다.

③ 개인정보 보호책임자는 개인정보취급자를 최소한으로 제한하여 지정하고, 수시로 관리·감독하여야 하며, 취급자에 대한 교육 및 보안서약 등을 통해 개인정보 침해사고를 사전에 예

방하여야 한다.

④ 개인정보 보호 운영책임자는 개인정보 보호책임자가 위임한 업무를 수행하며, 분야별 책임자 및 분야별 개인정보 보호 운영책임자의 업무를 관리한다.

제6조 (분야별 책임자의 지정 및 업무) ① 개인정보 보호책임자는 주요 개인정보를 취급하는 부서의 장을 분야별 책임자로 지정할 수 있다.

② 분야별 책임자는 해당부서의 다음 각 호의 업무를 위임받아 수행할 수 있다.

1. 개인정보 처리 실태의 정기적인 조사 및 개선
2. 개인정보 처리와 관련한 불만의 처리 및 피해 구제
3. 개인정보파일의 보호 및 관리 · 감독
4. 개인정보 보호 관련 자료의 관리
5. 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기
6. 그 밖에 해당부서의 개인정보 보호를 위해 필요한 사항 등

③ 분야별 책임자는 개인정보 보호 업무의 효율적인 수행을 위하여 분야별 개인정보 보호 운영책임자를 임명할 수 있으며, 이 때 행정부서의 과(팀)단위의 과(팀)장, 상급실무자, 학부 단위의 지도교수 등을 분야별 개인정보 보호 운영책임자로 지정하여 운영할 수 있다.

④ 분야별 개인정보 보호 운영책임자는 개인정보 보호와 관련하여 분야별 책임자가 위임한 업무와 기타 관련 업무를 수행한다.

제7조 (개인정보취급자의 역할 및 책임) ① 개인정보취급자는 개인정보를 처리함에 있어서 개인정보가 안전하게 관리될 수 있도록 하여야 하며, 다음 각 호와 같은 역할 및 책임을 이행한다.

1. 개인정보의 처리
 2. 개인정보 보호책임자가 위임한 개인정보보호와 관련된 업무
 3. 개인정보 보호책임자에게 개인정보 파일 등록 신청
 4. 개인정보파일 파기
 5. 개인정보 파기 시 개인정보파일의 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 정보주체로부터 개인정보를 수집·이용·제3자 제공함에 있어 법령 등에서 정한 경우를 제외하고는 반드시 [별지 제1호 서식] 개인정보의 수집이용에 대한 동의서를 참조하여 동의서식(전자 문서 포함)을 마련하고 개인정보를 수집·이용·제3자 제공 하여야 한다.
- ③ 제2항에서 정보주체가 만14세 미만 아동인 경우 법정대리인으로부터 동의를 받아 수집·이용·제3자 제공 하여야 한다. 이때 아동에게 법정대리인의 성명, 연락처, 관계에 대해 수집 이유를 밝히고 수집하여 법정대리인의 동의를 받을 수 있으며, 아동과 법정대리인의 관계 확인을 위해 신분증 사본 등의 서류를 요구할 수 있다.

④ 개인정보취급자는 고유식별정보 및 민감정보 처리 시 정보주체로부터 별도의 동의를 받아 수집·이용·제3자 제공 하여야 한다. 다만, 주민등록번호의 경우 반드시 법률 또는 대통령령 등에서 구체적으로 수집·이용·제3자 제공을 허용하는 경우를 제외하고서는 수집·이용·제3자 제공 하여서는 아니 된다.

⑤ 개인정보취급자는 정보주체로부터 자신의 개인정보에 대한 열람·정정·처리정지·삭제 등의 요구를 받을 경우 [별지 제6호 서식]에 의해야 하며, 요구를 받은 경우 정당한 사유가 있는 경우를 제외하고는 10일 이내 요구에 [별지 제8호 서식]을 활용하여 응해야 한다.

⑥ 개인정보취급자는 다음의 사항에 해당하는 경우 정보주체로부터 열람·정정·처리정지·삭제 등의 요구에 대해 그 사유를 알리고 열람 등을 [별지 제7호 서식]을 활용하여 거절 할 수 있다. 다만, 거절 시 열람 등의 요구를 접수한 지 10일 이내에 정보주체에게 알려야 한다.

1. 법률에 따라 열람이 금지되거나 제한되는 경우
2. 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우
3. 「고등교육법」에 따른 각급 학교, 「평생교육법」에 따른 평생교육시설, 그 밖의 다른 법률에 따라 설치된 고등교육기관에서의 성적 평가 또는 입학자 선발에 관한 업무
4. 학력·기능 및 채용에 관한 시험, 자격 심사에 관한 업무
5. 보상금 산정 등에 대하여 진행 중인 평가 또는 판단에 관한 업무
6. 다른 법률에 따라 진행 중인 감사 및 조사에 관한 업무

⑦ 개인정보취급자는 정보주체가 열람 등의 요구를 하는 경우 정보주체 본인 또는 대리인임을 확인하기 위한 신분증 사본 등을 확인하여야 한다.

제4장 개인정보 보호 교육

제8조 (개인정보보호 교육 계획의 수립) ① 개인정보 보호책임자는 다음 각 호의 사항을 포함하는 연간 개인정보보호 교육계획을 수립한다.

1. 교육목표 및 대상
2. 교육내용
3. 교육일정 및 방법

② 개인정보 보호책임자는 수립한 개인정보보호 교육 계획을 실시한 이후에 교육의 성과와 개선 필요성을 검토하여 차년도 교육계획 수립에 반영하여야 한다.

제9조 (개인정보보호 교육의 실시) ① 개인정보 보호책임자는 정보주체 정보보호에 대한 교직원 인식 제고를 위해 노력해야 하며, 개인정보의 오·남용 또는 유출 등을 적극 예방하기 위해 매년 정기적으로 년 1회 이상의 개인 정보보호 교육을 실시하여야 한다.

② 교육 방법은 집체 교육 뿐만 아니라, 인터넷 교육 등 다양한 방법을 활용하여 실시하고, 필요한 경우 상급기관, 외부 전문기관이나 전문 요원에 위탁하여 교육을 실시 할 수 있다.

③ 개인정보보호에 대한 중요한 전파 사례가 있거나 개인 정보보호 업무와 관련하여 변경된

사항이 있는 경우, 개인정보 보호책임자는 부서회의 등을 통해 수시 교육을 실시 할 수 있다.

④ 개인정보 처리업무를 위탁하는 경우 정보주체의 개인정보가 분실, 도난, 유출, 변조 또는 훼손되지 않도록 수탁자를 교육해야 한다.

제5장 기술적 안전조치

제10조 (접근권한의 관리) ① 개인정보처리시스템 책임자는 개인정보처리시스템에 대한 접근 권한을 부여할 경우, 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.

② 개인정보처리시스템 책임자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여야 하며, 권한 부여, 변경 또는 말소에 대한 내역은 최소 3년간 보관하여야 한다.

③ 개인정보처리시스템 책임자는 개인정보처리시스템에 접속할 수 있는 사용자 계정을 발급하는 경우 개인정보 취급자별로 사용자 계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

④ 개인정보처리시스템 책임자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호는 문자, 숫자의 조합 · 구성에 따라 최소 10자리 또는 8자리 이상의 길이로 다음 각 호와 같이 설정하여야 한다.

1. 최소 10자리 이상 : 영대문자(A~Z, 26개), 영소문자(a~z, 26개), 숫자(0~9, 10개, 특수문자(#, [, “, < 등, 32개) 중 2종류 이상으로 조합 · 구성한 경우
2. 최소 8자리 이상 : 영대문자, 영소문자, 숫자, 특수문자 중 3종류 이상으로 구성한 경우
3. 비밀번호는 추측하거나 유추하기 어렵도록 설정 : 일련번호(12345678 등), 전화번호, 키보드 상에서 나란히 있는 문자열(qwer 등)은 사용 금지
4. 비밀번호는 최소 6개월마다 변경하도록 변경기간을 적용
5. 단, 정보시스템(서버, 네트워크장비, 정보보호시스템, 홈페이지 관리자페이지 등)의 비밀번호 설정 방식은 정보보안규정을 적용

⑤ 개인정보처리시스템 책임자는 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.

제11조 (접근통제) ① 개인정보처리시스템 책임자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 조치를 하여야 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 유출시도 탐지 및 대응

② 개인정보처리시스템 책임자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용 될 수 있도록 방법을 강구 및 시행해야 적용해야 한다.

- ③ 개인정보처리시스템 책임자는 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 하여야 한다.
- ④ 개인정보처리시스템 책임자는 고유식별정보를 처리하는 경우 인터넷 홈페이지를 통해 고유식별 정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점을 점검하고 필요한 보완 조치를 해야 하며 연 1회 이상 개인정보 보호책임자에게 보고해야 한다.
- ⑤ 개인정보처리시스템 책임자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 하여야 한다.
- ⑥ 개인정보취급자는 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 개인정보취급자는 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.

제12조 (개인정보의 암호화) ① 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

- ② 개인정보 처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.
- ③ 개인정보 처리자가 내부망에 고유식별정보를 저장하는 경우에는 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.
- ④ 개인정보 처리자는 제1항, 제2항, 제3항에 따라 개인정보를 암호화하는 경우 안전한 암호 알고리즘으로 암호화하여 저장하여야 한다.
- ⑤ 개인정보 처리 시스템책임자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다.
- ⑥ 개인정보처리시스템 책임자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

제13조 (접속기록의 보관 및 점검) ① 개인정보처리시스템 책임자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 6개월 이상 보관·관리하여야 한다.

- ② 개인정보처리시스템 책임자는 개인정보의 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 반기별로 1회 이상 점검하여야 한다.
- ③ 개인정보처리시스템 책임자는 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.

제14조 (악성프로그램 등 방지) 개인정보처리시스템 책임자는 악성프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 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 업데이트 실시
3. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치

제6장 물리적 안전조치

제15조 (물리적 안전조치) ① 개인정보 처리시스템 책임자 및 개인정보 보호 운영책임자 는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 다음 각 호와 같은 출입통제 절차를 수립 · 운영하여야 한다.

1. 출입의 통제를 위하여 물리적 접근 방지를 위한 장치를 설치 · 운영하고 이에 대한 출입 내역을 전자적인 매체 또는 수기문서 대장에 기록
2. 물리적 접근 방지를 위한 장치(예시) : 비밀번호 기반 출입통제 장치, 스마트 카드 기반 출입 통제장치, 지문 등 바이오정보 기반 출입통제 장치 등
3. 출입 내역 기록 방법(예시) : 출입자, 출입일시, 출입목적, 소속 등

② 개인정보보호 담당자는 개인정보가 포함된 서류, 보조저장매체(이동형 하드디스크, USB메모리, SSD 등)를 잠금장치가 있는 캐비닛 등 안전한 장소에 보관하여야 한다.

③ 개인정보처리시스템 책임자는 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안 대책을 다음 각 호와 같이 마련하여야 한다.

1. 보조저장매체 보유 현황 파악 및 반출·입 관리 계획
2. 개인정보취급자 및 수탁자 등에 의한 개인정보 유출 가능성 고려
3. 보조저장매체의 안전한 사용 방법 및 비인가된 사용에 대한 대응
4. USB를 PC에 연결시 바이러스 점검 디폴트로 설정 등 기술적 안전조치 방안

제16조 (재해 및 재난 대비 안전조치) ① 개인정보처리시스템 책임자는 화재, 홍수, 단전 등의 재해 · 재난 발생 시 개인정보처리시스템 보호를 위한 대응절차를 마련하고 정기적으로 점검하여야 한다.

② 개인정보처리시스템 책임자는 개인정보처리시스템의 위기 발생 시 아래와 같은 예방, 대응, 복구 및 복원으로 이어지는 3가지 대응절차를 체계적으로 수행하여야 한다.

1단계 : [예방]

1. 위기상황이 발생하기 전 예상되는 문제들을 미리 보완하고 대비
 - 가. 개인정보처리시스템 정기점검, 운영매뉴얼 관리 등 안정화
 - 나. 전산실 온·습도 확인, 항온 항습기 정기점검 등
2. 위기대응 조직, 위기등급, 복구 목표 등 위기대응 체계 검토
 - 가. 재해·재난 시 비상연락망 체계구성 및 점검

나. 비상 시 인력운영 및 수급계획 점검

다. 유지보수 및 위탁운영 업체의 비상연락망 체계 구성 및 점검 등

3. 주기적 백업 실시 및 위기대응 훈련 실시를 통해 위기대응 준비

가. 정기적인 데이터 백업 및 소산 실행 결과를 백업관리대장에 작성

나. 재난 시 대응능력 향상을 위한 데이터 복구, 장애 대응 등 모의 훈련 실시 등

2단계 : [대응]

1. 재해·재난으로 위기상황 발생 시 상황별로 위기대응 체계에 따라 초기 대응 실시

가. 태풍·홍수·지진·건물붕괴·폭발 등의 위기상황 발생 시 화재진압·직원대피·비상전력 공급·침수차단 등의 초기대응 실시 등

2. 위기대응 조직을 소집하고 위기등급을 정의하여 위기상황 선포

가. 개인정보처리시스템 담당자는 피해현황 및 복구 예상시간을 파악하여 개인정보처리 시스템 책임자 및 개인정보 보호책임자에게 보고하고, 위기 등급에 따라 관련자 및 관련기관에 신고

나. 개인정보처리시스템 책임자는 피해현황을 검토하고 피해정도를 판단하여 위기등급을 선포하고 위기등급 별 대응 계획에 따라 대응 등

1. 초기대응 이후 개인정보 유출·손실·훼손에 따른 후속조치 실시

가. 개인정보 침해발생 시, 「개인정보 유출 및 침해사고 대응 시행세칙」에 따라 정보 주체에게 유출을 통지하고, 관련기관에 개인정보 유출 사실을 신고 등

3단계 : [복구 및 복원]

1. 복구목표에 따라 우선순위가 높은 업무부터 복구 및 복원 실시

가. 기관별 개인정보처리시스템 구성 현황 및 업무영향도 등을 종합하여 설정한 복구 우선순위가 높은 업무부터 단계적으로 복구하고, 소스 데이터 유실 등에 따라 백업 데이터를 이용하여 복원 실시

나. 시스템 가동 불가 시 데이터 백업 복구 실시

다. 사이버 공격으로 인한 개인정보 유출 발생 시, 「국가 사이버안전 매뉴얼」에 따라 대응 등
라. 복구 및 복원 완료 시, 위기상황의 종료를 선언하고 위기대응 시 이슈사항을 위기대응 체계에 반영하여 개선

마. 개인정보처리시스템 담당자는 위기상황 종료 시 조치결과를 개인정보 처리시스템 책임자에게 보고하고, 개인정보처리시스템 책임자는 이를 검토하여 향후 위기대응 체계에 반영 등

바. 위기상황으로 인한 피해를 수습하고 위기내용 학습

사. 피해수습 후 위기내용 재발방지 및 피해최소화를 위한 업무관련자 교육 등 진행

③ 위시발생기 다음의 역할분장 및 조직도를 참고하여 위기대응 조직을 구성하고 각각의 역할을 정의하여야 한다.

구 분	역 할
행정 부서 책임자 (기획관리처장)	<ul style="list-style-type: none"> - 소관 개인정보처리시스템 위기대응 업무의 총괄 - 위기선포 및 위기대응 조직 구성원에게 업무를 지시 - 위기대응 상황 종료 시 결과를 공유 - 위기 발생 시 사고 처리 및 예방에 대한 총괄책임
분야별 책임자 및 개인정보 취급자	<ul style="list-style-type: none"> - 위기상황 발생 시 각 업무기능의 복구 - 책임자의 위기선포에 따라 위기상황 전파 - 유관 기관과 연락망 가동 및 정보공유 - 평상 시 위기대응 절차 및 계획의 검토 - 위기 발생 시 사고 분석, 대응, 복구 등의 처리와 재발방지에 대한 책임
기술 담당자	<ul style="list-style-type: none"> - 개인정보처리시스템의 기술적 복구 및 운용 담당 - 책임자 및 담당자의 지시에 따라 필요한 활동 지원

제17조 (개인정보의 파기) ① 개인정보보호 취급자는 보유기간의 경과, 처리목적 달성, 해당 서비스의 폐지 등 그 개인정보가 불필요하게 되었을 경우 5일 이내에 파기하여야 하며, 개인정보의 파기에 관한 사항을 기록·관리하여야 하며, 파기 시에는 개인정보 보호책임자에게 결과를 보고해야 한다. 다만, 다른 법률에 따라 보존하여야 하는 경우에는 관련법에 따라 처리한다.

② 개인정보보호 책임자는 개인정보보호 취급자로부터 개인정보파일의 보유기간, 처리목적 등을 반영한 개인정보 파기 계획을 수립하여 시행·확인하여야 한다.

③ 복구 또는 재생되지 아니하도록 다음 각 호의 구분에 따른 방법으로 파기하여야 한다.

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

④ 개인정보보호 취급자가 개인정보의 일부만을 파기하는 경우, 제3항의 방법으로 파기하는 것이 어려울 때에는 개인정보처리시스템 운영자 및 개인정보 보호 운영책임자에게 승인 후 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

⑤ 개인정보보호 분야별책임자가 개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 해

당 개인정보를 다른 개인정보와 분리하여 저장·관리하여야 하며, 법령에 따라 해당 개인정보를 보존한다는 점을 분명히 표시하여야 한다.

⑥ 개인정보보호 책임자는 개인정보의 보유 기간 만료 등에 따른 구체적 파기 시점·방법 등을 반영한 개인정보 파기계획을 수립·시행하고 개인정보의 파기 결과를 확인하여야 한다.

⑦ 개인정보 파기 절차도

1. 파기검토

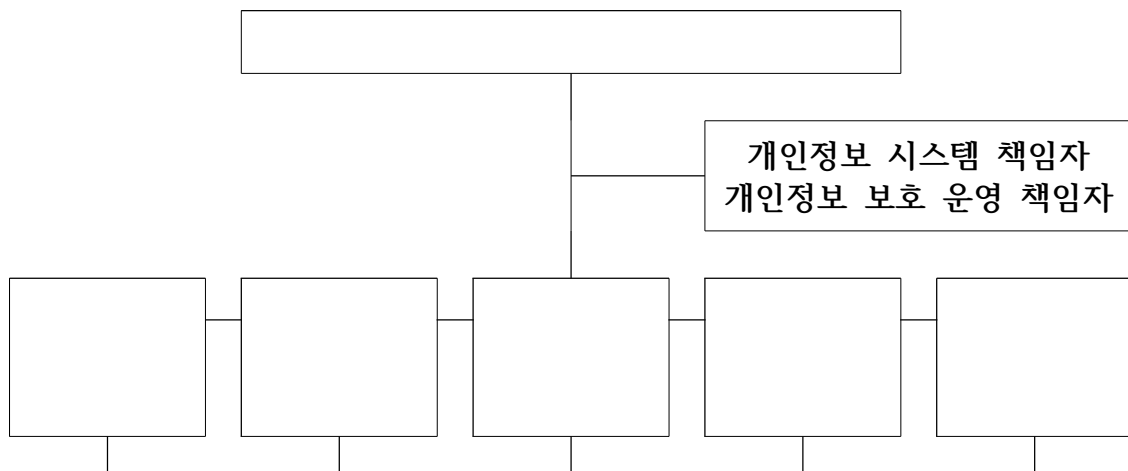
개인정보 취급자 (파기요청서 작성 및 결재상신)	→	분야별 책임자 승인	→	개인정보 보호 담당자 및 개인정보 시스템 책임자 승인	→	개인정보보호 책임자 승인
--	---	---------------	---	--	---	------------------

2. 파기 조치

개인정보 파기조치 후 (파기대장 작성 및 결재상신)	→	분야별 책임자 승인	→	개인정보 보호 담당자 및 개인정보 시스템 책임자 승인	→	개인정보보호 책임자 승인
---	---	---------------	---	--	---	------------------

제7장 관리적 안전조치

제18조 (개인정보 보호조직 구성 및 운영) ① 개인정보 보호책임자는 개인정보 처리과정 전반에 걸쳐 개인정보를 안전하게 관리하고 보호하기 위하여 다음의 구성도와 같은 개인정보 보호조직을 구성하고 운영하여야 한다.



--	--	--	--	--

② 개인정보보호 추진 체계별 역할

구분	담당자	역 할
개인정보 보호 책임자	금강대학교 총장	<ul style="list-style-type: none"> - 개인정보 보호 계획의 수립 및 시행 관리 감독 - 개인정보 처리실태 및 관행의 정기적인 조사 및 개선 - 개인정보 처리와 관련한 불만의 처리 및 피해 구제 총괄 - 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템 구축 총괄 - 개인정보보호 교육 계획의 수립 및 시행 - 개인정보파일의 보호 및 감독 총괄 - 개인정보 처리방침의 수립·변경 및 시행 - 개인정보보호 관련 자료의 관리 총괄 - 처리목적이 달성되거나 보유기간이 지난 개인정보의 파기
개인정보 보호 운영 책임자	개인정보 보호책임자가 지정한 자 (경영지원팀장)	<ul style="list-style-type: none"> - 개인정보에 대한 접근권한, 규정관리 업무 - 개인정보 보호 계획의 수립 및 시행 - 개인정보를 위한 교육 및 홍보에 관한 업무 - 개인정보보호 관련 자료의 관리 - 처리목적이 달성되거나 보유기간이 지난 개인정보의 파기

개인정보처리 시스템 책임자	개인정보 보호 책임자가 지정한 자 (정보지원팀장)	<ul style="list-style-type: none"> - 개인정보취급 현황 및 취급자 관리 업무 - 개인정보 처리실태 및 관행의 정기적인 조사 및 개선 - 개인정보파일의 보호 및 관리 감독 - 처리목적이 달성되거나 보유기간이 지난 개인정보의 파기 - 개인정보보호 관련 자료의 관리 - 개인정보 처리방침의 수립·변경 및 시행 - 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템 구축 - 기타 개인정보의 관리적·물리적 보호조치에 관한 업무 - 정보시스템의 부당한 접근 및 외부침입 등을 방지하기 위한 정보시스템의 구축 및 관리 업무 - 정보의 정확성 및 최신성 확보를 위한 시스템 관리 업무 - 침해사고 예방, 복구 및 보호 등의 업무 - 기타 개인정보의 기술적 보호조치에 관한 업무 - 금강대학교 산하 대학(원)·행정부서·부속기관·부설연구소 등이 운영하는 개인정보처리시스템의 운영에 대한 업무 - 개인정보처리시스템의 재해·재난 사고 시 해당 사고에 대한 분석, 대응, 복구 등의 위기 관리 업무 - 개인정보침해사고 발생 시 침해의 규모, 경위, 방법, 원인 및 관련자 조사에 관한 업무 (개인정보 유출 및 침해사고에 대한 세부사항은 「개인정보 유출 및 침해사고 대응 시행세칙」에 따른다)
개인정보 보호 분야별 책임자	개인정보를 보유·처리하는 각 부서장, 각 학부장 각 대학원의 원장, 각 부속기관장, 각 부설 연구원(소)장	<ul style="list-style-type: none"> - 소관 분야별 개인정보 보호 업무 수행 및 개인정보 취급자에 대한 지도·감독 - 소관 분야별 개인정보 열람·정정·삭제 요청 등의 민원 접수 및 처리 - 소관 분야별 개인정보보호와 관련한 현황(개인정보파일 대장, 개인정보 이용 및 제공·법 위반자 처리·개인정보 열람 및 정정처리 현황) 작성 및 개인정보 보호책임자에게 통보 - 기타 소관 분야별 개인정보 보호를 위해 필요한 사항 - 개인정보보호 관련 자료의 관리 - 처리목적이 달성되거나 보유기간이 지난 개인정보의 파기

개인정보 취급자	서비스 운영자 및 개인정보 접근 가능자 (실무자)	<ul style="list-style-type: none"> - 개인정보보호 활동 참여 - 내부관리계획의 준수 및 이행 - 개인정보파일의 등록, 변경 신청 - 개인정보파일의 파기절차에 따른 파기 수행 - 개인정보의 관리적, 기술적, 물리적 보호조치 기준 이행 - 소속 직원 또는 제3자에 의한 위법 및 부당한 개인정보 침해행위에 대한 점검 - 개인정보보호 관련 자료의 관리 - 처리목적이 달성되거나 보유기간이 지난 개인정보의 파기
-------------	--	---

제19조 (개인정보 유출사고 대응) ① 개인정보 보호책임자는 개인정보가 유출됨을 알게 되었을 때에는 지체 없이 정보주체에게 다음 각 호의 사실을 알려야 한다. 다만, 유출된 개인정보의 확산 및 추가유출을 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 방법에
등에 관한 정보
4. 대응조치 및 피해 구제절차
5. 정보주체에게 피해가 발생한 경우 신고 접수할 수 있는 담당부서 및 연락처

② 개인정보 보호책임자는 1천명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 서면 등의 방법과 함께 인터넷 홈페이지에 정보주체가 알아보기 쉽도록 위의 고지 사항을 7일 이상 게재하여야 한다.

③ 개인정보 보호책임자는 개인정보가 유출된 경우 그 피해를 최소화하기 위하여, 「개인정보 유출 및 침해사고 대응 시행세칙」에 따라 “개인정보 유출 및 침해사고 대응팀”을 구성하고 필요한 조치를 하여야 한다.

④ 개인정보보호 담당자는 1명이라도 정보주체에 관한 개인정보가 유출된 경우에는 유출내용 및 조치결과를 5일 이내에 교육부 정부 보호팀에 신고하여야 한다.

⑤ 개인정보보호 담당자는 1천명 이상의 개인정보가 유출된 경우에는 「개인정보 보호법」시행령 제39조(개인정보 유출 신고의 범위 및 기관)에 따라 한국인터넷진흥원에 신고하여야 한다.

제20조 (위험도 분석 및 대응) ① 개인정보 보호책임자는 개인정보처리시스템에서 처리되는 개인정보를 자산으로 관리하여야 하며, 개인정보 시스템책임자는 관리하는 개인정보 자산에 대하여 연 1회 이상 위험평가를 수행하여 위험요소를 최소화하여야 한다.

② 위험평가는 홈페이지 및 시스템 취약점 점검 등으로 수행할 수 있으며, 위험평가를 통해 발견된 위험요소를 최소화하기 위한 개선방안을 마련하여야 한다.

③ 개인정보보호 시스템책임자는 위험요소에 대한 개선조치가 잘되었는지 여부를 관리 · 감독

하여야 한다.

제21조 (수탁자에 대한 관리 및 감독) ① 개인정보보호 책임자는 개인정보 처리 업무를 위탁 받아 처리하는 자(이하 “수탁자”라 한다)를 선정할 때에는 인력과 물적 시설, 재정 부담능력, 기술 보유의 정도, 책임능력 등을 종합적으로 고려하여야 한다.

② 개인정보보호 취급자는 개인정보의 처리 업무를 수탁자에게 위탁하는 경우 다음 각 호의 내용이 포함된 개인정보 위탁 계약서(별지4)에 의해 행해져야 하며, 체크리스트(별지5)를 통해 개인정보 처리제한을 철저히 해야 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

③ 개인정보보호 취급자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실 · 도난 · 유출 · 변조 또는 훼손되지 않도록 수탁자를 교육하고, 처리현황 점검 등 수탁자가 개인정보를 안전하게 처리하는지 감독하여야 한다.

제8장 개인정보보호 위원회

제22조 (구성) ① 대학교는 체계적이고 효율적인 개인정보 보호정책의 수립 · 심의를 위하여 개인정보보호 위원회(이하 “위원회”라 한다)를 둔다.

② 위원회 위원은 정책부서 및 개인정보보호 업무관련성이 높은 기획관리처장, 기획관리부처장, 교학지원처장, 교학지원부처장, 로터스칼리지 원장, 대학원장, 정보지원팀장, 경영지원팀장을 당연직으로 구성한다.

③ 위원장은 금강대학교 총장으로 한다. 단, 위원장의 권한 및 책임은 기획관리처장에게 위임할 수 있다.

④ 위원장을 포함한 각 위원의 임기는 보직재임기간 및 해당업무기간으로 한다.

⑤ 본 위원회의 간사는 정보지원팀 및 경영지원팀 담당자가 한다.

⑥ 위원회 회의는 재적위원 과반수 출석과 출석위원 3분의 2이상의 찬성으로 의결한다.

제23조 (기능) 본 위원회는 다음 각 호의 기능을 전문적으로 심의 및 의결한다.

1. 개인정보보호 정책 · 규정 및 대책 수립에 관한 사항
2. 개인정보보호 관련 신규 추진 사업 및 연간계획 수립에 관한 사항
3. 대학교 개인정보 침해요인평가 및 실태조사에 관한 사항
4. 개인정보보호 위반자 심사 및 처리에 관한 사항
5. 기타 위 각호에 부수되는 제반 사항

제9장 개인정보보호 사무의 인수·인계

제24조(개인정보보호 사무의 인수·인계) ① 개인정보보호책임자와 개인정보담당자의 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 개인정보 보유목록
5. 개인정보 유출사례를 포함한 교육교재
6. 기타 개인정보보호 업무 수행에 필요한 사항

② 개인정보취급자의 변경 시 다음 각 호를 인수·인계 하여야 한다.

1. 취급하는 개인정보 보유목록
2. 통상적으로 이용·제공하는 개인정보에 관한 사항
3. 기타 개인정보보호 업무 수행에 필요한 사항

성명 : (서명)

개인정보의 수집·이용·제3자 제공에 대한 동의서 작성 요령

1. 준비 단계

- ▷ 업무처리에 필요한 개인정보 파악
 - 주민등록번호를 제외한 고유식별정보, 민감정보는 일반 개인정보와 구별하여 처리 (별도 동의 필요)
 - 고유식별정보 : 주민등록번호, 운전면허번호, 여권번호, 외국인등록번호
 - 민감정보 : 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 유전자정보, 범죄경력자료 등
- ▷ 개인정보 보유기간 확인
 - [별지제9호 서식]을 참조하여 보유기간을 확인 후 필요최소한의 보유기간 설정
- ▷ 수집·이용·제3자 제공 시 정보주체의 동의 필요 여부 확인
 - 주민등록번호는 반드시 법률, 대통령령에 의해서만 수집·이용 가능
 - 만14세 미만 아동의 개인정보 수집 시 법정대리인의 동의 필요
- ▷ 필수 사항, 선택 사항, 홍보 목적 개인정보 수집·이용·제3자 제공 여부
 - 선택 사항은 별도 동의를 받아야 함
 - 홍보 목적의 개인정보 수집·이용·제3자 제공시 별도 동의를 받아야 함
- ▷ 제3자 제공 시 고지해야 할 사항
 - ① 개인정보를 제공받는 자, ② 개인정보를 제공받는 자의 개인정보 이용 목적, ③ 제공하는 개인정보 항목, ④ 개인정보를 제공받는 자의 개인정보 보유 및 이용기간, ⑤ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

2. 작성 단계

- ▷ 동의서 작성시 글자 크기는 9포인트 이상으로 작성
- ▷ 다음 사항은 다른 내용보다 20 퍼센트 이상 크게, 글씨의 색깔, 굵기 또는 밑줄 모두를 적용하여 명확하게 표시하여야 함
 - 민감정보, 고유식별정보
 - 개인정보의 이용 목적
 - 개인정보를 제공받는 자 및 제공받는 자의 개인정보 이용 목적
 - 개인정보의 보유 및 이용 기간(제공 시에는 제공받는 자의 보유 및 이용 기간)
 - 수집·이용 목적 중 재화나 서비스의 홍보 또는 판매 권유 등을 위해 정보주체에 연락할 수 있다는 사실

[별지 제2호 서식] 바이오정보 수집·이용에 대한 동의서

바이오정보 수집·이용에 대한 동의서

금강대학교가 취급하는 모든 개인정보는 관련 법령에 근거하거나 정보주체의 동의에 의하여 수집·보유 및 처리되고 있습니다. 금강대학교는 개인정보보호법 등 관련 법령의 규정에 따라 수집·보유 및 처리하는 개인정보를 공공업무의 적절한 수행과 금강대학교 구성원의 권익을 보호하기 위해 적법하게 취급할 것입니다. 이에 따라 개인정보가 안전하게 관리될 수 있도록 필요한 사항을 아래와 같이 처리하고 있습니다.

■ [필수항목] 바이오정보의 수집·이용 동의

수집·이용 목적	수집 항목	보유·이용 기간	동의 여부
이용자 식별 및 근태관리	지문정보 (원본정보 및 특징정보)	<ul style="list-style-type: none"> • 원본정보 : 특징정보 생성시 까지 • 특징정보 : 퇴직 시 까지 	<input type="checkbox"/> 동의함 <input type="checkbox"/> 동의안함

※ 필수항목은 필요 최소한의 정보로서 동의거부 시 「시간외 근무수당」 지급이 불가능합니다.

20 년 월 일

소 속 :

사 번 :

성 명 :

(서명)

금강대학교 기획관리처장 귀하

[별지 제3호 서식] 개인정보의 목적 외 이용 및 제3자 제공 동의서

개인정보의 목적 외 이용 및 제3자 제공 동의서

금강대학교는 서비스 향상과 구성원의 이익 제공을 위하여 개인정보를 제3자와 제휴하고 있으며, 관계 법령에 따라 개인정보 제3자 제공 시 개인정보가 안전하게 관리될 수 있도록 필요한 사항을 규정하고 있습니다. 대학교의 개인정보 제3자 제공 내용은 아래와 같습니다.

■ 개인정보 제3자 제공 내역

개인정보를 제공받는 자	제공 목적	제공 항목	보유 및 이용 기간
00업체	비교과프로그램 운영	성명	비교과 프로그램 종류 후 파기

※ 위의 개인정보 제공에 대한 동의를 거부할 권리가 있습니다. 그러나 동의를 거부할 경우 비교과 프로그램 참여가 불가능합니다.

 위와 같이 개인정보를 제공하는데 동의하십니까? ☐ 예 ☐ 아니오

■ 기타 고지 사항

“개인정보 보호법 제18조제2항 제2호에 따라 정보주체의 동의 없이 개인정보 제3자에게 제공합니다.

개인정보 제공사유	개인정보 항목	제공 근거
비교과 프로그램운영	주민등록번호	0000법

소 속 : ○○학부

학 과 :

학 년 :

성 명 : (인)

금강대학교 교학지원처장 귀하

[별지 제4호 서식] 표준 개인정보처리위탁 계약서 및 체크리스트

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.

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

표준 개인정보처리위탁 계약서(안)

○○○(이하 “갑”이라 한다)과 △△△(이하 “을”이라 한다)는 “갑”의 개인정보 처리업무를 “을”에게 위탁함에 있어 다음과 같은 내용으로 본 업무위탁계약을 체결한다.

제1조 (목적) 이 계약은 “갑”이 개인정보처리업무를 “을”에게 위탁하고, “을”은 이를 승낙하여 “을”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 시행규칙, 「개인정보의 안전성 확보조치 기준」(행정안전부 고시 제2017-1호) 및 「표준 개인정보 보호지침」(행정안전부 고시 제2017-1호)에서 정의된 바에 따른다.

제3조 (위탁업무의 목적 및 범위) “을”은 계약이 정하는 바에 따라 () 목적으로 다음과 같은 개인정보 처리 업무를 수행한다.¹⁾

- 1.
- 2.

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

계약 기간 : 2000년 0월 0일 ~ 2000년 0월 0일

제5조 (재위탁 제한) ① “을”은 “갑”의 사전 승낙을 얻은 경우를 제외하고 “갑”과의 계약상의 권리와 의무의 전부 또는 일부를 제3자에게 양도하거나 재위탁할 수 없다.

② “을”이 다른 제3의 회사와 수탁계약을 할 경우에는 “을”은 해당 사실을 계약 체결 7일 이전에 “갑”에게 통보하고 협의하여야 한다.

제6조 (개인정보의 안전성 확보조치) “을”은 「개인정보 보호법」 제23조제2항 및 제24조제3항 및 제29조, 같은 법 시행령 제21조 및 제30조, 「개인정보의 안전성 확보조치 기준」(행정안전부 고시 제2017-1호)에 따라 개인정보의 안전성 확보에 필요한 기술적·관리적 조치를 취하여야 한다.

제7조 (개인정보의 처리제한) ① “을”은 계약기간은 물론 계약 종료 후에도 위탁업무 수행 목

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

적 범위를 넘어 개인정보를 이용하거나 이를 제3자에게 제공 또는 누설하여서는 안 된다.

② “을”은 계약이 해지되거나 또는 계약기간이 만료된 경우 위탁업무와 관련하여 보유하고 있는 개인정보를 「개인정보 보호법 시행령」 제16조 및 「개인정보의 안전성 확보조치 기준」(행정안전부 고시 제2017-1호)에 따라 즉시 파기하거나 “갑”에게 반납하여야 한다.

③ 제2항에 따라 “을”이 개인정보를 파기한 경우 지체없이 “갑”에게 그 결과를 통보하여야 한다.

제8조 (수탁자에 대한 관리·감독 등) ① “갑”은 “을”에 대하여 다음 각 호의 사항을 감독할 수 있으며, “을”은 특별한 사유가 없는 한 이에 응하여야 한다.

1. 개인정보의 처리 현황
2. 개인정보의 접근 또는 접속기록
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 “갑”은 “을”에 대하여 제1항 각 호의 사항에 대한 실태를 점검하여 시정을 요구할 수 있으며, “을”은 특별한 사유가 없는 한 이행하여야 한다.

③ “갑”은 처리위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 1년에 ()회 “을”을 교육할 수 있으며, “을”은 이에 응하여야 한다²⁾

④ 제1항에 따른 교육의 시기와 방법 등에 대해서는 “갑”은 “을”과 협의하여 시행한다.

제9조 (정보주체 권리보장) ① “을”은 정보주체의 개인정보 열람, 정정·삭제, 처리 정지 요청 등에 대응하기 위한 연락처 등 민원 창구를 마련해야 한다.

제10조 (개인정보의 파기) ① “을”은 제4항의 위탁업무기간이 종료되면 특별한 사유가 없는 한 지체 없이 개인정보를 파기하고 이를 “갑”에게 확인받아야 한다.

제11조 (손해배상) ① “을” 또는 “을”의 임직원 기타 “을”의 수탁자가 이 계약에 의하여 위탁 또는 재위탁 받은 업무를 수행함에 있어 이 계약에 따른 의무를 위반하거나 “을” 또는 “을”의 임직원 기타 “을”의 수탁자의 귀책사유로 인하여 이 계약이 해지되어 “갑” 또는 개인정보주체 기타 제3자에게 손해가 발생한 경우 “을”은 그 손해를 배상하여야 한다.

② 제1항과 관련하여 개인정보주체 기타 제3자에게 발생한 손해에 대하여 “갑”이 전부 또는 일부를 배상한 때에는 “갑”은 이를 “을”에게 구상할 수 있다.

본 계약의 내용을 증명하기 위하여 계약서 2부를 작성하고, “갑”과 “을”이 서명 또는 날인한 후 각 1부씩 보관한다.

갑
○○시 ○○구 ○○동 ○○번지
성 명 : (인)

을
○○시 ○○구 ○○동 ○○번지
성 명 : (인)

2) 「개인정보의 안전성 확보조치 기준」(행정안전부 고시 제 호) 및 「개인정보 보호법」 제 26조에 따라 개인정보처리자 및 취급자는 개인정보보호에 관한 교육을 의무적으로 시행하여야 한다.

[별지 제5호 서식] 표준 개인정보처리위탁 체크리스트

단 계	번 호	점검 사항	대상
계 약 전	1	위탁자는 위탁할 업무의 개인정보 위험성을 확인하였는가?	위탁자
	2	위탁자는 수탁자의 개인정보 보호 역량을 확인하였는가?	위탁자
	3	위탁자는 위탁하여 처리할 개인정보의 범위를 명확히 하고 수탁자와 사전 협의 하였는가?	위탁자
	4	위·수탁자는 다음 6가지 내용이 포함된 위·수탁 문서를 작성하였는가? ① 위탁업무의 목적 및 범위 ② 위탁업무 수행 목적 외 개인정보 처리 금지에 관한 사항 ③ 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항 ④ 개인정보의 기술적·관리적 보호조치에 관한 사항 ※ 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항 ⑤ 재위탁 제한에 관한 사항 ⑥ 수탁자가 준수하여야할 의무를 위반한 경우 손해배상 등 책임에 관한 사항	위탁자 수탁자
	5	만약 위·수탁 업무 종료 후에도 수탁자가 개인정보를 보관하는 등 추가 처리를 해야 하는 사유가 있다면 미리 위·수탁 문서에 이를 포함 하였는가?	
	6	만약 법령상 수탁자에게 개인정보를 보관해야 하는 의무가 발생하는 경우 위탁자에게 이를 미리 알리고 위·수탁 문서 내에 법률상 근거와 개인정보 보관 기간·목적 등을 명시하였는가?	
업 무 수 행 중	7	위탁자는 위탁 업무 내용과 수탁자를 홈페이지 등에 공개하였는가?	위탁자
	8	위탁자는 수탁자의 개인정보 처리가 안전한지 여부를 감독하기 위한 계획을 수립하고 시행하였는가?	위탁자
	9	수탁자는 법 제29조의 안전조치 의무를 다하였는가? ① 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행 ② 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치 ③ 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치 ④ 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치 ⑤ 개인정보에 대한 보안프로그램의 설치 및 갱신 ⑥ 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치	수탁자
	10	위탁자는 수탁자 대상 개인정보보호 교육을 위한 계획을 세우고 시행하였는가?	
	11	위탁자와 수탁자는 개인정보 열람·정정·파기 요청 등 정보주체의 권리 행사를 보장하기 위한 창구를 마련하였는가?	위탁자 수탁자
	12	수탁자는 개인정보 파기 사유가 발생한 경우 지체 없이 이를 파기하였는가?	수탁자
업 무 종 료 후	13	위탁자는 수탁자의 개인정보 파기를 확인하였는가?	위탁자

[별지 제6호 서식] 개인정보 열람, 정정·삭제, 처리정지 요구서

개인정보(☐ 열람 ☐ 정정·삭제 ☐ 처리정지) 요구서

※ 아래 작성방법을 읽고 굵은 선 안쪽의 사항만 적어 주시기 바랍니다.

(앞 쪽)

접수번호	접수일	처리 기간
		10일 이내

정보주체	성 명	전 화 번 호
	생년월일	
	주 소	

대리인	성 명	전 화 번 호
	생년월일	정보주체와의 관계
	주 소	

요구내용	<input type="checkbox"/> 열람	<input type="checkbox"/> 개인정보의 항목 및 내용
		<input type="checkbox"/> 개인정보 수집·이용의 목적
		<input type="checkbox"/> 개인정보 보유 및 이용 기간
		<input type="checkbox"/> 개인정보의 제3자 제공 현황
		<input type="checkbox"/> 개인정보 처리에 동의한 사실 및 내용
	<input type="checkbox"/> 정정·삭제	※ 정정·삭제하려는 개인정보의 항목과 그 사유를 적습니다.
	<input type="checkbox"/> 처리정지	※ 개인정보의 처리정지를 원하는 대상·내용 및 그 사유를 적습니다.

「개인정보 보호법」 제35조제1항·제2항, 제36조제1항 또는 제37조제1항과 같은 법 시행령 제41조제1항, 제43조제1항 또는 제44조제1항에 따라 위와 같이 요구합니다.

년 월 일

요구인

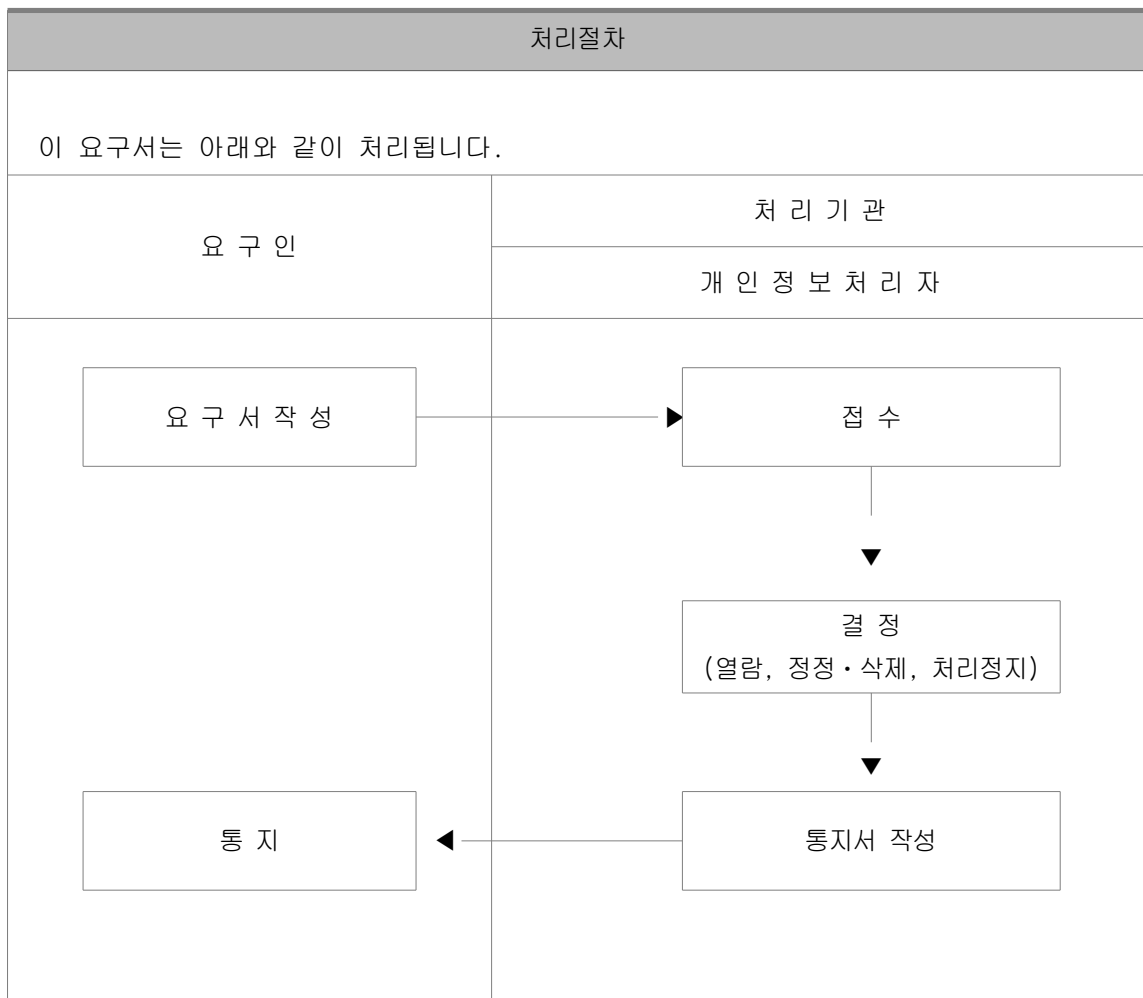
(서명 또는 인)

금 강 대 학 교 귀하

작성방법

1. ‘대리인’ 란은 대리인이 요구인일 때에만 적습니다.
2. 개인정보의 열람을 요구하려는 경우에는 ‘열람’ 란에 ☒ 표시를 하고 열람하려는 사항을 선택하여 ☒ 표시를 합니다. 표시를 하지 않은 경우에는 해당 항목의 열람을 요구하지 않은 것으로 처리됩니다.
3. 개인정보의 정정·삭제를 요구하려는 경우에는 ‘정정·삭제’ 란에 ☒ 표시를 하고 정정하거나 삭제하려는 개인정보의 항목과 그 사유를 적습니다.
4. 개인정보의 처리정지를 요구하려는 경우에는 ‘처리정지’ 란에 ☒ 표시를 하고 처리정지 요구의 대상·내용 및 그 사유를 적습니다.

210mm×297mm[일반용지 70g/㎡(재활용품)]



[별지 제7호 서식] 개인정보 열람, 일부열람, 열람연기, 열람거절 통지서

개인정보 (☐ 열람 ☐ 일부열람 ☐ 열람연기 ☐ 열람거절) 통지서

(앞 쪽)

수신자번호:

주소:

요구 내용			
열람 일시			열람 장소
통지 내용 (<input type="checkbox"/> 열람 <input type="checkbox"/> 일부열람 <input type="checkbox"/> 열람연기 <input type="checkbox"/> 열람거절)			
열람 형태 및 방법	열람 형태	<input type="checkbox"/> 열람·시청 <input type="checkbox"/> 사본·출력물 <input type="checkbox"/> 전자파일 <input type="checkbox"/> 복제물·인화물 <input type="checkbox"/> 기타	
	열람 방법	<input type="checkbox"/> 직접방문 <input type="checkbox"/> 우편 <input type="checkbox"/> 팩스 <input type="checkbox"/> 전자우편 <input type="checkbox"/> 기타	
납부 금액	①수수료	②우송료	계(①+②)
	원	원	원
	수수료 산정 명세		
사 유			
이의제기방법			

「개인정보 보호법」 제35조제3항·제4항 또는 제5항과 같은 법 시행령 제41조제4항 또는 제42조제2항에 따라 귀하의 개인정보 열람 요구에 대하여 위와 같이 통지합니다.

년 월 일

금 강 대 학 교 총 장 직인

[별지 제8호 서식] 개인정보 정정·삭제, 처리정지 요구에 대한 결과 통지서

개인정보 ([] 정정·삭제, [] 처리정지) 요구에 대한 결과 통지서

수신자 우편번호:

주소:

요구 내용	
<input type="checkbox"/> 정정·삭제 <input type="checkbox"/> 처리정지 조치 내용	
<input type="checkbox"/> 정정·삭제 <input type="checkbox"/> 처리정지 결정 사유	
이의제기방법	

「개인정보 보호법」 제36조제6항 및 같은 법 시행령 제43조제3항 또는 같은 법 제37조제5항 및 같은 법 시행령 제44조제2항에 따라 귀하의 요구에 대한 결과를 위와 같이 통지합니다.

년 월 일

금강대학교총장 직인

유의사항

개인정보의 정정·삭제 또는 처리정지 요구에 대한 결정을 통지받은 경우에는 개인정보처리자가 '이의제기방법'란에 적은 방법으로 이의제기를 할 수 있습니다.

[별지 제9호 서식] 개인정보파일 보유기간 책정기준표

개인정보파일 보유기간 책정기준표

보유기간	대상 개인정보파일
영구	1. 학생 및 교직원의 지위, 신분, 재산을 증명하기 위해 운용하는 개인정보파일 중 영구보존이 필요한 개인정보파일 2. 국민의 건강증진과 관련된 업무를 수행하기 위해 운용하는 개인정보파일 중 영구보존이 필요한 개인정보파일
준영구	1. 학생 및 교직원의 신분, 재산을 증명하기 위해 운용하는 개인정보파일 중 개인이 사망, 폐지 그 밖의 사유로 소멸되기 때문에 영구보존할 필요가 없는 개인정보파일 2. 학생 및 교직원의 신분증명 및 의무부과, 특정대상 관리 등을 위하여 행정기관이 구축하여 운영하는 행정정보시스템의 데이터 셋으로 구성된 개인정보 파일 3. 대학교 개인정보파일 표준목록의 보유기간에서 정한 개인정보파일
30년	1. 관계법령에 따라 10년 이상 30년 미만의 기간 동안 민.형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일 2. 대학교 개인정보파일 표준목록의 보유기간에서 정한 개인정보파일
10년	1. 관계법령에 따라 5년 이상 10년 미만의 기간 동안 민.형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일 2. 대학교 개인정보파일 표준목록의 보유기간에서 정한 개인정보파일
5년	1. 관계법령에 따라 3년 이상 5년 미만의 기간 동안 민.형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일 2. 대학교 개인정보파일 표준목록의 보유기간에서 정한 개인정보파일
3년	1. 행정업무의 참고 또는 사실증명을 위하여 1년 이상 3년 미만의 기간 동안 보존할 필요가 있는 개인정보파일 2. 관계 법령에 따라 1년 이상 3년 미만의 기간 동안 민.형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일 3. 각종 증명서 발급과 관련된 개인정보파일 (단, 다른 법령에서 증명서 관련 보유기간이 별도로 규정된 경우 해당 법령에 따름) 4. 대학교 개인정보파일 표준목록의 보유기간에서 정한 개인정보파일
1년	1. 상급기관(부서)의 요구에 따라 단순 보고를 위해 생성한 개인정보파일

[별지 제10호 서식] 개인정보파일 파기 요청서

개인정보파일 파기 요청서

작성일		작성자 (해당 업무 처리자)	
파기 대상 개인정보파일			
생성일자		개인정보취급자	
주요 대상업무		현재 보관건수	
파기 사유			
파기 일정			
특기사항			
파기 승인일		승인자 (개인정보관리책임자, CPO)	
파기 장소			
파기 방법			
파기 수행자 (해당 업무 처리자)		입회자 (개인정보보호담당자)	
폐기 확인 방법			
백업 조치 유무			
매체 폐기 여부			

[별지 제12호 서식] 개인정보 유출신고서

개인정보 유출신고서

기관명					
정보주체에의 통지 여부					
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
	개인정보보 호책임자				
	개인정보취 급자				

유출신고접수기관	기관명	담당자명	연락처