개인정보보호 내부 관리계획

2026. 2.

계 명 대 학 교

개정 이력

개정일자	소속	개인정보 보호담당자	개정 내용
2014.1.2.	전산개발팀	정훈	1. 신규 작성
2015.2.23.	전산개발팀	김도균	1. 법 개정에 따른 내용변경 2. 직제개편에 따른 분야별책임자 변경 3. 기타 미비사항 보완
2016.3.7.	전산개발팀	김도균	1. 법 개정에 따른 내용변경 2. 직제개편에 따른 분야별책임자 변경 3. 기타 미비사항 보완
2016.12.1.	전산개발팀	안용호	1. 개정된 개인정보 보호법 반영 2. 직제개편에 따른 분야별책임자 변경 3. 개인정보 처리에 관한 내부 절차 추가 4. 개인정보 안정성 확보조치 기준 변경에 따른 절차 추가 5. 기타 미비사항 보완
2018.2.8.	전산개발팀	안용호	1. 용어 정의 일부 변경 2. 악성프로그램 등 방지 내용 변경 3. 위험도 분석 및 대응방안 추가 4. 침해사고 구제방법 내용 변경
2019.2.25.	전산개발팀	안용호	1. 개인정보보호 분야별 책임자 변경 2. 유출통지 인원 변경 3. 비밀번호 작성 규칙 변경 4. 개인정보의 목적 외 이용 및 제3자 제공 대장 양식 수정 5. 기타 미비사항 보완
2020.2.19.	전산개발팀	서창범	1. 개정된 개인정보 보호법 반영 2. 직제개편에 따른 분야별책임자 변경 3. 개인정보 안정성 확보조치 기준 변경 내용 반영 4. 재해 · 재난 대비 안전조치 대응방안 내용 보완
2021.2.17.	전산개발팀	서창범	1. 개인정보보호 행정기관을 행정안전부에서 개인정보보호위원회로 변경 2. 개인정보 침해사고 대응방안 내용 보완

			3. 기타 미비사항 보완
2022.2.18.	전산개발팀	최은영	1. 직제개편에 따른 분야별책임자 변경 2. 침해사고 인지경로(개인정보침해신고센터) 변경 교육사이버안전센터(한국교육학술정보원) → 한국인터넷진흥원 3. 영상정보처리기기 운영관리 문구 수정 4. 침해사고 발생 시 재발 방지를 위한 개인정보보호 특별 교육 조항 추가
2023.2.22.	전산개발팀	최은영	1. 직제개편에 따른 개인정보 보호조직, 분야별책임자, 기술적 조치 시행부서 일부 변경
2024.2.27.	전산개발팀	최은영	1. 개정된 개인정보 보호법 반영 2. 직제개편에 따른 분야별책임자 변경 3. 기타 자구 수정
2025.2.24.	전산개발팀	최은영	1. 직제개편에 따른 개인정보 보호조직, 분야별책임자 변경 2. [붙임1] 자체점검 항목 변경 3. 기타 자구 수정
2026.2.20.	전산개발팀	최은영	1. 직제개편에 따른 개인정보 보호조직, 분야별책임자 변경 2. 기타 자구 수정

< 목 차 >

1. 총칙 ····· 5
  1.1 목적 ····· 5
  1.2 적용범위 ····· 5
  1.3 용어정의 ····· 5
2. 내부 관리계획의 수립 및 시행 ····· 6
  2.1 내부 관리계획의 수립 ····· 6
  2.2 내부 관리계획의 공표 ····· 7
3. 개인정보 보호조직 구성·운영 ····· 7
  3.1 개인정보 보호조직 ····· 7
  3.2 역할별 임무 ····· 9
4. 개인정보의 관리적 안전조치 ····· 11
  4.1 고유식별정보·민감정보 처리 제한(법 제23조~제24조) ····· 11
  4.2 개인정보의 수집, 이용(법 제15조~제16조) ····· 11
  4.3 개인정보 제공(법 제17조~18조, 영 제15조, 규칙 제3조) ····· 12
  4.4 개인정보 처리업무 위탁시 수탁자에 대한 관리 및 감독(법 제26조) ····· 14
  4.5 개인정보 파기(법 제21조) ····· 15
  4.6 정보주체의 권리 보장 및 행사 절차 ····· 15
5. 개인정보의 기술적·물리적 안전조치 ····· 16
  5.1 물리적 접근권한 및 관리 ····· 16
  5.2 출력·복사 시 안전조치 ····· 16
  5.3 개인정보취급자 접근권한 관리 ····· 17
  5.4 개인정보의 암호화 ····· 17
  5.5 접근통제 ····· 18
  5.6 접속기록의 위·변조 방지 ····· 19
  5.7 악성프로그램 등 방지 ····· 19
  5.8 기술적 안전조치 ····· 19
  5.9 기술적·관리적 안전조치 수행 계획 ····· 20
  5.10 고정형 영상정보처리기기의 설치 및 운영관리 ····· 21
  5.11 위험도 분석 및 대응방안 ····· 22
6. 개인정보 침해사고 대응방안 ····· 22
  6.1 침해사고 정의 ····· 22
  6.2 침해사고 대상 ····· 22
  6.3 침해사고 유형 ····· 22
  6.4 침해사고 발생 시 조치방법 ····· 23

6.5 침해사고 유출통지 ····23
6.6 침해사고 대응반 조직(연락) 및 역할 ····27
6.7 침해사고 발생 시 업무분장 ····27
6.8 침해사고 신고방법 ····28
6.9 침해사고 구제방법 ····28
6.10 침해사고 처리보고 ····29
6.11 사고예방 ····29
7. 재해·재난 대비 안전조치 대응방안 ····30
7.1 재해·재난 발생 시 조치 방법 ····30
7.2 재해·재난 발생 시 업무분장 ····31
7.3 재해·재난 대비 개인정보처리시스템 백업 계획 ····32
7.4 재해·재난 대비 개인정보처리시스템 복구 계획 ····32
7.5 재해·재난 대비 개인정보처리시스템 정기 점검 및 사후처리 계획 ····32
7.6 개인정보처리시스템 구성 현황 ····32
8. 개인정보보호 교육 수행 ····32
8.1 개인정보보호 교육 계획의 수립 ····32
8.2 개인정보보호 교육의 실시 ····33
9. 개인정보 자체점검 실시 및 결과 반영 ····34
9.1 자체점검 주기 및 절차 ····34
9.2 자체점검 실시 ····35
9.3 자체점검 결과 반영 ····35

1. 총칙

1.1 목적

개인정보보호 내부 관리계획(이하 '본 계획' 또는 '내부 관리계획' 이라 한다.)은「개인정보 보호법」제29조(안전조치의무) 및 같은 법 시행령 제30조(개인정보의 안전성 확보 조치)에 따라 계명대학교(이하 '우리 대학교' 라 한다.)가 취급하는 개인정보를 처리함에 있어 개인정보가 분실, 도난, 유출, 위조, 변조, 훼손, 오·남용 등이 되지 아니하도록 함으로써 정보주체자의 권익 보호 및 교직원이 준수하여야 하는 세부적인 기준을 정함을 목적으로 한다.

1.2 적용범위

본 계획은 개인정보처리시스템, PC, 종이, 고정형 영상정보처리기기 등을 통해서 수집, 이용, 제공 또는 관리되는 모든 형태의 개인정보 및 개인영상정보기기(CCTV)에 대해서도 적용되며, 이러한 개인정보를 취급하는 내부직원(계약직 등 비정규직 포함) 및 외부 위탁업체 직원에 대해 적용된다.

1.3 용어정의

본 계획에서 사용하는 용어의 정의는 다음 각 호와 같다.

가. 개인정보

- 살아있는 개인에 관한 정보로서 성명, 주민등록번호, 영상 등 개인을 알아볼 수 있는 정보(해당 정보만으로는 개인을 알아볼 수 없더라도 다른 정보와 결합하여 알아볼 수 있는 것을 포함)를 말한다.

나. 개인정보파일

- 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.

다. 정보주체

- 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.

라. 개인정보 보호대상

- 개인정보처리시스템, PC, 종이,고정형 영상정보처리기기 등에서 업무상 필요에 의하여 처리 되고 있는 개인정보를 말한다.

마. 개인정보 처리

- 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.

바. 개인정보 보호책임자

- 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지거나 업무처리를 최종적으로 결정하는 자로서,「개인정보 보호법 시행령」제32조제2항제1호 및 제2호에 해당하는 자를 말하며,「개인정보 보호법」제31조에 따른 업무를 수행한다.

사. 개인정보보호 담당자
- 개인정보 보호책임자 또는 분야별책임자 업무를 보좌하기 위해서 지정된 자를 말한다.

아. 개인정보보호 분야별 책임자
- 대학 각 부서의 개인정보 업무를 지휘·감독하는 자를 말한다.

자. 개인정보처리자
- 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.

차. 개인정보취급자
- 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.

카. 개인정보처리시스템
- 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 응용시스템을 말한다.

타. 고정형 영상정보처리기기
- 일정한 공간에 설치되어 지속적 또는 주기적으로 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 시행령 제3조에 따른 폐쇄회로텔레비전(CCTV) 및 네트워크 카메라를 말한다.

파. 개인영상정보
- 고정형 영상정보처리기기에 의하여 촬영·처리되는 영상정보 중 개인의 초상, 행동 등과 관련된 영상으로서 해당 개인을 식별할 수 있는 정보를 말한다.

하. 고정형 영상정보처리기기 운영자
- 「개인정보 보호법」제25조제1항 각 호에 따라 고정형 영상정보처리기기를 설치·운영하는 자를 말한다.

2. 내부 관리계획의 수립 및 시행

2.1 내부 관리계획의 수립

가. 개인정보보호 담당자는「개인정보 보호법」제29조와 같은 법 시행령 제30조 및 「개인정보의 안전성 확보조치 기준」(개인정보보호위원회고시 제2023-6호, 2023. 9. 22.) 제4조에 따라 우리 대학교의 개인정보보호를 위한 전반적인 사항을 포함하여 내부 관리계획을 수립하여야 한다.

나. 개인정보보호 담당자는 개인정보보호를 위한 내부 관리계획의 수립 시, 개인정보보호와 관련된 법령 및 규정을 준수하도록 내부 관리계획을 수립하여야 한다.

다. 개인정보 보호책임자는 개인정보보호 담당자가 수립한 내부 관리계획의 타당

성을 검토하여 개인정보보호를 위한 내부 관리계획을 승인하여야 한다.

라. 개인정보보호 담당자는 개인정보보호 관련 법령의 제·개정 사항 등을 반영하기 위하여 매년 2월까지 내부 관리계획의 타당성과 개정 필요성을 검토하여야 한다.

마. 개인정보보호 담당자는 모든 항목의 타당성을 검토한 후 개정할 필요가 있다고 판단되는 경우 2월까지 내부 관리계획의 개정안을 작성하여 개인정보 보호책임자에게 보고하고 개인정보 보호책임자의 승인을 받아야 한다.

2.2 내부 관리계획의 공표

가. 개인정보 보호책임자는 내부 관리계획을 학칙 또는 우리 대학교 규정에 정하지 않은 경우, 30일 이내, 교내 전 교직원 및 학생에게 공표한다.

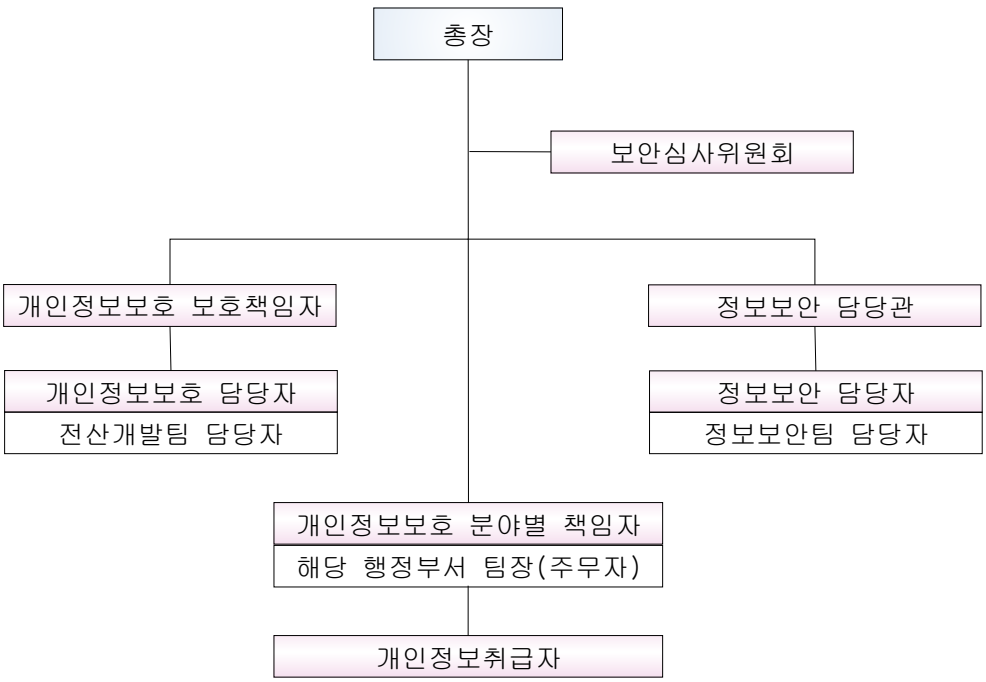
나. 내부 관리계획은 교내 전 교직원 및 학생이 언제든지 열람(홈페이지 게재, 유인물 배포, E-mail 발송 등)할 수 있도록 하여야 하며, 변경사항이 있을 경우에는 이를 즉시 공지하여야 한다.

3. 개인정보 보호조직 구성·운영

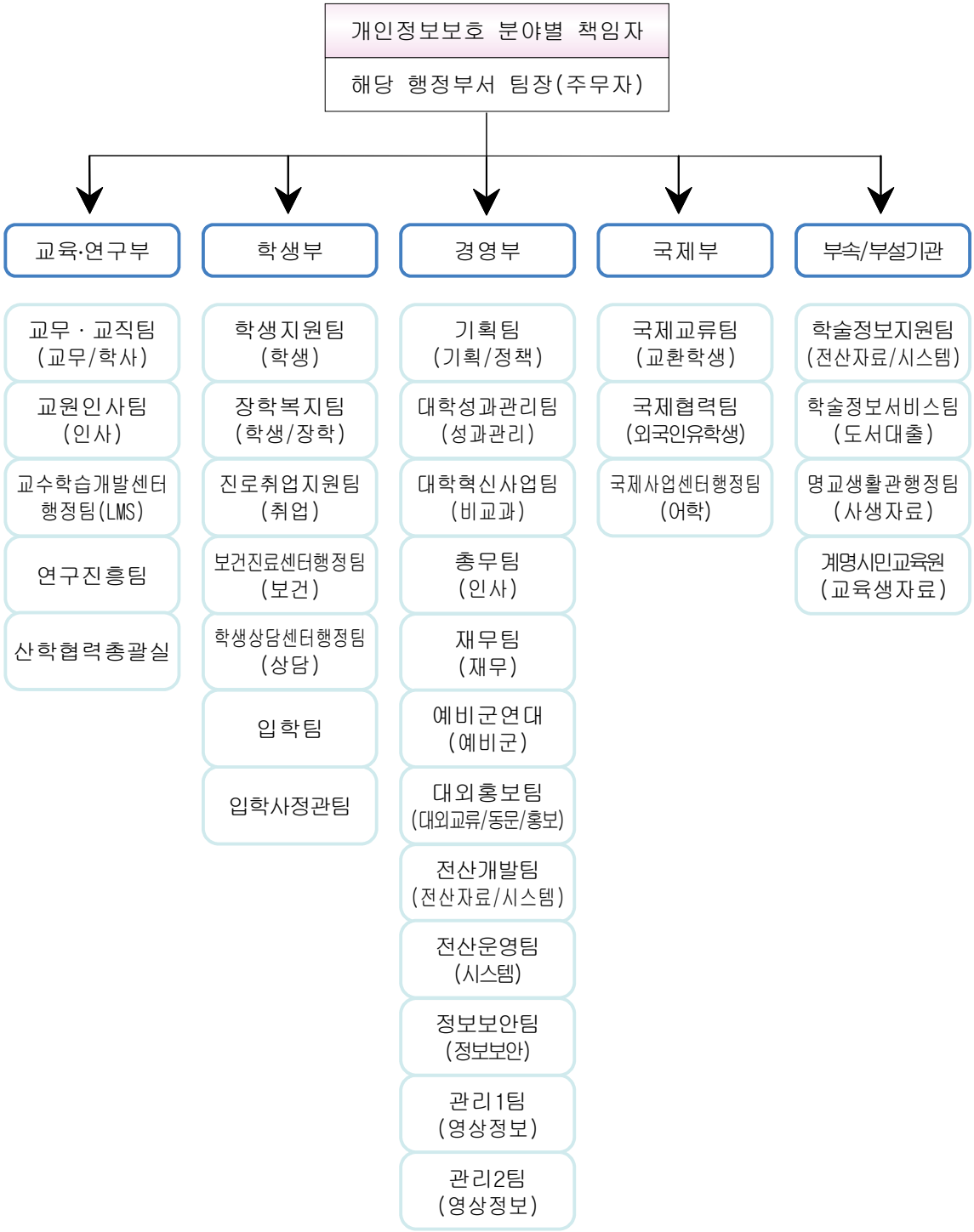
개인정보 처리에 관한 업무를 총괄하는 개인정보 보호책임자는 개인정보 분야별 책임자와 개인정보보호 담당자를 지정하여 개인정보 보호조직을 구성하고, 각각의 역할과 책임을 정의한다.

3.1 개인정보 보호조직

가. 우리 대학교 개인정보보호정책을 수행하고 유사시 신속하고 효율적인 대응을 도모할 개인정보 보호조직은 다음과 같다.



<그림1> 계명대학교 개인정보 보호조직



<그림2> 계명대학교 개인정보보호 분야별 책임자(※주요 부서만 기재)

3.2 역할별 임무

직책	담당	임무
개인정보 보호책임자	기획처장	- 개인정보보호 정책의 검토 · 승인 및 총괄업무 - 정보주체 개인정보의 수집 · 이용 · 제공 및 관리에 관한 업무의 총괄 - 개인정보보호 분야별 책임자 및 취급자의 의무와 책임의 규정 및 총괄관리 - 내부 관리계획의 수립 및 승인 - 개인정보보호 관련 내부 지침 제 · 개정 - 개인정보의 기술적 · 관리적 안전조치 기준 이행 총괄 - 직원 또는 제3자에 의한 위법 · 부당한 개인정보 침해행위에 대한 점검, 대응, 사후조치 - 정보주체로부터 제기되는 개인정보에 관한 고충이나 의견의 처리 및 감독 총괄 - 개인정보 보호책임자는 개인정보보호분야별 책임자 및 최소한의 개인정보취급자 지정 - 개인정보보호에 대한 교육 및 보안서약 등을 통해 개인정보 침해사고를 사전에 예방 - 본 계획에 규정된 개인정보보호와 관련된 제반 조치의 시행 총괄 - 기타 정보주체의 개인정보보호에 필요한 사항
개인정보보호 담당자	전산개발팀 담당자	- 개인정보보호 계획 수립 및 시행 - 개인정보처리 실태 점검 및 개선 권고 - 개인정보 처리와 관련된 불만 처리 및 피해 구제 - 개인정보보호 교육 계획 수립 및 시행 - 개인정보파일 및 대장 등록 · 파기, 승인, 관리 감독 - 개인정보처리방침 수립 및 시행 - 개인정보보호 관련 자료 관리

직책	담당	임무
개인정보보호 분야별 책임자	개인정보 취급 부서의 팀장(주무자)	- 개인정보취급자 지정 · 관리감독 및 교육 - 개인정보파일의 등록, 파기, 변경 확인 - 개인정보 수집 · 이용 · 제공 등에 대한 절차 및 기준마련 - 입 · 출력자료, 전산기기 등의 안전성 확보 책임 - 개인정보파일 지정 · 관리 · 보호 · 파기 - 공개 대상 개인정보파일 등록 · 공개 - 공개 대상 개인정보파일의 처리방침 수립 · 시행 및 공개 - 고정형 영상정보처리기기 운영 · 관리 방침 수립 · 시행 - 개인정보보호 관련 자료 관리 및 제출 - 개인정보 처리와 관련한 요구 처리 및 피해 구제 - 개인정보 유출 통지 및 피해확산 방지 - 개인정보취급자에 대한 교육 및 자체점검 실시 - 개인정보 관련 개선 권고 및 시정조치사항 이행 등
개인정보 취급자		- 개인정보보호 활동 참여 - 내부 관리계획의 준수 및 이행 - 개인정보의 기술적 · 관리적 안전조치 기준 이행 - 직원 또는 제3자에 의한 위법 · 부당한 개인정보 침해행위에 대한 점검 등 - 기타 정보주체의 개인정보보호를 위해 필요한 사항의 이행

4. 개인정보의 관리적 안전조치

4.1 고유식별정보 · 민감정보 처리 제한(법 제23조~제24조)

가. 정보주체에게 고유식별정보 · 민감정보 처리에 대해 별도로 동의를 받거나, 법령에서 처리를 요구하거나 허용하는 경우에 한하여 사용할 수 있다.

나. 개인정보처리자는「개인정보 보호법」제24조의2(주민등록번호 처리의 제한)에 따라 정보주체의 동의가 있더라도 주민등록번호를 수집해서는 아니된다. 단, 같은 법에 의거 아래의 예외적 허용 사유에 해당되는 경우는 예외로 한다.

<주민등록번호 처리의 예외적 허용 사유>

① 법률 · 대통령령 · 국회규칙 · 대법원규칙 · 헌법재판소규칙 · 중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우
② 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위해 명백히 필요한 경우
③ 기타 주민등록번호 처리가 불가피한 경우로서 보호위원회가 고시로 정하는 경우

다. 인터넷 홈페이지를 통하여 회원으로 가입하는 단계에서는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하여야 한다.

4.2 개인정보의 수집, 이용(법 제15조~제16조)

가. 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우 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 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우
4) 정보주체와의 체결한 계약을 이행하거나 계약을 체결하는 과정에서 정보주체의 요청에 따른 조치를 이행하기 위하여 필요한 경우
5) 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, 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다.
7) 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우

나. 정보주체의 동의를 받아 수집 · 이용하는 경우 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.

1) 개인정보의 수집 · 이용 목적
2) 수집하려는 개인정보의 항목

3) 개인정보의 보유 및 이용 기간
4) 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

다. 개인정보처리자는 당초 수집 목적과 합리적으로 관련된 범위에서 정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 대통령령으로 정하는 바에 따라 정보주체의 동의 없이 개인정보를 이용할 수 있다.

4.3 개인정보 제공(법 제17조~18조, 영 제15조, 규칙 제3조)

가. 개인정보 분야별 책임자는 다음 각 호의 어느 하나에 해당하는 경우 제3자 제공 및 목적 외 이용할 수 있다. 이 경우 개인정보취급자는 개인정보 보호법 및 기타법령 등에 제공 근거가 있는지 확인 후 제공하여야 한다.

1) 정보주체로부터 별도의 동의를 받은 경우
2) 다른 법률에 특별한 규정이 있는 경우
3) 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
4) 개인정보를 목적 외의 용도로 이용하거나 제3자에게 제공하지 않으면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로 개인정보보호위원회의 심의·의결을 거친 경우
5) 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우
6) 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우
7) 법원의 재판업무 수행을 위하여 필요한 경우
8) 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우
9) 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우

※ 개인정보 수집근거가 11페이지 4.2의 '가' 항의 2), 3), 5) 인 경우 그 수집목적범위 내 제3자 제공 가능

나. 개인정보취급자는 '가' 항의 어느 하나의 경우에 해당하여 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우에는 이용목적, 이용하고자 하는 처리 정보의 범위가 명시된 공문으로 제공하여야 하며, 제공 시 유출방지(행정전자서명, 관련 보안기술 적용)등의 조치를 취해야 한다. 이와 함께 **개인정보의 목적 외 이용 및 제3자 제공 대장[붙임 9]**도 함께 작성하여 보관한다. 부득이 이메일, USB, CD의 매체를 이용할 경우는 반드시 보안조치(암호화 등)를 취한 후 제공하여야 한다.

다. 개인정보취급자는 '가' 항의 어느 하나의 경우에 해당하여 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우에는 개인정보를 제공받는 자에게 이용목적, 이용 방법, 그 밖에 필요한 사항에 대하여 제한을 하거나, 개인정보의 안전성 확보를 위하여 필요한 조치(기술적·관리적 보호 조치, 문서화 요청

등)를 마련하도록 요청하여야 한다. 이 경우는 요청을 받은 자는 개인정보의 안전성 확보를 위하여 필요한 조치를 하여야 한다.

※ 제3자 제공시 안전성 확보 방안 예시
① 제공되는 개인정보 ○○○는 요청하신 ○○○ 목적으로만 이용이 가능하며 ○○○까지만 이용 및 보유가 가능합니다.
② 제공되는 개인정보 ○○○는 제공 목적 달성 시 즉시 삭제해 주십시오.
③ 제공되는 개인정보 ○○○는 본 기관의 허락 없이 타 기관에 재 제공을 금하며, 재제공한 내역이 발견되면 향후 귀 기관에 정보가 제공되지 않습니다.
④ 제공된 개인정보의 안전한 관리는 귀 기관의 책임이며 본 기관은 이에 대해 어떠한 책임도 지지 않습니다.

라. 개인정보 보호책임자는 개인정보 보호법(제17조~18조, 영 제15조, 규칙 제3조)에 의거하여 개인정보에 대해 수집, 이용 시 동의하지 않은 제3자 및 기관에 해당 개인정보를 제공한 사실이 확인되었을 경우 즉시 해당기관에 관련 개인정보의 제공을 중단하고, 제공근거 및 안전성 확보를 위하여 필요한 대책을 마련하도록 요청하여야 한다.

마. 목적 외 이용 및 제3자 제공에 관한 담당자별 업무절차

1) 해당부서에서 자체적으로 목적 외 이용 및 제공이 가능한 경우

- 개인정보취급자: 부서장 결재를 받은 공문으로 이용 및 제공하여야 하며, **개인정보의 목적 외 이용 및 제3자 제공 대장[붙임 9]**을 작성하여 개인정보보호 담당자에게로 제출(협조문)하여야 한다. 이 경우 요청된 공문이나 내부 결재문서 등이 있으면 함께 첨부하여 요청한다.
- 개인정보보호 담당자: 개인정보취급자로부터 받은 대장을 자체 관리하고, 목적 외 이용 및 제공이 일어난 날로부터 30일 이내에 10일 이상 홈페이지 개인정보처리방침 등에 고지하여야 한다. 누락된 부분에 대해서는 매년 실시하는 개인정보의 목적 외 이용 및 제3자 제공에 대한 일제정비를 실시하여 고지한다.
- 개인정보 보호책임자: 개인정보보호 담당자로부터 보고 받은 개인정보의 목적 외 이용 및 제3자 제공 대장에 대해서 법적근거, 동의여부 등을 파악하여 개인정보의 이용 및 제공에 관한 적법함을 판단한 후 과도한 이용 및 제공이 있을 경우 해당 개인정보취급자 및 부서장에 대해 개선조치를 요구하여야 한다.

2) 해당부서에서 자체적으로 목적 외 이용 및 제공이 불가능한 경우

- 개인정보취급자: 전산개발팀으로 **개인정보의 목적 외 이용 및 제3자 제공 대장[붙임 9]**을 작성하여 부서장 결재를 받은 공문(협조문, 전산처리의뢰서 포함)을 제출한 후 관련 개인정보를 제공받는다. 이 경우 요청된 공문이나 관련문서 등이 있으면 함께 첨부하여 요청한다.

- 개인정보보호 담당자: 개인정보취급자로부터 받은 대장을 자체 관리하고, 목적 외 이용 및 제공이 일어난 날로부터 30일 이내에 10일 이상 홈페이지 개인정보처리방침 등에 고지하여야 한다. 누락된 부분에 대해서는 매년 실시하는 개인정보의 목적 외 이용 및 제3자 제공에 대한 일제정비를 실시하여 고지한다.
- 개인정보 보호책임자: 개인정보보호 담당자로부터 보고 받은 개인정보의 목적 외 이용 및 제3자 제공 대장에 대해서 법적근거, 동의여부 등을 파악하여 개인정보의 이용 및 제공에 관한 적법함을 판단한 후 과도한 이용 및 제공이 있을 경우 해당 개인정보취급자 및 부서장에 대해 개선조치를 요구하여야 한다.

바. 개인정보보호 담당자는 개인정보취급자로부터 받은 개인정보의 목적 외 이용 및 제3자 제공 대장을 홈페이지 개인정보처리방침 등에 고지하여야 한다. 누락된 부분에 대해서는 매년 실시하는 개인정보의 목적 외 이용 및 제3자 제공에 대한 일제정비를 실시하여 고지한다.

4.4 개인정보 처리업무 위탁시 수탁자에 대한 관리 및 감독(법 제26조)

가. 개인정보보호 분야별 책임자 또는 개인정보취급자는 개인정보의 처리 업무에 대하여 제3자에게 위탁계약을 체결하는 경우에 위탁업무 수행 목적 외 개인정보의 처리 금지와 기술적·관리적 보호 조치 또는 그 밖에 안전한 관리를 위하여 수탁자와 합의 후 다음 각 호의 내용이 포함된 문서 또는 전자적 기록으로 보존하여야 한다.

① 위탁업무의 목적과 범위 ② 재 위탁 제한에 관한 사항 ③ 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항 ④ 위탁업무와 관련하여 보유하고 있는 개인정보 관리 현황 점검 등 감독에 관한 사항 ⑤ 수탁자가 기술적·관리적으로 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

나. 개인정보의 업무를 위탁하는 개인정보취급자는 인터넷 홈페이지 등에 위탁하는 업무의 내용과 수탁자의 정보를 지속적으로 게재하여야 한다.

다. 위탁한 개인정보보호 분야별 책임자는 업무위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 계약 후 개인정보 안전 관리 여부를 감독하기 위한 계획을 수립 후 수탁자를 교육하고, 점검을 하여야 한다.

라. 개인정보보호 분야별 책임자는 위탁계약 완료 즉시 위탁내용과 수탁자의 정보, 위탁에 따른 관리·감독 계획, 점검계획을 개인정보 보호책임자에게 보고하고, 점검결과 및 기타 특이사항 등을 수시로 보고하여야 한다.

마. 수탁자는 개인정보취급자로부터 위탁받은 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공하여서는 아니 된다.

4.5 개인정보 파기(법 제21조)

가. 개인정보취급자는 개인정보파일의 보유기간 경과, 처리목적 달성 등 파기 사유가 발생한 경우 해당 개인정보파일을 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 예외로 한다.

나. 개인정보취급자는 개인정보파일의 보유기한 도래 10일 전까지 **개인정보파일 파기 요청서[붙임 3]**를 작성하여 개인정보보호 담당자에게 등록된 파일의 파기를 요청하여야 한다. 이 경우 사전에 반드시 전산개발팀과 협의하여 향후 업무처리에 있어서 발생할 수 있는 문제점에 대해서 논의하여야 하며, 필요한 경우 시스템을 보완하여야 한다.

다. 개인정보파일 파기 신청을 받은 개인정보보호 담당자는 그 사실을 검토 후 개인정보보호위원회 개인정보보호종합지원시스템(intra.privacy.go.kr)에 등록된 파일인 경우 파기요청을 하여야 하며, 개인정보보호 담당자는 **개인정보파일 파기 관리대장[붙임 4]**에 해당 사실을 기록·관리한다.

라. 개인정보보호 담당자는 개인정보 보호책임자의 파기 승인 후 지체 없이 파기하여야 한다.

마. 개인정보를 파기할 때에는 개인정보처리시스템에 포함된 자료 뿐 아니라 PC에 저장된 파일 및 수기문서 모두를 파기하여야 하며, 파기 시에는 복구 또는 재생되지 않도록 하여야 한다.

1) 전자적 파일 형태인 경우: 복원이 불가능한 방법으로 영구 삭제

2) 그 외의 경우(인쇄물, 기록물 등): 파쇄 또는 소각

바. 개인정보보호 담당자는 개인정보파일 삭제 후 개인정보취급자에게 즉시 그 사실을 알려야 하며, 개인정보취급자는 개인정보파일 파기 후 업무처리에 이상이 있는지를 반드시 확인하여야 한다.

사. 개인용 PC에 저장되어 있는 임시 활용한 개인정보 혹은 불필요한 파일 등은 수시로 삭제하여야 한다.

4.6 정보주체의 권리 보장 및 행사 절차

가. 개인정보의 열람, 정정 및 삭제, 처리정지 등에 대한 조치는 해당 개인정보를 수집·취급하고 있는 개인정보취급자가 처리하여야 하며, 개인정보보호 분야별 책임자는 이를 확인·감독하여야 한다.

나. 정보주체가 개인정보의 열람, 정정·삭제, 처리정지, 자동화된 결정에 대한 거부·설명, 본인전송요구 등의 요구를 하는 경우에 해당 개인정보취급자는 정보주체에게 **개인정보(열람, 정정·삭제, 처리정지, 자동화된 결정에 대한 거부·설명, 본인전송요구 등) 요구서[붙임 5]**를 작성하여 제출하도록 안내하여야 한다.

다. 개인정보취급자는 정보주체가 자신의 개인정보 열람을 요구한 경우 시행령으로 정하는 기간인 10일 내에 열람 조치하고 조치 사실을 정보주체에게 통보하여야 한다.

라. 개인정보를 열람한 정보주체가 개인정보취급자에게 그 개인정보의 정정 또는 삭제를 요구하였을 때에는 다른 법령에 규정되어 있는 경우를 제외하고는 지체없이 정정·삭제 등 필요한 조치를 한 후 10일 이내에 조치 결과를 정보주체에게 알려야 한다.

마. 개인정보취급자는 정보주체로부터 개인정보 처리정지 요구를 받았을 때에는 지체 없이 개인정보 처리의 전부 또는 일부를 정지하고 10일 이내에 조치 사실을 통보하여야 한다.

바. 위 다에서 마의 정보주체에 대한 결과 통보는 **개인정보(정정·삭제, 처리정지) 요구에 대한 결과 통지서 [붙임 7]**를 활용하여 **서면, 전자우편, 문자전송 등 정보주체가 확인 가능한 방법으로 통지한다.**

사. 법의 단서조항에 따라 부득이 열람, 정정 등의 조치를 할 수 없는 경우 **개인정보(열람, 일부열람, 열람연기, 열람거절)통지서 [붙임 6]**를 작성하여 요구서를 받은 날로부터 10일 이내에 해당 정보주체에게 통보하여야 한다.

5. 개인정보의 기술적·물리적 안전조치

개인정보 관련 정책 및 법적 요구사항 만족과 우리 대학교 정보보안 강화를 위해 아래와 같이 개인정보 처리 안전조치를 수행한다.

5.1 물리적 접근권한 및 관리

가. 개인정보보호 분야별 책임자는 개인정보와 개인정보처리시스템의 안전한 보관을 위한 물리적 잠금장치 등의 물리적 접근방지를 위한 안전조치를 취하여야 한다.

나. 개인정보보호 분야별 책임자는 물리적 접근방지를 위한 별도의 보호시설에 출입하거나 개인정보를 열람하는 경우, 그 출입자에 대한 출입 사실 및 열람 내용에 관한 출입자 **관리대장 [붙임 8]**을 작성하여 출입자를 통제하여야 한다.

다. 개인정보보호 분야별 책임자는 물리적 접근권한 관리대장의 출입 및 열람 내용을 주기적으로 검토하여 정당하지 않은 권한으로 출입하거나 열람하는 경우가 있는지를 점검하여 확인하여야 한다.

5.2 출력·복사 시 안전조치

가. 개인정보보호 분야별 책임자는 개인정보가 포함된 정보를 출력하거나 복사할 경우에 개인정보 유출사고를 방지하기 위한 안전조치를 취하여야 한다.

나. 개인정보보호 분야별 책임자는 민감한 개인정보 또는 다량의 개인정보가 포함된 정보를 출력하거나 복사할 경우 출력·복사자의 성명, 일시 등을 기재하여 개인정보 유출 등에 대한 책임 소재를 확인할 수 있는 강화된 안전조치를 추가로 적용하여야 한다.

다. 개인정보취급자는 개인정보의 이용을 위하여 출력 및 복사한 개인정보의 이용 목적이 완료된 경우 분쇄기로 분쇄하거나 소각하는 등의 안전한 방법으로

파기하여야 한다.

5.3 개인정보취급자 접근권한 관리

가. 개인정보보호 분야별 책임자는 개인정보처리시스템에 대한 접근 권한을 서비스 제공에 필요한 최소한의 인원에게만 부여한다.

나. 개인정보보호 분야별 책임자는 개인정보취급 업무를 담당하는 교직원의 담당 업무에 따라 개인정보 취급권한을 부여하며, 부서/직급별에 개인정보에 대한 접근권한(읽기/쓰기/수정/삭제 권한)을 차등 부여한다. (추가적 권한 부여가 필요한 경우, 공문서 요청/승인 절차에 따라 검토 후 부여한다.)

다. 개인정보보호 분야별 책임자는 개인정보취급자가 전보 또는 퇴직 등 인사이동으로 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소한다.

라. 개인정보 분야별 책임자는 개인정보취급자가 정보통신망을 통하여 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 공인인증서 등 안전한 인증수단을 적용하여야 한다.

마. 개인정보보호 분야별 책임자는 '가' 또는 '라'에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관한다.

바. 개인정보보호 분야별 책임자는 개인정보취급자 및 정보주체가 안전한 비밀번호를 설정하여 이용할 수 있도록 다음의 조건에 만족하는 비밀번호를 적용하여 이용하도록 한다.

1) 영문, 숫자, 특수문자를 조합하여 최소 9자리 이 상의 길이로 구성
2) 연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않는 것을 권고
3) 비밀번호는 주기적으로 변경하고 장기간 사용 금지

사. 개인정보 보호책임자는 매월 셋째 주 수요일을 사이버·보안 진단의 날로 지정하여 부서별 정기점검을 실시하도록 한다.

아. 개인정보보호 담당자는 사이버보안 진단의 정기점검을 실시하여 개인정보취급자가 개인정보처리시스템에 접속하여 처리한 기록과 시스템 이상 유무를 확인·검토하며, 결과를 시스템에 기록 관리한다.

5.4 개인정보의 암호화

가. 개인정보보호 분야별 책임자는 주민등록번호, 비밀번호, 여권번호, 운전면허번호, 외국인등록번호, 생체인식정보에 대해서는 암호화하여 저장하도록 개인정보취급자에게 숙지시켜야 한다.

나. 개인정보 보호책임자는 정보통신망을 통해 개인정보 및 인증정보가 송수신될 때 안전을 보장하기 위하여 보안서버 등을 구축하도록 조치해야 한다.

다. 개인정보보호 담당자는 개인정보처리시스템 및 통신시스템 저장시스템 등을 관리, 운영함에 있어 암호화가 이루어질 수 있도록 개인정보 보호책임자와 협의한다.

라. 개인정보취급자는 개인정보를 개인용 컴퓨터에 저장하지 않도록 해야 한다.

마. 개인정보취급자는 홈페이지, P2P, 공유설정 등으로 인하여 개인정보가 노출되지 않도록 PC에 접근 차단 조치를 하여야 한다.

바. 개인정보가 포함되어 있는 자료를 홈페이지 등에 게재할 경우 해당 게시물의 게재자는 개인정보 보호책임자의 사전 검토에 따른 승인을 받은 후 게재하여야 한다.

사. 개인정보보호 담당자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립, 시행하고 개인정보 보호책임자의 승인을 받아야 한다.

1) 생성: 암복호화 생성시에 안전한 난수 발생기를 이용하며, 안정성이 검증된 알고리즘을 사용하여 생성한다.

2) 이용: 비 인가된 사용자는 암호 키에 접근할 수 없도록 접근을 제어해야 한다.

3) 보관: 생성된 암호키는 암호 키 손상시 시스템 또는 암호화된 정보의 복구를 위하여 별도의 매체에 저장 후 안전한 장소에 보관하여야 한다.

4) 배포: 키는 사용자, 시스템, 애플리케이션, 보안정책과 키가 잘 연계되어야 하며, 관리자와 사용자에 대한 접근제어는 명확히 구분되어야 한다.

5) 파기: 파기사유가 발생한 경우(침해,유출 등) 복구,재생 할 수 없는 방법으로 파기하여야 한다. 그리고 원본 이외에 백업 데이터가 존재하는지 여부를 확인한 후 파기하여야 한다.

5.5 접근통제

가. 개인정보 보호책임자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음의 각 호의 기능을 포함한 시스템을 설치 및 운영하도록 관리·감독한다.

1) 개인정보처리시스템에 대한 접속 권한을 IP 주소 등으로 제한하여 인가받지 않은 접근을 제한

2) 개인정보처리시스템에 접속한 IP 주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지

나. 개인정보 보호책임자는 개인정보취급자가 생일, 주민등록번호, 전화번호 등 추측하기 쉬운 숫자나 개인관련 정보를 패스워드로 이용하지 않도록 비밀번호 작성규칙을 수립하고, 이를 적용 및 운용하여야 한다. 개인정보취급자는 개인정보 보호책임자가 수립한 비밀번호 작성규칙을 준수하여야 한다.

다. 개인정보 보호책임자는 개인정보보호 담당자와 함께 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통해 열람권한이 없는 자에게 공개되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터에 조치를 취하여야 한다.

라. 개인정보보호 분야별 책임자는 개인정보취급 업무를 담당하는 교직원의 담당

업무에 따라 개인정보 취급권한을 부여하며, 부서/직급별에 따라 개인정보에 대한 접근권한(읽기/쓰기/수정/삭제 권한)을 차등 부여한다.

5.6 접속기록의 위·변조 방지

가. 개인정보 보호책임자는 접속 기록의 위·변조 방지를 위해 개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리(입·출력, 수정)하는 경우에는 계정, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등 접속기록을 저장하도록 전산관련 개인정보보호 분야별 책임자에게 지시한다.

나. 개인정보 보호책임자는 '가' 항의 접속기록에 대해 월 1회 이상 정기적으로 확인·감독한다.

다. 개인정보보호 분야별 책임자는 '가' 항의 접속기록에 대해 위·변조 방지를 위해 별도의 저장매체에 백업 보관하며, 2년 이상 보관하도록 조치한다.

5.7 악성프로그램 등 방지

가. 개인정보처리자는 개인정보처리시스템 또는 업무용 컴퓨터에 악성 프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 한다.

나. 보안 프로그램의 자동 업데이트 기능을 사용하거나, 일 1회 이상 업데이트를 적용하여야 한다.

다. 악성 프로그램관련 경보가 발령된 경우 또는 사용 중인 응용프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 적용하여야 한다.

5.8 기술적 안전조치

가. 우리 대학교에서 보유하고 있는 개인정보관리의 안전성 확보를 위해 필요한 기술적 조치를 아래와 같이 계획하여 수행한다.

구분	안전조치	추진일정	시행부서
접근통제 강화	서버감사시스템 점검	월 1회 점검	정보보안팀
	네트워크 구성 일제 점검 및 취약점 파악		
	보안시스템 일제 점검 및 취약점 파악		
	접근권한 점검		
	접근제어시스템 점검		
	내부정보 유출 방지 시스템 점검		
서버 보안강화	시스템 취약점 점검		
컴퓨터 보안강화	백신서버 정책 점검 및 문제 컴퓨터 파악		
웹사이트 보안강화	개인정보 노출 방지 취약점 점검		
	Web방화벽 정책 점검 및 취약점 파악		

나. 개인정보의 안전한 관리를 위해 항목별 현황파악과 저장 시 필요한 법적

기준을 적용한다.

암호화 대상	Database 명	개인정보처리 시스템	처리부서	관리부서
주민등록번호, 여권번호, 운전면허번호, 외국인등록번호, 생체인식정보	학사 및 행정용 Database	EDWARD 시스템	주민등록번호, 여권번호, 운전면허번호, 외국인등록번호, 생체인식정보를 수집·관리하는 부서	전산개발팀
비밀번호			전산개발팀	

5.9 기술적·관리적 안전조치 수행 계획

구분	항목	세부항목
관리체계 구축	개인정보보호 기반 마련	개인정보 보호조직 구성
		개인정보 (분야별)보호책임자, 개인정보보호 담당자 및 개인정보취급자 인식 제고
		개인정보 처리방침 개선
		개인정보 내부 자체점검 수행
		개인정보 보호지침 개정
	위탁업무에 따른 개인정보보호 활동	위탁업체 대상 개인정보 처리현황에 대해 관리·감독
		위탁계약 사항 점검
	개인정보보호 교육 추진	개인정보보호 교육 계획 수립
		개인정보 (분야별)보호책임자, 개인정보취급자 등에 대한 교육 실시
보호대책 수립 및 시행	개인정보 목적 외 이용·제3자 제공 절차 운영	개인정보를 목적 외 이용하거나 제3자 제공에 따른 절차 수립
		개인정보 목적 외 이용, 제3자 제공 대장 점검
	개인정보 파일관리	개인정보처리방침의 이력관리 및 현행화 점검
		개인정보파일의 등록 및 변경사항 점검
		개인정보파일 등록항목 점검
	개인정보 영향평가 수행	개인정보 영향평가 수행 계획 수립 및 시행
	고정형 영상정보처리기기	고정형 영상정보처리기기 운영·관리 방침 개정

	설치 및 운영	
침해사고 대책	개인정보 노출방지 및 자율 개선	개인정보 노출방지 모니터링 및 정기점검 실시
	개인정보 침해사고 대응절차 수립	개인정보 유·노출 및 침해사고 발생에 대한 대응절차 수립
		대응절차 전파 및 신속하게 대응할 수 있는 체계 구축
	개인정보처리시스템의 안전한 이용 및 관리	개인정보처리시스템 접근권한 점검
		개인정보처리시스템 접속기록 정기점검
개인정보 기술적 안전조치	네트워크 구성 점검 및 취약점 파악	네트워크 시스템 전체 점검
	보안시스템 일제 점검 및 취약점 파악	방화벽 시스템 정책점검 및 취약점 파악
	서버 시스템 취약점 점검	전체 시스템 취약점 파악
	백신 및 자동패치 프로그램 점검	백신서버 및 자동패치서버 점검 사용자 컴퓨터 Agent 확인
	웹사이트 개인정보 노출방지 점검	전체 웹사이트 점검

5.10 고정형 영상정보처리기기의 설치 및 운영관리

가. 고정형 영상정보처리기기 운영·관리부서의 장(이하 개인영상정보 보호책임자)은 고정형 영상정보처리기기 설치 시「개인정보 보호법」제25조(고정형 영상정보처리기기의 설치·운영 제한)에 따라 이해관계인의 의견수렴 절차를 거쳐야 한다.

나. '가' 항에 따라 고정형 영상정보처리기기를 설치·운영 하려는 경우 불특정 다수가 이용하는 목욕실, 화장실, 발한실(發汗室), 탈의실 등 개인의 사생활을 현저히 침해할 우려가 있는 장소의 내부를 볼 수 있도록 고정형 영상정보처리기기를 설치·운영하여서는 아니 된다.

다. '가' 항에 따라 고정형 영상정보처리기기를 설치·운영 하려는 경우 녹음기능을 사용하여서는 안되며, 기기를 임의조작하거나 다른 곳을 비춰서는 안된다.

라. 개인영상정보 보호책임자는 다음 각 호의 항이 포함된 안내판을 설치하여야 한다.

1) 설치 목적 및 장소
2) 촬영 범위 및 시간
3) 관리책임자의 성명 및 연락처

마. 개인정보 보호책임자는 영상정보처리기기 운영·관리 방침을 수립하여 홈페이지 등에 공개하여야 한다.

바. 개인영상정보 보호책임자는 본 계획의 준수 여부에 대한 자체점검을 실시하여야 한다.

사. 개인영상정보 보호책임자는 개인영상정보기기의 운영을 위하여 내부 관리계획 5.1에서 5.10까지의 기술적·관리적 안전조치를 준수하여야 한다.

5.11 위험도 분석 및 대응방안

가. 개인정보파일 및 고유식별정보 보유에 대한 위험도 현황을 조사하고 위험도 점검 항목을 분석한다.

나. 위험도분석 결과보고서를 작성하고 점검결과에 따라 고유식별정보 암호화를 수행한다.

6. 개인정보 침해사고 대응방안

'개인정보 침해사고 대응방안'은 개인정보의 처리·운용 과정에서 내부의 과실 및 오·남용 또는 외부 해킹 등으로 침해·유출 사고가 발생할 경우, 체계적이고 신속한 대응으로 피해를 최소화하려는데 목적이 있다.

6.1 침해사고 정의

개인정보 침해사고란 법규를 위반하여 개인정보를 외부의 제3자에게 노출·제공하는 것과 해킹에 의한 유출·업무무비 등의 제반적 사고를 총칭한다.

6.2 침해사고 대상

가. 개인정보를 수집, 처리 시 개인정보에 관한 권리 또는 이익의 침해를 받은 자

나. 개인정보파일을 보유함에 있어 개인정보에 관한 권리 또는 이익의 침해를 받은 자

6.3 침해사고 유형

사고유형	내용	인지경로
과실로 인한 개인정보 침해	- 정보주체의 동의 또는 법적근거 없이 개인정보를 제3자에게 제공하는 등 개인정보의 관리(수집·저장·이용·파기)가 미흡하여 정보주체에게 침해를 주는 경우	① 상시모니터링 ② 한국인터넷진흥원 ③ 침해신고
과실로 인한 개인정보 유·노출	- 개인정보가 포함된 서면, 이동식 저장장치, 휴대용 컴퓨터를 분실 또는 도난 당한 경우 - 권한이 없는 자에게 개인정보를 잘못 전달한 경우	
오·남용으로 인한 개인정보 유출	- 개인정보 부당이용 또는 사적유용을 목적으로 유출하는 경우	

외부 침투에 의한 개인정보 유출	- 홈페이지 해킹 등 외부 침투에 의해 정보주체의 개인정보가 유출되는 경우	

6.4 침해사고 발생 시 조치방법

단계	조치방법	세부 조치 사항
확인 단계	① 사고 인지 · 접수	- 침해 · 유출 사고 상황 파악 - 개인정보 보호책임자에게 보고 - 침해 · 유출 사고대응반 설치 - 개인정보보호 손해배상 책임보험사에 신속히 연락
	② 확인조사 실시	- 침해 · 유출 사고 내용(원인, 규모 등) 세부조사 ※ 법령 위반사실 증빙자료 취합
	③ 피해확산 여부 확인	- 확인조사 결과에 따른 분석을 통해 추가 유출가능성 및 피해 확산 여부 확인 - 해명 보도 자료 등 배포
조치 단계	④ 유출통지	- 정보주체에게 72시간 이내 통지
	⑤ 유출통지 신고	- 개인정보보호위원회 또는 지정기관에 72시간 이내 신고
	⑥ 사례전파 및 시스템 보완	- 기술적, 관리적 보완조치

가. 개인정보취급자는 개인정보 침해가 발생한 것을 인지하거나 의심되는 경우 지체 없이 **개인정보 침해사실 신고서[붙임 10]**를 작성하여 개인정보보호 담당자에게 신고하여야 한다.

나. 개인정보보호 담당자는 사고 접수 내역을 **개인정보 침해사고 관리대장[붙임 11]**에 기록하고 개인정보 보호책임자에게 즉시 보고한다.

6.5 침해사고 유출통지

가. 과실로 인한 개인정보 침해 사고

- 정보주체의 동의 또는 법적근거 없이 개인정보를 제3자에게 제공하는 등 개인정보의 관리가 미흡하여 정보주체에게 침해를 주는 경우

1) 침해사고 인지 및 접수
   - 개인정보보호 담당자는 정기 실태점검 또는 침해신고(접수)를 통해 개인정보관리 침해사실 인지 및 접수
   - 개인정보보호 담당자는 위반사항이 중대한 경우 개인정보 보호책임자에게 보고
   - 개인정보 보호책임자는 침해사고대응반 설치

2) 확인조사 실시
   - 침해사고대응반에서는 개인정보 침해사고가 인지 또는 접수되어 침해사고 발생이 우려되는 부서에 대하여 확인조사 및 위험사실 확인
     ※ 필요 시 외부 전문가 협조 요청

- 사고발생 부서는 침해사고대응반의 현장 확인조사 시 적극 협조

3) 개선조치 및 사례전파

- 침해사고대응반은 확인조사 결과를 분석하여 개인정보 보호책임자에게 보고
- 침해사고대응반은 개인정보 침해사고 발생을 방지하기 위한 대책을 부서에 제시하고 필요한 경우 개선권고 요청
- 침해사고대응반은 관리미흡에 의한 사고사례를 내부에 전파하고, 유사한 사례가 발생하지 않도록 조치
- 실태점검 항목 강화 등 개인정보관리 철저를 위한 대책 강구

4) 해당자 처분 및 조치

- 개인정보 보호책임자에게 세부조사 결과 보고
- 위반사항의 중요도에 따라 처분 및 조치 요청
- 재발 방지를 위한 개인정보보호 특별 교육 이수 명령

나. 과실로 인한 개인정보 유·노출 사고

- 개인정보가 포함된 서면, 이동식 저장장치, 휴대용 컴퓨터를 분실 또는 도난당한 경우 - 권한이 없는 자에게 개인정보를 잘못 전달한 경우

1) 유·노출 사고 인지 및 접수

- 개인정보보호 담당자는 상시 모니터링, 실태점검을 통한 부주의 등 과실로 인한 개인정보 유·노출 사실 확인 또는 내·외부 침해신고 접수를 통해 유·노출 사고 인지
- 개인정보보호 담당자는 위반사항이 중대한 경우 개인정보 보호책임자에게 보고
- 개인정보 보호책임자는 침해사고대응반 설치

2) 확인조사 실시

- 침해사고대응반은 자체점검을 위한 자료(서비스 종류 및 로그값)를 확보하고, 현장 확인조사를 통해 과실여부, 침해규모, 경위, 방법 등을 조사
  ※ 필요 시 외부 전문가 협조 요청
- 사고발생 부서는 침해사고대응반의 현장 확인조사 시 적극 협조

3) 피해 확산 여부 확인

- 침해사고대응반은 확인조사 결과에 따른 분석을 통해 추가 유·노출 가능성 및 피해 확산 여부 확인
- 인터넷 등 언론동향 대응을 위한 보도자료 등 배포

4) 유출통지

- 침해사고대응반은 개인정보가 유출되었을 경우, 유출 사실을 지체 없이(72시간 이내) 정보주체에게 통지
- 다만, 유출된 개인정보의 확산 및 추가 유출을 방지하기 위하여 접속경로

의 차단, 취약점 점검·보완, 유출된 개인정보의 삭제 등 긴급한 조치가 필요한 경우에는 그 조치를 한 후 지체 없이 정보주체에게 통지

- 1천명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 서면 등의 방법과 함께 인터넷 홈페이지에 정보주체가 알아보기 쉽도록 7일 이상 게재

5) 유출통지 신고

- 1천명 이상 유출된 경우에는 정보주체에게 유출 사실을 통지한 사항 및 피해를 최소화하기 위한 대책과 필요한 조치 결과를 개인정보보호위원회 또는 전문기관에 신고

6) 사례전파로 동일사례 발생 방지

- 부주의 등 과실로 인한 개인정보 유·노출 사고사례를 내부에 전파하고, 유사한 사례가 발생하지 않도록 조치
- 재발 방지를 위한 기술적 조치와 개인정보보호 교육 및 실태점검 강화

7) 사고내용 세부조사

- 침해사고대응반은 확인조사 결과 세부조사가 필요하다고 판단되는 경우, 개인정보 보호책임자에게 필요성 보고

8) 해당자 처분 및 조치

- 개인정보 보호책임자에게 세부조사 결과 보고
- 위반사항의 중요도에 따라 처분 및 조치 요청
- 재발 방지를 위한 개인정보보호 특별 교육 이수 명령

다. 오·남용으로 인한 개인정보 유출 사고

1) 유출 사고 인지 및 접수

- 개인정보보호 담당자는 상시 모니터링, 실태점검 등을 통한 고의적 유출 사실 확인 또는 내·외부 침해신고 접수를 통해 사고 인지
- 개인정보보호 담당자는 위반사항이 중대한 경우 개인정보 보호책임자에게 보고
- 개인정보 보호책임자는 침해사고대응반 설치

2) 확인조사 실시

- 침해사고대응반은 자체점검을 위한 자료(서비스 종류 및 로그값)를 확보하고, 현장 확인조사를 통해 과실 여부, 침해규모, 경위, 방법 등을 조사
  ※ 필요 시 외부 전문가 협조 요청
- 사고발생 부서는 침해사고대응반의 현장 확인조사 시 적극 협조

3) 피해 확산 여부 확인

- 침해사고대응반은 확인조사 결과에 따른 분석을 통해 추가 유·노출 가능성 및 피해 확산 여부 확인
- 인터넷 등 언론동향 대응을 위한 보도자료 등 배포

4) 유출통지

- 침해사고대응반은 개인정보가 유출되었을 경우, 유출 사실을 지체 없이(72

시간 이내) 정보주체에게 통지

- 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 지체 없이 정보주체에게 통지
- 1천명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 서면 등의 방법과 함께 인터넷 홈페이지에 정보주체가 알아보기 쉽도록 7일 이상 게재

5) 유출통지 신고

- 1천명 이상 유출된 경우에는 정보주체에게 유출 사실을 통지한 사항 및 피해를 최소화하기 위한 대책과 필요한 조치 결과를 개인정보보호위원회 또는 전문기관에 신고

6) 사례전파로 동일사례 발생 방지

- 부주의 등 과실로 인한 개인정보 유·노출 사고사례를 내부에 전파하고, 유사한 사례가 발생하지 않도록 조치
- 재발 방지를 위한 기술적 조치와 개인정보보호 교육 및 실태점검 강화

7) 사고내용 세부조사

- 침해사고대응반은 확인조사 결과 세부조사가 필요하다고 판단되는 경우, 개인정보 보호책임자에게 필요성 보고

8) 해당자 처분 및 조치

- 개인정보 보호책임자에게 세부 조사결과 보고
- 위반사항의 중요도에 따라 처분 및 조치 요청
- 재발 방지를 위한 개인정보보호 특별 교육 이수 명령

※ 세부조사 결과 개인정보 부당이용 또는 사적유용을 목적으로 유출된 경우 고발 조치

라. 외부 침투에 의한 개인정보 유출 사고

1) 외부 침투에 의한 유출 사고 확인

- 개인정보보호 담당자는 외부침투(해킹 등)에 의한 개인정보 유출사실 확인
- 사이버공격 대응절차에 따른 경계단계별 대응반 가동 상태 확인
- 개인정보보호 담당자는 확인한 침해사실에 대해 개인정보 보호책임자에게 보고
- 개인정보 보호책임자는 침해사고대응반 설치

2) 피해 확산 여부 확인

- 침해사고대응반은 확인조사 결과에 따른 분석을 통해 추가 유·노출 가능성 및 피해 확산 여부 확인
- 인터넷 등 언론동향 대응을 위한 보도자료 등 배포

3) 유출통지

- 침해사고대응반은 개인정보가 유출되었을 경우, 유출 사실을 지체 없이(72시간 이내) 정보주체에게 통지

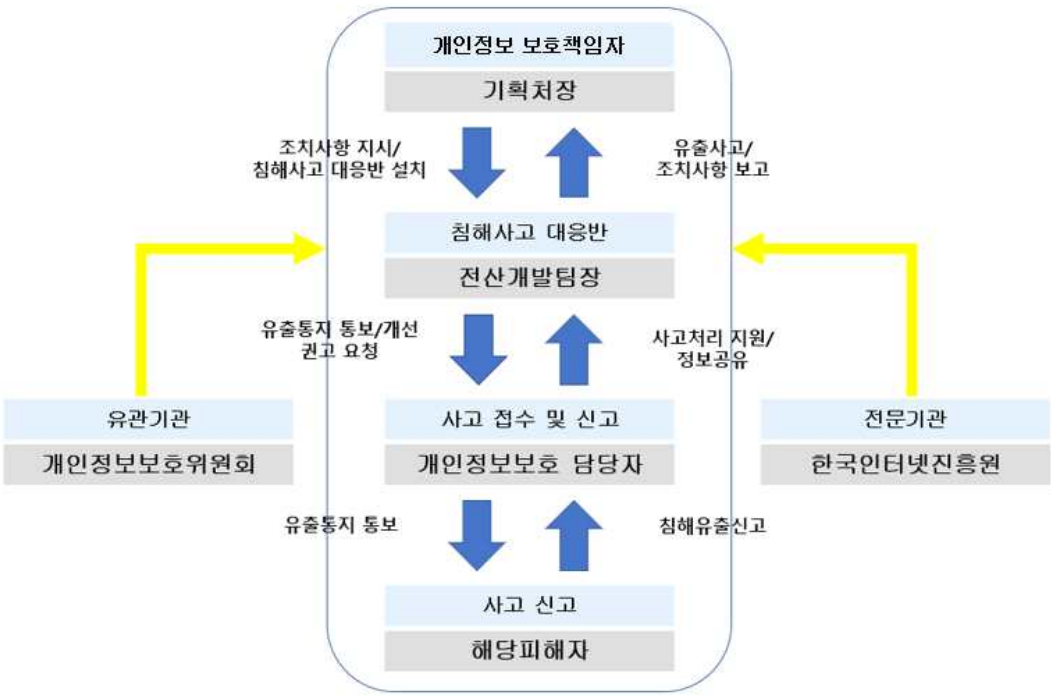
- 다만, 유출된 개인정보의 확산 및 추가 유출을 방지하기 위하여 접속경로의 차단, 취약점 점검·보완, 유출된 개인정보의 삭제 등 긴급한 조치가 필요한 경우에는 그 조치를 한 후 지체 없이 정보주체에게 통지
- 1천명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 서면 등의 방법과 함께 인터넷 홈페이지에 정보주체가 알아보기 쉽도록 7일 이상 게재

4) 유출통지 신고
- 1천명 이상 유출된 경우에는 정보주체에게 유출 사실을 통지한 사항 및 피해를 최소화하기 위한 대책과 필요한 조치 결과를 개인정보보호위원회 또는 전문기관에 신고

5) 사고 사례전파 및 시스템보완
- 침해사고대응반은 개인정보 유출 및 침해에 관한 사고사례를 전파하고 유사사례가 발생하지 않도록 조치
- 정보보안 담당자는 보안시스템 점검 강화 등의 기술적인 보안 조치

6) 해킹사고 세부조사 및 조치
- 침해사고대응반은 국가정보원, 한국교육학술정보원 등에 세부조사 의뢰
- 세부조사 결과, 해킹사고의 업무상 과실 등 책임이 있는 담당자를 확인하여 고발 조치

6.6 침해사고 대응반 조직(연락) 및 역할



6.7 침해사고 발생 시 업무분장

조직별	담당자	담당 업무
개인정보	기획처장	- 개인정보 침해사고 대응 총괄 지휘

보호책임자		
개인정보 침해사고 대응반	개인정보보호 담당자 개인정보보호 분야별 책임자, 정보보안 담당자, 전산담당자, 기타 협조부서	- 개인정보 침해사고 인지 · 접수 - 개인정보 침해사고 대응 절차 수립 - 개인정보 침해사고 사실 확인조사 실시 - 정보주체에게 유출사실 통지 - 개인정보보호위원회 또는 전문기관에 유출 통지 신고 - 외부요인에 의한 유출의 경우, 국가정보원, 한국교육학술정보원(KERIS), 개인정보보호위원회 등과 협조하여 사고 해결 - 사고내용 세부조사 및 사후 인사조치가 필요한 경우 유관부서와 협조
사고발생부서	개인정보취급자	- 내부요인에 의한 침해 · 유출의 경우, 사고대응반에 사고내용 신고 - 침해사고대응반과 협력하여 사고처리 적극 지원
사고신고자	정보주체	- 개인정보를 침해 받은 피해자

6.8 침해사고 신고방법

①		②		③
개인정보취급자		개인정보보호 담당자		
개인정보 유출신고서 [붙임 13]	=>	개인정보 유출신고서 [붙임 13]	=>	개인정보보호위원회 한국인터넷진흥원
대응조치 및 피해구제	<=	대응조치 및 피해구제 지원	<=	

가. 신고방법은 개인정보보호위원회 또는 한국인터넷진흥원의 전화, 팩스, 이메일, 우편 또는 개인정보보호포털(www.privacy.go.kr) 로 신고

- 시간적 여유가 없거나 그밖에 특별한 사정이 있는 때에는 먼저 전화로 신고한 후, 나중에 **개인정보 유출신고서[붙임 13]** 제출

나. 1천명 이상의 개인정보가 유출된 경우에는 72시간 이내에 개인정보보호위원회 또는 한국인터넷진흥원 중 한 곳에 신고

- 또한 홈페이지에 정보주체가 알아보기 쉽도록 해당 사항을 7일 이상 게제

6.9 침해사고 구제방법

가. 정보주체는「개인정보 보호법」제39조에 따라 개인정보취급자가 법을 위반한 행위로 손해를 입은 경우 개인정보취급자에게 손해배상을 청구할 수 있으며 이 경우 개인정보취급자는 고의 또는 과실이 없음을 입증하지 아니하면

책임을 면할 수 없다.

나. 개인정보취급자는 개인정보가 유출되었음을 알게 되었을 때에는 지체없이 개인정보보호 담당자에게 신고하여야 하며, 개인정보 보호책임자는 **개인정보 유출 신고서[붙임 13]**를 작성 후 개인정보 보호책임자에게 보고한다. 해당 정보주체에게는 다음 각 호의 사실을 통지한다.

1) 유출된 개인정보의 항목
2) 유출된 시점과 경위
3) 유출에 의한 피해를 최소화하기 위해 정보주체가 할 수 있는 방법 등
4) 개인정보처리자의 대응조치 및 피해 구제절차
5) 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

다. 개인정보주체는 개인정보침해로 인한 피해를 구제 받기 위하여 개인정보 분쟁조정위원회, 한국인터넷진흥원 개인정보 침해-신고센터 등에 분쟁해결이나 상담 등을 신청할 수 있다.

1) 개인정보분쟁조정위원회: (국번없이) 1833-6972 (www.kopico.go.kr)
2) 개인정보침해신고센터: (국번없이) 118 (privacy.kisa.or.kr)
3) 대검찰청: (국번없이) 1301 (www.spo.go.kr)
4) 경찰청: (국번없이) 182 (ecrm.police.go.kr)

라. 개인정보의 열람, 정정·삭제, 처리정지 등에 대한 정보주체자의 요구에 대하여 공공기관의 장이 행한 처분 또는 부작위로 인하여 권리 또는 이익을 침해 받은 자는 행정심판법이 정하는 바에 따라 행정심판을 청구할 수 있다.

※ 중앙행정심판위원회: (국번없이) 110 (www.simpan.go.kr)

6.10 침해사고 처리보고

가. 개인정보보호 담당자는 **개인정보 침해사고 처리보고서[붙임 12]**를 작성하여 개인정보 보호책임자에게 보고한다.

나. 처리보고서 제출 후 30일 이내에 근본원인 분석 및 예방을 위한 개선 대책을 마련하고, 전 직원을 대상으로 사고 처리 경과 및 예방을 위한 교육을 실시하여 사고의 재발을 방지한다.

다. 개인정보취급자는 동일 혹은 유사 사고가 발생하지 않도록 개인정보 관리에 철저를 가하여야 하며, 개인정보 보호책임자는 이를 위한 직원에 대하여 불이익 조치를 명할 수 있다.

6.11 사고예방

가. 사고예방 활동

1) 개인정보 침해·유출 사고를 대비하여 사전 사고예방 활동 실시
2) 개인정보보호 관리수준 현장조사
3) 개인정보 통합관제 실시
4) 웹사이트 개인정보 노출점검 실시

나. 사고요인 점검

1) 수집단계에서의 침해·유출 사고요인 점검
2) 불필요한 개인정보 수집 여부 점검
3) 수집된 개인정보의 개인정보보호 처리방침 게재 여부 점검
4) 개인정보 수집 시 정보주체 동의 여부 점검

다. 저장 및 관리단계에서의 침해·유출 사고요인 점검
1) 수집된 개인정보 불법적인 유출 위협 상태 점검
2) 수집 목적 달성 또는 보유기간 초과 여부 점검
3) 관리자 또는 이용자의 실수로 인한 개인정보 노출 여부 점검
4) 권한관리 등 시스템 오류로 인한 개인정보 노출 여부 점검

라. 이용 및 제공단계에서의 침해·유출 사고요인 점검
1) 개인정보보호 처리방침에 명시되지 않은 위탁사업자나 제3의 서비스 제공자에게 개인정보 제공 여부 점검
2) 개인정보를 제3자에게 양도하는 등 불법적 거래 여부 점검

마. 파기단계에서의 침해·유출 사고요인 점검
1) 수집 목적 달성 또는 보유기간 초과한 개인정보 파기 여부 점검
2) 권한이 없는 이용자의 개인정보 파기 여부 점검

바. 개인정보 특별점검 실시
1) 개인정보의 관리 미흡으로 개인정보 유출사고 발생 가능성이 우려되는 경우, 개인정보 특별점검 실시
2) 대상: 개인정보취급자 및 일반직원

7. 개인정보 재해·재난 대비 안전조치 대응방안

화재, 홍수, 단전 등의 재해·재난 발생시 체계적이고 신속한 대응으로 피해를 최소화 하며, 안전하게 복구하려는데 목적이 있다.

7.1 재해·재난 발생 시 조치 방법

단계	조치방법	세부 조치 사항
확인 단계	① 사고 인지·접수	- 재해·재난 사고 현황 파악 - 개인정보 보호책임자에게 보고 - 비상통지 - 개인정보 재해·재난 대응반 설치
	② 확인조사 실시	- 재해·재난 사고 내용(원인, 규모 등) 세부조사 - 개인정보 유출 여부 확인 (유출 확인시 '6.개인정보 침해사고 대응방안' 에 따라 조치)
	③ 예상복구 시간 파악	- 확인조사 결과에 따른 분석을 통해 예상복구 시간 파악

조치 단계	④ 재해 · 재난 복구 준비	- 시스템 복구 관련 담당자에게 연락 - H/W, S/W 공급지원업체에 복구 촉구
	⑤ 재해 · 재난 복구 활동	- 예상복구 시간 보고 - 상실데이터, 어플리케이션 동작 확인 - 긴급물자, 필요자원 조달 및 승인
	⑥ 안정화 및 시스템 보완	- 복구 시스템 안정화 점검 - 기술적, 관리적 보완조치

7.2 재해 · 재난 발생 시 업무분장

조직별	담당자	담당 업무
개인정보 보호책임자	기획처장	- 개인정보 재해·재난 사고 대응 총괄 지휘 및 최종 의사결정 - 위기 선포 및 해제, 위기대응 조직 구성·운영 지시 - 주요 조치계획 및 대외 보고(총장, 이사회 등) 승인
개인정보 재해·재난 대응반	개인정보보호 담당부서(총괄)	- 사고 접수 및 상황 파악, 초기 대응계획 수립·조정 - 피해 규모 및 영향도 분석, 법적 신고·통지 필요 여부 검토 - 재해·재난 대응 절차서·매뉴얼, 비상연락망 수립·관리 - 관계 기관(개인정보위, KISA 등) 신고 및 협조 창구 역할
	개인정보보호 분야별 책임자(각 부서장)	- 소관 시스템·업무의 사고 발생 여부 및 피해 범위 확인 - 긴급 조치(접속 차단, 서비스 중단 등) 시행 및 결과 보고 - 부서 단위 복구계획 수립, 복구 우선순위 및 필요 자원 산정
	정보보안 담당자	- 침해 경로 및 원인 분석, 2차 피해 방지 기술조치 수행 - 서버·네트워크·보안장비 점검 및 긴급 복구, 로그 분석 - 재해복구시스템 전환, 백업 데이터 복원 지원 및 결과 보고
	전산담당자	- 개인정보처리시스템 운영 중단·재개 등 시스템 운용 조정 - 백업 데이터 확인, 복구 작업 수행 및 데이터 무결성 검증 - 복구 완료 후 서비스 상태 모니터링 및 장애 재발 방지 조치
	기타 협조부서(감사·대외, 총무 등)	- 개인정보보호 담당부서 판단에 따른 법적 쟁점 자문, 손해배상·소송 등 법률지원 - 언론·민원 대응 전략 수립 지원, 보도자료·공지문 법적 리스크 검토 - 보험·위기관리 등 대외 기관과의 협의 지원

7.3 재해·재난 대비 개인정보처리시스템 백업 계획

가. 개인정보처리시스템은 백업시스템을 구축하여 재해·재난에 대비 안전조치를 취하여야 한다.

나. 정기적으로 백업을 수행하여 개인정보처리시스템 이외의 별도의 보조저장매체나 별도의 저장장치에 보관하여야 한다.

다. 개인정보처리시스템은 정보의 중요도를 구분하고, 그에 따라 백업대상, 백업주기, 백업방법 및 백업데이터 보관주기 등을 정한다.

라. 백업 데이터는 원본이 있는 곳과 동일한 자연 재해의 피해를 입지 않도록 멀리 떨어진 장소에 위치하도록 하며, 물리적으로 접근을 통제한다.

7.4 재해·재난 대비 개인정보처리시스템 복구 계획

가. 최단 시간 내에 복구함을 원칙으로 하되, 복구 방법이 시스템의 안정성을 저해할 우려가 있을 경우에는 안정성을 중시하는 방법을 택하여 복구를 하여야 한다.

나. 일부 업무가 처리 중에 있는 경우에는 최대한 처리 중인 업무에 영향을 주지 않는 범위 내에서 하여야 한다.

다. 복구를 위하여 부득이 처리 중인 업무를 중단시켜야 할 경우에는 제반 상황을 고려해서 신중하게 결정을 하여야 한다.

라. 네트워크 또는 공조 시설 등 타 시스템에 영향을 미칠 수 있는 부문에서 장애가 발생한 경우 이에 대한 복구를 최우선적으로 하여야 한다.

7.5 재해·재난 대비 개인정보처리시스템 정기 점검 및 사후처리 계획

가. 개인정보처리시스템에 대해 월 1회 이상 정기점검을 실시하여야 한다.

나. 재해·재난 발생시 개인정보 재해·재난 대비 안전조치 대응방안에 따라 사후조치를 진행한다.

7.6 개인정보처리시스템 구성 현황

우선순위	시스템 명	개인정보 보유량 (단위: 만건)	민감·교유식별정보 포함 여부	주된 시스템 연계 장비·설비 등	복구 목표 시간	복구 목표 시점
1	EDWARD 시스템	69.0	Y	DB서버, WAS서버, WEB서버, 보안장비 등	2	재해·재난 발생 전 최종 백업 시점
2	교수학습지원 시스템	9.8	N	DB서버, WAS서버, WEB서버, 보안장비 등	4	
3	동산도서관 통합정보시스템	13.0	N	DB서버, WAS서버, WEB서버, 보안장비 등	6	

8. 개인정보보호 교육 수행

개인정보취급자의 개인정보보호에 대한 인식 제고와 정책 및 법률 준수사항 실천을 향상시키기 위한 개인정보보호 교육과 정기적인 점검을 실시한다.

8.1 개인정보보호 교육 계획의 수립

가. 개인정보 보호책임자는 다음의 각 호의 사항을 포함하는 연간 개인정보보호 교육계획을 매년 3월 초까지 수립한다.

1) 교육목적 및 대상

2) 교육내용

3) 교육일정 및 방법

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

8.2 개인정보보호 교육의 실시

가. 개인정보 보호책임자는 개인정보 및 정보보호에 대한 교직원 및 위탁업체들의 인식 제고를 위해 노력해야 하며, 개인정보의 오·남용 또는 유출 등을 적극 예방하기 위해 우리 대학교 개인정보관련 업무를 수행하는 모든 교직원 및 위탁업체를 대상으로 다음과 같은 방법으로 연 1회 이상의 개인정보보호 교육을 실시한다.

1) 정기 교육

교육대상	전 교직원
교육방법	하반기 개인정보 보호에 관한 온라인 동영상 교육 실시
교육내용	개인정보 보호법 주요 내용 개인정보보호 정책 설명

2) 개인정보취급자 교육

가) 개인정보보호 기본 교육

교육대상	전 교직원
교육방법	개인정보보호 담당자
교육내용	개인정보 보호법 주요 내용 개인정보 보호정책 내부 관리계획 및 개인정보처리방침 안내 개인정보 보안에 대한 자체점검 방법 및 절차 안내 EDWARD 시스템 및 홈페이지 게시 기능을 이용한 각종 개인정보 처리업무에 대한 안내

나) 「사이버·보안진단의 날」

(1) 시행일: 매월 셋째 주 수요일

(2) 교육내용

- 개인정보보호 주요 이슈 및 교육부 공지사항 설명 및 해결책 공지
- 개인정보 처리(이용, 제공, 파기 등)에 관한 내부 절차 안내

- 소속 부서원들에 대한 사용자 PC 보안 및 개인정보 보호교육 시행

3) 개인정보보호 담당자 교육

가) 개인정보보호위원회 및 교육부 주관 개인정보 보호 교육 연 2회 이상 참석

나) 외부 개인정보 보호 전문 세미나 및 컨퍼런스 참석

다) 개인정보보호 전문기관 요청 연 1회 이상의 전문 교육 시행

4) 개인정보 보호책임자 교육

가) 개인정보보호위원회 및 교육부 주관 개인정보 보호책임자(CPO) 교육 참석

나) 외부 개인정보 보호 전문 세미나 및 컨퍼런스 참석

5) 개인정보처리 위탁업체 교육

- 개인정보를 관리하고 위탁하는 부서는 위탁업체를 대상으로 자체 교육을 실시(연 1회 이상)

6) 개인정보보호 특별 교육

가) 개인정보 침해사고 발생 시 재발 방지를 위해 해당자 또는 관련 부서를 대상으로 교육 실시

나) 교육 대상자는 개인정보 보호책임자가 지정하는 개인정보보호 교육을 이수하고 그 결과(이수증 등)를 제출

나. 교육 방법은 집체 교육뿐만 아니라, 인터넷 교육, 유인물 등 다양한 방법을 활용하여 실시하고, 필요한 경우 외부 전문기관이나 전문 강사에 위탁하여 교육을 실시할 수 있다.

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

라. 개인정보 보호책임자 및 개인정보보호 담당자는 개인정보취급자에 대하여 교내 교육이 아닌 외부 집합교육 및 사이버교육을 포함한 개인정보보호 교육에 적극 참여하도록 독려하여야 하며, 개인정보취급자는 이를 성실히 따라야 한다.

마. 개인정보보호 담당자는 교육 전·후 교육 계획서 및 교육 결과서 작성 등 증빙자료를 첨부하여 개인정보 보호책임자의 결재를 받아 보관한다.

9. 개인정보 자체점검 실시 및 결과 반영

개인정보취급자가 개인정보보호정책을 숙지하여 이행할 수 있도록 정기점검을 실시하고, 점검결과에 따라 대응 및 개선사항을 도출하여 업무에 반영한다.

9.1 자체점검 주기 및 절차

가. 개인정보 보호책임자는 개인정보보호를 위한 내부 관리계획 및 관련 법령에서 정하는 개인정보보호 규정을 성실히 이행하는지를 주기적으로 점검 하여야 한다.

나. 개인정보 보호책임자는 개인정보 자체점검을 위한 점검대장, 점검절차 및 방법 등 자체점검의 실시에 관하여 필요한 별도의 계획을 수립할 수 있다.

다. 개인정보보호 자체점검은 최소 연 1회 이상 실시한다.

9.2 자체점검 실시

개인정보보호 정책에 대한 이행여부 점검으로 미흡한 사항을 조기 발견하여, 보안 사고를 예방하며 효과적인 대책마련으로 대외적인 신뢰성 확보를 통해 본교 이미지 제고를 목적으로 한다.

가.「사이버 · 보안 진단의 날」

「사이버 · 보안 진단의 날」을 지정하여 개인정보취급자의 컴퓨터 안전성 정기점검, 비밀 현황 확인 등 자체보안점검을 실시한다.

1) 시행시기: 매월 셋째 주 수요일
2) 주관부서: 정보보안팀

나. 개인정보 일제정비

1) 기간: 상반기
2) 주관부서: 전산개발팀
3) 대상부서: 교내 전 부서
4) 심사자
   가) 개인정보 보호책임자: 기획처장
   나) 개인정보보호 담당자: 전산개발팀 담당자

9.3 자체점검 결과 반영

가. 개인정보보호 담당자는 자체점검 실시 결과 현황을 취합 정리하여 개인정보보호책임자에게 보고하여야 하며, 관련 자료는 문서화하여 보관한다.

나. 개인정보 보호책임자는 개인정보 보호를 위한 자체점검 실시 결과, 개인정보의 관리운영상의 문제점을 발견하거나 관련 직원이 본 계획의 내용을 위반할 때에는 총장에게 보고 후 시정 · 개선 또는 인사발령 등 필요한 조치를 취하여야 한다.

다. 개인정보 보호책임자는 개인정보 위반 사실에 대한 시정 · 개선 조치가 이행되지 않거나, 개인정보보호에 심각한 영향이 발생할 수 있는 우려가 있는 경우 총장에게 보고 후 개인정보취급자 등에 대한 인사발령 등의 필요한 추가 조치를 취할 수 있다.

[붙임 1] 자체점검 항목 및 관리현황

구분	순번	세부점검항목
내부 관리계획의 수립 및 시행	1	개인정보의 안전한 처리를 위한 내부 관리계획이 수립되어 있는가?
	2	내부 관리계획의 중요한 변경 사항이 있는 경우 반영하고 수정이력을 관리하고 있는가?
개인정보 보호조직 구성 · 운영	3	개인정보 보호책임자가 지정 되어 있는가?
	4	개인정보 보호책임자는 교육, 관리·감독 등 역할을 수행하고 있는가?
개인정보의 관리적 보호조치	5	개인정보 수집 시, 정보주체의 동의를 받고 있는가?
	6	고유식별정보(주민등록번호, 여권번호 등) 수집 시, 별도로 동의를 받고 있는가?
	7	서비스 제공을 위해 꼭 필요한 최소한의 정보만을 수집하는가?
	8	제3자 제공에 관한 사항을 정보주체에게 알리고 동의를 받는가?
	9	개인정보의 처리 업무를 위탁하는 경우, 문서(계약서등)에 의하여 하고 있는가?
	10	위탁업무의 내용과 수탁자(위탁받아 처리하는 자)를 공개하고 있는가?
	11	개인정보 수집 목적을 넘어 이용하거나 제공하는 경우, 별도 동의를 받거나 다른 법률에 근거하고 있는가?
	12	개인정보 처리목적 달성 시, 지체 없이 파기하고 있는가?
	13	다른 법령에 따라 개인정보를 파기하지 않고, 보존하는 경우, 다른 개인정보와 분리하여 저장/관리 하는가?
	14	개인정보를 파기할 때, 다시 복원하거나 재생할 수 없는 형태로 완벽하게 파기하는가?
	15	개인정보 파기에 관한 사항을 기록하고 관리하는가?
	16	개인정보파일을 운용하는 경우, 개인정보보호종합지원시스템(intra.privacy.go.kr)에 등록 하였는가?
	17	개인정보 처리방침을 공개하고 있는가?
	18	개인정보 처리방침의 변경 내용을 지속적으로 공개 및 이력관리를 하는가?
	19	수탁자에 대한 교육 및 감독을 수행하고 있는가?
개인정보의 기술적 · 물리적 보호조치	20	개인정보를 처리하는 시스템, 업무용컴퓨터에 백신소프트웨어를 설치·운영 하는가?
	21	개인정보취급자가 교외에서 시스템을 접속하는 경우 백신프로그램이 자동으로 설치되고 있는가?
	22	개인정보를 처리하는 시스템에 비인가 접근 등에 대한 상시 모니터링을 수행하는가?
	23	인터넷 홈페이지 취약점 점검 등을 수행 하는가?

	24	개인정보처리시스템의 중요도(민감도) 및 업무연관성 등을 고려하여 담당자별 차등 접근권한 절차를 마련하는가?
	25	전보 또는 퇴직 인력에 대해 개인정보처리시스템의 접근권한을 즉시 삭제 하는가?
	26	접근권한 부여·변경·말소에 대한 이력관리를 수행하는가?
	27	비밀번호 작성규칙을 수립하여 개인정보처리시스템에 적용하고 있는가?
	28	비밀번호를 일정 횟수 이상 잘못 입력한 경우 접근 제한 등 기술적 조치를 하고 있는가?
	29	비밀번호를 주기적으로 변경하도록 변경기간을 적용하는가?
	30	개인정보처리시스템에서 일정시간 업무를 하지 않는 경우 시스템 접속 차단을 하고 있는가?
	31	비인가된 P2P, 웹하드 등 공유설정에 대한 차단을 하고 있는가?
	32	개인정보취급자가 정보통신망을 통해 외부에서 접속하려는 경우 가상사설망(VPN) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증 수단을 적용하고 있는가?
	33	전산실, 자료보관실 등 개인정보를 취급하는 공간에 대해 출입통제 절차를 수립·운영 하고 있는가?
	34	개인정보가 포함된 서류 및 저장매체(USB, CD) 등을 잠금장치가 있는 안전한 장소에 보관하는가?
	35	고유식별정보(주민등록번호, 여권번호 등) 및 비밀번호가 암호화 되어 있는가?
	36	비밀번호는 일방향 암호화를 적용하여 저장되는가?
	37	개인정보 암호화 시, 안전한 알고리즘을 사용하고 있는가?
	38	사용자 PC부터 웹서버 구간 간 암호화를 적용 하였는가?
	39	개인정보처리시스템 접속기록을 2년 이상 보관 관리하는가?
	40	개인정보처리시스템 접속 기록이 위·변조 및 도난, 분실되지 않도록 분리된 내부망에 안전하게 보관하고 있는가?
	41	개인정보처리시스템의 접속기록 점검 및 후속조치를 수행 하는가?
	42	고정형 영상정보처리기기 운영·관리방침이 수립되어 있는가?
	43	고정형 영상정보처리기기 설치 시, 안내판을 설치하였는가?
개인정보 침해사고 대응방안	44	개인정보의 유·노출 및 침해사고에 대한 대응절차가 수립되어 있는가?
개인정보 재해·재난 대비 안전조치 대응방안	45	재해·재난 발생 시 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차 마련·점검하고 있는가?
	46	재해·재난 발생 시 개인정보처리시스템 백업 및 복구를 위한 계획을 마련하고 있는가?
개인정보보호 교육 수행	47	개인정보보호 교육 계획이 수립되어 있는가?
	48	개인정보 보호책임자가 교육을 받고 있는가?
	49	개인정보 담당자가 교육을 받고 있는가?
	50	개인정보취급자에 대한 교육을 수행하고 있는가?

[붙임 2] 개인정보파일 보유기간 책정 기준표(개인정보보호위원회 개인정보보호지침)

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

[붙임 3]

개인정보파일 파기 요청서

※부서명:

(붉은색 부분만 작성) **※ 반드시 전산개발팀 담당자와 협의후 작성하시기 바랍니다.**

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

[붙임 4]

개인정보파일 파기 관리대장

번호	개인정보 파일명	자료의 종류	생성일	파기일	파기사유	처리담당자	처리부서장

[붙임 5]

개인정보(열람, 정정·삭제, 처리정지, 동의철회, 자동화된 결정 거부·설명, 본인전송요구 등) 요구서

개인정보([ ] 열람 [ ] 정정·삭제 [ ] 처리정지 [ ] 동의철회 [ ] 자동화된 결정 거부·설명 [ ] 본인전송요구 등) 요구서

※ 아래 작성방법을 읽고 굵은 선 안쪽의 사항만 적어 주시기 바랍니다. (앞 쪽)

접수번호	접수일	처리기간 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	[ ] 열람	[ ] 개인정보의 항목 및 내용 [ ] 개인정보 수집·이용의 목적 [ ] 개인정보 보유 및 이용 기간 [ ] 개인정보의 제3자 제공 현황 [ ] 개인정보 처리에 동의한 사실 및 내용
	[ ] 정정·삭제	※ 정정·삭제하려는 개인정보의 항목과 그 사유를 적습니다.
	[ ] 처리정지	※ 개인정보의 처리정지를 원하는 대상·내용 및 그 사유를 적습니다.
	[ ] 동의철회	※ 동의철회를 원하는 대상·내용 및 그 사유를 적습니다.
	자동화된 결정 [ ] 거부, [ ] 설명 [ ] 검토	※ 거부·설명·검토를 원하는 자동화된 결정 대상·내용 및 그 사유를 적습니다.
	[ ] 본인전송요구	[ ] 전송을 요구하는 개인정보 [ ] 전송을 받으려는 형태(PDF,CSV,XLS 등) [ ] 전송을 받으려는 수단(이동통신단말장치 또는 전자우편 등)

「개인정보 보호법」 제35조제1항·제2항, 제35조의2제1항, 제36조제1항, 제37조제1항, 제37조의2제1항·제2항과 같은 법 시행령 제41조제1항, 제43조제1항, 제44조제1항, 제44조의2제1항·제2항에 따라 위와 같이 요구합니다.

년 월 일

요구인 (서명 또는 인)

○○○○ 귀하

작 성 방 법

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 처리정지 또는 동의철회를 요구하려는 경우에는 '처리정지' 또는 '동의철회' 란에 [√] 표시를 하고 처리정지 또는 동의철회 요구의 대상·내용 및 그 사유를 적습니다.
5. 자동화된 결정에 대한 거부 또는 설명 또는 검토를 요구하려는 경우 해당 란에 √] 표시를 하고 거부 또는 설명 또는 검토 요구의 대상·내용 및 그 사유를 적습니다.

[붙임 6]

개인정보(열람, 일부열람, 열람연기, 열람거절) 통지서

개인정보 ([ ] 열람 [ ] 일부열람 [ ] 열람연기 [ ] 열람거절) 통지서

(앞 쪽)

수신자 (우편번호 : , 주소 :)

요구 내용			
열람 일시		열람 장소	
통지 내용 ([ ] 열람 [ ] 일부열람 [ ] 열람연기 [ ] 열람거절)			
열람 형태 및 방법	열람 형태	[ ]열람·시청 [ ]사본·출력물 [ ]전자파일 [ ]복제물·인화물 [ ]기타	
	열람 방법	[ ]직접방문 [ ]우편 [ ]팩스 [ ]전자우편 [ ]기타	
납부 금액	①수수료 원	②우송료 원	계(①+②) 원
	수수료 산정 명세		
사 유			
이의제기방법	※ 개인정보처리자는 이의제기방법을 적습니다.		

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

년 월 일

발 신 명 의 직인

[붙임 7]

개인정보(정정・삭제, 처리정지) 요구에 대한 결과 통지서

개인정보 ([ ] 정정・삭제, [ ] 처리정지) 요구에 대한 결과 통지서	
수신자 (우편번호: , 주소:)	
요구 내용	
□ 정정・삭제 □ 처리정지 조치 내용	
□ 정정・삭제 □ 처리정지 결정 사유	
이의제기방법	※ 개인정보처리자는 이의제기방법을 기재합니다.
「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 발 신 명 의 직인	
유의사항	
개인정보의 정정・삭제 또는 처리정지 요구에 대한 결정을 통지받은 경우에는 개인정보처리자가 '이의제기방법'란에 적은 방법으로 이의제기를 할 수 있습니다.	

[붙임 8]

(통제구역 등) 출입자 관리대장

년		소 속	성 명	출입사유	확 인	비 고
월	일					

[붙임 9]

개인정보의 목적 외 이용 및 제3자 제공 대장

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

[붙임 10]

개인정보 침해사실 신고서

<table>
<tr><td rowspan="5">신고인</td><td colspan="2">성명</td><td></td></tr>
<tr><td colspan="2">생년월일</td><td></td></tr>
<tr><td rowspan="3">연락처</td><td>전화번호(핸드폰)</td><td></td></tr>
<tr><td>전자우편</td><td></td></tr>
<tr><td>주소</td><td></td></tr>
<tr><td rowspan="3">접수부서</td><td colspan="2">부서명</td><td></td></tr>
<tr><td rowspan="2">연락처</td><td>전화번호</td><td></td></tr>
<tr><td>주소</td><td></td></tr>
<tr><td>신고내용</td><td colspan="3"></td></tr>
<tr><td colspan="4">위와 같이 개인정보침해사실을 신고합니다.

붙임 :

년 월 일

신고인 : (서명 또는 인)</td></tr>
</table>

[붙임 11]

개인정보 침해사고 관리대장

접수		신고개요	침해사고 등급	처리 유형	종결 일자	처리내용	비고
일시	신고자 유형						

* 신고자 유형은 직원/고객으로 구분
* 신고 개요는 신고 내용을 기록
* 침해사고 등급은 1-8등급으로 구분
* 처리유형은 사실 확인 중/ 상담 및 자료 제공/ 타 기관 이송/ 위법성 통보/ 수사 의뢰/법 위반 확인 불가/ 기타(징계위원회 회부)로 구분
* 종결일자는 개인정보 침해사고 처리보고서 접수일을 기준으로 기록
* 처리내용은 처분 유형을 사법처리(징역, 벌금, 추징, 재판계류 중, 수사 중) 징계 처분(파면, 해임, 정직, 감봉, 견책, 기타)로 구분
* 비고란에는 처리보고서 문서번호를 기록

[붙임 12]

개인정보 침해사고 처리보고서

<table>
<tr><td>보고일자</td><td colspan="2"></td><td>문서번호</td><td></td></tr>
<tr><td>침해신고 접수정보</td><td colspan="4"></td></tr>
<tr><td>침해사고 등급</td><td colspan="2">(　　) 등급</td><td>침해대상정보</td><td></td></tr>
<tr><td>접수일시</td><td colspan="2"></td><td>신고일자</td><td></td></tr>
<tr><td>침해사고 처리책임자</td><td colspan="2"></td><td>신고자 연락처</td><td></td></tr>
<tr><td>신고 내용</td><td colspan="4"></td></tr>
<tr><td rowspan="2">대응 과정</td><td>일시</td><td colspan="3">대응활동</td></tr>
<tr><td></td><td colspan="3"></td></tr>
<tr><td>침해 내용</td><td colspan="4"></td></tr>
<tr><td>침해 발생 경위</td><td colspan="4"></td></tr>
<tr><td>관련자</td><td colspan="4"></td></tr>
<tr><td>침해 발생 원인</td><td colspan="4"></td></tr>
<tr><td>증거자료</td><td colspan="4"></td></tr>
<tr><td>복구 및 재발방지 조치</td><td colspan="4"></td></tr>
<tr><td>처분</td><td colspan="4"></td></tr>
</table>

* 침해 내용 : 확인된 침해 정보의 세부사항, 규모 및 침해 방법(노출, 외부자 제공, 수집, 접근, 분석, 이용, 내부자 제공, 불법 저장, 불안전한 저장, 파기, 비파기 등 세부사항) 기재

[붙임 13]

개인정보 유출신고(보고)서

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
	개인정보 보호책임자				
	개인정보 취급자				

유출신고 접수기관	기관명	담당자명	연락처