

개인정보보호의 안전성 확보를 위한

개인정보 내부관리 계획

2020. 2. 24.

국제대학교

목 차

제1장 총칙

제1조(목적)

제2조(적용범위)

제2장 내부관리계획의 수립 및 시행

제3조(내부관리계획의 수립 및 승인)

제4조(내부관리계획의 공표)

제3장 개인정보보호 조직 편제

제5조(용어 정의)

제6조(국제대학교 개인정보 관리 조직도)

제7조(역할별 업무)

제8조(개인정보 보호원칙)

제9조(개인정보보호책임자의 지정)

제10조(개인정보보호책임자의 의무와 책임)

제11조(개인정보취급자의 범위 및 의무와 책임)

제4장 개인정보의 수집 · 이용

제12조(개인정보의 수집 및 수집 제한)

제13조(개인정보의 수집에 대한 고지)

제14조(개인정보의 목적 외 이용 등)

제15조(개인정보 수집 출처 등 고지)

제16조(개인정보의 파기)

제17조(법령에 따른 개인정보의 보존)

제18조(동의를 받는 방법)

제19조(법정대리인의 동의)

제20조(민감정보 처리)

- 제21조(고유식별정보 처리에 대한 동의)
- 제22조(주민등록번호 처리의 제한)
- 제23조(주민등록번호 이외의 회원가입 방법 제공)
- 제24조(수탁자의 선정 시 고려사항)
- 제25조(위탁에 따른 개인정보 보호 조치의무)
- 제26조(정보주체와 재위탁의 관계)
- 제27조(개인정보 취급자의 제한)

제5장 개인정보 처리방침 작성

- 제28조(개인정보 처리방침의 공개)
- 제29조(개인정보 처리방침의 변경)
- 제30조(개인정보 처리방침의 작성기준 등)
- 제31조(개인정보 처리방침의 기재사항)

제6장 개인정보의 기술적·관리적 보호조치

- 제32조(개인정보보호 수준진단)
- 제33조(개인정보 영향평가)
- 제34조(개인정보의 안전성 확보 조치)
- 제35조(개인정보취급자에 대한 감독)
- 제36조(물리적 접근제한)
- 제37조(출력 복사 시 보호조치)
- 제38조(개인정보취급자 접근권한 관리 및 인증)
- 제39조(개인정보의 암호화)
- 제40조(접근통제)
- 제41조(접속 기록의 위변조 방지)
- 제42조(보안프로그램의 설치 및 운영)
- 제43조(영상정보처리기기의 설치 및 운영관리)
- 제44조(악성프로그램 등 방지)
- 제45조(물리적 접근제한)
- 제46조(기술적·관리적 보호조치 수행계획)

제7장 개인정보보호 교육

제47조(개인정보보호 교육 계획의 수립)

제48조(개인정보보호 교육의 실시)

제49조(개인정보보호 교육 계획서)

제8장 개인정보 보안점검 및 내부감사 실시

제50조(자체감사 주기 및 절차)

제51조(내부 감사)

제52조(자체감사 결과 반영)

제9장 개인정보 유·노출 및 침해대응 대책

제53조(개인정보 유·노출 및 침해사고 대응 절차도)

제54조(개인정보의 유출)

제55조(통지시기 및 항목)

제56조(통지방법)

제57조(개인정보 유출신고)

제58조(피해구제 대책)

제10장 개인정보보호 사무의 인수·인계

제59조(개인정보보호 사무의 인수·인계)

제1조(목적)

개인정보보호 내부관리계획(이하 '본 계획' 또는 '내부관리계획'이라 한다)은 개인정보 보호법 제29조(안전조치의무) 내부관리계획의 수립 및 시행 의무에 따라 제정된 것으로 우리학교가 취급하는 개인정보를 체계적으로 관리하여 개인정보가 분실, 도난, 누출, 변조, 훼손, 오.남용 등이 되지 아니하도록 함을 목적으로 한다.

제2조(적용범위)

본 계획은 정보통신망을 통하여 수집, 이용, 제공 또는 관리되는 개인정보뿐만 아니라 서면 등 정보통신망 이외의 수단을 통해서 수집, 이용, 제공 또는 관리되는 개인정보 및 영상정보처리기기(CCTV)에 대해서도 적용되며, 이러한 개인정보를 취급하는 교직원 및 외부위탁업체에 대해 적용된다.

제3조(내부관리계획의 수립 및 승인)

- ① 개인정보 보호담당자는 우리학교의 개인정보보호를 위한 전반적인 사항을 포함하여 내부관리계획을 수립하여야 한다.
- ② 개인정보 보호담당자는 개인정보보호를 위한 내부관리계획의 수립 시 개인정보보호와 관련한 법령 및 관련 규정을 준수하도록 내부관리계획을 수립하여야 한다.
- ③ 개인정보 보호책임자는 개인정보 보호담당자가 수립한 내부관리계획의 타당성을 검토하여 개인정보보호를 위한 내부관리계획을 승인하여야 한다.
- ④ 개인정보 보호담당자는 개인정보보호 관련 법령의 제.개정 사항 등을 반영하기 위하여 매년 1월말까지 내부관리계획의 타당성과 개정 필요성을 검토하여야 한다.
- ⑤ 개인정보 보호담당자는 모든 항목의 타당성을 검토한 후 개정할 필요가 있다고 판단되는 경우 2월말까지 내부관리계획의 개정안을 작성하여 개인정보 보호책임자에게 보고하고 개인정보 보호책임자의 승인을 받아야 한다.

제4조(내부관리계획의 공표)

- ① 개인정보 보호책임자는 승인한 내부관리계획을 매년 2월말까지 우리학교 직원에게 공표한다.

- ② 내부관리계획은 직원이 언제든지 열람할 수 있는 방법으로 비치하여야 하며, 변경사항이 있는 경우에는 이를 공지하여야 한다.

III 제3장 개인정보보호 조직 편제

제5조(용어 정의)

본 계획에서 사용하는 용어의 정의는 다음 각 호와 같다.

1. "개인정보"라 함은 생존하는 개인에 관한 정보로서 성명/주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호/문자/음성/음향 및 영상 등의 정보(해당 정보만으로 특정한 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)를 말한다.
2. "개인정보 처리자"라 함은 업무를 목적으로 개인정보파일을 운용하기 위하여 개인정보를 처리하는 기관으로서, "국제대학교"를 말한다.
3. "개인정보 보호책임자"라 함은 우리학교의 개인정보 처리에 관한 업무를 총괄해서 책임지거나 업무처리를 최종적으로 결정하는 자로서, 법 제31조 및 개인정보 보호법 시행령(이하 "시행령"이라 한다) 제32조제2항에 따른 지위에 해당하는 자를 말한다.
4. "개인정보보호 관리자"라 함은 개인정보 보호책임자의 개인정보 보호업무에 대해 위임을 받아 업무를 총괄하고 관리하는 자를 말한다.
5. "개인정보보호 업무 분야별책임자"(이하 "분야별책임자"라 한다)란 업무를 위하여 개인정보파일을 처리하는 부서의 장으로 개인정보 보호책임자가 지정한 자를 말한다.
6. "개인정보 보호담당자"란 각급기관의 실질적인 개인정보 보호업무를 담당하는 자로 개인정보 처리자가 지정한 자를 말한다.
7. "개인정보보호 시스템 관리자"는 "개인정보 보호담당자"를 도와 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 관리하고 정보보호업무를 추진하는 자를 말한다.
8. "개인정보취급자"란 개인정보처리자의 지휘감독을 받아 개인정보를 처리하는 자로서 직원, 파견근로자, 시간제근로자 등을 말한다.
9. "개인정보파일"이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.
10. "개인정보의 처리"란 개인정보를 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 연계, 연동 그 밖에 이와 유사

한 행위를 말한다.

11. "개인정보처리시스템"이란 개인정보를 처리할 수 있도록 체계적으로 구성된 데이터베이스시스템을 말한다.
12. "고유식별번호"란 법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 주민등록번호, 여권번호, 운전면허의 면허번호, 외국인등록번호를 말한다.
13. "민감정보"란 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활, 유전정보, 범죄경력 정보 등에 관한 정보와 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보를 말한다.
14. "영상정보처리기기"란 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 시행령 제3조에 따른 폐쇄회로 텔레비전(CCTV) 및 네트워크 카메라를 말한다.
15. "개인영상정보"란 영상정보처리기기에 의하여 촬영·처리되는 영상정보 중 개인의 초상, 행동 등 사생활과 관련된 영상으로서 해당 개인의 동일성 여부를 식별할 수 있는 정보를 말한다.
16. "영상정보처리기기운영자"란 법 제25조제1항 각 호에 따라 영상정보처리기기를 설치·운영하는 자를 말한다.
17. "공개된 장소"란 공원, 도로, 지하철, 상가 내부, 주차장 등 정보주체가 접근하거나 통행하는 데에 제한을 받지 아니하는 장소를 말한다.
18. "정보주체"란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.

제6조(국제대학교 개인정보 관리 조직도) (개정 2019. 2.)



[총괄 책임자 및 분야별 책임자]

| 구분 | 담당부서 | 직위 | 연락처 | 비고 |
|--------|-------|--------|--------------|----|
| 총괄책임자 | 사무처 | 사무처장 | 031-6108-104 | |
| 총괄부책임자 | 전산정보원 | 전산정보원장 | 031-6108-740 | |
| 분야별책임자 | 기획처 | 기획처장 | 031-6108-107 | |
| 분야별책임자 | 교무처 | 교무처장 | 031-6108-111 | |
| 분야별책임자 | 학생지원처 | 학생지원처장 | 031-6108-103 | |
| 분야별책임자 | 입시홍보처 | 입시홍보처장 | 031-6108-110 | |
| 분야별책임자 | 학술정보원 | 학술정보원장 | 031-6108-043 | |
| 분야별책임자 | 평생교육원 | 평생교육원장 | 031-6108-105 | |
| 분야별책임자 | 산학협력단 | 산학협력단장 | 031-6108-109 | |

| | | | | |
|--------|------|-----|------|--|
| 분야별책임자 | 각 학과 | 학과장 | 과사무실 | |
|--------|------|-----|------|--|

[개인정보 취급자]

| 구분 | 담당부서 | 실무담당 | 연락처 | 개인정보파일 |
|---------|--------|------|--------------|--------------------|
| 개인정보취급자 | 사무처 | 팀장 | 031-6108-736 | 인사, 등록 |
| 개인정보취급자 | 기획처 | 팀장 | 031-6108-096 | 발전기금 |
| 개인정보취급자 | 교무처 | 팀장 | 031-6108-712 | 학적, 수업, 교직, 성적, 졸업 |
| 개인정보취급자 | 학생지원처 | 팀장 | 031-6108-721 | 학생, 장학, 취업, 기숙사 |
| 개인정보취급자 | 입시홍보처 | 팀장 | 031-6108-701 | 입학지원자명단 |
| 개인정보취급자 | 학술정보원 | 팀장 | 031-6108-727 | 대출/반납이용자 |
| 개인정보취급자 | 평생교육원 | 실장 | 031-6108-729 | 보육교사, 평생교육 수강생 |
| 개인정보취급자 | 산학협력단 | 팀장 | 031-6129-352 | |
| 개인정보취급자 | 정보지원센터 | 팀장 | 031-6108-741 | |
| 개인정보취급자 | 각 학과 | 조교 | 과사무실 | |

제7조(역할별 업무)

가. 개인정보보호책임자 - 개인정보의 처리에 관한 업무 총괄책임

- 1) 개인정보보호 계획의 수립 및 시행
- 2) 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
- 3) 개인정보 처리 관련 불만 처리 및 피해 구제
- 4) 개인정보 유출 및 오·남용 방지를 위한 내부통제시스템 구축
- 5) 개인정보보호 교육 계획의 수립 및 시행
- 6) 개인정보파일의 보호 및 관리·감독
- 7) 법 제30조에 따른 '개인정보처리방침'의 수립·변경 및 시행
- 8) 개인정보보호 관련 자료의 관리
- 9) 개인정보파일의 보유기간 산정
- 10) 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기

나. 보안위원회(개인정보보호위원회) - 개인정보보호에 관한 사항을 심의·의결

- 1) 개인정보보호 기본계획 및 시행계획

- 2) 개인정보보호에 관한 정책 및 제도개선에 관한 사항
- 3) 처리정보의 이용 및 제공에 관한 사항
- 4) 처리정보의 열람 및 정정청구에 관한 심의
- 5) 그 밖에 개인정보보호에 관한 사항

다. 개인정보보호분야별책임자 - 개인정보를 보유·처리하는 과 단위의 부서장

- 1) 부서내의 개인정보관리
- 2) 개인정보 취급자의 개인정보보호 업무의 지도.감독
- 3) 시스템 로그파일 등 접속기록의 주기적 분석 및 오.남용 사고의 예방
- 4) 개인정보에 관한 업무 인계.인수 확인
- 5) 개인정보파일을 보유한 부서의 개인정보취급자는 개인정보종합정보시스템에 개인정보파일을 등록, 수정, 파기 등 의무적으로 관리
- 6) 개인정보취급자에 대한 교육

라. 개인정보보호 담당자

- 1) 개인정보보호 계획 및 방침 운영
- 2) 개인정보침해 대응
- 3) 개인정보처리 실태관리 및 각종 자료 취합
- 4) 개인정보보호법 관련 업무 전반
- 5) 개인정보보호교육 업무
- 6) 개인정보보호책임관이 위임한 개인정보보호와 관련된 업무
- 7) 개인정보처리와 관련된 시스템 연계등과 관련된 업무

마. 개인정보 취급자

- 1) 업무를 수행함에 있어서 처리되는 개인정보에 대한 보호관리(개인정보의 수집-보유-이용 및 제공-파기단계에서의 관리)
- 2) 웹사이트에 게재되는 개인정보에 대한 보호관리
- 3) CCTV 화상정보에 대한 보호관리
- 4) 개인정보의 열람, 정정, 삭제시 보호관리

바. 시스템운영담당자

- 1) 기술적 안정성 확보
- 2) 관리적 안정성 확보
- 3) 시스템 연계시 협의
- 4) 개인정보수집 사실 안내

제8조(개인정보 보호원칙)

- ① 개인정보처리자는 개인정보 처리 목적을 명확하게 하고, 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여 직접적으로 필요한 범위 내에서만 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하지 않아야 한다.
- ② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.
- ③ 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험정도를 고려하여 적절한 기술적·관리적 및 물리적 보안조치를 통하여 개인정보를 안전하게 관리하여야 한다.
- ④ 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하며, 열람청구권 등 정보주체의 권리를 보장하여야 한다.
- ⑤ 개인정보처리자는 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.
- ⑥ 개인정보처리자는 개인정보의 처리에 관한 정보주체의 동의를 얻은 경우라도 구체적인 업무의 특성상 가능한 경우에는 특정 개인을 알아볼 수 없는 형태로 개인정보를 처리하여야 한다.

제9조(개인정보보호책임자의 지정)

- ① 우리학교는 “개인정보 보호법 시행령 제32조 제2항의 사항”에 의하여 해당 학교의 행정사무를 총괄하는 부서의 장 또는 개인정보 처리관련 업무를 담당하는 부서의 장을 개인정보보호책임자로 임명하고, “개인정보보호책임자”의 업무를 위임받아 진행하는 자를 개인정보보호 관리자로 하며, 개인정보를 처리하는 부서의 장을 개인정보보호 분야별책임자로 임명한다.

제10조(개인정보보호책임자의 의무와 책임)

- ① 개인정보보호책임자는 정보주체의 개인정보를 보호하고 개인정보와 관련한 정보주체의 불만을 처리하기 위하여 다음 각 호의 임무를 수행한다.
 1. 정보주체 개인정보의 수집·이용·제공 및 관리에 관한 업무의 총괄
 2. 개인정보보호분야별책임자 및 취급자의 의무와 책임의 규정 및 총괄관리
 3. 내부관리계획의 수립 및 승인
 4. 개인정보의 기술적·관리적 보호조치 기준 이행 총괄
 5. 직원 또는 제3자에 의한 위법·부당한 개인정보 침해행위에 대한 점검, 대응, 사후

조치 총괄

6. 정보주체로부터 제기되는 개인정보에 관한 고충이나 의견의 처리 및 감독 총괄
 7. 직원 및 개인정보취급업무 수탁자 등에 대한 교육 총괄
 8. 본 계획에 규정된 개인정보보호와 관련된 제반 조치의 시행 총괄
 9. 기타 정보주체의 개인정보보호에 필요한 사항
- ② 개인정보보호책임자는 개인정보취급자를 최소한으로 제한하여 지정하고 수시로 관리·감독하여야 하며, 직원에 대한 교육 및 보안서약 등을 통해 개인정보 침해사고를 사전에 예방한다.
 - ③ 개인정보보호책임자는 개인정보 관련 업무의 효율적 운영을 위하여 개인정보 관리 전담부서의 직원 중 1인 이상을 개인정보 보호담당자 및 관리자로 임명한다.
 - ④ 개인정보보호담당자는 개인정보보호책임자를 보좌하여 개인정보보호 업무에 대한 실무를 총괄하고 관리한다.
 - ⑤ 개인정보보호책임자는 개인정보관리에 대하여 개인정보보호분야별책임자를 지정하여 관리할 수 있다.

제11조(개인정보취급자의 범위 및 의무와 책임)

- ① 개인정보취급자의 범위는 우리학교 내에서 정보주체들의 개인정보 수집, 보관, 이용, 제공, 관리 또는 파기 등의 업무를 수행하는 자를 말하고, 정규직 이외에 임시직, 계약직 직원도 포함될 수 있다.
- ② 개인정보취급자는 정보주체의 개인정보보호와 관련하여 다음과 같은 역할 및 책임을 이행한다.
 1. 개인정보보호 활동 참여
 2. 내부관리계획의 준수 및 이행
 3. 개인정보의 기술적·관리적 보호조치 기준 이행
 4. 직원 또는 제3자에 의한 위법·부당한 개인정보 침해행위에 대한 점검 등
 5. 기타 정보주체의 개인정보보호를 위해 필요한 사항의 이행

IV 제4장 개인정보의 수집·이용

제12조(개인정보의 수집 및 수집 제한)

- ① 개인정보처리자는 다음 각 호의 경우에 개인정보를 수집할 수 있으며, 그 수집 목적의 범위에서 이용할 수 있다.
 1. 정보주체로부터 사전에 동의를 받은 경우

2. 법령에서 개인정보를 수집·이용할 수 있음을 구체적으로 명시하거나 허용하고 있는 경우
3. 법령에서 개인정보처리자에게 구체적인 의무를 부과하고 있고, 개인정보처리자가 개인정보를 수집·이용하지 않고는 법령에서 부과하는 구체적인 의무를 이행하는 것이 불가능하거나 현저히 곤란한 경우
4. 개인정보를 수집·이용하지 않고는 법령 등에서 정한 소관업무를 수행하는 것이 불가능하거나 현저히 곤란한 경우
5. 정보주체 또는 제3자(정보주체를 제외한 그 밖의 모든 자를 말한다)의 생명, 신체, 재산에 대한 피해를 방지해야 할 급박한 상황이어서 개인정보를 수집·이용해야 할 필요성이 명백히 인정됨에도 불구하고 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 연락을 취할 수 없는 상황이어서 사전에 동의를 받을 수 없는 경우
6. 개인정보처리자가 법령 또는 정보주체와의 계약에 따른 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 개인정보의 수집·이용에 관한 동의 여부 및 동의 범위 등을 선택하고 결정할 권리보다 우선하는 경우. 다만, 이 경우 개인정보의 수집·이용은 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 범위로 한정된다.
 - ② 개인정보처리자가 정보주체로부터 직접 명함 또는 그와 유사한 매체(이하 "명함 등"이라 한다)를 제공받음으로써 개인정보를 수집하는 경우, 정보주체가 동의 의사를 명확히 표시하거나 그렇지 않은 경우 명함 등을 제공하는 정황 등에 비추어 사회통념상 동의 의사가 있었다고 인정되는 범위 내에서만 이용할 수 있다.
 - ③ 개인정보처리자가 인터넷 홈페이지 등 공개된 매체 또는 장소(이하 "인터넷 홈페이지 등"이라 한다)에서 개인정보를 수집하는 경우, 해당 개인정보는 본인의 개인정보를 인터넷 홈페이지 등에 게시하거나 게시하도록 허용한 정보주체의 동의 의사가 명확히 표시되거나 인터넷 홈페이지 등의 표시 내용에 비추어 사회통념상 동의의사가 있었다고 인정되는 범위 내에서만 이용할 수 있다.
 - ④ 개인정보처리자는 계약 등의 상대방인 정보주체가 대리인을 통하여 법률행위 또는 의사표시를 하는 경우 대리인의 대리권 확인을 위한 목적으로만 대리인으로부터 또는 의사표시를 하는 경우 대리인의 개인정보를 수집·이용할 수 있다.
 - ⑤ 근로자와 사용자가 근로계약을 체결하는 경우 「근로기준법」 제2조제5호의 임금지급, 교육, 증명서 발급, 근로자 복지제공을 위하여 근로자의 동의 없이 개인정보를 수집·이용할 수 있다.

제13조(개인정보의 수집에 대한 고지)

- ① 정보주체로부터 12의 1항의 내용에 의한 동의를 받고자 하는 경우 또는 개인정보를 제3자로부터 제공받는 경우에는 미리 다음 각 호의 사항을 서면 또는 인터넷 홈페이지 등을 통하여 내용을 쉽게 확인할 수 있도록 정보주체에게 고지하거나 개인정보처리방침에 명시하여야 한다.
 - 1. 개인정보 보호책임자의 성명, 소속, 전화번호
 - 2. 개인정보의 구체적인 수집목적 및 이용목적
 - 3. 동의 철회, 열람 또는 정정 요구 등 정보주체 및 법정대리인의 권리와 그 행사방법
 - 4. 정보주체로부터 수집하고자 하는 개인정보 항목
 - 5. 수집하는 개인정보의 보유·이용기간 및 법적 근거 등 보유 근거
 - 6. 기타 개인정보에 대한 처리 또는 관리 방식

제14조(개인정보의 목적 외 이용 등)

- ① 법 제18조의 "제3자"란 정보주체와 정보주체 또는 그의 법정대리인으로부터 개인정보를 실질적·직접적으로 수집·보유한 개인정보처리자를 제외한 모든 자를 의미하며, 법 제26조제2항에 따른 수탁자는 제외한다.
- ② 개인정보처리자가 법 제18조제2항에 따라 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우에는 제공과 동시에 또는 필요한 경우에는 제공한 이후에 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 자는 그에 따른 조치를 취하고 그 사실을 개인정보를 제공한 개인정보처리자에게 문서로 알려야 한다.
- ③ 법 제18조제2항에 따라 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우에는 개인정보를 제공하는 자와 개인정보를 제공받는 자는 개인정보의 안전성에 관한 책임관계를 명확히 하여야 한다.
- ④ 개인정보처리자가 법 제18조제3항제1호에 따라 정보주체에게 개인정보를 제공받는 자를 알리는 경우에는 그 성명(법인 또는 단체인 경우에는 그 명칭)과 연락처를 함께 알려야 한다.
- ⑤ 개인정보처리자가 법 제18조제2항제4호에 따라 개인정보를 제3자에게 제공하는 경우에는 다른 정보와 결합하여서도 특정 개인을 알아볼 수 없는 형태로 제공하여야 한다.

제15조(개인정보 수집 출처 등 고지)

- ① 개인정보처리자가 정보주체 이외로부터 수집한 개인정보를 처리하는 때에는 정당한 사유가 없는 한 정보주체의 요구가 있는 날로부터 3일 이내에 다음 각 호의 모든 사항을 정보주체에게 알려야 한다.
 1. 개인정보의 수집 출처
 2. 개인정보의 처리 목적
 3. 법 제37조에 따른 개인정보 처리의 정지를 요구할 권리가 있다는 사실
- ② 법 제20조제2항 각 호에 근거하여 제1항에 따른 정보주체의 요구를 거부하는 경우에는 정당한 사유가 없는 한 정보주체의 요구가 있는 날로부터 3일 이내에 그 거부의 근거와 사유를 정보주체에게 알려야 한다.

제16조(개인정보의 파기)

- ① 개인정보처리자는 개인정보의 보유기간이 경과된 경우에는 정당한 사유가 없는 한 보유기간의 종료일로부터 5일 이내에, 개인정보의 처리 목적 달성, 해당 서비스의 폐지, 사업의 종료 등 그 개인정보가 불필요하게 되었을 때에는 정당한 사유가 없는 한 개인정보의 처리가 불필요한 것으로 인정되는 날로부터 5일 이내에 그 개인정보를 파기하도록 하여야 한다.
- ② 개인정보처리자는 개인정보를 파기할 경우 다음 각 호 중 어느 하나의 조치를 하여야 한다.
 1. 완전파괴(소각·파쇄 등)
 2. 전용 소자장비를 이용하여 삭제
 3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행
- ③ 개인정보처리자가 개인정보의 일부만을 파기하는 경우, 제2항의 방법으로 파기하는 것이 어려운 때에는 다음 각 호의 조치를 하여야 한다.
 1. 전자적 파일 형태인 경우 : 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독
 2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 해당 부분을 마스킹, 천공 등으로 삭제
- ④ 개인정보처리자는 개인정보의 파기에 관한 사항을 기록·관리하여야 한다.
- ⑤ 개인정보파기의 시행 및 확인은 개인정보 보호책임자의 책임하에 수행되어야 하며, 개인정보 보호책임자는 개인정보 파기 시행 후 파기 결과를 확인하여야 한다. 단 분야별 책임자를 지정한 경우에는 분야별책임자가 개인정보 보호책임자의 승인을 득 한 후 이를 수행할 수 있다.

제17조(법령에 따른 개인정보의 보존)

개인정보처리자가 법 제21조제1항 단서에 따라 개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 법령에 따라 해당 개인정보 또는 개인정보파일을 보존한다는 사실을 분명히 표시하여야 한다.

제18조(동의를 받는 방법)

- ① 개인정보처리자는 법 제15조제1항제1호에 따라 개인정보의 수집과 이용을 위하여 정보주체의 동의를 받고자 하는 경우에는 기본적인 재화 또는 서비스의 제공을 위하여 반드시 필요한 최소한의 개인정보와 부가적인 재화 또는 서비스의 제공을 위하여 필요한 최소한의 개인정보를 구분하여 정보주체에게 알리고 동의를 받아야 한다.
- ② 개인정보처리자가 법 제15조제1항제1호, 법 제17조제1항제1호, 법 제23조제1호 및 법 제24조제1항제1호에 따라 개인정보를 처리하기 위하여 정보주체의 동의를 얻고자 하는 경우에는 정보주체의 동의가 필요한 경우와 필요하지 않은 경우를 구분하고, 후자의 경우에는 정보주체의 동의 없이 개인정보를 처리할 수 있다는 점과 그 사유를 알려야 한다.
- ③ 개인정보처리자는 법 제18조제2항제1호에 따라 정보주체로부터 별도의 동의를 받고자 하는 경우에는 정보주체가 다른 개인정보처리의 목적과 별도로 동의 여부를 표시할 수 있도록 조치를 취하고 동의를 받아야 한다.
- ④ 개인정보처리자가 시행령 제17조제1항제2호에 따라 전화에 의한 동의와 관련하여 통화내용을 녹취할 때에는 녹취사실을 정보주체에게 알려야 한다.
- ⑤ 개인정보처리자는 만 14세 미만 아동의 개인정보를 처리하기 위하여 개인정보보호법에 따른 동의를 받아야 할 때에는 그 법정대리인의 동의를 받아야 한다. 이 경우 법정대리인의 동의를 받기 위하여 필요한 최소한의 정보는 법정대리인의 동의 없이 해당 아동으로부터 직접 수집할 수 있다.

제19조(법정대리인의 동의)

- ① 시행령 제17조제2항에 따라 개인정보처리자가 법정대리인의 성명·연락처를 수집할 때에는 해당 아동에게 자신의 신분과 연락처, 법정대리인의 성명과 연락처를 수집하고자 하는 이유를 알려야 한다.
- ② 시행령 제17조제1항 각 호의 동의를 얻는 방법은 법 제22조제5항에 따라 법정대리인으로부터 동의를 얻는 경우에도 적용된다.
- ③ 개인정보처리자는 법 제22조제5항에 따라 수집한 법정대리인의 개인정보를 법정대리인의 동의를 얻기 위한 목적으로만 이용하여야 하며, 법정대리인의 동의 거부가 있거나 법정대리인의 동의 의사가 확인되지 않는 경우 수집일로부터 5일 이내에 파기

해야 한다.

제20조(민감정보 처리)

- ① 개인정보처리자가 법 제23조제1호에 따라 민감정보의 처리를 위하여 정보주체에게 동의를 받고자 하는 경우에는 다른 개인정보와 민감정보를 구분하여 민감정보에 대하여는 정보주체가 별도로 동의할 수 있도록 조치를 취하여야 한다.
- ② 개인정보처리자는 제1항에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.
 1. 민감정보의 수집·이용 목적
 2. 수집하려는 민감정보의 항목
 3. 민감정보의 보유 및 이용 기간
 4. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

제21조(고유식별정보 처리에 대한 동의)

- ① 개인정보처리자가 법 제24조제1항제1호에 따라 고유식별정보의 처리를 위하여 정보주체에게 동의를 받고자 하는 경우에는 다른 개인정보와 고유식별정보를 구분하여 고유식별정보에 대하여는 정보주체가 별도로 동의할 수 있도록 조치를 취하여야 한다.
- ② 개인정보처리자는 제1항에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.
 1. 고유식별정보의 수집·이용 목적
 2. 수집하려는 고유식별정보의 항목
 3. 고유식별정보의 보유 및 이용 기간
 4. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

제22조(주민등록번호 처리의 제한)

개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다.

1. 법령에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우
2. 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인

정되는 경우

3. 제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 행정자치부령으로 정하는 경우

제23조(주민등록번호 이외의 회원가입 방법 제공)

개인정보처리자가 법 제24조의2제3항에 따라 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법(이하 "대체수단"이라 한다)을 제공해야 하는 경우, 정보주체는 주민등록번호가 아닌 대체수단을 사용하여서도 회원으로 가입할 수 있다는 점을 회원가입절차를 위한 화면을 통하여 명시적으로 알리고 회원가입을 받아야 한다.

제24조(수탁자의 선정 시 고려사항)

- ① 개인정보의 처리 업무를 위탁하는 개인정보처리자(이하 "위탁자"라 한다)가 개인정보 처리 업무를 위탁받아 처리하는 자(이하 "수탁자"라 한다)를 선정할 때에는 인력과 물적 시설, 재정 부담능력, 기술 보유의 정도, 책임능력 등을 종합적으로 고려하여야 한다.
- ② 개인정보처리자가 개인정보의 처리 업무를 위탁하는 때에는 수탁자의 처리 업무의 지연, 처리 업무와 관련 없는 불필요한 개인정보의 요구, 처리기준의 불공정 등의 문제점을 종합적으로 검토하여 이를 방지하기 위하여 필요한 조치를 마련하여야 한다.

제25조(위탁에 따른 개인정보 보호 조치의무)

- ① 개인정보처리자가 개인정보의 처리 업무를 위탁하는 경우 다음 각 호의 내용이 포함된 문서에 의하여야 한다.
 1. 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
 2. 개인정보의 기술적·관리적 보호조치에 관한 사항
 3. 위탁업무의 목적 및 범위
 4. 재위탁 제한에 관한 사항
 5. 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
 6. 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항
 7. 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항
- ② 수탁자는 위탁받은 개인정보를 보호하기 위하여 행정자치부장관이 고시하는 「개인정보의 안전성 확보조치 기준」에 따른 기술적·관리적·물리적 조치를 하여야 한다.
- ③ 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리 현황 점검 등 수탁자가 개인정보를

안전하게 처리하는지를 관리·감독 하여야 한다.

제26조(정보주체와 재위탁의 관계)

- ① 정보주체는 수탁자로부터 개인정보 처리 업무를 재위탁 받아 처리하는 자(이하 "재수탁자"라 한다)가 재위탁 받은 개인정보 처리 업무를 수행하면서 발생하는 손해에 대한 배상을 청구할 수 있다.
- ② 개인정보 처리 업무의 재위탁에 대해서는 법 제26조를 준용한다.

제27조(개인정보 취급자의 제한)

- ① 개인정보 분야별관리자는 개인정보를 취급할 수 있는 자를 다음 각 호의 1에 해당하는 자로 정하여 최소한으로 제한하여야 한다.
 - 1. 정보주체를 직접 상대로 하여 업무를 수행하는 자
 - 2. 개인정보 보호책임자 등 개인정보관리 업무를 수행하는 자
 - 3. 데이터베이스를 포함한 전산 관련 업무를 수행하는 자
 - 4. 기타 업무상 개인정보의 취급이 불가피한 자

V 제5장 개인정보 처리방침 작성

제28조(개인정보 처리방침의 공개)

- ① 개인정보처리자가 법 제30조제2항에 따라 개인정보 처리방침을 수립하거나 변경하는 경우에는 인터넷 홈페이지를 통해 지속적으로 게재하여야 하며 이 경우 "개인정보 처리방침"이라는 명칭을 사용하되, 글자 크기, 색상 등을 활용하여 다른 고지사항과 구분함으로써 정보주체가 쉽게 확인할 수 있도록 하여야 한다.
- ② 개인정보처리자가 인터넷 홈페이지를 운영하지 않는 경우 또는 인터넷 홈페이지 관리상의 하자가 있는 경우에는 시행령 제31조제3항 각 호의 어느 하나 이상의 방법으로 개인정보 처리방침을 공개하여야 한다.
- ③ 개인정보처리자가 시행령 제31조제3항제3호의 방법으로 개인정보 처리방침을 공개하는 경우에는 간행물·소식지·홍보지·청구서 등이 발행될 때마다 계속하여 게재하여야 한다.

제29조(개인정보 처리방침의 변경)

개인정보처리자가 개인정보 처리방침을 변경하는 경우에는 변경 및 시행의 시기, 변경된 내용을 지속적으로 공개하여야 하며, 변경된 내용은 정보주체가 쉽게 확인할 수 있

도록 변경 전·후를 비교하여 공개하여야 한다.

제30조(개인정보 처리방침의 작성기준 등)

- ① 개인정보처리자가 개인정보 처리방침을 작성하는 때에는 법 제30조제1항제1호부터 제5호 및 시행령 제31조제1항 각 호의 사항을 명시적으로 구분하되, 알기 쉬운 용어로 구체적이고 명확하게 표현하여야 한다.
- ② 개인정보처리자는 개인정보의 처리 목적에 필요한 최소한의 개인정보라는 점을 밝혀야 한다.
- ③ 개인정보처리자가 목적에 필요한 최소한의 개인정보 이외에 개인별 맞춤서비스 등을 위하여 처리하는 개인정보의 항목이 있는 경우에는 양자를 구별하여 표시하여야 한다.

제31조(개인정보 처리방침의 기재사항)

- ① 개인정보처리자가 개인정보 처리방침을 작성할 때에는 법 제30조제1항에 따라 다음 각 호의 사항을 모두 포함하여야 한다.
 - 1. 개인정보의 처리 목적
 - 2. 개인정보의 처리 및 보유 기간
 - 3. 개인정보의 제3자 제공에 관한 사항(해당되는 경우에만 정한다)
 - 4. 개인정보처리의 위탁에 관한 사항(해당되는 경우에만 정한다)
 - 5. 정보주체의 권리·의무 및 그 행사방법에 관한 사항
 - 6. 처리하는 개인정보의 항목
 - 7. 개인정보의 파기에 관한 사항
 - 8. 개인정보 보호책임자에 관한 사항
 - 9. 개인정보 처리방침의 변경에 관한 사항
 - 10. 시행령 제30조제1항에 따른 개인정보의 안전성 확보조치에 관한 사항
- ② 개인정보처리자는 제1항의 필수적 기재사항 이외에도 다음 각 호의 사항을 개인정보 처리방침에 포함할 수 있다.
 - 1. 정보주체의 권익침해에 대한 구제방법
 - 2. 개인정보의 열람청구를 접수·처리하는 부서

VI 제6장 개인정보의 기술적·관리적 보호조치

제32조(개인정보보호 수준진단)

- ① 개인정보처리자는 자율적인 개인정보 보호활동을 촉진하고 지원하기 위하여 개인정보보호 수준진단을 실시할 수 있다.
- ② 개인정보처리자는 필요 시 (가칭)“개인정보보호 점검·지원반”을 구성·운영할 수 있다.
- ③ (가칭)“개인정보보호 점검·지원반”은 다음 각호의 업무를 수행한다.
 - 1. 개인정보보호 업무를 위한 지침 및 계획 수립 지원
 - 2. 개인정보 영향평가 및 개인정보보호 수준진단 지원
 - 3. 개인정보 유·노출 점검 및 현장 컨설팅(정기, 특별)
 - 4. 개인정보 보호 역량 강화 지원 등

제33조(개인정보 영향평가)

개인정보처리자는 다음 각 호의 어느 하나에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우 그 위험요인의 분석과 개선사항 도출을 위하여 개인정보 영향평가를 수행하여야 한다.

- 1. 구축·운용 또는 변경하려는 개인정보파일로서 5만명 이상의 정보주체에 관한 법 제 23조에 따른 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일
- 2. 구축·운용하고 있는 개인정보파일을 해당 기관 내부 또는 외부에서 구축·운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50만명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일
- 3. 구축·운용 또는 변경하려는 개인정보파일로서 100만명 이상의 정보주체에 관한 개인정보파일
- 4. 법 제33조제1항에 따른 개인정보 영향평가를 받은 후에 개인정보 검색체계 등 개인정보파일의 운용체계를 변경하려는 경우 그 개인정보파일. 이 경우 영향평가 대상은 변경된 부분으로 한정한다.

제34조(개인정보의 안전성 확보 조치)

- ① 개인정보처리자는 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 다음 각 호의 관리적·기술적·물리적 보호조치를 하여야 한다.
 - 1. 개인정보를 안전하게 처리하기 위한 내부 관리계획의 수립·시행
 - 2. 개인정보에 대한 접근 통제 및 접근 권한의 제한·관리 조치
 - 3. 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치
 - 4. 개인정보 침해사고 발생 시 대응하기 위한 접속기록의 보관 및 위·변조 방지를 위한 조치

5. 개인정보에 대한 보안프로그램의 설치 및 갱신·점검 조치
6. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치

제35조(개인정보취급자에 대한 감독)

- ① 개인정보처리자는 개인정보취급자를 업무상 필요한 한도 내에서 최소한으로 두어야 하며, 개인정보취급자의 개인정보 처리범위를 업무상 필요한 한도 내에서 최소한으로 제한하여야 한다.
- ② 개인정보처리자는 개인정보취급자로 하여금 보안서약을 제출하도록 하는 등 적절한 관리·감독을 해야 한다.

제36조(물리적 접근제한)

- ① 개인정보보호분야별책임자는 개인정보와 개인정보처리시스템의 안전한 보관을 위한 물리적 잠금장치 등의 물리적 접근방지를 위한 보호조치를 취하여야 한다.
- ② 개인정보보호분야별책임자는 물리적 접근방지를 위한 별도의 보호시설에 출입하거나 개인정보를 열람하는 경우, 그 출입자에 대한 출입사실 및 열람 내용에 관한 관리대장을 작성하도록 하여야 한다.
- ③ 개인정보 보호책임자는 물리적 접근제한 관리대장의 출입 및 열람 내용을 주기적으로 검토하여 정당하지 않은 권한으로 출입하거나 열람하는 경우가 있는지를 점검하여 확인하여야 한다.

제37조(출력 복사 시 보호조치)

- ① 개인정보보호분야별책임자는 개인정보가 포함된 정보를 출력하거나 복사할 경우에 개인정보 유출사고를 방지하기 위한 보호조치를 취하여야 한다.
- ② 개인정보보호분야별책임자는 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 보호조치를 추가로 적용할 수 있다.
- ③ 개인정보취급자는 개인정보의 이용을 위하여 출력 및 복사한 개인정보의 이용 목적이 완료된 경우 분쇄기로 분쇄하거나 소각하는 등의 안전한 방법으로 파기하여야 한다.

제38조(개인정보취급자 접근권한 관리 및 인증)

- ① 개인정보보호분야별책임자는 개인정보처리시스템에 대한 접근 권한을 서비스 제공에 필요한 최소한의 인원에게만 부여한다.
- ② 개인정보보호분야별책임자는 개인정보취급 업무를 담당하는 직원의 담당업무에 따라

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

- ③ 개인정보보호분야별책임자는 개인정보취급자가 전보 또는 퇴직 등 인사이동으로 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소한다.
- ④ 개인정보보호분야별책임자는 개인정보취급자가 정보통신망을 통하여 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 공인인증서 등 안전한 인증 수단을 적용하여야 한다.
- ⑤ 개인정보보호분야별책임자는 제1항 내지 제4항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관한다.

제39조(개인정보의 암호화)

- ① 개인정보보호분야별책임자는 주민등록번호 등 개인정보보호법에서 규정한 고유식별번호 및 민감정보에 대해서는 안전한 암호 알고리즘으로 암호화하여 저장하여야 한다.
- ② 개인정보취급자는 비밀번호를 사용하는 경우 복호화되지 아니하도록 일방향 암호화 하여 저장하여야 한다.
- ③ 개인정보보호분야별책임자는 정보통신망을 통해 정보주체의 개인정보 및 인증정보를 송수신 할 때에는 안전한 보안서버 구축 등의 조치를 통해 이를 암호화해야 한다.
- ④ 개인정보취급자는 정보주체의 개인정보를 개인용 컴퓨터(PC)에 저장할 때에는 이를 암호화해야 한다.

제40조(접근통제)

- ① 개인정보 보호책임자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 시스템을 설치 및 운영한다.
 - 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
- ② 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.
- ③ 개인정보 보호책임자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통해 열람권한이 없는 자에게 공개되지 않도록 개인정보처리시스템 및 개인정보

취급자의 컴퓨터에 조치를 취하여야 한다.

- ④ 개인정보보호관리자는 매월 셋째주 수요일을 사이버보안 진단의 날로 지정하여 부서별 정기점검을 실시하도록 한다.

제41조(접속 기록의 위변조 방지)

- ① 개인정보보호분야별책임자는 접속 기록의 위변조 방지를 위해 개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리(입/출력, 수정, 등 DB접근)하는 경우에는 **계정, 접속일시, 정보주체 정보, 접속자 정보, 수행업무 등을 저장한다.**
- ② 개인정보 보호책임자는 제1항의 접속기록에 대해 **년1회 이상 보관, 월 1회 이상 점검한다.**
- ③ 개인정보보호분야별책임자는 제1항의 접속기록에 대해 위.변조 방지를 위해 별도의 저장매체에 백업 보관하며, 보관기간은 **최소 1년 이상으로 한다. 다만, 5만명 이상의 정보주체에 관하여 개인정보를 처리하거나, 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관,관리하여야 한다.**

제42조(보안프로그램의 설치 및 운영)

- ① 개인정보 보호책임자는 개인용 컴퓨터(PC) 등을 이용하여 개인정보를 취급하는 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.

제43조(영상정보처리기기의 설치 및 운영관리)

- ① 영상정보처리기기 운영.관리 부서의 장(이하 개인영상정보 보호책임자)은 영상정보처리기기 설치 시 "개인정보보호법 제23조"에 따라 전문가 및 이해관계인의 의견수렴 절차를 거쳐야 한다.
- ② 제1항에 따라 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 영상정보처리기기를 설치.운영하여서는 아니 된다.
- ③ 제1항에 따라 영상정보처리기기를 설치.운영 하려는 경우 녹음기능을 사용하여서는 아니 되며, 기기의 임의조작하거나 다른 곳을 비춰서는 아니 된다.
- ④ 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
- ⑤ 개인정보 보호책임자는 영상정보처리기기 운영·관리 방침을 수립하여 홈페이지 등에 공개하여야 한다.
- ⑥ 개인영상정보 보호책임자는 본 계획의 준수 여부에 대한 자체점검을 실시하여 매년 3월 말까지 그 결과를 개인정보 보호책임자에게 통보한다.
- ⑦ 개인영상정보 보호책임자는 개인영상정보기기의 운영을 위하여 내부관리계획 9에서 20까지의 기술적·관리적 보호조치를 준수하여야 한다.

제44조(악성프로그램 등 방지)

개인정보처리자는 악성 프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다.

1. 보안 프로그램의 자동 업데이트 기능을 사용하거나, 또는 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지
2. 악성 프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영 체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 실시

제45조(물리적 접근제한)

- ① 우리학교에서 보유하고 있는 개인정보관리의 안전성 확보를 위해 필요한 기술적 조치를 아래와 같이 계획하여 수행한다.(개정 2019.02.)

| 구분 | 보호조치 | 추진일정 | 시행부서 |
|------------|--|-------|-------|
| 접근통제 강화 | 네트워크 구성 일제 점검 및 취약점 파악 | 년간 1회 | 전산정보원 |
| | 보안시스템 일제 점검 및 취약점 파악 | 년간 1회 | |
| 서버 보안강화 | 시스템 취약점 점검 | 년간 1회 | |
| 컴퓨터 보안강화 | 백신서버 정책 점검 및 문제 컴퓨터 파악 개인정보 탐색 및 관리 | 년간 1회 | |
| 웹사이트 보안 강화 | 개인정보 노출 방지 취약점 점검 | 년간 1회 | |

② 개인정보의 안전한 관리를 위해 항목별 현황파악과 저장 시 필요한 법적 기준을 적용한다. (개정 2019.02. .)

| 암호화 대상항목 | DB명 | 개인정보처리시스템 | 처리부서 | 관리부서 |
|----------|-----------|-----------|--------------|-------|
| 주민등록번호 | 학사DB/행정DB | 종합정보시스템 | 교무처/입시홍보/사무처 | 전산정보원 |
| 비밀번호 | 학사DB/행정DB | 종합정보시스템 | 교무처/사무처 | |
| 외국인등록번호 | 학사DB/행정DB | 종합정보시스템 | 교무처/입시홍보/사무처 | |
| 여권번호 | 학사DB/행정DB | 종합정보시스템 | 교무처/입시홍보/사무처 | |
| 카드번호 | 학사DB/행정DB | 종합정보시스템 | 교무처/사무처 | |
| 통장번호 | 학사DB/행정DB | 종합정보시스템 | 교무처/사무처 | |

제46조(기술적·관리적 보호조치 수행계획) (개정 2017.03.23.)

| 구분 | 항목 | 2017년 | |
|---------------------------|----------------------|--------|--------------------------------------|
| | | 추진 월 | 내용 |
| 개인정보 관리체계 기반수립 | 개인정보보호 내부지침 및 가이드 제정 | 1월~3월 | 개인정보지침 수립/제작 |
| | 개인정보 보호조직 구성 | 5월 | 조직 구성 |
| | 개인정보취급자 인식제고 | 4월,10월 | 개인정보 취급자 교육 |
| | 개인정보 취급방침 개선 | 4월 | 취급방침 작성 적용 |
| | 개인정보 내부 감사 수행 | 12월 | 내부감사 실시 |
| 개인정보 기술적 보호조치 방안 | 개인정보영향평가 (보완조치) | 5월~7월 | 개인정보 위험 요인 컨설팅 |
| | 네트워크 구성 점검 및 취약점 파악 | 8월 | 네트워크 시스템 전체 점검 |
| | 보안시스템 일제 점검 및 취약점 파악 | 8월 | 방화벽시스템 정책점검 및 취약점 파악 |
| | 서버 시스템 취약점 점검 | 8월 | 전체시스템 취약점 파악 |
| | 백신 및 자동패치 프로그램 점검 | 11월 | 백신서버 및 자동패치서버 점검 사용자 컴퓨터 Agent 확인 |

| | | | |
|---------------------------|---------------------|--------|---------------------|
| | 웹사이트 개인정보 노출방지 점검 | 학기별 | 전체 웹사이트 점검 |
| 개인정보 관리적 보호조치 방안 | 개인정보처리시스템접근권한 검토 | 3월~12월 | 개인정보취급자 권한에 따른 통제적용 |
| | 개인정보 파기 정책 및 절차 검토 | 3월~5월 | 관련 법률과 비교 |
| | | 6월~12월 | 관련법 반영하여 정책 개선 |
| | 개인정보 포함서류 보관 안전성 검토 | 10월 | 개인정보 지침 수립 |
| | | 12월 | 물리적 보안 장치 적용 |

VII 제7장 개인정보보호 교육

제47조(개인정보보호 교육 계획의 수립)

- ① 개인정보처리자는 다음 각 호의 사항을 포함하는 연간 개인정보보호 교육계획을 수립한다.
 1. 교육목적 및 대상
 2. 교육내용
 3. 교육 일정 및 방법
 4. 그 밖에 개인정보 보호 교육을 위하여 필요한 사항
- ② 각급기관의 장은 개인정보취급자 등을 대상으로 개인정보보호에 필요한 교육을 실시하여야 한다.
- ③ 개인정보 보호책임자는 신규 채용자, 전입자에게 개인정보 보호 교육을 하여야 한다.
- ④ 개인정보 보호책임자는 개인정보 관련 전문기관 교육 및 기술 세미나 참석을 장려하는 등 개인정보 담당자의 업무 전문성을 제고하기 위하여 노력하여야 한다.
- ⑤ 개인정보 보호책임자는 수립한 개인정보보호 교육 계획을 실시한 이후에 교육의 성과와 개선 필요성을 검토하여 차년도 교육계획 수립에 반영하여야 한다.

제48조(개인정보보호 교육의 실시)(개정 2017.03.23.)

- ① 개인정보 보호책임자는 정보주체정보보호에 대한 직원들의 인식제고를 위해 노력해야 하며, 개인정보의 오·남용 또는 유출 등을 적극 예방하기 위해 매년 정기적으로 년1회 이상의 개인정보보호 교육을 실시한다.

- ② 년1회의 정기 교육은 상반기에 1회, 하반기에 1회 실시하는 것을 원칙으로 하며, 최소 년 1회를 실시하는 것으로 한다.
- ③ 교육 방법은 집체 교육뿐만 아니라, 인터넷 교육, 그룹웨어 교육 등 다양한 방법을 활용하여 실시하고, 필요한 경우 상급기관, 외부 전문기관이나 전문요원에 위탁하여 교육을 실시할 수 있다.
- ④ 개인정보보호에 대한 중요한 전파 사례가 있거나 개인정보보호 업무와 관련하여 변경된 사항이 있는 경우, 개인정보 보호책임자는 부서 회의 등을 통해 수시 교육을 실시할 수 있다.

제49조(개인정보보호 교육 계획서)(개정 2017.03.23.)

- ① 본교 개인정보관련 업무를 수행하는 모든 교직원 및 위(수)탁업체 직원을 대상으로 다음과 같이 개인정보보호교육을 실시한다.

1. 1차 교육

| | |
|-------|--|
| 교육과정명 | 개인정보보호 법의 이해와 본교 정보보호 정책 소개 |
| 교육 대상 | 개인정보보호책임자, 담당자, 취급자, 위(수)탁사 직원 |
| 교육자 | 개인정보보호 전문 강사 |
| 교육 일시 | 6월(2시간) |
| 교육 방법 | 교육자료 배포를 통한 강의 |
| 교육 내용 | 개인정보 보호법의 주요 내용 개인정보보호 정책 소개 본교 정보보호 관련 규정 및 정책 소개 개인정보보호 내부관리 계획서 소개 |

2. 2차 교육

| | |
|-------|---|
| 교육과정명 | 본교 개인정보보호 내부관리계획서 소개 |
| 교육 대상 | 개인정보보호책임자, 담당자, 취급자, 위(수)탁사 직원 |
| 교육자 | 개인정보보호 전문 강사 |
| 교육 일시 | 11월(2시간) |
| 교육 방법 | 교육자료 배포를 통한 강의 |
| 교육 내용 | 개인정보 보안점검 방법 및 절차 개인정보 내부감사 실시 방법 및 절차 |

VIII 제8장 개인정보 보안점검 및 내부감사 실시

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

제50조(자체감사 주기 및 절차)

- ① 개인정보보호책임자는 개인정보보호를 위한 내부관리 계획 및 관련 법령에서 정하는 개인정보보호 규정을 성실히 이행하는지를 주기적으로 감사 또는 점검하여야 한다.
- ② 개인정보보호책임자는 개인정보 자체감사를 위한 감사대상, 감사절차 및 방법 등 감사의 실시에 관하여 필요한 별도의 계획을 수립할 수 있다.
- ③ 개인정보보호 자체감사는 최소 년1회 이상 실시한다.
- ④ 사이버보안 진단의 날
'사이버보안 진단의 날'을 지정하여 개인정보취급자(전교직원)의 컴퓨터 안전성 정기점검, 비밀현황 확인 등 자체보안점검을 실시한다.
 1. 시행시기 : 매월 셋째 주 수요일
 2. 주관부서 : **전산정보원**
 3. 세부사항 : 매년 초 '사이버보안 진단의 날' 세부 추진 계획서를 작성하여 시행한다.

제51조(내부 감사)

개인정보보호 정책에 대한 이행여부 점검으로 미흡한 사항을 조기 발견하여, 보안사고

를 예방하며 효과적인 대책마련으로 대외적인 신뢰성 확보를 통해 본교 이미지 제고를 목적으로 한다.

① 개요

| | |
|-------|--|
| 목적 | 개인정보 처리 실태의 미비점 발견 및 보완 |
| 주기 | 년 1회 |
| 주요 내용 | 개인정보 관련 법 준수 여부 점검 개인정보보호 지침 이행 여부 점검 * 상세 항목은 별첨 참고 |

② 내부감사 기간 및 대상 부서

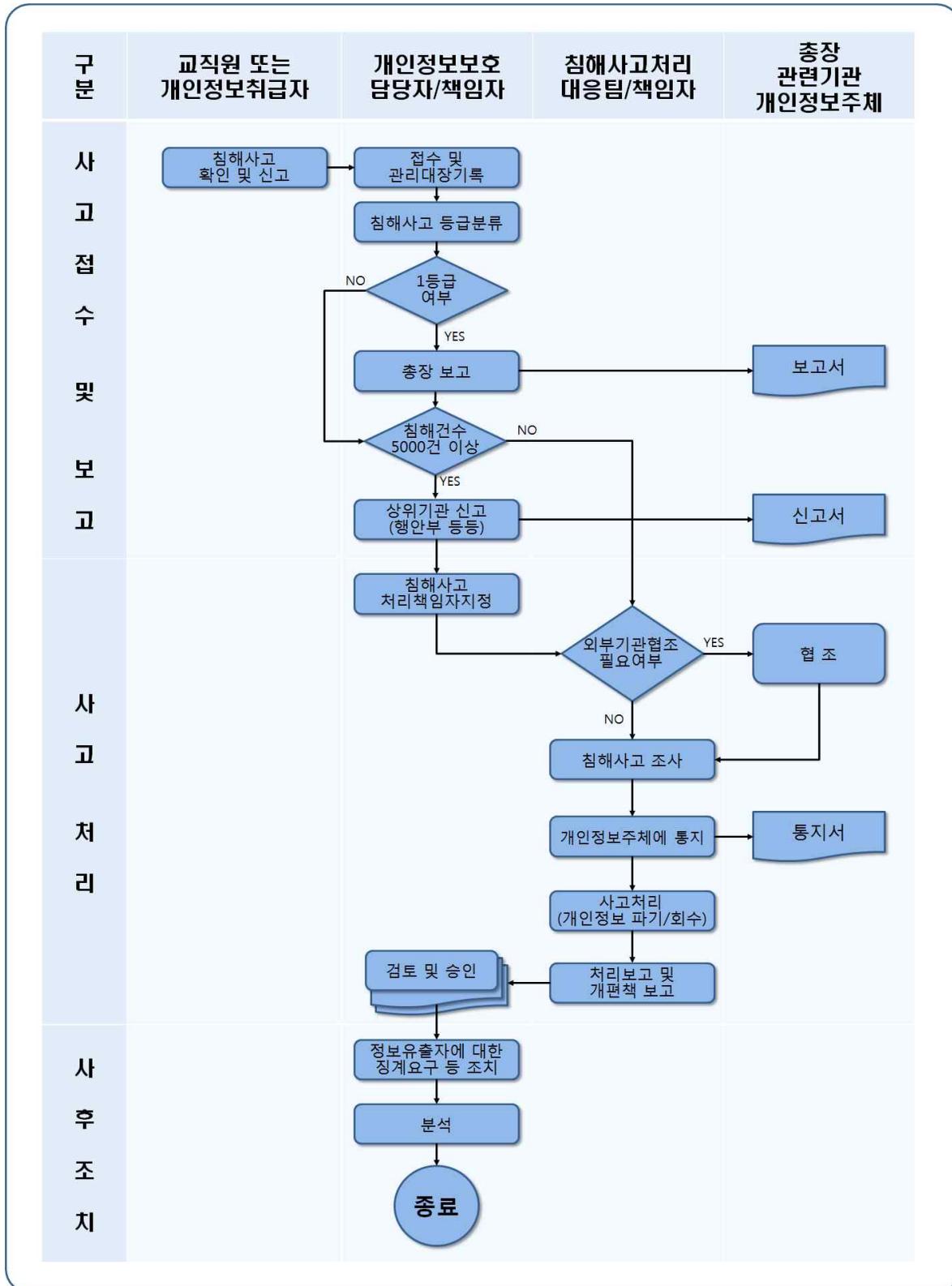
| | |
|-------|--|
| 기간 | 매년 12월 |
| 주관부서 | 전산정보원 |
| 대상 부서 | 교내 전부서 |
| 심사자 | <ul style="list-style-type: none"> - 개인정보보호책임자(사무처장) - 정보보안책임관(전산정보원장) - 개인정보보호관리자(사무팀장) - 개인정보보호담당자(전산정보원 운영팀장) - 개인정보보호시스템관리자(전산정보원 팀원) |

제52조(자체감사 결과 반영)

- ① 개인정보보호관리자는 자체감사 실시 결과 현황을 취합 정리하여 개인정보보호책임자에게 보고하여야 하며, 관련자료는 문서화하여 보관한다.
- ② 개인정보보호책임자는 개인정보 보호를 위한 자체감사 실시 결과, 개인정보의 관리 운영상의 문제점을 발견하거나 관련 직원이 본 계획의 내용을 위반할 때에는 총장에게 보고 후 시정.개선 또는 인사발령 등 필요한 조치를 취하여야 한다.
- ③ 개인정보보호책임자는 개인정보 위반사실에 대한 시정.개선 조치가 이행되지 않거나, 개인정보보호에 심각한 영향이 발생할 수 있는 우려가 되는 경우 총장에게 보고 후 개인정보 취급자 등에 대한 인사발령 등의 필요한 추가 조치를 취할 수 있다.

IX 제9장 개인정보 유·노출 및 침해대응 대책

제53조(개인정보 유·노출 및 침해사고 대응 절차도) (개정 2016.05.03.)



제54조(개인정보의 유출)

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

1. 개인정보가 포함된 서면, 이동식 저장장치, 휴대용 컴퓨터 등을 분실하거나 도난당한 경우
2. 개인정보가 저장된 데이터베이스 등 개인정보처리시스템에 정상적인 권한이 없는 자가 접근한 경우
3. 개인정보처리자의 고의 또는 과실로 인해 개인정보가 포함된 파일 또는 종이문서, 그 밖에 저장매체가 권한이 없는 자에게 잘못 전달된 경우
4. 그 밖에 권한이 없는 자에게 개인정보가 전달되거나 개인정보처리시스템 등에 접근 가능하게 된 경우

제55조(통지시기 및 항목)

- ① 개인정보처리자는 실제로 유출 사고가 발생한 것으로 확인된 때에는 정당한 사유가 없는 한 5일 이내에 해당 정보주체에게 다음 각 호의 사항을 알려야 한다.
 1. 유출된 개인정보의 항목
 2. 유출된 시점과 그 경위
 3. 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
 4. 개인정보처리자의 대응조치 및 피해구제절차
 5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처
- ② 개인정보처리자는 제1항 제2호의 경우 개인정보 유출 사고가 최초 발생한 시점과 알게 된 시점 사이에 시간적 차이가 있는 경우에는 이에 대한 과실유무를 입증하여야 한다.
- ③ 개인정보처리자는 제1항 각 호의 조치를 취한 이후에는 정보주체에게 다음 각 호의 사실만을 일차적으로 알리고, 추후 확인되는 즉시 알릴 수 있다.
 1. 정보주체에게 유출이 발생한 사실
 2. 제1항의 통지항목 중 확인된 사항

제56조(통지방법)

- ① 개인정보처리자는 정보주체에게 제55조제1항 각 호의 사항을 통지할 때에는 서면, 전자우편, 모사전송, 전화, 휴대전화 문자전송 또는 이와 유사한 방법을 통하여 5일

이내에 정보주체에게 알려야 한다.

- ② 개인정보처리자는 제1항의 통지방법과 동시에, 홈페이지 등을 통하여 55의 제1항 각 호의 사항을 공개할 수 있다.

제57조(개인정보 유출신고)

- ① 개인정보처리자는 1명이라도 정보주체에 관한 개인정보가 유출된 경우에는 유출내용 및 조치결과를 5일 이내에 상급기관을 경유하여 교육부에 보고하여야 한다. 다만 1천명 이상의 개인정보가 유출된 경우에는 행정자치부장관 또는 시행령 제39조제2항 각 호의 전문기관 중 어느 하나에 신고하여야 한다.
- ② 제1항에 따른 보고와 신고는 별지 제5호 서식에 따른 개인정보 유출신고(보고)서를 통하여 하여야 한다.
- ③ 개인정보처리자는 전자우편, 모사전송 또는 인터넷 사이트를 통하여 유출 보고 또는 신고를 할 시간적 여유가 없거나 그 밖에 특별한 사정이 있는 때에는 먼저 전화를 통하여 55의 1항 각 호의 사항을 신고한 후, 별지 제5호 서식에 따른 개인정보 유출신고서를 제출할 수 있다.
- ④ 개인정보처리자는 1천명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 제56조에 따른 통지와 함께 인터넷 홈페이지에 정보주체가 알아보기 쉽도록 55의 제1항 각 호의 사항을 7일 이상 게재하여야 한다.

제58조(피해구제 대책)

- ① 피해예방 : 사전에 정보주체에게 피해가 발생하지 않도록 개인정보처리자는 개인정보보호법을 준수하고(본 내부관리계획의 I ~IX에 대한 내용을 숙지하고 조치) 주의와 감독에 만전을 기하여야 함.

[참고] 개인정보보호법 제39조에 의거하여 정보주체는 개인정보처리자가 법을 위반한 행위로 손해를 입으면 손해를 배상할 수 있다. 이 경우 개인정보처리자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다.

또한, 개인정보처리자가 이 법을 준수하고 상당한 주의와 감독을 게을리하지 아니한 경우 개인정보의 분실·도난·유출·변조 또는 훼손으로 인한 손해배상 책임을 감경 받을 수 있다.

- ② 분쟁조정위원회 조정신청 : 정보주체가 피해 구제를 위하여 분쟁조정위원회로 분쟁 조정을 신청할 경우 조정위원회의 권고를 참고하여 원만한 해결을 위한 합의를 마련해야 함.

[참고] 개인정보보호법 제43조에 의거하여 정보주체는 비용, 절차 등의 사유로 소송을 통한 피해 구제가 어려울 경우 분쟁조정위원회로 분쟁조정을 신청할 수 있다. 이 분쟁조정위원회의 조정은 법원의 판결에 의하지 않고 조정위원회의 권고에 의하여 양당사자가 서로 양보하여 합의로서 해결하는 절차로 당사자가 수락하여 조정이 성립되면 법원의 확정판결과 동일한 효력이 발생하게 된다.

X 제10장 개인정보보호 사무의 인수·인계

제59조(개인정보보호 사무의 인수·인계) (개정 2016.05.03.)

- 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 유출 사례를 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

[별첨] 내부감사 항목

| 분야 | | 법 조항 | 점검 항목 |
|---------------------|----------|--------------|--|
| 1. 개인정보의 수집·제공 | | 제15조 | 1. 개인정보 수집에 따른 정보주체의 동의 여부 및 동의를 받을 때 필수 사항(4개*) 고지 및 내용의 적정성 여부 * 필수항목 : ①수집의 목적, ②개인정보의 항목, ③개인정보 보유 및 이용 기간, ④동의 거부권 및 거부 시 불이익 |
| | | 제16조 | 1-2. 필수 정보 항목 이외 선택 항목 동의 거부시 재화 또는 서비스 거부 여부 |
| | | 제22조 | 1-1. 홍보 또는 마케팅 목적으로 동의를 받을 때 기본 동의와 구분하여 동의를 받는 지 여부 |
| | | 제22조 | 1-3. 만 14세 미만 아동의 개인정보 처리시 법정대리인(부모 등)의 동의 여부 |
| | | 제17조 | 2. 제3자에게 개인정보 제공시 법률 근거 여부, 정보주체의 동의 여부 및 동의를 받을 때 필수 사항(5개*) 고지 및 내용의 적정성 여부 * 필수항목 : ①제공 받는 자, ②이용목적, ③개인정보의 항목, ④개인정보 보유 및 이용기간, ⑤동의 거부권 및 거부 시 불이익 |
| | | 제17조 | 2-1. 국외 3자 제공시 정보주체의 별도 동의 여부 및 개인정보보호법을 위반하여 국외 이전 계약 체결 여부 |
| | | 제23조 제24조 | 3. 민감정보, 고유식별정보 수집에 따른 법령 근거 유무 또는 별도의 동의를 받고 있는지 여부 * 고유식별정보 : 여권번호, 운전면허번호, 외국인등록번호 * 민감정보 : 개인의 과거 및 현재의 병력(病歷), 신체적·정신적 장애, 유전정보, 사상, 정치 등 |
| 2. 주민등록번호 처리 제한 | | 제24조의 2 | 4. 법에 근거하지 않고 주민등록번호를 수집 및 처리하고 있는지 여부 |
| | | 제24조의 2 | 5. 법령에 근거하여 회원가입 시 주민등록번호를 대신할 방법(i-PIN, 핸드폰 등) 제공 여부 |
| 3. 개인정보의 파기 | | 제21조 | 6. 보유기간 경과, 처리 목적(제공받은 경우 제공받은 목적) 달성 후 지체 없이 영구 삭제하고 있는지 여부 |
| | | 제21조 | 7. 법령에 따라 보존할 경우 다른 개인정보와 분리하여 보관하는지 여부 - 파기전 삭제 개인정보의 분리 보관 |
| 4. 업무위탁 계약 | | 제26조 | 8. 업무 위탁 계약문서에 필수 반영사항(7개*)이 포함되었는지 여부 * 필수사항 : ①위탁업무 수행 목적외 처리금지, ②기술·관리적 보호조치, ③목적·범위, ④재위탁 제한, ⑤접근 제한 등 안전조치, ⑥관리·감독사항, ⑦손해배상 등 책임에 대한 사항 |
| 5. 개인정보 취급자 감독 | | 제28조 | 9. 개인정보취급자(업무 담당자)에 대한 적절한 관리·감독(접근통제, 보안각서 징구, 교육 등)을 실시하고 있는지 여부 |
| 6. 개인정보 처리방침의 수립·공개 | | 제30조 | 10. 개인정보처리방침의 공개 및 필수 사항(10개*) 포함 여부 * 필수항목 : ①개인정보의 처리 목적, ②처리 및 보유 기간, ③제3자 제공에 관한 사항(해당 시), ④업무위탁에 관한 사항(해당 시), ⑤정보주체 권리·의무 및 행사 방법, ⑥개인정보의 항목, ⑦개인정보 파기, ⑧안전성 확보 조치, ⑨처리방침 변경에 관한 사항, ⑩개인정보보호책임자에 관한 사항 |
| 7. 안정성 확보 조치 | 내부 관리 계획 | 제29조 | 11. 내부관리계획 수립·시행 여부 * 3쪽 내부관리 계획 목차 예시 참조 |
| | 접근 | 제29조 | 12. 시스템에 대한 접근권한 부여시 필요 최소한의 범위로 업무 담당자에 따라(1인 |

| 분야 | 법조항 | 점검 항목 |
|---------------|------|--|
| 권한 관리 및 접근 통제 | | 1계정) 차등 부여하는지 여부 - 개인정보 처리자 및 관리자에게만 접근 권한 부여 - 계정 공유 위반 존재 여부 |
| | 제29조 | 13. 접근권한의 부여·변경·말소 내역을 기록 및 관리하고, 최소 3년간 보관 하는지 여부 - 퇴직자, 인사 이동 사항 등 반영 여부 |
| | 제29조 | 14. 안전한 비밀번호 작성규칙을 수립 및 적용 하는지 여부 * 비밀번호 작성 규칙 - 최소 10자리 이상 : 하나의 문자종류로 구성된 경우 - 최소 8자리 이상 : 2 종류 이상의 문자를 이용하여 구성된 경우 - 제3자에게 노출되었을 경우 지체없이 새로운 비밀번호로 변경해야 함 |
| | 제29조 | 15. 불법적 접근 및 침해사고 방지를 위한 (방화벽 : FW)(침입방지 : IPS) 시스템을 설치 및 운영하고 있는지 여부 - 시스템 및 DB 접근제어 시스템 도입 시 양호 - FW, IPS 정책의 현행화 필요 |
| | 제29조 | 16. 개인정보취급자가 외부에서 정보통신망을 통한 접속 시 가상사설망(VPN), 전용선 등 안전한 접속수단을 제공하고 있는지 여부 - 최소 취급자 IP 또는 Mac 주소만 접속 가능하도록 통제 |
| | 제29조 | 17. P2P, 웹하드 등 비인가 프로그램 및 공유 설정 등을 통해 열람권한이 없는 자에게 공개·유출되지 않도록 접속 차단을 실시하고 있는지 여부 |
| | 제29조 | 18. 본인 확인을 위해 성명, 주민등록번호를 사용할 수 있는 경우에도 공인인증서, 휴대전화 등을 통해 추가적인 정보를 확인하는지 여부 |
| 개인 정보 암호화 | 제29조 | 19. 비밀번호, 바이오 정보 등을 외부에 송·수신 하거나, 내부에 저장하는 경우 SSL 등 암호화 조치 적용 여부 |
| | 제29조 | 20. 비밀번호, 바이오 정보의 내부 저장 시 일방향 암호화(해시함수) 알고리즘을 적용하고 있는지 여부 |
| | 제29조 | 21. 고유식별정보를 인터넷과 내부망의 중간지점(DMZ)에 저장하는 경우 암호화 조치를 적용하는지 여부 |
| 접속 기록 보관 | 제29조 | 22. 취급자의 접속기록을 최소 1년 이상 보관 및 관리하고, 도난 및 분실되지 않도록 안전하게 보관 및 관리하는지 여부 |
| | 제29조 | 23. 취급자의 접속이력 기록시 필수 사항(4개*)을 기록하고 있는지 여부 * 필수항목 : ①ID, ②날짜 및 시간, ③접속자 IP주소, ④수행 업무(열람, 수정, 삭제, 인쇄, 입력 등) |
| 보안 프로그램 | 제29조 | 24. 보안 프로그램(백신)을 자동 업데이트 또는 1일 1회 이상 업데이트 하여 최신의 상태로 유지하고 있는지 여부 - PC나 서버에 보안 프로그램 설치 여부 |
| PC | 제29조 | 25. 비밀번호 설정 안된 공유폴더 존재여부, PC내에서 개인정보 파일 저장시 비밀번호 설정 |

개인정보파일 보유기간 책정 기준표

| 보유기간 | 대상 개인정보파일 |
|------|---|
| 영구 | <ol style="list-style-type: none"> 1. 국민의 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 | <ol style="list-style-type: none"> 1. 국민의 신분, 재산을 증명하기 위해 운용하는 개인정보파일 중 개인이 사망, 폐지 그 밖의 사유로 소멸되기 때문에 영구 보존할 필요가 없는 개인정보파일 2. 국민의 신분증명 및 의무부과, 특정대상 관리 등을 위하여 행정기관이 구축하여 운영하는 행정정보시스템의 데이터 셋으로 구성된 개인정보파일 |
| 30년 | <ol style="list-style-type: none"> 1. 관계 법령에 따라 10년 이상 30년 미만의 기간 동안 민. 형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일 |
| 10년 | <ol style="list-style-type: none"> 1. 관계 법령에 따라 5년 이상 10년 미만의 기간 동안 민. 형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일 |
| 5년 | <ol style="list-style-type: none"> 1. 관계 법령에 따라 3년 이상 5년 미만의 기간 동안 민. 형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일 |
| 3년 | <ol style="list-style-type: none"> 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 | <ol style="list-style-type: none"> 1. 상급기관(부서)의 요구에 따라 단순 보고를 위해 생성한 개인정보파일 |

개인정보 열람 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 | <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 | |

「개인정보 보호법」 제35조제2항과 같은 법 시행령 제41조제3항에 따라 위와 같이 요구합니다.

년 월 일

요구인

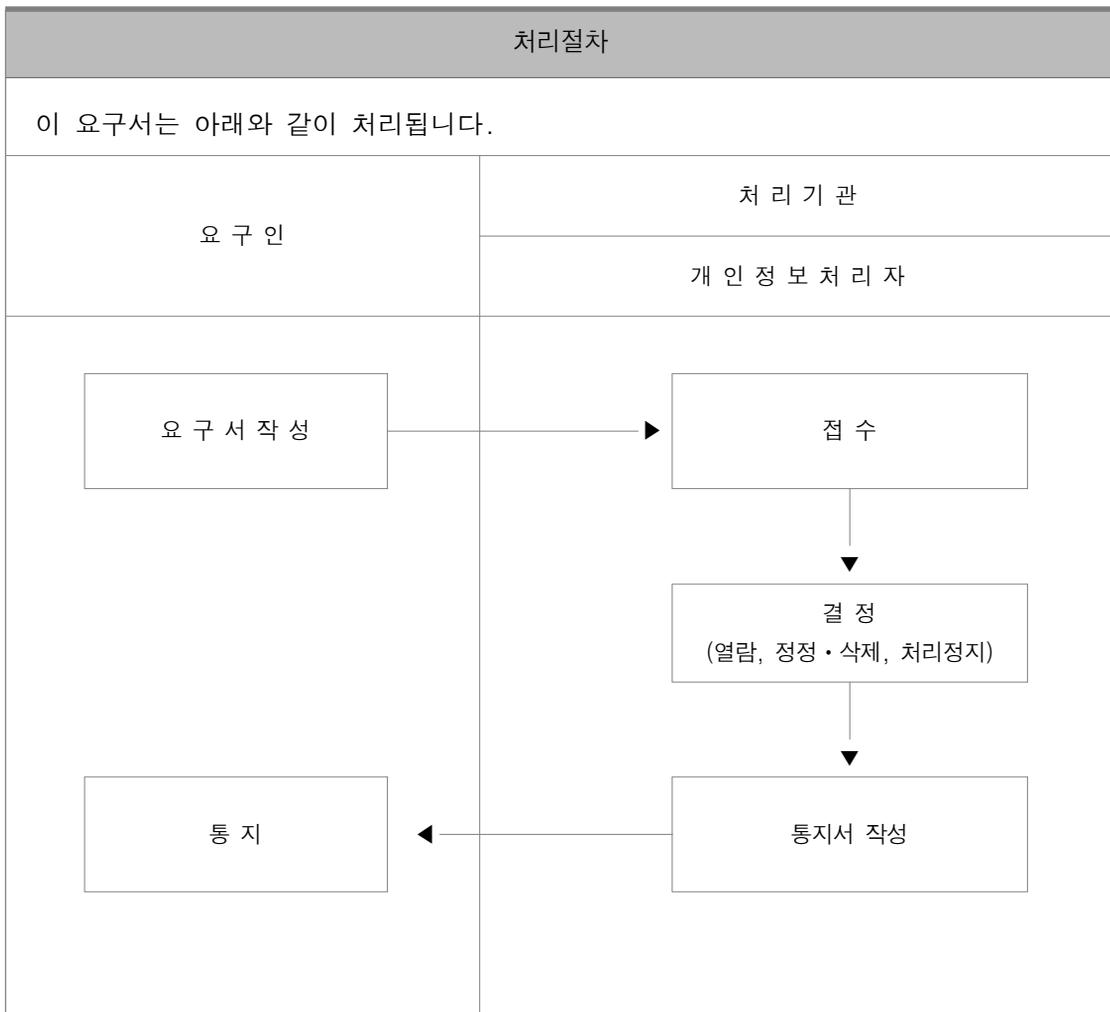
(서명 또는 인)

행정안전부장관 귀하

작성 방법

1. '대리인' 란은 대리인이 요구인일 때에만 적습니다.
2. '요구내용' 란은 열람하려는 사항을 선택하여 [√] 표시를 합니다. 표시를 하지 않은 경우에는 해당 항목의 열람을 요구하지 않은 것으로 처리됩니다.

210mm×297mm[백상지(80g/㎡) 또는 중질지(80g/㎡)]



위 임 장

| | | |
|--------|------|-----------|
| 위임받는 자 | 성명 | 전 화 번 호 |
| | 생년월일 | 정보주체와의 관계 |
| | 주소 | |
| 위임자 | 성명 | 전화번호 |
| | 생년월일 | |
| | 주소 | |

「개인정보 보호법」 제38조제1항에 따라 위와 같이 개인정보의 (열람, 정정·삭제, 처리정지)의 요구를 위의 자에게 위임합니다.

년 월 일

위임자

(서명 또는 인)

0 0 0 0 귀하

개인정보 (열람 일부열람 열람연기 열람거절) 통지서

(앞 쪽)

수신자 (우편번호: , 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) |
| | 수수료 산정 명세 | | 원 원 원 |
| 사유 | | | |
| 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

발신명의 직인

유의사항

1. 개인정보 열람 장소에 오실 때에는 이 통지서를 지참하셔야 하며, 요구인 본인 또는 그 정당한 대리인임을 확인하기 위하여 다음의 구분에 따른 증명서를 지참하셔야 합니다.
 - 가. 요구인 본인에게 공개할 때: 요구인의 신원을 확인할 수 있는 신분증명서(주민등록증 등)
 - 나. 요구인의 대리인에게 공개할 때: 대리인임을 증명할 수 있는 서류와 대리인의 신원을 확인할 수 있는 신분증명서
2. 수수료 또는 우송료는 다음의 구분에 따른 방법으로 냅니다.
 - 가. 국가기관인 개인정보처리자에게 내는 경우: 수입인지
 - 나. 지방자치단체인 개인정보처리자에게 내는 경우: 수입증지
 - 다. 국가기관 및 지방자치단체 외의 개인정보처리자에게 내는 경우: 해당 개인정보처리자가 정하는 방법

※ 국회, 법원, 헌법재판소, 중앙선거관리위원회, 중앙행정기관 및 그 소속 기관 또는 지방자치단체인 개인정보처리자에게 수수료 또는 우송료를 내는 경우에는 「전자금융거래법」 제2조제11호에 따른 전자지급수단 또는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제10호에 따른 통신과금서비스를 이용하여 수수료 또는 우송료를 낼 수 있습니다.
3. 열람제한, 열람연기 또는 열람거절의 통지를 받은 경우에는 개인정보처리자가 이의제기방법란에 적은 방법으로 이의제기를 할 수 있습니다.

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 | ※ 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

발신명의 직인

유의사항

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

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(보고) 접수기관 | 기관명 | 담당자명 | 연락처 |
| | | | |

개인정보파일 ([] 등록 [] 변경등록) 신청서

※ ‘변경정보 및 변경사유’ 란은 변경등록시에만 작성합니다.

| | | |
|------|-----|---------|
| 접수번호 | 접수일 | 처리기간 7일 |
|------|-----|---------|

| | | | |
|---------|----|------|------|
| 공공기관 명칭 | 주소 | 등록부서 | 전화번호 |
|---------|----|------|------|

| 등록항목 | 등록정보 | 변경정보 및 변경사유 |
|---|------|-------------|
| 개인정보파일 명칭 | | |
| 개인정보파일의 운영 근거 및 목적 | | |
| 개인정보파일에 기록되는 개인정보의 항목 | | |
| 개인정보의 처리방법 | | |
| 개인정보의 보유기간 | | |
| 개인정보를 통상적 또는 반복적으로 제공하는 경우 그 제공받는 자 | | |
| 개인정보파일을 운용하는 공공기관의 명칭 | | |
| 개인정보파일로 보유하고 있는 개인정보의 정보주체 수 | | |
| 해당 공공기관에서 개인정보 처리 관련 업무를 담당하는 부서 | | |
| 개인정보의 열람 요구를 접수·처리하는 부서 | | |
| 개인정보파일에서 열람을 제한하거나 거절할 수 있는 개인정보의 범위 및 그 사유 | | |

「개인정보 보호법」 제32조제1항과 같은 법 시행령 제34조제1항에 따라 위와 같이 개인정보파일 ([] 등록 [] 변경등록)을 신청합니다.

년 월 일

신청기관

(서명 또는 인)

행정안전부장관 귀하

개인정보파일대장

| | | | |
|-------|----|------|------|
| 기관 명칭 | 주소 | 등록부서 | 전화번호 |
|-------|----|------|------|

| 등록항목 | 등록정보 |
|---|------|
| ① 개인정보파일 명칭 | |
| ② 개인정보파일의 운영 근거 및 목적 | |
| ③ 개인정보파일에 기록되는 개인정보의 항목 | |
| ④ 개인정보의 처리방법 | |
| ⑤ 개인정보의 보유기간 | |
| ⑥ 개인정보를 통상적 또는 반복적으로 제공하는 경우 그 제공받는 자 | |
| ⑦ 개인정보파일을 운용하는 기관의 명칭 | |
| ⑧ 개인정보파일로 보유하고 있는 개인정보의 정보주체 수 | |
| ⑨ 해당기관에서 개인정보 처리 관련업무를 담당하는 부서 | |
| ⑩ 개인정보의 열람 요구를 접수·처리하는 부서 | |
| ⑪ 개인정보파일에서 열람을 제한하거나 거절할 수 있는 개인정보의 범위 및 그 사유 | |

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 | | | |

[별지 제9호서식]

개인정보파일 파기 요청서

| | | | |
|-----------------|--|---------------------|--|
| 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 파기 여부 | | | |

개인영상정보 관리대장

| 번호 | 구분 | 일시 | 파일명/ 형태 | 담당자 | 목적/ 사유 | 이용· 제공받는 제3자 /열람등 요구자 | 이용· 제공 근거 | 이용· 제공 형태 | 기간 |
|----|--|----|------------|-----|-----------|-----------------------------------|-----------------|-----------------|----|
| 1 | <input type="checkbox"/> 이용 <input type="checkbox"/> 제공 <input type="checkbox"/> 열람 <input type="checkbox"/> 파기 | | | | | | | | |
| 2 | <input type="checkbox"/> 이용 <input type="checkbox"/> 제공 <input type="checkbox"/> 열람 <input type="checkbox"/> 파기 | | | | | | | | |
| 3 | <input type="checkbox"/> 이용 <input type="checkbox"/> 제공 <input type="checkbox"/> 열람 <input type="checkbox"/> 파기 | | | | | | | | |
| 4 | <input type="checkbox"/> 이용 <input type="checkbox"/> 제공 <input type="checkbox"/> 열람 <input type="checkbox"/> 파기 | | | | | | | | |
| 5 | <input type="checkbox"/> 이용 <input type="checkbox"/> 제공 <input type="checkbox"/> 열람 <input type="checkbox"/> 파기 | | | | | | | | |
| 6 | <input type="checkbox"/> 이용 <input type="checkbox"/> 제공 <input type="checkbox"/> 열람 <input type="checkbox"/> 파기 | | | | | | | | |
| 7 | <input type="checkbox"/> 이용 <input type="checkbox"/> 제공 <input type="checkbox"/> 열람 <input type="checkbox"/> 파기 | | | | | | | | |