

강남대학교 개인정보 내부관리계획

2020년 7월

총무처 총무구매팀

□ 목적

- 본 개인정보보호 내부관리계획(안)은 「개인정보보호법」 및 동법 시행령, 시행규칙 제정·시행에 따른 명시적 의무사항의 이행을 위한 내부관리 계획의 수립을 위한 목적으로 「표준 개인정보보호 지침(행정안전부고시, 2011.9.30)」 및 「교육부 개인정보 보호지침(교육부훈령 135호, 2015.4.20)」에 따라 대학 내부의 추진체계 마련 및 업무담당자의 세부적 업무처리 기준 표준안을 마련하여 정보주체의 자유와 권리를 보호하고, 대학의 안정적인 개인정보보호 체계를 구축하는데 목적이 있다.

□ 구성

- 본 개인정보보호 내부관리계획(안)은 아래와 같이 구성되어 있다.

번호	내 용	페이지
1.	개인정보 내부관리계획(안)	1
2.	개인정보보호 교육 계획	21
3.	개인정보 침해사고 대응 방침 및 매뉴얼	22
4.	개인정보처리시스템 자율점검표	52
5.	개인정보처리시스템 자율점검 가이드라인	56
6.	개인정보파일 표준목록(예시)	102
	- 개인정보파일 표준목록	102
	- 개인정보 제3자 제공 표준목록	105
	- 개인정보 위탁 표준목록	108
7.	개인정보 처리단계별 준수사항 및 위반시 벌칙사항	109
8.	표준 개인정보처리 위탁 계약서(안)	113
9.	교직원 개인정보보호 서약서 양식	115
10.	개인정보 처리 위탁 계약 보안 서약서 양식	116

1. 강남대학교 개인정보 내부관리계획

I 개요

1 목적

「개인정보 보호법」 제29조와 동 법 시행령에 따라 개인정보처리자가 개인정보를 처리함에 있어서 개인정보가 분실·도난·유출·변조·훼손되지 아니하도록 안전성을 확보하기 위한 기술적·관리적·물리적 조치 계획을 수립하는 것을 목적으로 한다.

2 근거

- 「개인정보보호법」 제29조(안전조치의무)
- 「개인정보 보호법」 시행령 제30조(개인정보의 안전성 확보조치)의 제1호
- 개인정보의 안전성 확보조치 기준(행정자치부고시 제2016-35호, 2016.8.31)
- 교육부 개인정보 보호지침 (교육부훈령 제135호, 2015.4.20)

3 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 영상정보기기(CCTV등)에 대해서도 적용되며, 이러한 개인정보를 취급하는 내부 직원 및 외부위탁업체에 대해서도 적용된다.
- 필요 시 처리기준, 절차, 양식 등은 『교육부 개인정보보호 지침』에 의거하여 시행한다.

II 용어 정의

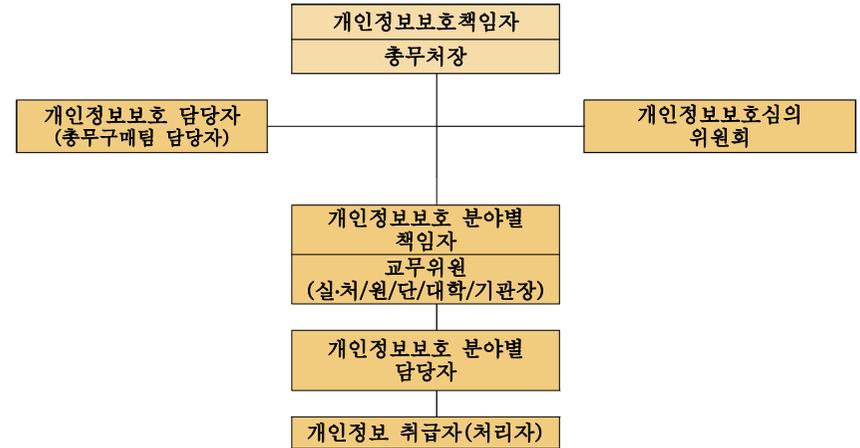
- “개인정보”란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.

- ▶ 고유식별정보 : 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호
- ▶ 민감정보 : 사상, 신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활, 유전정보, 범죄경력 정보 등에 관한 정보와 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보

- “정보주체”란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서, 개인정보 보호법에 의해 보호대상이 되는 정보의주체가 되는 사람을 말한다.
- “개인정보파일”이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.
- “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 개인 등을 말한다.
- “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 유사한 행위를 말한다.
- “개인정보 보호책임자”라 함은 개인정보의 처리에 관한 업무를 총괄해서 책임지는 자를 말한다.
- “개인정보보호 분야별 책임자”란 업무를 위하여 개인정보파일을 처리하는 부서의 장으로 개인정보 보호책임자가 지정한 자를 말한다.

- “개인정보 취급자”란 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 직접 개인정보에 관한 업무를 담당하는 자와 그 밖에 업무상 필요에 의해 개인정보에 접근하여 처리하는 모든 자를 말한다.
- “개인정보처리시스템”이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성된 데이터베이스시스템을 말한다.
- “접속기록”이라 함은 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무 내역에 대하여 식별자·접속일시·접속자를 알 수 있는 정보, 수행업무 등 접속한 사실을 전자적으로 기록한 것을 말한다.
- “바이오정보”란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 생성되거나 가공된 정보를 말한다.
- “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.
- “영상정보처리기기”란 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 CCTV 및 네트워크 카메라를 말한다.
- “개인영상정보”란 영상정보처리기기에 의하여 촬영·처리되는 영상 정보 중 개인의 초상, 행동 등 사생활과 관련된 영상으로서 해당 개인의 동일성 여부를 식별할 수 있는 정보를 말한다.
- “영상정보처리기기운영자”란 법 제25조제1항 각 호에 따라 영상정보처리기기를 설치·운영하는 자를 말한다.

III 개인정보보호 조직 편제



□ 개인정보보호 추진 체계별 역할

구분	담당자	역할
개인정보 보호책임자	교무위원에 상당하는 행정사무 총괄하는 자	-개인정보 보호 계획의 수립 및 시행 -개인정보 처리 실태 및 관행의 정기적인 조사 및 개선 -개인정보 처리와 관련한 불만의 처리 및 피해 구제 -개인정보 유출 및 오용 남용 방지를 위한 내부통제시스템의 구축 -개인정보 보호 교육 계획의 수립 및 시행 -개인정보파일의 보호 및 관리 감독 -개인정보 처리방침의 수립, 변경 및 시행 -개인정보 보호 관련 자료의 관리 -처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기 등
개인정보보호 담당자	개인정보보호 책임자가 지정한 자	-개인정보보호 계획 운영 -상위기관 업무협조 및 지적사항 관리 -개인정보 열람·정정청구 청구운영 -분야별 개인정보보호 운영실태 점검 및 담당자 교육
개인정보보호 분야별 책임자	개인정보 취급 부서의 실·처/원/단/대학/기관장	-개인정보보호 분야별담당자 관리·지원
개인정보보호 분야별 담당자	개인정보보호 분야별 담당관이 지정한 자	-개인정보보호 기술적·관리적 보호, 법정 서식 및 대장 작성·유지 -개인정보보호 실태에 대한 자체 점검표 취합·통보
개인정보취급자(처리자)	서비스 운영자 및 개인정보 접근 가능자	-개인정보보호 활동 참여 -내부관리계획의 준수 및 이행 -개인정보의 기술적·관리적 보호조치 기준 이행 -소속 직원 또는 제3자에 의한 위법·부당한 개인정보 침해행위에 대한 점검 등

IV 강남대학교 개인정보의 안전성 확보 조치

1 접근권한 관리

- 개인정보처리자는 개인정보처리시스템(학적, 도서관, 대학원, 평생교육, 취업, 장학, 교무, 인사 등)에 대한 접근권한을 업무 수행에 필요한 최소한의 범위로 차등 부여하여야 한다.
- 개인정보처리자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템(학적, 도서관, 대학원, 평생교육, 취업, 장학, 교무 등)의 접근권한을 변경 또는 말소하여야 한다. 그 기록은 최소 3년간 보관하여야 한다.
 - ※ '개인정보의 안전성 확보조치 기준'(행정자치부고시 제2016-35호) 제4조
- 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자 계정을 발급하는 경우, 개인정보취급자 별로 한 개의 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.
 - 개인정보취급자 또는 정보주체 중복 로그인 방지 기능 도입
 - 한명의 개인정보취급자가 여러 업무를 수행해야 하는 경우, 해당 개인정보취급자에게 각 업무별로 사용자계정을 발급할 수 있다.
(개인정보취급자 1명이 서로 권한이 다른 조회, 삭제 등 2개의 업무 수행시, 조회업무용과 삭제업무용으로 구분하여 2개의 사용자계정 발급 가능)

2 비밀번호 관리

- 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다.
 - 비밀번호 최소 길이 : 구성 문자의 종류에 따라 10자리 또는 8자리 이상으로 구성
 - 최소 10자리 이상 : 영대문자(A~Z, 26개), 영소문자(a~z, 26개), 숫자(0~9, 10개) 및 특수문자(32개)중 2종류 이상으로 구성한 경우
 - 최소 8자리 이상 : 영대문자(A~Z, 26개), 영소문자(a~z, 26개), 숫자(0~9, 10개) 및 특수문자(32개)중 3종류 이상으로 구성한 경우

- 추측하기 어려운 비밀번호 생성
 - 생성한 비밀번호에 12345 등과 같은 일련번호, 전화번호 등 쉬운 문자열 포함 금지
 - love, happy 등과 같은 잘 알려진 단어, 키보드 상 나란히 있는 문자열 포함 금지
- 비밀번호 주기적 변경 : 비밀번호 유효기간(3개월) 설정, 장기간 사용 금지
- 동일한 비밀번호 사용 제한 : 2개의 비밀번호 교대 사용 금지
- 국가정보보안 기본 지침 제39조(비밀번호관리) 및 개인정보안전성 확보조치 기준 제4조(접근권한의 관리) 준수

3 접근통제 시스템 설치 및 운영

- 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음의 사항을 포함한 시스템 설치·운영하여야 한다.
 - 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol)주소 등으로 제한하여 인가받지 않은 접근을 제한
 - 개인정보처리시스템에 접속한 IP(Internet Protocol)주소 등을 분석하여 불법적인 개인정보 유출 시도를 탐지
- 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하여야 한다.
 - 외부망으로부터 개인정보처리시스템에 대한 접속은 원칙적으로 차단
 - 업무용 컴퓨터(노트북 등), 모바일 기기 등으로 외부에서 정보통신망을 통해 개인정보처리시스템에 접속하는 경우에도 가상사설망, 전용선 등 안전한 접속수단 적용
- 개인정보처리자는 인터넷 홈페이지에서 다른 법령에 근거하여 정보주체의 본인확인을 위해 성명, 주민등록번호를 사용할 수 있는 경우에도 정보주체의 추가적인 정보를 반드시 확인하여야 한다.
 - 추가적 정보 확인 방법 : I-pin, 공인인증서, 휴대전화, 주민등록증 발급일자, email 주소

- 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 업무용 컴퓨터에 조치를 취하여야 한다.
 - 잘 알려진 웹 취약점 항목들을 포함한 웹 취약점 점검·조치
 - 사용되지 않거나 관리되지 않는 사이트 또는 URL에 대한 삭제·차단 조치
 - 관리자 페이지 홈페이지에 대해 노출 차단 등의 보호 조치
 - 개인정보 노출점검 및 차단솔루션 도입
- 개인정보처리자는 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기에서 P2P, 공유설정은 기본적으로 사용하지 않는 것이 원칙이나, 업무상 꼭 필요한 경우, 권한 설정 등의 조치를 통해 권한이 있는 자만 접근할 수 있도록 설정하여, 열람권한이 없는 자에게 처리중인 개인정보가 공개되거나 유출되지 않도록 하여야 한다.
 - 드라이브 전체 또는 불필요한 폴더 공유 금지
 - 공유 폴더에 개인정보 파일이 포함되지 않도록 정기적 점검·조치
- 개인정보처리자는 공개된 무선망을 이용하여 개인정보를 처리하는 경우 개인정보가 신뢰되지 않은 무선접속장치(AP), 무선 전송 구간 및 무선접속장치(AP)의 취약점에 의해 공개 또는 유출되지 않도록 안전 조치를 하여야 한다.
 - 개인정보 송·수신 시 SSL, VPN등의 보안기술이 적용된 전용 프로그램을 사용하여 송·수신 또는 암호화 송·수신
 - 개인정보가 포함된 파일 송·수신시 파일 암호화 저장 후 송·수신
 - 개인정보 유출 방지조치가 적용된 공개된 무선망 이용
- 고유식별정보를 처리하는 개인정보처리자는 인터넷 홈페이지를 통해 고유식별정보가 유출·변호·훼손되지 않도록 연1회 이상 취약점을 점검하여야 한다.
 - 웹 취약점 점검 시 잘 알려진 웹 취약점 항목들을 포함하여 점검

※ 웹 취약점 점검 항목 예시 : SQL_Injection, Cross-site-script취약점, File-Upload 취약점, Zero board취약점, Directory Listing취약점, File Download 취약점 등

- 시큐어 코딩 적용, 관리자 페이지 노출 및 웹 셸 등 정기적 점검·조치
- 홈페이지 취약점 점검 시, 기록을 남겨 책임 추적성 확보 및 향후 개선 조치에 이용
- 개인정보처리자가 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 접근통제 기능을 이용할 수 있다.
- 개인정보처리자는 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.
 - 비밀번호, 패턴, PIN 등을 사용하여 화면 잠금 설정
 - 디바이스 암호화로 애플리케이션, 데이터 등을 암호화
 - USIM 카드에 저장된 개인정보 보호를 위한 USIM카드 잠금 설정
 - 모바일 기기 제조사 및 이동통신사가 제공하는 기능을 이용한 원격 잠금, 원격 데이터 삭제 등의 조치
 - 중요한 개인정보를 처리하는 모바일 기기는 MDM¹⁾(Mobile Device Management) 등 모바일 단말 관리 프로그램을 설치, 원격 잠금, 원격 데이터 삭제, 접속 통제 등의 조치

4] 개인정보의 암호화

- 개인정보처리자는 고유식별정보(주민등록번호, 운전면허번호, 외국인

1) MDM : 무선망을 이용해 원격으로 스마트폰, 태블릿 PC 등의 모바일 기기를 제어하는 솔루션, 분실된 모바일 기기의 위치를 추적, 원격 잠금 설정, 원격 정보 삭제, 특정 사이트 접속 제한, 카메라 등 기능제어, 앱 설치 통제 등의 기능 제공

등록번호, 여권번호), 비밀번호, 바이오정보 등 개인정보는 암호화하여야 한다.

- 저장한 개인정보는 암호화 하여 저장·관리, 특히 비밀번호는 복호화 되지 않도록 일방향암호화(해쉬함수)하여 저장·관리
- 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간지점(DMZ)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.
- 개인정보처리자는 정보주체의 개인정보를 정보통신망을 통하여 송·수신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.
- 개인정보처리자, 개인정보취급자는 업무용 컴퓨터(PC)에 개인정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 저장하여야 한다.

5] 접속기록의 보관 및 점검

- 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 최소 1년 이상 보관·관리하여야 한다.
 - 접속기록 보관내용 : 식별자ID, 접속일시, 접속자 IP 주소, 수행업무 등
- ※ '개인정보의 안정성 확보조치 기준'(행정자치부고시 제2014-7호)
- 개인정보처리자는 개인정보의 유출·변조·훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 반기별로 1회 이상 점검 하여야 한다.
 - 비 인가된 개인정보 처리, 대량의 개인정보의 조회, 정정, 다운로드, 삭제 등의 비정상 행위 탐지하여 적절한 대응 조치
- 개인정보처리자는 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.
 - 정기적인 접속기록 백업 수행, 별도의 보조저장매체나 저장장치에 보관

- 접속기록 위·변조 방지 위해 CD-ROM 등 덮어쓰기 방지 매체 사용, 수정가능 매체(하드디스크 등)를 활용하여 백업 시, 위·변조 확인 가능한 별도 장비에 보관·관리

6] 악성프로그램 등 방지

- 개인정보취급자는 악성 프로그램으로부터 정보주체의 개인정보가 손상·유출이 되지 않도록 업무용 컴퓨터에 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 하며, 다음 사항을 준수하여야 한다.
 - 보안 프로그램의 자동 업데이트 기능을 사용하거나 일 1회 이상 업데이트 실시하여 최신의 상태로 유지
 - 악성 프로그램관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 즉시 업데이트 실시

7] 물리적인 접근제한

- 개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 한다.
 - 물리적 접근 방지를 위한 장치(예시) : 비밀번호 기반 출입통제 장치, 스마트카드 기반 출입 통제 장치, 지문 등 바이오정보 기반 출입통제 장치 등
- 개인정보처리자 및 개인정보취급자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.
 - 보조저장매체 보유 현황 파악 및 반·출입 관리 계획 수립
 - 개인정보취급자(교·직원, 파견근로자, 시간제근로자 등) 및 용역업체의 직원 등에 의한 비인가된 보조저장매체 반·출입에 대한 대응

⑧ 개인정보의 파기

- 개인정보취급자는 개인정보의 보유 및 이용기간 경과 또는 목적 달성시 지체 없이 복구 불가능한 방법(파쇄, 소각 등)으로 파기하여야 하며, 파기 전 개인정보파일명, 개인정보 항목, 수집 및 이용기간, 파기일자, 파기담당자, 파기사유 등을 개인정보 보호책임자에게 신고하여야 한다.
- 개인정보의 보유 및 이용기간 경과 또는 목적이 달성되었다고 하더라도 법령에 따라 보존하여야 하는 경우, 다른 개인정보와 분리하여 저장·관리
- 전문 업체에 위탁할 경우 개인정보처리 위탁 계약을 하여야 하며, 개인정보보호 및 정보보안 서약서 징구 및 파기 완료에 대한 확인을 문서로서 작성·보관

○ 개인정보 파기 절차

절차	주요내용	담당자	비고
1	- 개인정보 파기 요청서 작성 및 제출 ※「교육부 개인정보보호 지침」 [서식 9] 개인정보파일 파기 요청서 참조	개인정보취급자	
↓			
2	- 파기 요청 검토 및 승인·반려	개인정보 보호책임자 개인정보보호 담당자	
↓			
3	- 승인 시, 개인정보 파일 파기 실시 (접속로그 기록 확인) - 개인정보파일 파기 관리대장 작성(업무 분야별 작성) ※「교육부 개인정보보호 지침」 [서식 10] 개인정보파일 파기 관리대장 참조 - 개인정보파일 파기 결과 보고	개인정보취급자	
↓			
4	- 개인정보파일 파기 결과 확인	개인정보 보호책임자 개인정보보호 담당자	담당부서
↓			
5	- 행정자치부 개인정보보호 종합지원시스템 파일 삭제 - 개인정보처리방침에 공개된 개인정보파일 삭제	개인정보 보호책임자	담당부서

V 개인정보보호 교육

① 교육목적

- 안전하게 개인정보가 관리될 수 있도록 개인정보 보호책임자, 담당자, 취급자 각 급별 개인정보보호에 대한 인식을 제고시키고 개인정보보호 대책의 필요성을 이해시키기 위한 교육을 실시한다.

② 교육대상 : 개인정보 보호책임자, 담당자, 취급자

③ 교육실시

- 개인정보 보호책임자 : 연 1회 이상 이수
 - 개인정보 보호 담당자 : 연 2회 이상 이수
 - 개인정보 취급자 : 연 1회 이상 이수
 - 신규 입사자/전입자 : 연 1회 실시
- ※ 교육부 정보보호교육센터(sec.keris.or.kr)을 통해 개인정보보호 교육 이수 상시 가능

④ 교육내용

- 개인정보보호의 중요성 설명
- 내부관리계획의 준수 및 이행
- 위험 및 대책이 포함된 조직 보안 정책, 보안지침, 지시 사항, 위험관리 전략
- 개인정보시스템 하드웨어 및 소프트웨어를 포함한 시스템의 정확한 사용법
- 개인정보의 기술적·관리적 보호조치 기준 이행
- 개인정보보호 위반을 보고해야 할 필요성
- 개인정보보호 업무의 절차, 책임, 작업 설명

○ 개인정보보호 관련자들의 금지 항목들

○ 개인정보보호 준수사항 이행 관련 절차 등

※ 담당자 역할 및 처리업무 특성에 따라 교육 내용 차등 구성

14	주차관리대행	파킹클라우드	성명, 핸드폰, 차량번호	안전시설팀
15	학생부종합전형 평가시스템	포에듀	이름, 주민번호, 수험번호, 전형명, 지원학과, 재학/출신 고교명, 졸업(예정)년도	입학전형관리팀
16	교내 방범장치운영	에스원	성명, 사번(학번)사번, 부서, 주민번호	안전시설팀

※ 개인정보 취급·위탁계약 체결 시 '표준위탁계약서'를 활용한 문서기반의 계약 필요

※위탁업체가 변경되거나 추가되는 경우, 즉시 홈페이지 내 개인정보처리방침에 반영할 것

2] 수탁자 교육 및 관리·감독 계획

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

- 수탁자 개인정보 처리 관리·감독

- 일정 : 수탁자 관리·감독 계획 수립(3월), 분기별 점검 실시
- 점검내용 : 개인정보보호 체크리스트에 따른 이행 여부 점검
- 점검방식 : 2명 1개조 점검반 편성*하여 서비스별 업무 위탁 기관 점검 실시
 - * 개인정보보호 담당자 및 분야별 담당자로 구성
- 점검결과 : 미흡항목 개선 계획 및 조치 결과 제출

- 수탁자 개인정보보호 교육

- 일정 : 수탁자 개인정보보호 계획 수립(3월), 분기별 교육 실시
- 교육내용 : 개인정보 처리방법, 안전성 확보를 위한 기술적·관리적 조치 등
- 교육대상 : 수탁자 중 개인정보를 취급·관리하는 전 직원 대상

※ 개인적인 사정으로 교육 불참의 경우, 수탁자 자체 교육 실시 건도 교육으로 인정

VI 수탁자에 대한 관리 및 감독에 관한 사항

1] 강남대학교 위탁업무 현황

구분	위탁업무	수탁업체명	취급항목	관리부서
1	전자출결	(주)씨드시스템	성명, 학번(사번), 수업현황, 수강현황	교무팀
2	종합정보시스템	(주)에듀씨앤에스	성명, 학번(사번), 이메일, 전화번호, 주소, 부서, 우편번호, 생년월일	전산정보원
3	원서접수대행	(주)유웨이어플라이	이름, 주민번호, 수험번호, 전형명, 지원학과, 전화번호, 휴대전화번호, 추가전화번호, 주소, 재학/출신 고교명, 졸업(예정)년도, 계좌번호, 이메일	입학전형관리팀, 대학원교학팀
4	등록금수납대행	(주)유웨이어플라이	성명, 수험번호	회계경리팀
5	학생역량관리시스템	(주)이데링크	성명, 학번(사번), 이메일, 학부(과), 전화번호, 주소, 상담정보	교육성과센터
6	등록금 수납, 송금	KB국민은행	성명, 학번(사번), 이메일, 전화번호, 주소, 부서, 우편번호, 생년월일	회계경리팀
7	도서관시스템	라이브텍	성명, 학번(사번), 이메일, 전화번호, 주소, 부서, 우편번호, 생년월일	중앙도서관
8	등록금 수납, 송금	신한은행	성명, 학번(사번), 이메일, 전화번호, 주소, 부서, 우편번호, 생년월일	회계경리팀
9	증명서발급업무	아이앤티	학번, 사번, 성명	교무팀
10	입시종합정보시스템 복취 중원	엠엔씨에이프로	이름, 주민번호, 수험번호, 전형명, 지원학과, 전화번호, 휴대전화번호, 추가전화번호, 주소, 재학/출신 고교명, 졸업(예정)년도, 계좌번호, 이메일	입학전형관리팀
11	등록금 수납, 송금	영동농협	성명, 학번(사번), 이메일, 전화번호, 주소, 부서, 우편번호, 생년월일	회계경리팀
12	e러닝시스템	유비온	성명, 학번(사번), 소속, 연락처, 이메일	교수학습지원센터
13	평생교육원시스템	이노정보기술	이름, 집주소, E-Mail, 집연락처, 핸드폰(연락처), 보훈대상자, 학번, 학년, 성별, 학과명, 수강과목, 학점	평생교육원

VII 개인정보 침해대응 및 피해구제

1 개인정보 유출 등의 통지

- 개인정보 보호책임자는 개인정보가 유출됨을 알게 되었을 때에는 지체없이 개인정보처리자에게 알려야 한다. 개인정보처리자는 정보주체에게 다음의 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.
 - 유출된 개인정보의 항목
 - 유출된 시점과 그 경위
 - 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
 - 대응조치 및 피해 구제절차
 - 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처
- 1만명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 서면 등의 방법과 함께 인터넷 홈페이지에 정보주체가 알아보기 쉽도록 위의 고지 사항을 7일 이상 게재해야 한다.
- 개인정보처리자는 개인정보가 유출된 경우 그 피해를 최소화하기 위하여 “침해사고대응팀”을 구성하고 대응 매뉴얼에 따라 필요한 조치를 해야한다.
 - ☞ (붙임2) 강남대학교 개인정보 침해사고 대응 매뉴얼

2 개인정보 유출 등의 신고

- 1명이라도 정보주체에 관한 개인정보가 유출된 경우에는 유출내용 및 조치결과를 5일 이내에 교육부 정보보호팀에 신고하여야 한다.
- 개인정보처리자는 1만명 이상의 개인정보가 유출된 경우에는 「개인정보보호법」 시행령 제39조(개인정보 유출 신고의 범위 및 기관)에 따라 한국정보화진흥원, 한국인터넷진흥원에 신고하여야 한다.

VIII 개인정보의 목적 외 이용 및 제3자 제공 처리절차

① 기본 원칙

○ 자료제공 판단 기준

- 자료제공이 필요한 경우 목적의 정당성, 수단의 적정성, 피해의 최소화성, 법익의 균형성에 대하여 종합적으로 검토한 후 필요한 최소한의 범위 내에서 제공하여야 한다.

· 목적의 정당성 : 구체적으로 어떠한 목적을 위하여 당해 개인정보가 필요한지?
· 수단의 적정성 : 당해 개인정보를 제공함으로써 공익목적 달성할 수 있는 것인지?
· 피해의 최소화성 : 목적달성을 위하여 필요한 최소한의 정보는 어디까지인지?
· 법익의 균형성 : 제공에 따른 이익과 정보주체가 받을 수 있는 예상피해를 비교하여 전자가 우월하다고 할 수 있는지 여부 판단

○ 요청 기관의 적격 여부 확인

- 자료제공이 필요한 경우 제공가능 여부를 아래의 기준에 따라 확인하고 제공하여야 한다.

· 요청 기관의 개별법에 자료요청의 근거조항이 구체적으로 명시된 경우 제공 가능
· 요청 기관의 개별법에 자료요청 근거법이 없는 경우, 정보주체의 동의가 있었는지 여부 등 예외적 제공가능 사항에 해당되는지 확인한 후 제공 여부 결정

○ 제공항목 판단

- 직접 수집한 정보 여부 확인하여야 한다.
- 강남대학교 에서 직접 수집·생산한 정보가 아닌 경우 자료제공 불가
 ※단, 정보주체의 별도 동의가 있는 경우 제공 가능
- 요청 목적에 부합하는 최소 항목만 제공(개인정보 최소 제공 원칙)

- 고유식별정보(주민등록번호, 여권번호, 운전면허번호, 외국인등록번호)는 법령(법률, 시행령, 시행규칙)에 처리를 요구(허용)하도록 규정되어 있는 경우만 제공하여야 한다.

② 개인정보 제공 기준

○ 수집목적 범위 내에서 제공하는 경우

- 정보주체의 동의를 받은 경우 개인정보의 제3자 제공이 가능하다.
- 개인정보보호법 제15조제1항 제2호·제3호 및 제5호에 따라 개인정보를 수집한 목적 범위에서 개인정보를 제공하는 경우 제3자 제공이 가능하다.

○ 수집목적 외의 용도로 제공하는 경우

- 「개인정보보호법」 제18조 제2항 각 호에 해당하는 경우는 예외적으로 제공 가능 다만, 정보주체 또는 제3자의 권익을 부당하게 침해할 우려가 있다고 인정되는 때에는 제공 불가하다.

○ 업무의 일부 또는 전부를 위탁하는 경우

- 개인정보 처리 업무를 위탁하는 경우 위탁업무의 목적 등이 포함된 문서에 의하여야 하며 위탁사항에 구체적으로 표기된 범위 내에서 제공하여야 한다.

※ 위탁자의 이익을 위해 처리하는 경우는 업무 위탁에 해당되며 개인정보를 제공 받는 제3자의 이익을 위해 처리하는 경우에는 제3자 제공에 해당

③ 안전성 확보 조치

- 개인정보 자료 제공은 문서로 시행되어야 하며, 문서에 제공 목적 이외의 이용금지, 사용 목적 달성 후 폐기, 사후관리 실태 확인 등의 안전성 확보 조치 문구를 표기하여 시행하여야 한다.

4 목적 외 이용·제3자 제공 시 절차

절 차	주요내용
1. 법적근거 검토	- 목적 외 이용·제3자 제공이 가능한 경우에 해당하는지 법적근거 검토
↓	
2. 동의절차 이행	- 법적 근거가 없는 경우 정보주체로부터 별도의 동의를 받아야 함 ※ 동의서는 [별지 2 서식] 참조
↓	
3. 대장 기록관리	- '개인정보의 목적 외 이용 및 제3자 제공 대장'을 기록·관리하여야함(개인정보 분야별 책임자) ※ 「교육부 개인정보 보호지침」 [서식 8] 개인정보의 목적 외 이용 및 제3자 제공 대장 활용
↓	
4. 보호조치 요구	- 제3자 제공시에는 이용목적, 이용방법, 이용기간, 이용형태 등을 제한하거나 개인정보의 안전성 확보를 위하여 필요한 조치("라. 안전성 확보 조치" 참조)를 마련하도록 문서로 요청
↓	
5. 조치결과 제출	- 안전성 확보조치 요청을 받은 자(제공받는자)는 그에 따른 조치를 취한 후, 그 결과를 개인정보를 제공한 개인정보처리자에게 문서로 알려야 함
↓	
6. 주요 내용 공개	- 30일 이내에 관보 또는 인터넷 홈페이지에 10일 이상 계속 게재

IX 정기 감사 및 결과반영(선택)

1 정기 감사 및 절차

- 개인정보 보호책임자는 개인정보보호를 위한 내부관리계획 및 관련 법령에서 정하는 개인정보보호 규정을 성실히 이해하는지를 정기적으로 감사 또는 점검하여야 한다.
 - 개인정보 보호책임자는 개인정보 자체감사를 위한 감사대상, 감사 절차 및 방법 등 감사의 실시에 필요한 별도의 계획을 수립하여 매년 1회 이상 실시할 수 있다.
 - 정기 감사 결과 반영
 - 개인정보 보호책임자는 개인정보보호를 위한 자체감사 실시결과 개인정보의 관리·운영상의 문제점을 발견하거나 개인정보취급자가 본 계획의 내용을 위반할 때에는 시정·개선 등 필요한 조치를 취하여야 한다.
 - 개인정보 보호책임자는 개인정보 위반사실에 대한 시정·개선 조치가 이행되지 않거나, 개인정보보호에 심각한 영향이 발생할 수 있는 우려가 되는 경우 개인정보취급자 등에 대하여 인사위원회 심의 요구 등 필요한 추가 조치를 취할 수 있다.
- ☞ (붙임3) 강남대학교 개인정보처리시스템 자율 점검표 및 가이드라인

2. 개인정보보호 교육 계획

□ 목적

- 강남대학교 교·직원의 개인정보 보호 인식 제고를 통해 유·노출 사고 예방, 대응역량 강화 등 개인정보 관리수준 향상

□ 대상

- 교내 개인정보보호 분야별 담당자, 취급자, 학과 조교 등

□ 시기

- 개인정보 처리의 오·남용, 유출 등을 적극 예방하기 위해 매년 1회 이상 개인정보보호 교육 실시
 - (상반기) 교내 개인정보취급자 및 분야별 담당자, 신규·파견자 및 외부위탁운영업체
 - (하반기) 부내 전 직원 및 외부위탁운영업체
 - (연 중) 부내 개인정보 보호책임자 및 개인정보 보호담당자

□ 교육방법

- 집합교육, 외부기관 행사 참여, 개인정보보호 종합지원 포털 등

□ 교육 내용

구분	교육내용	시기	시간	교육대상	비고
상/하반기 실시	· 개인정보 보호와 업무처리 · 개인정보보호 처리절차별 유의사항	7월	2시간	부내 과(팀)별 개인정보취급자	
	· 「개인정보보호법」 및 「교육부 개인정보 보호지침」 개정 사항	7월, 1월	2시간	부내 신규·파견자 및 외부위탁운영업체 직원	
	· 사례를 통한 개인정보 Life-cycle · 개인정보 유출, 위반사례 소개 등	직장교육	1시간	교내 전 직원 (개인정보 취급자 포함)	
연 중	· 개인정보 보호 관련 교육(행사) 참여	-	1회이상	개인정보 보호책임자	사이버 또는 집합교육
		-	2회이상	개인정보 보호담당자	

3. 강남대학교 개인정보 침해사고 대응 방침 및 메뉴얼

1. 개요

□ 목적

- 강남대학교 개인정보 침해사고 대응방안은 강남대학교에서 개인정보 운용 과정에서 내부의 과실 및 오·남용 또는 외부 해킹 등으로 침해·유출 사고가 발생할 경우, 체계적이고 신속한 대응으로 피해를 최소화하려는데 목적이 있다.

□ 적용범위

- 강남대학교에서 처리하는 모든 개인정보 및 그 개인정보를 취급하는 개인정보취급자(외부인력 포함)의 침해·유출 사고 대응절차를 기술한다.
- 내·외부적 요인으로 개인정보 침해 및 유출 사고가 발생할 경우 적용한다.

□ 용어 정의

- 침해사고 : 비인가 된 접근, 전산 시스템의 오남용(비 인가된 사용)을 의미한다. 비인가 된 시스템 사용 또는 사용자의 계정 도용, 악성코드 유입 및 실행, 정보 서비스의 방해뿐만 아니라 해킹사고와 바이러스 사고도 포함한다. 또한 보안정책에 위반되는 행위 역시 침해사고로 정의한다. 침해사고 대응팀은 본 침해사고의 범위에 정의된 사고를 중심으로 대응조치를 취하도록 한다.
- 개인정보 유출 : 개인정보의 유출이라 함은 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고, 정보주체의 개인정보에 대하여 개인정보처리자가 통제를 상실하거나 또는 권한 없는 자의 접근을 허용한 것으로서, 다음의 어느 하나에 해당하는 경우를 말한다.

- 개인정보가 포함된 서면, 이동식 저장장치, 휴대용 컴퓨터 등을 분실하거나 도난당한 경우
 - 개인정보가 저장된 데이터베이스 등 개인정보처리시스템에 정상적인 권한이 없는 자가 접근한 경우
 - 개인정보처리자의 고의 또는 과실로 인해 개인정보가 포함된 파일 또는 종이문서, 그 밖에 저장매체가 권한이 없는 자에게 잘못 전달된 경우
 - 그 밖에 권한이 없는 자에게 개인정보가 전달되거나 개인정보처리시스템 등에 접근 가능하게 된 경우
- 악성 프로그램 유포 : 제작자가 의도적으로 다른 정보통신 이용자에게 피해를 주고자하는 악의적 목적으로 만든 프로그램 및 실행 가능한 코드를 의미한다. "악성코드"라 표현하기도 하며, 이메일, 메신저, 문서의 매크로 기능 등을 이용하여 악성프로그램을 유포시키고 공격에 사용한다. 주요 형태로는 컴퓨터 바이러스, 인터넷 워, 트로이 목마 등이 공격에 이용된다.
- 서비스거부 공격(DoS, Denial of Service) : 시스템 또는 네트워크 서비스의 정상적인 운영을 방해하는 공격으로, 시스템을 다운시키거나, 네트워크에 과부하의 트래픽을 유발시켜 사용자들이 서비스를 이용하지 못하게 하는 공격이다.
- 시스템 침입(비 인가된 접근) : 시스템 또는 네트워크의 취약성을 이용하여 시스템에 침입하는 공격이다. 보통 특정 취약점을 공격하는 해킹프로그램을 이용하거나, 잘못된 서버운영상의 문제(예, 디폴트 패스워드를 사용하는 경우 등)를 이용하여 시스템에 침입한다.
- 오남용(비 인가된 사용) : 시스템 및 네트워크 자원을 허가받지 않은 방법으로 사용하거나 악용하는 공격이다. 스팸메일을 보낼 때 다른 사이트의 시스템을 이용하는 방법이나 다른 사람의 계정을 도용하는 행위 등이 대표적인 예이다.

- 정보수집 : 특정 사이트의 시스템 및 네트워크에 대한 정보를 수집하기 위한 공격으로 포트스캔, 전화번호 스캔 등이 있다. 공격자는 정보 수집을 통해 특정 사이트에 어떠한 시스템이 존재하는지, 어떠한 서비스가 제공되는지, 어떠한 네트워크 구조를 갖고 있는지, 그리고 어떠한 취약성이 있는지를 조사하게 된다.
- 침해사고대응팀 : 해킹 또는 바이러스, 개인정보 유·노출 사고 발생에 따른 사고의 분석, 처리, 사후 복구, 사후 예방 조치 등을 주요 업무로 하는 침해사고 대응반을 말한다.
- 개인정보 보호책임자 : 침해사고대응 체계를 수립하고 관련 내용을 개인정보보호 담당자에게 교육 및 훈련시키도록 한다.
- 개인정보보호 담당자 : 침해사고와 관련된 내용을 숙지하고, 침해사고 발생 시 본 매뉴얼에 따라 대응 할 수 있도록 한다.
- 개인정보취급자 : 침해사고와 관련된 내용을 숙지하고, 침해사고 발생 시 본 매뉴얼에 따라 개인정보 보호책임자 또는 개인정보 보호담당자에게 보고해야 한다.

□ 관련법규

- 법적근거
 - 「개인정보보호법」
 - 「개인정보보호법시행령」 (대통령령 제24425호)
 - 「국가사이버안전관리규정」 (대통령훈령 제291호)
 - 「정보통신기반보호법」
 - 「전자정부법」
- 기타사항
 - 「표준 개인정보보호 지침」 (안전행정부고시 제2011-45호)

- 「개인정보의 안전성 확보조치 기준」 (행정자치부고시 제2016-35호)
- 「교육부 개인정보보호 지침」 (교육부훈령 제135호)
- 「강남대학교 개인정보보호에 관한 규정」

□ 사고유형

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	
과실로 인한 개인정보 유·노출	•개인정보가 포함된 서면, 이동식 저장장치, 휴대용 컴퓨터를 분실 또는 도난 당한 경우 •권한이 없는 자에게 개인정보를 잘못 전달한 경우	①강남대학교 강남팀 ②KERS 개인정보보호부 ③침해신고 ④상시모니터링
오·남용으로 인한 개인정보 유출	•개인정보 부당이용 또는 사적용을 목적으로 유출하는 경우	
외부 침투에 의한 개인정보 유출	•홈페이지 해킹 등 외부 침투에 의해 정보주체의 개인정보가 유출되는 경우	

2. 침해·유출 사고 시 조치방법

□ 침해·유출 사고 시 단계별 조치방법

단계	조치방법	세부 조치 사항
확인단계	① 사고 인지·접수	• 침해·유출 사고 상황 파악 • 개인정보 보호책임자에게 보고 • 침해·유출 사고대응반 설치
	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
조치단계	④ 유출통지	• 정보주체에게 5일 이내 통지
	⑤ 유출통지 신고	• 행정자치부 또는 한국인터넷진흥원(KISA), 한국정보화진흥원(NIA)에 5일 이내 신고
	⑥ 사례전파 및 시스템 보완	• 기술적, 관리적 보완조치

□ 사고 유형별 조치방법

○ 과실로 인한 개인정보 침해 사고

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

- 침해사고 인지 및 접수
 - 개인정보 보호담당자는 정기 실태점검 또는 침해신고(접수)를 통해 발생부서의 개인정보관리 침해사실 인지 및 접수
 - 개인정보 보호담당자는 개인정보 관리가 미흡한 부서에 대하여 개인정보 보호책임자에게 보고
 - 개인정보 보호책임자는 침해사고대응반 설치
- 확인조사 실시
 - 침해사고대응반에서는 개인정보 침해사고가 인지 또는 접수되어 침해사고 발생이 우려되는 부서에 대하여 확인조사 및 위협사실 확인
 - ※ 필요 시 외부 전문가 협조 요청
 - 사고 발생부서는 침해사고대응반의 현장 확인조사 시 적극 협조
- 개선조치 및 사례전파
 - 침해사고대응반은 확인조사 결과를 분석하여 개인정보 보호책임자에게 보고
 - 침해사고대응반은 개인정보 침해사고 발생을 방지하기 위한 대책을 해당 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

○ 과실로 인한 개인정보 유·노출 사고

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

- 유·노출 사고 인지 및 접수
 - 개인정보 보호담당자는 상시 모니터링, 실태점검을 통한 부주의 등 과실로 인한 개인정보 유·노출 사실 확인 또는 내·외부 침해신고 접수를 통해 유·노출 사고 인지
 - 개인정보 보호담당자는 위반사항이 중대한 경우 개인정보 보호책임자에게 보고
 - 개인정보 보호책임자는 침해사고대응반 설치
- 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
 - 사고 발생부서는 침해사고대응반의 현장 확인조사 시 적극 협조
- 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
- 유출통지
 - 침해사고대응반은 개인정보가 유출되었을 경우, 유출 사실을 지체 없이(5일 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
- 1만명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 서면 등의 방법과 함께 인터넷 홈페이지에 정보주체가 알아보기 쉽도록 7일 이상 게재
- 유출통지 신고
 - 1명이라도 정보주체에 관한 개인정보가 유출된 경우에는 유출내용 및 조치결과를 5일 이내에 교육부 정보보호팀에 신고
 - 1만명 이상 유출된 경우에는 정보주체에게 유출 사실을 통지한 사항 및 피해를 최소화하기 위한 대책과 필요한 조치 결과를 행정자치부 또는 전문기관(한국인터넷진흥원, 한국정보보호진흥원)에 신고
- 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
- 사고내용 세부조사
 - 침해사고대응반은 확인조사 결과 세부조사가 필요하다고 판단 되는 경우, 개인정보 보호책임자에게 필요성 보고
- 해당자 처분 및 조치
 - 개인정보 보호책임자에게 세부조사 결과 보고
 - 위반사항의 중요도에 따라 처분 및 조치 요청

○ 오·남용으로 인한 개인정보 유출 사고

- 유출 사고 인지 및 접수
 - 개인정보 보호담당자는 상시 모니터링, 실태점검 등을 통한 고의적 유출 사실 확인 또는 내·외부 침해신고 접수를 통해 사고 인지
 - 침해사고대응반은 사고 사실을 개인정보 보호책임자에게 보고
 - 개인정보 보호책임자는 침해사고대응반 설치
- 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
 - 사고 발생부서는 사고대응반의 현장 확인조사 시 적극 협조
- 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
- 유출통지
 - 침해사고대응반은 개인정보가 유출되었을 경우, 유출 사실을 지체 없이(5일 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
 - 1만명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 서면 등의 방법과 함께 인터넷 홈페이지에 정보주체가 알아보기 쉽도록 7일 이상 게재

- 유출통지 신고
 - 1명이라도 정보주체에 관한 개인정보가 유출된 경우에는 유출 내용 및 조치결과를 5일 이내에 교육부 정보보호팀에 신고
 - 1만명 이상 유출된 경우에는 정보주체에게 유출 사실을 통지한 사항 및 피해를 최소화하기 위한 대책과 필요한 조치 결과를 행정자치부 또는 전문기관(한국인터넷진흥원, 한국정보화진흥원)에 신고
- 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
- 사고내용 세부조사
 - 침해사고대응반은 확인조사 결과 세부조사가 필요하다고 판단 되는 경우, 개인정보 보호책임자에게 필요성 보고
- 해당자 처분 및 조치
 - 개인정보 보호책임자에게 세부 조사결과 보고
 - 위반사항의 중요도에 따라 처분 및 조치 요청
 - ※ 세부조사 결과 개인정보 부당이용 또는 사적유용을 목적으로 유출된 경우 고발 조치

○ 외부 침투에 의한 개인정보 유출 사고

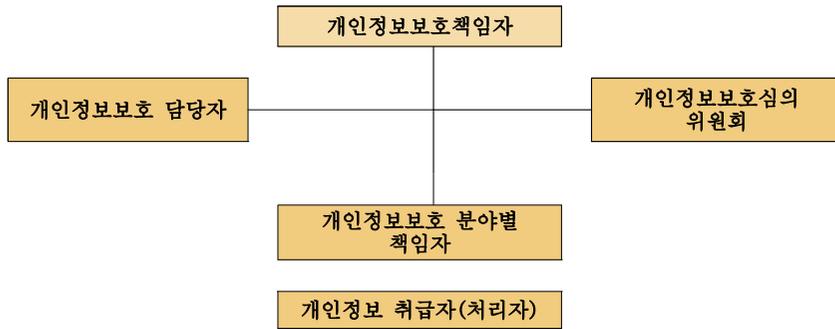
- 외부 침투에 의한 유출 사고 확인
 - 개인정보 보호담당자는 외부침투(해킹 등)에 의한 개인정보 유출사실 확인
 - 사이버공격 대응절차에 따른 경계단계별 대응반 가동 상태 확인

- 개인정보 보호담당자는 확인한 침해사실에 대해 개인정보 보호 책임자에게 보고
- 개인정보 보호책임자는 침해사고대응반 설치
- 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
- 유출통지
 - 침해사고대응반은 개인정보가 유출되었을 경우, 유출 사실을 지체 없이(5일 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
 - 1만명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 서면 등의 방법과 함께 인터넷 홈페이지에 정보주체가 알아보기 쉽도록 7일 이상 게재
- 유출통지 신고
 - 1만명 이상 유출된 경우에는 정보주체에게 유출 사실을 통지한 사항 및 피해를 최소화하기 위한 대책과 필요한 조치 결과를 행정자치부 또는 전문기관(한국인터넷진흥원, 한국정보화진흥원)에 신고
- 사고 사례전파 및 시스템보완
 - 침해사고대응반은 개인정보 유출 및 침해에 관한 사고사례를

- 전파하고 유사사례가 발생하지 않도록 조치
- 정보화 담당자는 보안시스템 점검 강화 등의 기술적인 보안 조치
- 해킹사고 세부조사 및 조치
 - 침해사고대응반은 교육사이버안전센터, 행정자치부 등에 세부조사 의뢰
 - 세부조사 결과, 해킹사고의 업무상 과실 등 책임이 있는 담당자를 확인하여 고발 조치

3. 침해사고 대응반 조직 및 역할

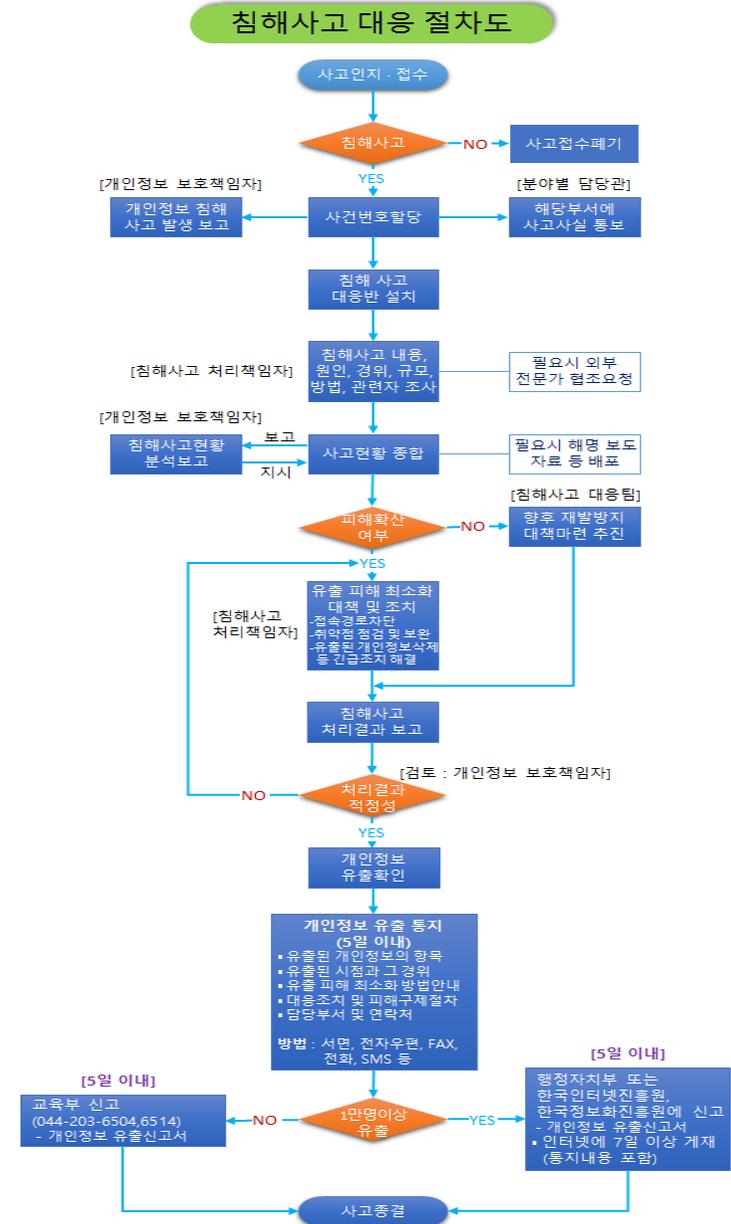
□ 침해사고 대응반 조직체계



□ 역할

조직별	담당자	담당 업무
개인정보 보호책임자	총무처장	<ul style="list-style-type: none"> 개인정보 침해사고 대응 총괄 지휘
개인정보 침해사고 대응반	개인정보보호담당자 개인정보보호 분야별 책임자, 정보안전담당자, 기타 협조부서	<ul style="list-style-type: none"> 개인정보 침해사고 인지, 접수 개인정보 침해사고 대응 절차 수립 개인정보 침해사고 사실 확인조사 실시 정보주체에게 유출사실 통지 행정자치부 또는 전문기관에 유출통지 신고 외부요인에 의한 유출의 경우, 교육사이버안전센터, 행정자치부 등과 협조하여 사고 해결 사고내용 세부조사 및 사후 인사조치가 필요한 경우 유관부서와 협조
사고 발생부서	개인정보취급자	<ul style="list-style-type: none"> 내부요인에 의한 침해, 유출의 경우, 사고대응반에 사고내용 신고 침해사고대응반과 협력하여 사고처리 적극 지원
사고신고자	정보주체	<ul style="list-style-type: none"> 개인정보를 침해 받은 피해자

□ 개인정보 침해사고 대응절차



□ 개인정보 침해사고 대응절차 요약

개인정보 침해사고가 의심된다면

개인정보 침해사고 유형

- 개인정보가 포함된 서면, 저장매체, 휴대용 컴퓨터 등을 분실 또는 도난 당한 경우
- 개인정보가 포함된 파일 또는 문서, 저장매체가 권한이 없는 자에게 잘못 전달된 경우
- 그 밖에 권한이 없는 자에게 개인정보가 전달된 경우 등

전직원(취급자)

개인정보 침해 사고 의심

❖ 침해가 발생한 것을 인지한 경우 또는 그러한 침해의 발생이 의심되는 경우 지체 없이 소속 부서의 분야별 담당관에게 신고

분야별 담당관

개인정보 침해 상황 파악

❖ 분야별 담당관은 소속 부서 직원의 신고에 따라 유출여부, 유출시기, 유출원인 및 유출규모(수량)를 신속하게 확인
❖ 소속 부서(학과)의 장에게 보고한 후 개인정보보호 담당자에게 신고

소속 부서의 장

침해사고 처리 책임자 역할 수행

❖ 소속 부서의 장은 침해사고 처리 책임자로 지정되며 처리 및 재발방지에 대한 책임을 지고 침해사고 대응팀과 협력하여 사고 해결 노력

개인정보보호 담당자

침해사고 대응절차 수행

❖ 침해신고 내용을 개인정보 보호책임자에게 보고
❖ 개인정보 침해사고를 접수하고 침해사고 대응 절차 개시

개인정보보호책임자

침해사고 대응 총괄 지휘

❖ 침해사고 대응 총괄 지휘

□ 개인정보 침해사고 정보주체 통지 세부내용

구 분	내 용
통지 방법	1. 서면, 전자우편, 모사전송, 전화, 문자전송 또는 이와 유사한 방법(필수 사항) 2. 1번 통지방법과 동시에 홈페이지 등을 통하여 공개 (1번 통지방법으로 연락 불가시 홈페이지 게시, 단 1만명 이상 정보주체의 개인정보 유출시에는 홈페이지에 7일 이상 외우적으로 게시) * 개인정보보호법 시행령 제40조 * 교육부 개인정보보호지침 제52조
통지 내용	1. 유출된 개인정보의 항목 2. 유출된 시점과 그 경위 3. 유출피해 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 대한 정보 4. 개인정보처리자의 대응조치 및 피해구제절차 5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처 * 개인정보보호법 제34조 * 교육부 개인정보보호지침 제51조
통지 시기	개인정보 유출사고를 안 때부터 지체 없이(5일 이내) 통보 단, 개인정보 구체적인 유출내용 확인 불가한 경우 다음사항 알리고 추후 확인된 사항, 추가안내 가능 1. 정보주체에게 유출이 발생한 사실 2. 통지내용 중 확인된 사항 * 개인정보보호법시행령 제40조 * 교육부 개인정보보호지침 제51조
통지결과 신고	통지결과(통지내용·결과, 홈페이지에 게시한 경우 게시기간 및 내용 화면 캡처 등 입증자료 첨부) 등 지체 없이 신고기관에 신고 * 개인정보보호법 제34조 * 교육부 개인정보보호지침 제53조

4. 사고 예방

□ 사고예방 활동

- 개인정보 침해·유출 사고를 대비하여 사정 사고예방 활동 실시
 - 개인정보보호 관리수준 현장조사
 - 개인정보 통합관계 실시
 - 웹사이트 개인정보 노출점검 실시

□ 사고요인 점검

- 수집단계에서의 침해·유출 사고요인 점검
 - 불필요한 개인정보 수집 여부 점검
 - 수집된 개인정보의 개인정보보호 처리방침 게재 여부 점검
 - 개인정보 수집 시 정보주체 동의 여부 점검
- 저장 및 관리단계에서의 침해·유출 사고요인 점검
 - 수집된 개인정보 불법적인 유출 위협 상태 점검
 - 수집 목적 달성 또는 보유기간 초과 여부 점검
 - 관리자 또는 이용자의 실수로 인한 개인정보 노출 여부 점검
 - 권한관리 등 시스템 오류로 인한 개인정보 노출 여부 점검
- 이용 및 제공단계에서의 침해·유출 사고요인 점검
 - 개인정보보호 처리방침에 명시되지 않은 위탁사업자나 제3의 서비스 제공자에게 개인정보 제공 여부 점검
 - 개인정보를 제3자에게 양도하는 등 불법적 거래 여부 점검
- 파기단계에서의 침해·유출 사고요인 점검
 - 수집 목적 달성 또는 보유기간 초과한 개인정보 파기 여부 점검

- 권한이 없는 이용자의 개인정보 파기 여부 점검

○ 개인정보 특별점검 실시

- 개인정보의 관리 미흡으로 개인정보 유출사고 발생 가능성이 우려되는 경우, 개인정보 특별점검 실시
- 대상 : 개인정보 취급자 및 일반직원

강남대학교 개인정보 침해사고 대응 매뉴얼

제1장 총칙

제1조 (목적) 본 지침은 강남대학교(이하 “본 대학”이라 한다)에서 발생하는 개인정보침해사고에 신속하게 대응하기 위한 사고대응 및 처리방법과 이를 위한 사전 준비사항에 대하여 침해사고로부터의 피해를 최소화하고 후속 보안 대책을 세울 수 있도록 하는데 그 목적이 있다.

제2조 (적용범위) 본 지침의 적용범위는 본 대학의 개인정보를 취급하는 대학 내부 교직원(계약직 등 비정규직 포함)을 대상으로 한다.

제3조 (용어정의) “개인정보의 유출”이란 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고, 정보주체의 개인정보에 대하여 개인정보처리자가 통제를 상실하거나 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 종이 문서, 그 밖에 저장매체가 권한이 없는 자에게 잘못 전달된 경우
4. 그 밖에 권한이 없는 자에게 개인정보가 전달되거나 개인정보처리시스템 등에 접근 가능하게 된 경우

제2장 개인정보침해사고 대응에 관한 역할

제4조 (개인정보 보호책임자) ① 개인정보 보호책임자는 개인정보침해사고 예방, 처리 및 재발방지의 총괄 관리를 한다.

② 개인정보 보호책임자는 개인정보 침해사건 발생 시 침해사고 처리책임자를 지정

하고 개인정보침해사고 대응팀을 소집하여 운영한다.

제5조 (개인정보침해사고 대응팀) 개인정보보호 분야별책임자로 구성되며 개인정보 보호책임자가 해당 침해사고 분석, 대응 및 복구에 필요한 관련자를 지정하여 소집한다. 필요시 업무담당자, 외부 전문가 등이 포함될 수 있다.

제6조 (침해사고 처리책임자) 해당 침해사고의 발생 부서(학과)의 장으로 지정되며 처리 및 재발방지에 대한 책임을 지고 개인정보침해사고 대응팀과 협력하여 사고를 해결한다.

제7조 (개인정보보호담당자) ① 개인정보침해사고를 접수하고 본 지침 제10조의 기준에 따라 등급을 분류하여 침해사고 대응 절차를 개시한다.

② 개인정보침해사고 대응팀의 간사로서 대내외 비상연락망을 관리하고 팀 내 연락 및 조정을 담당한다. [붙임5] 참조

③ 개인정보침해기록을 관리하고 필요시 관련자 및 기관에 보고한다.

제8조 (정보보안담당자) 정보보안담당자는 침해사고 발생 시 기술적인 분석을 제공한다.

제9조 (전직원) 대학의 내부 교직원(계약직 등 비정규직 포함)은 개인정보에 대한 침해가 발생한 것을 인지한 경우, 지체없이 개인정보보호담당자에게 신고하여야 한다.

제3장 침해사고의 분류

제10조 (개인정보침해의 분류) 개인정보침해사고는 다음과 같이 3등급으로 분류한다.

침해등급	내용	예시
1등급	법적 근거, 규정 또는 본인의 동의 없이 개인정보가 대학 외부의 제3자에게 노출 또는 제공	○ 해킹, DDOS, 내부자에 의한 개인정보 유출 ○ 본인 동의 없이 목적 외 이용 또는 제3자 제공 등
2등급	법적 근거, 규정 또는 본인의 동의 없이 개인정보를 수집, 접근, 분석, 이용, 내부자에게 제공, 저장, 파기	○ 개인정보취급 권한이 없는 직원이 개인정보 취급-훼손 ○ 개인정보 취급자에 의한 개인정보 훼손-침해 ○ 이용자의 동의 없는 개인정보 수집/이용 ○ 과도한 개인정보 수집 등
3등급	안전하지 않은 상태로 개인정보를 저장하거나, 파기해야 할 정보를 파기하지 않는 등 세부지침의 규정 위반	○ 주요 개인정보(고유식별번호 등) 암호화 미실시 ○ 개인정보에 대한 기술적-관리적 조치 미비 ○ 개인정보 수집 또는 제공받은 목적 달성 후 개인정보 미파기 등

제4장 개인정보침해 대응 절차

제11조 (개인정보침해 예방 및 탐지) ① 개인정보보호담당자는 웹사이트를 통한 개인정보 유출을 예방하기 위하여 개인정보 유출차단 시스템을 운영·관리한다.
② 게시판 등에 자료를 게재할 때 개인정보 유출에 대하여 주의를 환기시키기 위한 경고를 제공하여야 한다.
③ 개인정보보호담당자는 년 1회 웹사이트의 개인정보 노출 취약점 점검을 시행하고 개인정보보호책임자에게 결과를 보고한다.

제12조 (개인정보침해의 신고) ① 대학의 전직원(계약직 등 비정규직 포함)이 취급하는 개인정보에 대하여 본 지침 제10조에서 정의한 침해가 발생한 것을 인지한 경우 또는 그러한 침해의 발생이 의심되는 경우 지체없이 소속 부서의 분임담당관에게 신고하며 분임담당관은 개인정보보호담당자에게 신고하여야 한다.
② 개인정보침해사고 발생시 고의적으로 신고를 누락 한 경우 개인정보 보호책임자는 관련자에 대한 처분(징계 등)을 요청 할 수 있다.

제13조 (개인정보침해사고의 접수) ① 개인정보보호담당자는 개인정보침해사고를 접수한 경우 [붙임1] “개인정보 침해사고 관리대장” 에 사고 접수를 기록한다.
② 개인정보보호담당자는 접수 후 지체 없이 개인정보 보호책임자에게 보고 한다.

제14조 (개인정보침해사고 대응팀 구성) ① 개인정보 보호책임자는 유출 또는 제공된 정보의 종류에 따라, 발생 부서(학과)의 장으로 침해사고 처리책임자를 지정하고 개인정보침해사고 대응팀을 구성한다.
② 발생 부서(학과)를 적시할 수 없거나 발생 부서(학과)의 장이 침해사고에 연루된 경우 개인정보 보호책임자가 임의로 침해사고 처리책임자를 지정할 수 있다.
③ 개인정보침해사고 대응팀은 분야별 책임자 중에서 사안에 따라 선정한다.
④ 2, 3등급 침해의 경우 개인정보 보호책임자는 침해사고처리책임자와 협의하여 개인정보침해사고 대응팀을 구성하지 않을 수 있다.
⑤ 개인정보 보호책임자는 필요시 외부 전문가에게 분석을 의뢰할 수 있다.

제15조 (침해사고의 분석) ① 침해사고 처리책임자는 침해 사실 여부를 확인하고 사실로 확인될 경우 침해의 규모, 경위, 방법, 원인 및 관련자를 조사한다.
② 침해사고 처리책임자는 필요한 경우 개인정보침해사고 대응팀 또는 개인정보 보호책임자가 승인한 외부 전문가의 지원을 받아 증거자료를 수집한다.

제16조 (침해사고의 대응 및 복구) ① 1등급 침해의 경우 침해사고 처리책임자는 해당 개인정보를 파기 또는 회수하기 위한 조치를 취한다.
② 2등급의 경우 침해사고 책임자는 해당 개인정보를 파기, 회수 또는 복구하기 위한 조치를 취하거나 정보주체의 사후 동의를 받아 근거를 마련한다.
③ 3등급의 경우 침해사고 처리책임자는 해당 개인정보를 적절히 보호하거나 파기하기 위한 조치를 취한다.
④ 침해사고 처리책임자는 즉각적 조치가 가능한 경우 재발방지 조치를 취한다.

제17조 (침해사고의 종료) ① 침해사고 처리책임자는 [붙임2] 개인정보침해사고 처리보고서를 작성하여 개인정보 보호책임자에게 제출한다.
② 개인정보 보호책임자는 개인정보침해사고 처리보고서를 검토하고 승인한다.
③ 개인정보 보호책임자는 개인정보침해 관련자에 대한 처분(징계 등)을 해당부서에 요청할 수도 있다.
④ 개인정보보호담당자는 개인정보침해사고 처리보고서를 관리하고 처분(징계 등) 결과를 기록한다.

제18조 (침해사고 사후분석) ① 침해사고 처리책임자는 처리보고서 제출 후 30일 이내 근본원인 분석, 교훈 및 예방을 위한 개선대책을 마련하여 개인정보 보호책임자에게 제출한다.
② 개인정보 보호책임자는 개선안을 검토하여 시행 및 변경 여부와 시기를 결정한다.
③ 개인정보 보호책임자는 필요하다고 판단할 경우 사고의 교훈을 적절한 대상을 지정하여 전파 및 교육을 할 수 있다.
④ 개인정보 보호책임자는 개선안 시행, 교훈 전파 및 교육 후 그 성과를 검토한다.

제5장 개인정보침해사고의 관리

제19조 (개인정보침해사고의 보고) 개인정보 보호책임자는 1등급 사고의 경우 발생 즉시 및 수시로 그 진행 현황을 총장에게 보고한다.

제20조 (개인정보침해사고의 현황 관리) 개인정보 보호책임자는 개인정보침해사고 현황을 분석하여 추가적인 개선대책이 필요한 경우 개선 대책을 마련하여 시행한다. 개선 대책에는 교육자료 활용 등을 포함할 수 있다.

제21조 (개인정보침해사고 교육훈련) 개인정보 보호책임자는 전 직원에게 연1회 이상 개인

정보침해사과의 유형과 보고 방법을 교육하여야 한다.

제6장 개인정보의 유출·침해시 처리방안

제22조(개인정보유출 통지시기 및 항목) ① 개인정보보호 담당자는 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 개인정보보호담당자는 제1항 제2호의 경우 개인정보 유출 사고가 최초 발생한 시점과 알게 된 시점 사이에 시간적 차이가 있는 경우에는 이에 대한 과실유무를 입증하여야 한다.

③ 개인정보보호담당자는 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

제23조(개인정보유출 통지방법) ① 개인정보보호담당자는 정보주체에게 제22조제1항 각 호의 사항을 통지할 때에는 서면, 전자우편, 모사전송, 전화, 휴대전화 문자전송 또는 이와 유사한 방법을 통하여 5일 이내에 정보주체에게 알려야 한다.

② 개인정보보호담당자는 제1항의 통지방법과 동시에, 홈페이지 등을 통하여 제22조제1항 각 호의 사항을 공개할 수 있다.

제24조 (개인정보 유출 보고 절차) ① 개인정보보호담당자는 정보주체에 관한 개인정보 유출 내용 및 조치결과를 5일 이내에 교육부에 보고하여야 한다. 다만 1만명 이상의 개인정보가 유출된 경우에는 행정자치부장관 또는 개인정보보호법 시행령 제39조제2항 각 호의 전문기관(한국인터넷진흥원, 한국정보화진흥원) 중 어느 하나에 신고하여야 한다.

② 제1항에 따른 신고는 [붙임4] 개인정보 유출신고서를 작성하여 공문으로 신고하여야 한다.

③ 개인정보보호담당자는 전자우편, 모사전송 또는 인터넷 사이트를 통하여 유출 보고 또

는 신고를 할 시간적 여유가 없거나 그 밖에 특별한 사정이 있는 때에는 먼저 전화를 통하여 제22조제1항 각 호의 사항을 신고한 후, [붙임4] 개인정보 유출신고서를 제출할 수 있다.

④ 유출통지는 서면, 전자우편, 팩스, 전화, 문자전송 등의 방법으로 정보주체에게 개별 통지하여야 하며, 1만명 이상 개인정보 유출 시에는 개별 통지와 함께 홈페이지에 유출통지 내용(5개항목)을 7일 이상 게시하여야 합니다.

제25조 (개인정보침해 신고자의 보호) ① 개인정보침해 신고자의 신분은 침해사고 대응에 반드시 필요한 경우 반드시 필요한 담당자 및 권한자에게만 제공되어야 하며 외부로 노출되어서는 아니 된다.

② 개인정보침해 신고자는 어떠한 경우에도 신고로 인해 불이익을 당하는 경우가 없어야 한다.

제26조 (개인정보 침해신고에 대한 대응) 개인정보에 관한 권리 또는 이익을 침해받은 사람은 개인정보침해신고센터에 침해사실을 신고한 경우, 해당기관이 사실의 조사·확인을 통해 필요한 조치를 취하므로 사실조사에 적극 협조하여야 한다.

제27조 (개인정보 침해구제 절차) 개인정보 침해구제 절차는 다음과 같습니다.

- ① 개인정보 침해에 대한 신고(☎118, privacy.kisa.or.kr)
- ② 개인정보침해신고센터의 사실조사(서면, 방문조사 등)
- ③ 사실조사 결과 통보 및 위법 사실 발견시 조치(수사의뢰, 과태료 등)
- ④ 손해배상, 침해행위 중지, 재발방지 등에 대한 분쟁조정 (☎118, privacy.kisa.or.kr)
 - ※ 동일 피해를 입은 정보주체가 50명 이상인 경우 집단분쟁조정 신청 가능
- ⑤ 분쟁조정위원회 자료조사 및 조정안 작성
- ⑥ 조정안 제시(당사자들이 조정안 수용시 재판상 화해의 효력을 갖음)
- ⑦ 분쟁조정이 실패할 경우 민사소송 또는 단체소송 제기 가능(관할 지방법원)
 - ※ 단체소송은 권리침해행위의 금지·중지를 구하는 소송

부 칙

① (시행일) 이 지침은 2016년 4월 10일부터 시행한다.

[붙임5] 침해사고 비상연락망

구분	직책	성명	내선
개인정보보호 책임자	총무처장	조미관	031-280-3560
개인정보보호 담당자	부장	고광모	031-280-3170
침해사고처리책임자	침해사고 발생한 부서 실·처/대학/대학원 장 등		
분야별책임자	침해사고 발생한 부서 담당자		

[별표1] 개인정보침해사고 모의 시나리오

구분	행동 요령	행위자	비고
개인정보 침해사고의 발생	<ul style="list-style-type: none"> ○ 침해가 발생한 것을 인지한 경우 또는 그러한 침해의 발생이 의심되는 경우 지체없이 개인정보보호담당자에게 신고 	전직원	홈페이지 개인정보처리방침의 개인정보침해신고서 다운 및 작성
개인정보 침해사고의 접수	<ul style="list-style-type: none"> ○ 개인정보보호담당자는 개인정보침해사고를 접수한 경우 “개인정보 침해사고 관리대장”에 사고 접수를 기록한다. ○ 개인정보보호담당자는 접수 후 지체 없이 개인정보보호책임자에게 보고한다. 	개인정보 보호담당자	1등급 침해사고의 경우 발생 그 즉시 및 수시로 총장에게 보고
개인정보 침해사고 대응팀 구성	<ul style="list-style-type: none"> ○ 노출 또는 제공된 정보의 종류에 따라, 발생 부서의 분야별책임자로 침해사고 처리책임자를 지정하고 개인정보침해사고 대응팀을 구성한다. 	개인정보 보호책임자	2,3등급 침해의 경우 개인정보 보호책임자는 침해사고처리책임자와 협의하여 개인정보침해사고 대응팀을 구성하지 않을 수 있다. 개인정보 보호담당자는 개인정보가 유출된 경우에는 개인정보 침해 통지 및 조치 결과를 지체 없이 교육부에 공문으로 신고하여야 한다.
개인정보 침해사고의 분석	<ul style="list-style-type: none"> ○ 침해의 규모, 경위, 방법, 원인 및 관련자를 조사 ○ 필요시 개인정보침해사고 대응팀 또는 개인정보보호책임자가 승인한 외부 전문가의 지원을 받아 증거자료를 수집한다. ○ 개인정보 유출사실을 인지하였을 경우 지체 없이 해당 정보주체에게 관련 사실을 통지한다. 	침해사고 처리책임자	

구분	행동 요령	행위자	비고
개인정보 침해사고의 대응 및 복구	<ul style="list-style-type: none"> 1등급의 경우 침해사고 처리책임자는 해당 개인정보를 파기 또는 회수하기 위한 조치를 취한다. 2등급의 경우 침해사고 책임자는 해당 개인정보를 파기, 회수 또는 복구하기 위한 조치를 취하거나 정보주체의 사후 동의를 받아 근거를 마련한다. 3등급의 경우 침해사고 처리책임자는 해당 개인정보를 적절히 보호하거나 파기하기 위한 조치를 취한다. 침해사고 처리책임자는 즉각적 조치가 가능한 경우 재발방지 조치를 취한다. 	침해사고 처리책임자	
개인정보 침해사고의 종료	<ul style="list-style-type: none"> 침해사고 처리책임자는 개인정보침해사고 처리보고서를 작성하여 개인정보보호책임자에게 제출한다. 개인정보보호책임자는 개인정보침해사고 처리보고서를 검토하고 승인한다. 개인정보보호책임자는 개인정보침해 관련자에 대한 처분(징계 등)을 해당부서에 요청한다. 개인정보보호담당자는 개인정보침해사고 처리보고서를 관리하고 처분(징계 등) 결과를 기록한다. 	침해사고 처리책임자 / 개인정보보호책임자 및 담당자	
개인정보 침해사고 사후분석	<ul style="list-style-type: none"> 침해사고 처리책임자는 처리보고서 제출 후 30일 이내 근본원인 분석, 교훈 및 예방을 위한 개선대책을 마련하여 개인정보보호책임자에게 제출한다. 	침해사고 처리책임자	

4. 개인정보처리시스템 자율점검표

□ 개인정보처리 일반사항 점검표 (년 월 일)

법조항	항목	세부 점검 내용	Y	N	해당 없음	개선기한 (N 해당 시)
제26조	10-1	위탁 시 필수사항(7) 포함 한 문서(계약서)에 의한 계약 여부 * 7개 : 목적외 처리금지, 기술·관리적보호조치, 목적·범위, 재위탁제한, 접근제한 등 안전조치, 관리·감독사항, 손해배상책임				
제26조	10-2	위탁업무의 내용과 수탁자(위탁받아 처리하는 자)를 공개하고 있는가?				
제29조	11-1-1	개인정보의 안전한 처리를 위한 내부관리계획 수립되어 있는가?				
제29조	11-1-2	내부관리계획의 필수 반영사항(4개*) 포함 여부 * 5개 : 보호책임자 지정, 보호책임자/취급자의 역할·책임, 안전성확보조치, 취급자교육,수탁자에 대한 관리·감독				
제29조	11-6-1	전산실, 자료보관실 등 물리적 보관 장소에 대한 출입통제 절차를 수립·운영 하고 있는가?				
제29조	11-6-2	개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소 보관 여부				
제30조	12-1	개인정보 처리방침의 수립 여부				
제30조	12-2	개인정보처리방침에 필수 항목(8개*) 포함 여부 * 8개 : 처리 목적, 처리 및 보유기간, 제3자 제공 사항(해당 시), 위탁 사항(해당 시), 정보주체 권리·의무 및 행사방법, 처리 항목, 파기 사항, 안전성 확보 조치 사항				
제30조	12-3	개인정보처리방침을 홈페이지 등에 공개하고 이력관리를 하고 있는가?				
제31조	13-1	개인정보 보호책임자가 지정되어 있는가?				
제32조	14-1	개인정보파일을 운용하는 경우, 개인정보보호종합지원시스템(intra.privacy.go.kr)에 등록하였으며, 개인정보파일의 보유기간은 타당한가?				

□ 개인정보 파일별 점검표

(개인정보 파일명 :)

법조항	항목	세부 점검 내용	Y	N	해당 없음	개선기한 (N 해당 시)
제15조	1-1	개인정보 수집 시(회원가입, 게시판 등), 정보주체의 동의를 받고 있는가?				
제15조	1-2	정보주체 동의 시 필수 고지항목(4개*) 고지 여부				
제15조	1-3	필수 고지항목(4개*) 내용의 적정 여부 * 4개 : 목적, 항목, 보유 및 이용기간, 거부권 및 불이익				
제16조	2-1	목적에 필요한 최소한의 개인정보 수집 여부				
제16조	2-2	최소한 정보 외의 개인정보 수집에 대한 미동의를 이유로 재화 또는 서비스 제공 거부 여부				
제17조	3-1	제3자 제공에 관한 사항을 정보주체에게 알리고 동의를 받는가?				
제17조	3-2	정보주체 동의 시 필수 고지항목(5개*) 고지 여부				
제17조	3-3	필수 고지항목(5개*) 내용의 적정 여부 * 5개 : 제공받는 자, 목적, 항목, 보유 및 이용기간, 거부권 및 불이익				
제18조	4-1	개인정보 목적 외 이용·제공 근거				
제18조	4-2	동시에 의한 목적 외 이용, 목적 외 제3자 제공 시 필수 고지항목(5개*) 고지 여부				
제18조	4-3	필수 고지항목(5개*) 내용의 적정 여부 * 5개 : 제공받는 자, 목적, 항목, 보유 및 이용기간, 거부권 및 불이익				
제21조	5-1	보유기간 경과, 처리 목적(제공받은 경우 제공받은 목적) 달성 후 지체 없이 개인정보 파기 여부				
제21조	5-2	법령에 따라 보존할 경우 별도 분리 보관 여부				
제22조	6-1	동의 사항의 구분 동의 여부				
제22조	6-2	동의를 필요한 정보와 동의 없이 처리할 수 있는 정보의 구분 동의 여부				
제22조	6-3	홍보 권유에 활용하기 위한 정보와 그렇지 않은 정보의 구분 동의 여부				
제22조	6-4	선택항목 및 홍보 권유 정보의 미동의를 이유로 재화 또는 서비스 제공 거부 여부				
제22조	6-5	만 14세 미만 아동의 개인정보 수집 시, 법정대리인에게 동의를 받고 있는가?				
제23조	7-1	민감정보 처리 근거				
제24조	8-1	고유식별정보* 처리 근거 * 고유식별정보 : 여권번호, 운전면허번호, 외국인등록번호				
제24조의2	9-1	법에 근거하지 않은 주민등록번호 수집 및 처리 여부				
제24조의2	9-2	주민등록번호 외 회원가입 방법 제공 여부				

□ 개인정보처리 시스템별 점검표

(개인정보처리 시스템명:)

법조항	항목	세부 점검 내용	Y	N	해당 없음	개선기한 (N 해당 시)
제29조	11-2-1	개인정보처리시스템의 중요도(민감도) 및 업무연관성 등을 고려하여 담당자별 차등 접근권한 절차를 마련하는가?				
제29조	11-2-2	전보·퇴직 등 인사 이동으로 취급자가 변경 될 경우 시스템접근 권한을 즉시 변경 또는 말소하는가?				
제29조	11-2-3	접근권한의 부여·변경·말소 내역의 기록 관리 및 최소 3년간 보관하고 있는가?				
제29조	11-2-4	취급자별로 개별 계정 발급 및 계정 미공유 여부				
제29조	11-2-5	비밀번호 작성규칙을 수립하여 개인정보처리시스템에 적용하고 있는가?				
제29조	11-2-6	불법적 접근 및 침해사고 방지를 위한 시스템 설치·운영 여부, 침입 차단(F/W) · 방화(IPS) · 탐지(IDS) 등 접근통제시스템을 설치·운영 하는가?				
제29조	11-2-7	외부에서 정보통신망을 통한 접속 시 가상사설망, 전용선 등 안전한 접속수단 제공 여부				
제29조	11-2-8	본인 확인을 위해 성명, 주민등록번호를 사용할 수 있는 경우에도 정보주체의 추가적인 정보 확인 여부				
제29조	11-2-9	P2P, 웹하드 등 비인가 프로그램, 공유 설정 등에 대한 접속 차단을 실시하고 있는지 여부				
제29조	11-2-10	고유식별번호 처리 시 연 1회 이상 취약점 점검 실시 여부				
제29조	11-2-11	업무용 모바일 기기에 비밀번호 설정 여부				
제29조	11-3-1	고유식별정보, 비밀번호 및 바이오정보를 정보통신망을 통하여 송·수신하거나 보조저장매체를 통하여 전달 시 암호화 조치 여부				
제29조	11-3-2	비밀번호 및 바이오정보의 저장 시 암호화 조치 여부(단, 비밀번호의 경우 일방향 암호화)				
제29조	11-3-3	고유식별정보의 인터넷과 내부망의 중간지점(DMZ) 저장 시 암호화 조치 여부				
제29조	11-3-4	고유식별정보를 내부망에 저장 시 암호화 조치 또는 그에 상응하는 조치 적용 여부				

법조항	항목	세부 점검 내용	Y	N	해당 없음	개선기한 (N 해당 시)
제29조	11-3-5	고유식별정보, 비밀번호 및 바이오정보를 암호화하여 저장 시 안전한 암호알고리즘 사용 여부 확인				
제29조	11-3-6	고유식별정보를 업무용 컴퓨터 또는 모바일 기기에 저장시 안전한 암호화 알고리즘 사용 여부 확인				
제29조	11-4-1	취급자의 접속기록을 최소 6개월 이상 보관·관리 여부				
제29조	11-4-2	접속기록의 항목(4개*)이 적정한지 여부 * 4개 : ID, 날짜 및 시간, 접속자 IP 주소, 수행업무 (열람, 수정, 삭제, 인쇄, 입력 등)				
제29조	11-4-3	개인정보처리시스템의 접속기록 점검 및 후속조치를 정기별로 1회 이상 수행 하는가?				
제29조	11-4-4	접속기록이 위·변조 및 도난, 분실되지 않도록 접속기록을 안전하게 보관 여부				
제29조	11-5-1	보안프로그램의 설치·운영 여부-개인정보를 처리하는 시스템·업무용컴퓨터에 백신소프트웨어를 설치·운영 하는가?				
제29조	11-5-2	보안 프로그램의 자동 업데이트 또는 일 1회 이상 업데이트 실시 여부				

5. 개인정보처리시스템 자율점검 가이드라인

1 개인정보의 수집·이용 동의(법 제15조)

□ 세부점검항목(표)

분 야	세부 점검 항목	양호	개선 필요	해당 없음
제 15조(개인정보의 수집·이용 동의)	1-1. 개인정보 수집·이용 근거			
	1-2. 정보주체 동의 시 필수 고지항목(4개) 고지 여부			
	1-3. 필수 고지항목(4개) 내용의 적정 여부 * 4개 : 목적, 항목, 보유 및 이용기간, 거부권 및 불이익			

□ 점검 방법 및 평가 기준

1-1. 개인정보 수집·이용 근거

○ 개인정보 수집·이용 근거에 따라 정보주체로부터 개인정보를 수집하는지 확인

※ 다음 '개인정보 수집·이용 근거'를 참조하여 ①~⑥ 중 해당하는 숫자를 양호에 체크 단, ①~⑥에 해당하지 않고 개인정보를 수집할 경우 개선필요에 체크

< 개인정보 수집·이용 근거 >

- 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 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우
- ⑤ 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
- 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.

1-2. 정보주체 동의 시 필수 고지항목(4개) 고지 여부

- ※ 앞의 '1. 개인정보 수집·이용 근거 항목'에서 ①을 선택하지 않았을 경우 "해당없음"에 체크
- 정보주체의 동의를 받고 개인정보를 수집·이용하는 경우 필수 고지항목 4개를 고지하고 동의 받는지를 확인

< 동의 여부 획득 시 필수 고지사항 >

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 경우 그 불이익의 내용

- ☞ 정보통신망법에 따라 ①~③번은 고지하나, 상당수 홈페이지에서 ④를 고지하지 않고 있음, 또한 개인정보처리방침 전체를 고지하면서 ④가 포함되지 않은 상태로 고지하는 사례 다수 있음

1-3. 필수 고지항목(4개) 내용의 적정 여부

- ※ 앞의 '1. 개인정보 수집·이용 근거 항목'에서 ①을 선택하지 않았을 경우 "해당없음"에 체크
- 정보주체의 동의를 받고 개인정보를 수집·이용하는 경우 필수 고지항목(4개)의 내용이 적정한지 확인
 - 개인정보의 수집·이용 목적이 적정한지 여부 확인
 - 수집하려는 개인정보의 항목과 보유 및 이용기간 설정이 수집 목적 달성을 위해 적합하게 설정되었는지 여부 확인
 - 동의 거부 시 불이익 사항을 적시 하는 경우 그 적정성 확인
- ※ 필수항목, 선택항목에 따른 수집 목적을 명확히 하고, 목적 달성을 위해 불필요한 수집항목과 보유기간 등은 수집·이용하는 목적에 맞게 조정 필요
- ☞ '수집하려는 개인정보 항목'에서 성명이라고 고지하고 회원정보 입력 시 이름을 수집하는 경우(유사한 내용이라도 고지 시 명칭과 수집 시 명칭이 일치해야 함)
- ☞ '보유 및 이용 기간' 고지 시 구체적 보유기간을 명시하지 않고 "이용목적 달성 시 까지 보관"이라고 고지하는 경우

2 최소 수집 및 서비스 제공 거부(법 제16조)

□ 세부점검항목(표)

분 야	세부 점검 항목	양호	개선 필요	해당 없음
제 16조(최소 수집 및 서비스 제공 거부)	2-1. 목적에 필요한 최소한의 개인정보 수집 여부			
	2-2. 최소한 정보 외의 개인정보 수집에 대한 미동의를 이유로 재화 또는 서비스 제공 거부 여부			

□ 점검 방법 및 평가 기준

2-1. 목적에 필요한 최소한의 개인정보 수집 여부

- 정보주체로부터 수집하는 필수정보가 목적 달성을 위해 반드시 수집하여야 하는 최소한의 개인정보인지 여부 확인
- ※ 최소한의 개인정보 수집 여부에 대한 입증 책임은 개인정보처리자가 부담

2-2. 최소한 정보 외의 개인정보 수집에 대한 미동의를 이유로 재화 또는 서비스 제공 거부 여부

- 정보주체의 동의 획득 시 최소한의 정보(필수정보) 외의 개인정보 수집에 동의하지 않는다는 이유로 회원 가입 또는 기본적인 서비스 제공이 불가능한지 여부 확인
- ※ 동의하지 않는다는 이유로 회원 가입 또는 서비스 제공이 불가능할 경우, 개선 필요에 체크
 - 특히, 홈페이지 회원 가입 시 필수정보가 아닌, 선택정보로 되어 있는 개인정보를 입력하지 않을 경우 회원가입이 불가능한지 확인
- ☞ 홈페이지에서 선택 사항에 대한 동의 체크를 하지 않으면 다음으로 넘어가지 않은 사례 있음

3 개인정보의 제공(법 제17조)

□ 세부점검항목(표)

분야	세부 점검 항목	양호	개선 필요	해당 없음
제 17조(개인정보의 제공)	3-1. 개인정보 제3자 제공 근거			
	3-2. 정보주체 동의 시 필수 고지항목(5개)* 고지 여부			
	3-3. 필수 고지항목(5개)* 내용의 적정 여부 * 5개 : 제공받는 자, 목적, 항목, 보유 및 이용기간, 거부권 및 불이익			

□ 점검 방법 및 평가 기준

3-1. 개인정보 제3자 제공 근거

- 개인정보 제공 근거에 따라 정보주체의 개인정보를 제3자에게 제공하는지 여부를 확인
- ※ 다음 '개인정보 제공 근거'를 참조하여 ①~④ 중 하나의 숫자를 양호에 체크
만일, ①~④에 해당하지 않고 개인정보를 제공할 경우 개선필요에 체크
- ※ 고유식별정보, 민감정보의 경우 법령 상 제공하여 처리할 수 있는 규정이 있는 경우 동의 없이 제공 가능하며, 그렇지 않은 경우에는 동의 받고 제공할 수 있음
다만, 고유식별정보 중 주민등록번호는 법령 규정 외에는 처리 할 수 없음

< 개인정보 제공 근거 >

- 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 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우

3-2. 정보주체 동의 시 필수 고지항목(5개) 고지 여부

- ※ 앞의 '3-1. 개인정보 제3자 제공 근거'에서 ①을 선택하지 않았을 경우 해당없음에 체크
- 정보주체의 동의를 통해 개인정보를 제3자에게 제공하는 경우 필수 고지항목(5개)을 고지하고 동의를 받는지 여부를 확인

< 동의 여부 획득 시 필수 고지사항 >

- ① 개인정보를 제공받는 자
- ② 개인정보를 제공받는 자의 개인정보 이용 목적
- ③ 제공하는 개인정보의 항목
- ④ 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간
- ⑤ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우 그 불이익의 내용

- ☞ 홈페이지에서 제공 동의 획득 시 ⑤번에 대한 고지 없이 동의 받는 사례 있음

3-3. 필수 고지항목(5개) 내용의 적정 여부

- ※ 앞의 '3-1. 개인정보 제3자 제공 근거'에서 ①을 선택하지 않았을 경우 해당없음에 체크
- 온라인 회원 가입 서식과 홈페이지 게시판, 기타 서식을 통해 개인정보 제3자 제공의 동의 획득 시 고지항목(5개)의 적정 여부를 확인
 - 개인정보를 제공받는 자가 모두 포함되어 있는지 여부 확인
 - 제공받는 자의 개인정보 이용목적이 적정한지 여부 확인
 - 제공하려는 개인정보의 항목과 제공받는 자의 보유 및 이용기간 설정이 이용 목적 달성을 위해 불가피하게 설정되었는지 여부
 - 동의 거부 시 불이익 사항을 적시 하는 경우 그 적정성 확인
- ※ 법령 상 규정 또는 의무 이행을 위해 제공하는 경우 동의 획득하지 않고 제공할 수 있음, 다만, 법령에서 정한 목적 및 범위 내에서만 처리해야하며, 제공하는 사항에 대해 개인정보처리방침을 통해 공개해야 함
- ☞ 법령 상 정한 목적 및 범위를 초과하여 이용제공 하는 경우 처벌 받을 수 있음

4 개인정보의 이용·제공 제한(법 제18조)

□ 세부점검항목(표)

분 야	세부 점검 항목	양호	개선 필요	해당 없음
제 18조(개인정보의 이용·제공 제한)	4-1. 개인정보 목적 외 이용·제공 근거			
	4-2. 동의에 의한 목적 외 이용, 목적 외 제3자 제공 시 필수 고지항목(5개) 고지 여부			
	4-3. 필수 고지항목(5개) 내용의 적정 여부 * 5개 : 제공받는 자, 목적, 항목, 보유 및 이용기간, 거부권 및 불이익			

□ 점검 방법 및 평가 기준

4-1. 개인정보 목적 외 이용·제공 근거

- 「개인정보 목적 외 이용 및 제3자 제공 근거」에 따라 정보주체의 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는지 확인
- ※ 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고 다음 '개인정보 목적 외 이용 및 제3자 제공 근거'에 해당하는 경우 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있음. 다만, ⑤~⑨까지의 경우 공공기관의 경우로 한정함
- ※ 다음 '개인정보 목적 외 이용 및 제3자 제공 근거'를 참조하여 ①~⑨ 중 하나의 숫자를 양호에 체크
만일, ①~③에 해당하지 않고 개인정보를 목적 외 이용하거나 이를 제3자에게 제공할 경우 개선필요에 체크

< 개인정보 목적 외 이용 및 제3자 제공 근거 >

- ① 정보주체로부터 별도의 동의를 받은 경우
- ② 다른 법률에 특별한 규정이 있는 경우

- ③ 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의

4-2. 동의에 의한 목적 외 이용, 목적 외 제3자 제공 시 필수 고지항목(5개) 고지 여부

- ※ 앞의 '4-1. 개인정보 목적 외 이용 및 제3자 제공 근거'에서 ①을 선택하지 않았을 경우 해당없음에 체크

- 정보주체의 동의에 의한 목적 외 이용 및 제3자 제공 시 필수 고지항목(5개)을 고지하고 동의 받는지 여부를 확인

< 동의 여부 획득 시 필수 고지사항 >

- ① 개인정보를 제공받는 자
- ② 개인정보의 이용목적(제공 시 제공받는 자의 개인정보 이용 목적)
- ③ 이용 또는 제공하는 개인정보의 항목
- ④ 개인정보의 보유 및 이용기간(제공 시 제공 받는 자의 보유 및 이용 기간)
- ⑤ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우 그 불이익의 내용