

강남대학교 개인정보 내부관리계획

2019년 11월

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

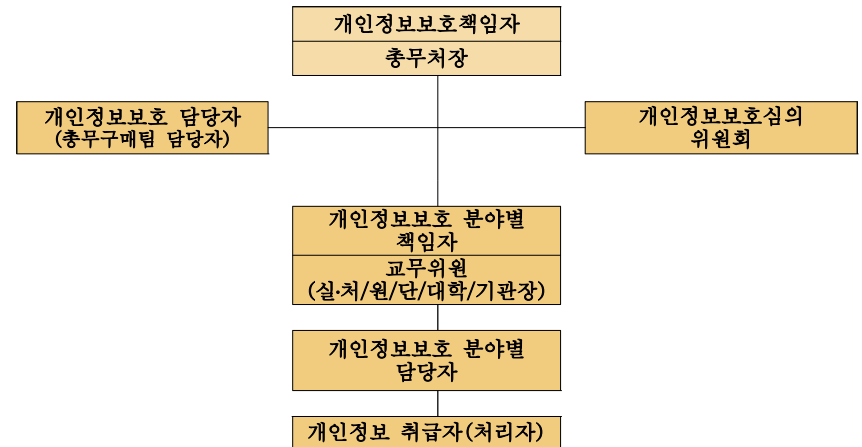
- “개인정보”란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.

- ▶ 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 사용자계정을 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: Ipin, 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 6개월 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

VI 수탁자에 대한 관리 및 감독에 관한 사항

1 강남대학교 위탁사업 현황

구분	위탁업무	수탁업체명	취급항목	관리부서
1	전자출결	㈜씨디시스템	성명, 학번(사번), 수업현황, 수강현황	교무팀
2	종합정보시스템	㈜에듀씨앤에스	이름, 집주소, E-Mail, 집연락처, 핸드폰(연락처), 생년월일, 주민번호, 학번, 학과, 학년, 성별, 전공, 학점, 평점, 국적	전산정보원
3	원서접수대행	㈜유웨이어플라이	이름, 주민번호, 수험번호, 전형명, 지원학과, 전화번호, 휴대전화번호, 추가전화번호, 주소, 재학/출신 고교명, 졸업(예정)년도, 계좌번호, 이메일	입학전형관리팀, 대학원교학팀
4	등록금수납대행	㈜유웨이어플라이	성명, 수험번호	회계경리팀
5	학생역량관리시스템	㈜포도소프트웨어	학과, 학번, 성명	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 녹취 중립	엠앤씨에이프로	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

14	주차관리대행	파킹클라우드	성명, 핸드폰, 차량번호	안전시설팀
15	학생부종합전형 평가시스템	포에듀	이름, 주민번호, 수험번호, 전형명, 지원학과, 재학/출신 고교명, 졸업(예정)년도	입학전형관리팀

※ 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

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 기록·관리	- '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 유·노출, 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 대응방안"은 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 피해를 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 ②KERIS 개인정보보호부 ③침해신고 ④상시모니터링
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	

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 피해를 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

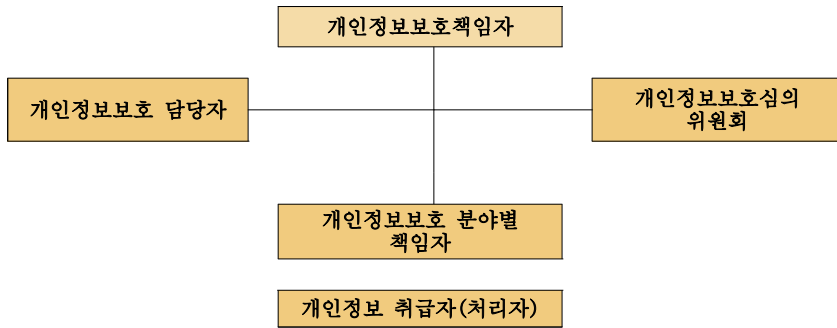
- 외부 침투에 의한 유출 사고 확인
 - 개인정보 보호담당자는 외부침투(해킹 등)에 의한 개인정보 유출사실 확인
 - 사이버공격 대응절차에 따른 경계단계별 대응반 가동 상태 확인

- 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

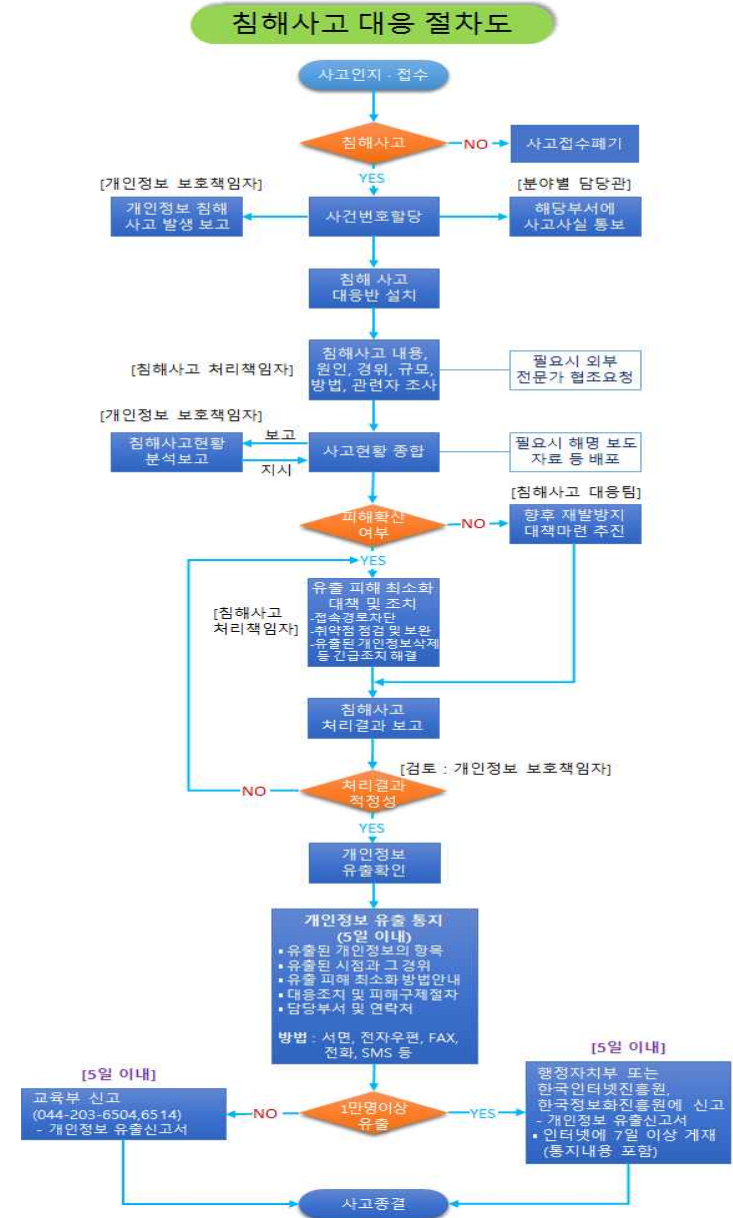
□ 침해사고 대응반 조직체계



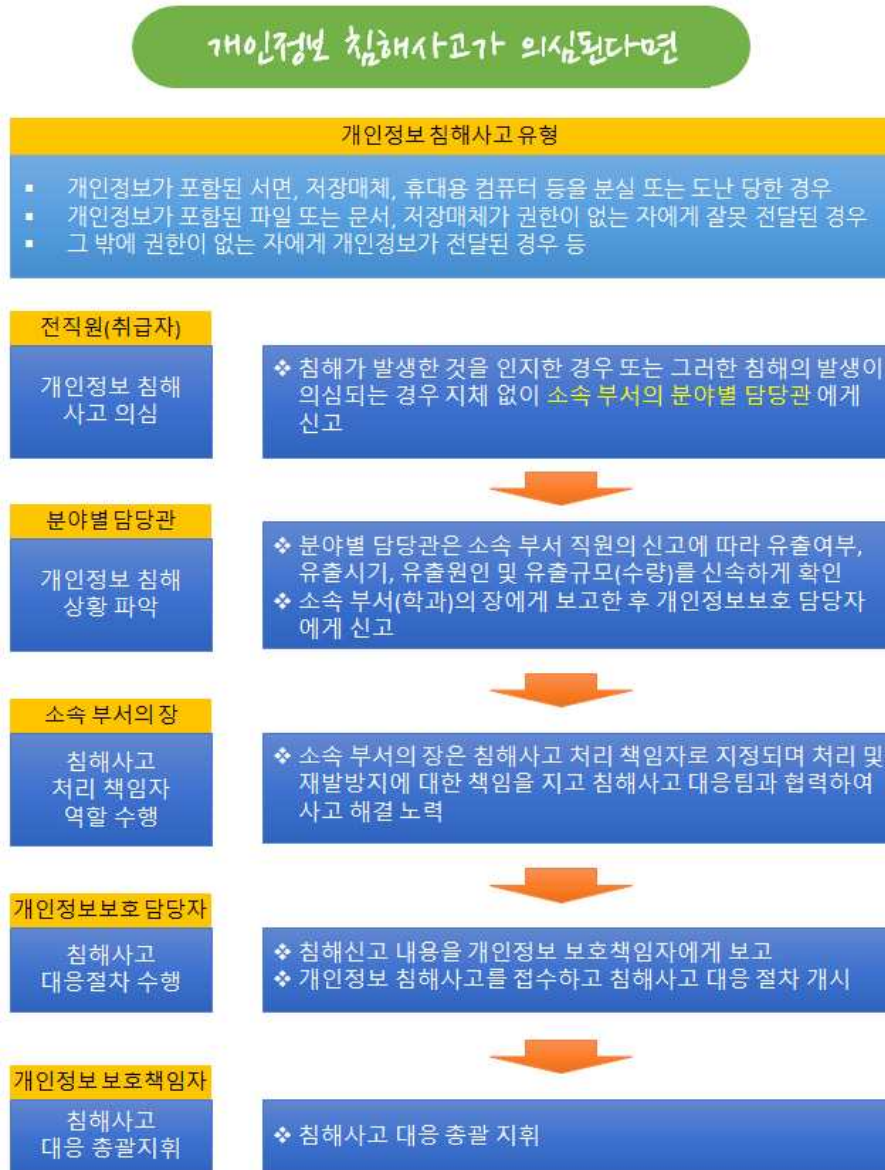
□ 역할

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 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 통합관제 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

정보침해사고의 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.

[붙임1] 개인정보침해사고 관리대장

접수		신고개요	등급	처리유형	종결일자	처리내용	비고
일시	신고자 유형						

- * 일시는 접수 일시를 기록
- * 신고자 유형은 직원/고객으로 구분
- * 신고 개요는 신고 내용을 개록
- * 등급은 1/2/3 등급으로 구분
- * 처리유형은 사실 확인 중/ 상담 및 자료제공/ 타기관 이송/ 위법성 통보/ 수사 의뢰/ 법 위반 확인 불가/ 기타(징계위원회 회부)로 구분
- * 정결일자는 개인정보침해사고 처리보고서 접수일을 기준으로 기록
- * 처리내용은 처분 유형을 사법처리(징역, 벌금, 추징, 재판계류중, 수사중)/ 징계 처분(파면, 해임, 정직, 강봉, 견책, 기타)로 구분
- * 비고란에는 처리보고서 문서번호를 기록

[붙임2] 개인정보침해사고 처리보고서

보고일자			문서번호	
침해 신고 / 접수 정보				
침해등급	<input type="checkbox"/> 1등급	<input type="checkbox"/> 2등급	<input type="checkbox"/> 3등급	침해대상정보 <input type="checkbox"/> 일반 개인정보 <input type="checkbox"/> 주민등록번호 <input type="checkbox"/> 계좌번호
접수일시			신고일자	
침해사고 처리책임자			신고자 연락처	
신고 내용				
대응 과정	일시	대응활동		
침해 내용	확인된 침해 정보의 세부사항, 규모 및 침해 방법(노출, 외부자 제공, 수집, 접근, 분석, 이용, 내부자 제공, 불법 저장, 불안정한 저장, 파괴, 비파괴 등 세부사항)			
침해 발생 경위				
관련자				
침해 발생 원인				
증거자료				
복구 및 재발방지 조치				
처분				

[붙임3] 개인정보 침해사실 신고서

신고인	성명		
	생년월일		
	연락처	전화번호(핸드폰)	
		전자우편	
주소			
접수부서	부서명		
	연락처	전화번호	
		주소	
신고내용			
위와 같이 개인정보침해 사실을 신고 합니다			
붙임 :			
년 월 일 신고인 : (서명 또는 인)			

[붙임4]

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

[붙임5] 침해사고 비상연락망

구분	직책	성명	내선
개인정보보호 책임자	총무처장	조민관	280-3560
개인정보보호 담당자	과장	고광모	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 : 목적의 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, 개인정보보호종합 지원시스템(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 반기별로 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)

분야	세부 점검 항목	양호	개선 필요	해당 없음
제15조(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)

분 야	세부 점검 항목	양호	개선 필요	해당 없음
제17조(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)

분야	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, ①~⑨에 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 이익을 위하여 필요하다고 인정되는 경우
- ④ 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우
- ⑤ 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우
- ⑥ 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우
- ⑦ 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우
- ⑧ 법원의 재판업무 수행을 위하여 필요한 경우
- ⑨ 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우

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

4-3. 필수 고지항목(5개) 내용의 적정 여부

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

- 정보주체의 동의에 의한 목적 외 이용 및 제3자 제공하는 경우 필수 고지항목(5개)의 내용이 적정한지
 - 개인정보를 제공받는 자가 모두 포함되어 있는지 여부 확인
 - 제공받는 자의 개인정보 이용 목적이 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

5 개인정보의 파기(법 제21조)

□ 세부점검항목(표)

분 야	세부 점검 항목	양호	개선 필요	해당 없음
제21조(개인정보의 파기)	5-1. 보유기간 경과, 처리 목적(제공받은 경우 제공받은 목적) 달성 후 지체 없이 개인정보 파기 여부			
	5-2. 법령에 따라 보존할 경우 별도 분리 보관 여부			

□ 점검 방법 및 평가 기준

5-1. 보유기간 경과, 처리 목적(제공받은 경우 제공받은 목적) 달성 후 지체 없이 개인정보 파기 여부

- 개인정보(파일)의 당초 수집목적이 달성되었거나, 보유기간이 경과된 경우에는 지체 없이(보유기간 종료일로부터 5일 이내) 파기하는지 여부 확인
 - 다만, 법령에 따라 보존이 필요한 경우에는 법령에 명시된 기간 동안 보존 할 수 있음
 - ※ 법령에 따라 보존 필요 시 기존 개인정보(파일)과 분리하여 보관하여야 함
 - ☞ 수집 목적이 달성되고, 보유기간이 경과된 후에도 보관 중인 경우 사례 흔함

5-2. 법령에 따라 보존할 경우 별도 분리 보관 여부

- 계약종료 및 탈퇴 등을 이유로 해당 정보주체의 개인정보를 삭제해야하나, 법령에 따라 보존이 필요한 경우 파기시점이 도래하지 않은 개인정보들과 분리(다른 table에 분리)하여 보관하는지 확인
 - 접근권한은 필수 요원(소송 담당자 등)에게만 부여해야 함

- ☞ 법령에 따라 분리 보관한다는 의미는 소송, 민원 등 특정한 상황이 아니면 접근할 필요가 없다는 것이며, 파기 시 삭제하지 않고 단순히 테이블 필드에 플래그 형태로 남기는 사례 있음
- ☞ 법령에 따라 보존하여야 하는 경우로는 전자상거래 거래기록 등이 있음

6 동의를 받는 방법(법 제22조)

□ 세부점검항목(표)

분 야	세부 점검 항목	양호	개선 필요	해당 없음
제22조 (동의를 받는 방법)	6-1. 동의 사항의 구분 동의 여부			
	6-2. 동의가 필요한 정보와 동의 없이 처리할 수 있는 정보의 구분 동의 여부			
	6-3. 홍보 권유에 활용하기 위한 정보와 그렇지 않은 정보의 구분 동의 여부			
	6-4. 선택항목 및 홍보 권유 정보의 미동의를 이유로 재화 또는 서비스 제공 거부 여부			
	6-5. 만 14세 미만 아동의 개인정보를 처리 시, 법정대리인의 동의 여부			

□ 점검 방법 및 평가 기준

6-1. 동의 사항의 구분 동의 여부

- 동의의 내용과 의미를 명확하게 인지한 상태에서 동의 여부를 결정할 수 있도록 통상의 동의*와 구분해서 동의 받고 있는지 여부 확인

*개인정보 수집·이용 동의(제15조 제1항 제1호)

< 구분 동의가 필요한 경우 >

- ① 제3자 제공 동의(제17조 제1항 제1호)
- ② 국외 제3자 제공 동의(제17조 제3항)
- ③ 목적 외 이용·제공 동의(제18조 제2항 제1호)
- ④ 마케팅 목적 처리 동의(제22조 제3항)
- ⑤ 법정대리인의 동의(제22조 제5항)
- ⑥ 민감정보의 처리 동의(제23조 제1항 제1호)
- ⑦ 고유식별정보 처리 동의(제24조 제1항 제1호)

☞ 위 7가지 동의 사항은 개인정보 수집에 따른 기본동의와 별도로 각각 구분하여 동의를 받아야 하는 사항이나, 일반동의만 1회 받는 사례 있음

6-2. 동의가 필요한 정보와 동의 없이 처리할 수 있는 정보의 구분 동의 여부

- 정보주체의 동의가 필요 없는 개인정보와 정보주체의 동의가 필요한 개인정보를 구분하는지 확인

< 동의가 필요 없는 개인정보 >

- ① 계약의 체결 및 이행을 위해 필수적인 정보
- ② 급박한 생명·신체·재산상 이익보호를 위해 필요한 정보
- ③ 법령상 의무 준수를 위해 불가피한 정보
- ④ 개인정보처리자의 정당한 이익을 위해 필요한 정보 등

- 고유식별정보 및 민감정보의 경우에는 계약의 체결 이행 등을 위해 필요하다고 해도 제24조, 제23조에 의거, 별도 동의 받거나 관련 법령에 의해 처리를 허용하고 있는지 여부 확인
- 개인정보처리자가 자신의 정당한 이익을 위해 동의 없이 처리한 경우 개인정보처리자가 이를 입증*할 수 있는지 확인

* 동의 없이 처리할 수 있는 개인정보라는 입증은 개인정보처리자가 해야하며, 입증하지 못하는 경우 동의 받지 않고 수집하는 것으로 처벌될 수 있음

※ 대부분 기관에서 동의 없이 수집 가능한 경우에도 추후 분쟁 등을 피하거나, 법령상 목적 외에 부가적인 목적 달성을 위해 필수사항에 포함하여 동의를 받고 있음

6-3. 홍보 권유에 활용하기 위한 정보와 그렇지 않은 정보의 구분 동의 여부

- 재화나 서비스를 홍보하거나 판매를 권유하기 위한 동의 획득 시 일반적인 개인정보 동의 여부와 구분하고 있는지 확인

☞ 개인정보 수집 목적에 '신제품 소개 및 안내' 등 홍보 및 마케팅 관련 목적을 기술 하고도, 홍보 및 마케팅 동의를 별도로 구분하여 받지 않고, 일반동의만 받는 사례 있음

6-4. 선택항목 및 홍보 권유 정보의 미동의를 이유로 재화 또는 서비스 제공 거부 여부

- 선택정보를 수집하거나, 홍보 권유를 위한 개인정보 동의에 대해 미동의 이유로 홈페이지 회원 가입 등 기본적인 재화 또는 서비스 제공을 거부하고 있는지 확인

< 기본적인 서비스 제공과 관계없는 동의 사항 >

- ① 선택정보의 처리에 대한 동의
- ② 직접 마케팅에 대한 동의
- ③ 목적외 이용·제공에 대한 동의

☞ 홈페이지에서 마케팅 목적 또는 선택정보 미동의시 회원가입이 안되는 사례 있음

6-5. 만 14세 미만 아동의 개인정보를 처리 시, 법정대리인의 동의 여부

- 개인정보파일의 정보주체들 중 만 14세 미만의 아동이 있을 경우, 해당 아동으로부터 개인정보를 수집 시 법정대리인으로부터 동의를 받았는지 확인

☞ 개인정보처리자는 만 14세 미만 아동의 법정대리인의 동의를 받기 위하여 해당 아동으로부터 직접 법정대리인의 성명·연락처에 관한 정보를 수집할 수 있음

7 민감정보의 처리 제한(법 제23조)

□ 세부점검항목(표)

분 야	세부 점검 항목	양호	개선 필요	해당 없음
제23조(민감정보의 처리 제한)	7-1. 민감정보 처리 근거			

□ 점검 방법 및 평가 기준

7-1. 민감정보 처리 근거

- 민감정보가 포함된 개인정보파일을 처리할 경우, 정보주체에게 별도 동의를 받거나 법령에 근거하였는지 확인

※ 정보주체의 동의에 의해 민감정보를 처리하는 경우 양호에 체크
 법령의 특별한 규정에 따라 민감정보를 처리하는 경우 양호에 ‘罙’ 표시

< 민감정보의 구분 >

① 사상·신념에 관한 정보	② 노동조합·정당의 가입·탈퇴에 관한 정보
③ 정치적 견해에 관한 정보	④ 건강, 성생활에 관한 정보
⑤ 유전자 검사 결과로 얻어진 유전정보	⑥ 범죄경력자료에 해당하는 정보

☞ 민감정보를 수집하면서 구분하여 동의 받지 않고 통상의 동의만 받는 사례 다수 있음

8 고유식별정보의 처리 제한(법 제24조)

□ 세부점검항목(표)

분야 (해당 법 조항)	세부 점검 항목	양호	개선 필요	해당 없음
제24조(고유식별정보의 처리 제한)	8-1. 고유식별정보* 처리 근거 * 고유식별정보 : 여권번호, 운전면허번호, 외국인등록번호			

□ 점검 방법 및 평가 기준

8-1. 고유식별정보 처리 근거

- 고유식별정보(주민등록번호를 제외)가 포함된 개인정보파일을 처리할 경우, 정보주체에게 별도 동의를 받거나 법령에 근거하였는지 확인

※ 정보주체의 동의에 의해 고유식별정보를 처리하는 경우 양호에 체크
법령의 특별한 규정에 따라 고유식별정보를 처리하는 경우 양호에 'Ⓜ' 표시

< 고유식별정보의 범위 >

- ① 주민등록번호* ② 여권번호 ③ 운전면허번호 ④ 외국인등록번호
* '14.8.7일 이후 법령 상 처리가 허용된 경우만 처리 할 수 있으며, 보유하고 있는 정보는 '16.8.6일까지 파기

☞ 고유식별정보를 수집하면서 구분하여 동의받지 않고 통상의 동의만 받는 사례 다수 있음

9 주민등록번호의 처리 제한(법 제24조의2)

□ 세부점검항목(표)

분야 (해당 법 조항)	세부 점검 항목	양호	개선 필요	해당 없음
제24조의2(주민등록번호 처리의 제한)	9-1. 법에 근거하지 않은 주민등록번호 수집 및 처리 여부			
	9-2. 주민등록번호 외 회원가입 방법 제공 여부			

□ 점검 방법 및 평가 기준

9-1. 법에 근거하지 않은 주민등록번호 수집 및 처리 여부

- 법령에서 구체적으로 주민등록번호의 처리를 요구하거나, 허용한 경우에만 주민등록번호를 처리하고 있는지 여부 확인

※ 법령의 특별한 규정에 따라 주민등록번호를 처리하는 경우 양호에 체크
※ 법령 상 처리가 허용된 경우만 처리 할 수 있으며, 보유하고 있는 정보는 '16.8.6일까지 파기

9-2. 주민등록번호 외 회원가입 방법 제공 여부

- 공공기관 및 공공기관 외의 인터넷 홈페이지를 운영하는 자로 전년도말 기준 직전 3개월간 인터넷 홈페이지를 이용자 수가 하루 평균 1만명 이상인 경우

- 인터넷 홈페이지를 통하여 회원으로 가입할 경우 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법(예: I-PIN, 공인인증서, 휴대전화 인증 등)을 제공하고 있는지 확인

10 업무위탁에 따른 처리 제한(법 제26조)

□ 세부점검항목(표)

분 야	세부 점검 항목	양호	개선 필요	해당 없음
제26조(업무위탁에 따른 처리 제한)	10-1. 위탁 시 필수사항(7개) 포함한 문서(계약서)에 의한 계약 여부 * 7개 : 목적외 처리금지, 기술·관리적 보호조치, 목적·범위, 재위탁 제한, 접근제한 등 안전조치, 관리·감독사항, 손해 배상책임			
	10-2. 수탁자 공개 여부			

□ 점검 방법 및 평가 기준

10-1. 위탁 시 필수사항(7개) 포함한 문서(계약서)에 의한 계약 여부

- 개인정보 처리에 관한 업무를 위탁하는 경우 필수사항(7개)을 포함한 문서(계약서)에 의한 계약을 체결하는지 확인
- 보안 약정서, 협약서 등의 형태의 계약 부속서류라 하더라도 필수사항(7개)이 모두 포함되어 있는 경우에는 인정됨

< 위탁계약 시 문서에 포함될 필수사항 >

- 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

☞ 계약서에 비밀 누설 금지 등의 사항만 포함하고, 필수사항(7개)을 누락한 사례 다수 있음

10-2. 수탁자 공개 여부

- 개인정보의 처리 업무를 위탁하는 경우 수탁자를 인터넷 홈페이지에 위탁하는 업무의 내용과 수탁자를 지속적으로 게재하고 있는지 여부 확인

- 인터넷 홈페이지에 공개할 수 없는 경우 다른 방법으로 공개 필요

< 인터넷 홈페이지가 없는 경우 수탁자 공개 방법 >

- ① 사업장의 보기 쉬운 장소에 게시
- ② 관보 또는 일반일간신문, 일반주간신문 또는 인터넷신문에 실는 방법
- ③ 정보주체에게 배포하는 각종 소식지에 포함하여 연 2회 이상 발행
- ④ 계약서 등에 실어 발급하는 방법

☞ 수탁사를 누락하거나, 업무 단위로 묶어 개별 수탁사를 파악하기 어려운 사례 있음

11-1 안전조치의무 (법 제29조)

□ 세부점검항목(표)

분 야	세부 점검 항목	양호	개선 필요	해당 없음
제29조 (안전조치의무)	1.내부관리계획 수립·시행			
	11-1-1. 내부관리계획 수립·시행 여부 11-1-2. 내부관리계획의 필수 반영사항(5개) 포함 여부 * 5개 : 보호책임자 지정, 보호책임자/취급자의 역할·책임, 안전성 확보 조치, 취급자 교육, 수탁자에 대한 관리·감독			

□ 점검 방법 및 평가 기준

11-1-1. 내부관리계획 수립·시행 여부

○ 개인정보의 안전한 처리를 위한 내부관리계획을 수립·시행하고 있는지 확인

- 내부관리계획이라는 명칭 이외의 다른 명칭(예: 개인정보보호정책 등)으로 수립하여도 점검항목 11-1-2의 사항이 모두 포함되어야 내부관리계획으로 인정됨

11-1-2. 내부관리계획의 필수 반영사항(5개) 포함 여부

○ 내부관리계획을 수립 시 보호책임자 지정 등 필수사항(5)을 모두 반영하여 수립하였는지 확인

< 내부관리계획 필수 항목(5) >

- ① 개인정보 보호책임자 지정에 관한 사항
- ② 개인정보 보호책임자 및 개인정보취급자의 역할·책임에 관한 사항
- ③ 개인정보의 안전성 확보에 필요한 조치에 관한 사항
- ④ 개인정보취급자에 대한 교육에 관한 사항
- ⑤ 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항
- ⑥ 그 밖에 개인정보 보호를 위하여 필요한 사항(예: 개인정보파일 보유기간 등)

11-2 안전조치의무 (법 제29조)

□ 세부점검항목(표)

분 야	세부 점검 항목	양호	개선 필요	해당 없음
제29조 (안전조치의무)	2.접근권한 관리 및 접근 통제	11-2-1. 시스템에 대한 접근권한을 필요 최소한의 범위로 업무 담당자에 따라 차등 부여 여부		
		11-2-2. 전보·퇴직 등 인사이동으로 취급자가 변경될 경우 접근권한 변경 또는 말소 여부		
		11-2-3. 접근권한의 부여·변경·말소 내역의 기록관리 및 최소 3년간 보관 여부		
		11-2-4. 취급자별로 개별 계정 발급 및 계정 미공유 여부		
		11-2-5. 안전한 비밀번호 작성규칙의 수립·적용 여부		
		11-2-6. 불법적 접근 및 침해사고 방지를 위한 시스템 설치·운영 여부		
		11-2-7. 외부에서 정보통신망을 통한 접속 시 가상사설망, 전용선 등 안전한 접속수단 제공 여부		
		11-2-8. 본인 확인을 위해 성명, 주민등록번호를 사용할 수 있는 경우에도 정보주체의 추가적인 정보를 확인		
		11-2-9. P2P, 웹하드 등 비인가 프로그램, 공유 설정 등에 대한 접속 차단 실시 여부		
		11-2-10. 고유식별번호 처리시 연 1회 이상 취약점 점검 실시 여부		
		11-2-11. 업무용 모바일 기기에 비밀번호 설정 여부		

□ 점검 방법 및 평가 기준

11-2-1. 시스템에 대한 접근권한을 필요 최소한의 범위로 업무 담당자에 따라 차등 부여 여부

- 개인정보처리시스템에 대한 접근권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에게 차등 부여하고 있는지 확인
 - 업무 성격에 따라 접근 권한의 팀별, 개인별 차등 부여 여부 확인
- ☞ 개발 초기 시 부여된 관리자 권한, 디폴트 권한 등으로 일괄 부여된 사례 있음

11-2-2. 전보·퇴직 등 인사이동으로 취급자가 변경될 경우 접근권한 변경 또는 말소 여부

- 개인정보취급자의 전보 또는 퇴직 등 인사이동 발생 시 개인정보처리시스템의 접근권한을 즉시 변경 또는 말소하는지 확인
- ☞ 퇴직자의 계정을 삭제하지 않고 남겨 놓은 사례 있음

11-2-3. 접근권한의 부여·변경·말소 내역의 기록관리 및 최소 3년간 보관 여부

- 개인정보취급자의 접근권한 부여 및 전보 또는 퇴직에 따른 변경, 말소에 대한 기록은 최소 3년간 보관하고 있는지 확인
 - ※ 변경 이력을 시스템에 자동으로 남기지 않는 경우 수기로 작성, 관리 여부 확인
- ☞ 권한 변경 이력을 보관하지 않거나, 3년 미만으로 보관하는 사례 있음

11-2-4. 취급자별로 개별 계정 발급 여부 및 계정 미공유 여부

- 개인정보처리시스템에 접속 할 수 있는 사용자 계정을 발급하는

경우, 취급자 별로 한 개의 사용자 계정을 발급하는지 확인

- 사용자 계정(ID)을 다수의 사용자가 공유하는지 여부 확인
- ☞ 업무 편의상 하나의 계정(ID)을 다수의 사용자가 공유하여 사용하는 사례 있음

11-2-5. 안전한 비밀번호 작성규칙의 수립·적용 여부

- 개인정보취급자 또는 정부주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립·적용하는지 확인
- ※ 내부관리계획의 안전성확보 조치 사항으로 포함되어 작성 할 수 도 있으며, 별도 비밀번호 작성규칙을 작성하여 운영할 수 있음

< 안전한 비밀번호 작성 규칙 >

- 최소 길이
 - 최소 10자리 이상 : 영어 대문자, 소문자, 숫자, 특수문자 중 2종류 조합
 - 최소 8자리 이상 : 영어 대문자, 소문자, 숫자, 특수문자 중 3종류 조합
- 추측하기 어려운 비밀번호
 - 일련번호, 전화번호 등 쉬운 문자열이 포함되지 않도록 함
 - 잘 알려진 단어, 키보드 상에서 나란히 있는 문자열이 포함되지 않도록 함
- 주기적 변경 : 비밀번호에 유효기간 설정하고 최소 6개월마다 변경
- 동일 비밀번호 사용 제한 : 2개의 비밀번호를 교대로 사용하지 않음

- ☞ 비밀번호 작성규칙에 불구하고 취급자 등이 시스템 접속 시 반영하지 않은 사례 있음

11-2-6. 불법적 접근 및 침해사고 방지를 위한 시스템 설치·운영 여부

- 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 접근통제시스템*을 설치 운영하는지 확인

* · 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가 받지 않은 접근을 제한하는 시스템(방화벽 등)

· 개인정보처리시스템에 접속한 IP주소 등을 분석하여 불법적인 개인정보 유출 시도를 탐지하는 시스템(IDS 또는 IPS 등)

※ 개인정보처리자가 별도의 개인정보처리시스템을 이용하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우, 접근통제시스템을 적용하지 아니할 수 있음. 단, 이 경우 업무용 컴퓨터 또는 모바일 기기의 운영 체제(OS)나 보안프로그램 등에서 제공하는 접근통제 기능을 이용 가능

☞ 웹호스팅 시 방화벽 등 보안장비 이용에 추가 비용이 들어 설치하지 않은 사례 있음

11-2-7. 외부에서 정보통신망을 통한 접속 시 가상사설망, 전용선 등 안전한 접속수단 제공 여부

○ 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리 시스템에 접속 시 안전한 접속수단(가상사설망(VPN), 전용선 등)을 통해서만 접속하는지 확인

☞ 홈페이지 관리자페이지 접속 시 단순 ID/패스워드로만 접속 가능한 사례 있음

11-2-8. 본인 확인을 위해 성명, 주민등록번호를 사용할 수 있는 경우에도 정보주체의 추가적인 정보를 확인

○ 인터넷 홈페이지에서 다른 법령에 근거하여 정보주체의 본인확인을 위해 성명, 주민등록번호를 사용할 수 있는 경우에도 정보주체의 추가적인 정보를 확인*하여야 함

* 추가적인 정보를 확인하는 방법에는 I-PIN, 공인인증서, 휴대전화, 주민등록증 발급 일자, 전자우편(e-mail) 주소 등이 있음

☞ 성명, 주민등록번호 만을 이용해서 본인확인하는 경우 공격의 대상이 되는 사례 있음

11-2-9. P2P, 웹하드 등 비인가 프로그램, 공유 설정 등에 대한 접속 차단 실시 여부

○ P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 업무용 PC에 조치를 취하고 있는지 확인

○ 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템, 업무용 PC 및 모바일 기기* 등에 조치를 취해야함

* 스마트폰, 스마트패드, 태블릿PC 등

☞ 업무용 모바일 기기의 분실에 따라 개인정보 유출되는 사례 있음

※ 모바일 기기(스마트폰, 스마트패드, 태블릿PC 등)의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 보호조치(비밀번호, 패턴, PIN 등 설정) 필요

○ 「홈페이지 개인정보 노출방지 가이드라인」에서 제시하고 있는 관리적, 기술적 노출방지 대책을 적용하고 있는지 확인

* 개인정보보호포털(<http://www.privacy.go.kr>)의 [자료실-지침자료]에서 확인 가능

☞ 웹서버 설정이 미흡하여 게시판 등에 올린 개인정보가 구글 등에 노출되는 사례 있음

※ 홈페이지 개발 및 운영 단계에서 웹 취약점 점검, 미관리 사이트 및 URL 차단 및 삭제, 관리자 페이지 노출 차단 등의 조치 시행 필요

11-2-10. 고유식별번호 처리시 연 1회 이상 취약점 점검 실시 여부

○ 인터넷 홈페이지를 통해 고유식별정보(주민등록번호, 여권번호, 운전면허번호, 외국인등록번호)를 처리하는 개인정보처리자는 고유식별정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점을 점검하고, 취약점에 대한 개선조치를 취하여야 함

☞ 홈페이지 취약점으로 인해 고유식별정보가 유출되는 사례 있음

11-2-11. 업무용 모바일 기기에 비밀번호 설정 여부

○ 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치*를 하여야 함

* 비밀번호, 패턴, PIN 등을 이용한 화면잠금, 디바이스 암호화, USIM 카드 잠금 설정, 원격 잠금 및 데이터 삭제 등

☞ 업무용 모바일 기기의 분실에 따라 개인정보 유출되는 사례 있음

11-3 안전조치의무 (법 제29조)

□ 세부점검항목(표)

분 야	세부 점검 항목	양호	개선 필요	해당 없음	
제29조 (안전조치의무)	3.개인정보의 암호화	11-3-1. 고유식별정보, 비밀번호 및 바이오정보를 정보통신망을 통하여 송·수신하거나 보조저장매체를 통하여 전달 시 암호화 조치 여부			
		11-3-2. 비밀번호 및 바이오정보의 저장 시 암호화 조치 여부 (단, 비밀번호의 경우 일방향 암호화)			
		11-3-3. 고유식별정보의 인터넷과 내부망의 중간지점(DMZ) 저장 시 암호화 조치 여부			
		11-3-4. 고유식별정보를 내부망에 저장 시 암호화 조치 또는 그에 상응하는 조치 적용 여부			
		11-3-5. 고유식별정보, 비밀번호 및 바이오정보를 암호화하여 저장 시 안전한 암호알고리즘 사용 여부 확인			
		11-3-6. 고유식별정보를 업무용 컴퓨터 또는 모바일 기기에 저장시 안전한 암호화 알고리즘 사용 여부 확인			

□ 점검 방법 및 평가 기준

11-3-1. 고유식별정보, 비밀번호 및 바이오정보를 정보통신망을 통하여 송수신하거나 보조저장매체를 통하여 전달 시 암호화 조치 여부

○ 고유식별정보, 비밀번호 및 바이오정보를 정보통신망을 통하여 내·외부로 송수신하거나 보조저장매체 등을 통해 전달하는 경우에 이를 암호화하는지 확인

☞ 내부망 내에서 송수신되는 고유식별정보는 업무상 필요할 경우 암호화 대상에서 제외할 수 있으나, 비밀번호와 바이오정보는 반드시 암호화해야 함

☞ 암호화 대상인 개인정보를 전용선을 통해 송수신 시, 반드시 암호화할 필요는 없음

- ☞ wire shark 등 프로그램을 통해 전송되는 패킷의 암호화 검사 시 암호화하지 않은 사례 있음
- (붙임) 「네트워크 전송 구간 암호화 여부 검사 방법(WireShark 사용법)」 참고

11-3-2. 비밀번호 및 바이오정보의 저장 시 암호화 조치 여부 (단, 비밀번호의 경우 일방향 암호화)

○ 비밀번호 및 바이오정보*를 저장 시 암호화하는지 확인

*식별 및 인증 등의 고유기능에 사용되는 경우로 한정되며 콜센터 등 일반 민원 상담시 저장되는 음성기록이나 일반 사진 정보는 암호화 대상에서 제외

○ 특히, 비밀번호는 복호화 되지 않도록 일방향 암호화(해시함수)하여 저장하는지 확인

11-3-3. 고유식별정보의 인터넷과 내부망의 중간지점(DMZ) 저장 시 암호화 조치 여부

○ 고유식별정보를 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ)에 저장하는 경우 암호화하여 저장하는지 확인

11-3-4. 고유식별정보를 내부망에 저장 시 암호화 조치 또는 그에 상응하는 조치 적용 여부

○ 내부망에 고유식별정보를 저장하는 경우에는 암호화의 적용여부 및 적용범위를 정하여 시행하고 있는지 확인

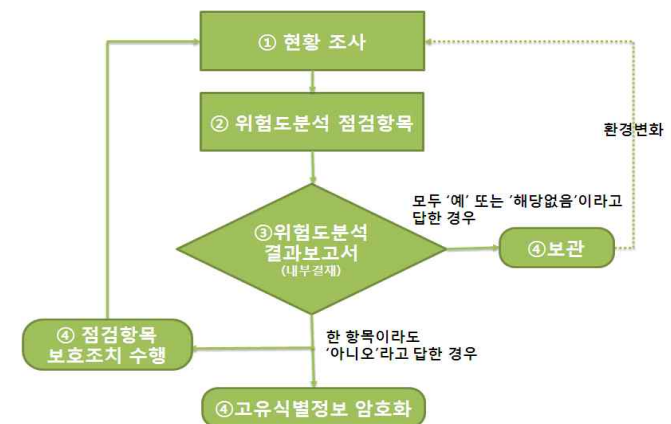
- 영향평가 대상이 되는 공공기관의 경우 개인정보영향평가의 결과에 따라 암호화 적용여부 및 범위를 정할 수 있음
- 영향평가 대상이 되는 공공기관의 경우를 제외하고는 위험도 분석에 따른 결과에 따라 암호화 적용여부 및 범위를 정함

< 개인정보 영향평가의 대상 >

- ① 구축·운용 또는 변경하려는 개인정보파일로서 5만명 이상의 정보주체에 관한 법 제23조에 따른 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일
- ② 구축·운용하고 있는 개인정보파일을 해당 공공기관 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 제33조 제1항에 따른 개인정보영향평가를 받은 후에 개인정보 검색체계 등 개인정보파일의 운용체계를 변경하려는 경우 그 개인정보파일

< 위험도 분석 절차 및 내용 >

- ① 위험도 분석을 위해 개인정보 파일 및 고유식별정보 보유 여부 등 현황조사
- ② 개인정보 파일단위별로 위험도 분석 항목별 점검을 수행
- ③ 위험도 분석 결과보고서를 작성하여 내부결재 후 보관
- ④ 점검 결과에 따라 고유식별정보 암호화 등을 수행



구분	점검항목
DB 및	12. 상시적으로 네트워크를 통한 비인가자의 DB 접근을 통제하고 있습니까?

Application 기반	13. DB서버 내에 불필요한 서비스 포트를 차단하고 있습니까?
	14. 상시적으로 DB 접속자 및 개인정보취급자의 접속기록을 남기고 있습니까?
	15. DB 접속기록을 주기적으로 모니터링하여 통제 하고 있습니까?
	16. DB서버에 접속하는 관리자 PC가 인터넷 접속되는 내부망의 네트워크와 분리되어 있습니까?
	17. 개인정보취급자의 역할에 따라 DB 접근권한을 차등화하여 부여하고 있습니까?
	18. 개인정보취급자의 전보, 이직, 퇴사 등 인사이동 발생 시 지체 없이 DB 접근권한을 변경하고 있습니까?
	19. DB접속자 및 개인정보취급자의 DB 로그인 비밀번호를 최소 3개월마다 변경하고 있습니까?
	20. DB접속자 및 개인정보취급자의 비밀번호 입력 시 5회 이상 연속 입력오류가 발생한 경우 계정 잠금 등 접근을 제한하고 있습니까?
	21. DB 및 DB접속 어플리케이션 서버에 대한 물리적 접근을 인가된 자로 한정하고 있습니까?
	22. DB 및 DB접속 어플리케이션 서버에서 보조기억매체(USB 등) 사용 시 관리자 승인 후 사용하고 있습니까?
	23. DB서버 및 DB접속 어플리케이션 서버에 접속하는 모든 개인정보취급자의 단말기(PC, 노트북 등)의 운영체제 보안패치를 제조사 공지 후 지체 없이 수행하고 있습니까?
	24. HDD등 DB 저장매체의 불용 처리 시(폐기, 양여, 교체 등) 저장매체에 저장된 개인정보는 모두 파기하고 있습니까?
웹(Web) 기반 ※웹사이트 운영시	25. 신규 웹 취약점 및 알려진 주요 웹(Web) 취약점 진단/보완을 년1회 이상 실시하거나, 상시적으로 비인가자에 의한 웹서버 접근, 홈페이지 위·변조 등을 자동으로 차단할 수 있는 보호 조치를 하고 있습니까?
	26. 웹서버 프로그램과 운영체제 보안패치를 제조사 공지 후 지체 없이 수행하고 있습니까?

11-3-6. 고유식별정보를 업무용 컴퓨터 또는 모바일 기기에 저장시 안전한 암호화 알고리즘 사용 여부 확인

- 고유식별정보를 업무용 컴퓨터 또는 모바일 기기에 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용
 - 안전한 암호알고리즘, 암호화 방식 등은 “개인정보 암호화 조치 안내서” 참조
 - * 개인정보보호 종합지원포털(<http://www.privacy.go.kr>)에서 다운로드 가능
- ☞ 안전하지 않은 알고리즘(MD5, SHA-1, 자체 함수제작 등) 및 양방향 암호화 방식으로 암호화한 사례 있음

11-3-5. 고유식별정보, 비밀번호 및 바이오정보를 암호화하여 저장 시 안전한 암호알고리즘 사용 여부 확인

- 개인정보처리시스템에 고유식별정보, 비밀번호, 바이오정보를 암호화하여 저장 시, 안전한 암호알고리즘을 사용해야 함
 - 안전한 암호알고리즘, 암호화 방식 등은 “개인정보 암호화 조치 안내서” 참조
 - * 개인정보보호 종합지원포털(<http://www.privacy.go.kr>)에서 다운로드 가능
- ☞ 안전한 암호알고리즘을 사용하더라도 암호화 키가 잘못 관리되어 유출될 수 있는 경우에는 암호화된 정보들이 유출될 수 있으므로 이를 안전하게 관리하여야 함

11-4 안전조치의무 (법 제29조)

□ 세부점검항목(표)

분 야	세부 점검 항목	양호	개선 필요	해당 없음
제29조 (안전조치의무)	4.접속기록의 보관	11-4-1. 취급자의 접속기록을 최소 6개월 이상 보관·관리 여부		
		11-4-2. 접속기록의 항목(4개)이 적정한지 여부 * 4개 : ID, 날짜 및 시간, 접속자 IP 주소, 수행 업무(열람, 수정, 삭제, 인쇄, 입력 등)		
		11-4-3. 접속기록 정기 점검		
		11-4-4. 접속기록이 위·변조 및 도난, 분실되지 않도록 안전하게 보관하는지 여부		

□ 점검 방법 및 평가 기준

11-4-1. 취급자의 접속기록을 최소 6개월 이상 보관·관리 여부

- 개인정보취급자가 개인정보처리시스템에 접속한 기록을 최소 6개월 이상 보관·관리하고 있는지 확인

☞ 홈페이지 관리자 페이지 접속 시 접속 기록을 남기지 않은 사례 있음

11-4-2. 접속기록의 항목(4개)이 적정한지 여부

- 개인정보처리시스템에 접속 시 필수항목(4)을 남기는지 확인

< 접속기록에 포함되어야 할 필수 항목 >

필수 기록 항목	설 명
① ID	개인정보취급자 식별 정보
② 날짜 및 시간	접속 일시
③ 접속자 IP 주소	접속지 정보
④ 수행 업무	열람, 수정, 삭제, 입력, 인쇄 등

※ 개인정보취급자 1명(Root, Admin 등)이 개인정보처리시스템을 관리하는 경우, 전자적 로그를 남기지 않고, 접속 기록을 수기로 작성하여 상급자의 승인을 받아도 가능

11-4-3. 접속기록 정기 점검

- 개인정보의 유출·변조·훼손 등에 대응하기 위해 개인정보처리시스템의 접속기록 등을 반기별로 1회 이상 점검하는지 여부 확인

11-4-4. 접속기록이 위·변조 및 도난, 분실되지 않도록 안전하게 보관 하는지 여부

- 정기적으로 접속기록 백업을 수행하여 개인정보처리시스템 이외의 별도의 보조저장매체나 별도의 저장장치에 보관하고 있는지 확인
 - 접속기록에 대한 위·변조를 방지하기 위해 CD-ROM 등과 같은 덮어쓰기 방지 매체를 사용하는 것이 바람직함
 - 접속기록을 수정 가능한 매체(HDD 또는 테이프 등)에 백업하는 경우에는 무결성 보장을 위해 위·변조 여부를 확인할 수 있는 정보를 별도의 장비에 보관·관리할 수 있음

11-5 안전조치의무 (법 제29조)

□ 세부점검항목(표)

분 야	세부 점검 항목	양호	개선 필요	해당 없음
제29조 (안전조치의무)	5.보안프로그램 설치·운영	11-5-1. 보안 프로그램의 설치·운영 여부		
		11-5-2. 보안 프로그램의 자동 업데이트 또는 일 1회 이상 업데이트 실시 여부		

□ 점검 방법 및 평가 기준

11-5-1. 보안 프로그램의 설치·운영 여부

- 악성 프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하고 있는지 확인

11-5-2. 보안 프로그램의 자동 업데이트 또는 일 1회 이상 업데이트 실시 여부

- 보안 프로그램의 자동 업데이트 기능을 사용하거나, 또는 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지하고 있는지 확인
 - 악성 프로그램관련 경보가 발령된 경우
 - 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 업데이트를 하고 있는지 확인

☞ 백신프로그램 업데이트 및 OS 최신 패치 확인 시 업데이트를 미실시하는 사례 있음

11-6 안전조치의무 (법 제29조)

□ 세부점검항목(표)

분 야	세부 점검 항목	양호	개선 필요	해당 없음
제29조 (안전조치의무)	6.물리적 접근 방지	11-6-1. 전산실, 자료보관실 등 물리적 보관 장소에 대한 출입통제 절차 수립·운영 여부		
		11-6-2. 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소 보관 여부		

□ 점검 방법 및 평가 기준

11-6-1. 전산실, 자료보관실 등 물리적 보관 장소에 대한 출입통제 절차 수립·운영 여부

- 전산실·자료보관실을 별도로 두고 있는 경우에는 비인가자의 접근으로 인한 개인정보의 절도, 파괴 등의 물리적 위협으로부터 정보자산을 보호하기 위해 출입통제 절차를 수립하는지 확인
 - 비밀번호 기반 출입통제 장치, 스마트카드 기반 출입 통제장치 등 물리적 접근통제 장치를 설치·운영하고 이에 대한 출입 내역을 전자적인 매체 또는 수기문서 대장에 기록하고 있는지 확인

11-6-2. 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소 보관 여부

※ 별도의 개인정보처리시스템을 운영하지 아니하고, 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 해당없음에 체크

- 개인정보가 포함된 서류나 보조기억매체(USB, CD 등) 등은 잠금장치가 부착되어 있는 금고 또는 잠금장치가 있는 캐비닛 등에

안전하게 보관하고 있는지 확인

☞ 개인정보가 포함된 서류 등을 캐비닛에 보관하지 않고 책상에 방치하는 사례 있음

12 개인정보 처리방침의 수립·공개 (법 제30조)

□ 세부점검항목(표)

분 야	세부 점검 항목	양호	개선 필요	해당 없음
제30조(개인정보 처리 방침의 수립·공개)	12-1. 개인정보 처리방침의 수립 여부			
	12-2. 개인정보 처리방침에 필수 항목(8개)* 포함 여부 * 8개 : 처리 목적, 처리 및 보유기간, 제3자 제공 사항(해당 시), 위탁 사항(해당 시), 정보주체 권리·의무 및 행사 방법, 처리 항목, 파기 사항, 안전성 확보 조치 사항			
	12-3. 개인정보 처리방침의 홈페이지 등 공개 여부			

□ 점검 방법 및 평가 기준

12-1. 개인정보 처리방침의 수립 여부

○ 개인정보 처리에 관한 ‘개인정보처리방침’을 수립하고 있는지 확인

12-2. 개인정보 처리방침에 필수 항목(8개) 포함 여부

○ 개인정보처리방침 공개 시 필수 항목을 포함하여 공개하는지 확인

< 개인정보처리 방침 필수 항목 >

- | | |
|-----------------------------|----------------------|
| ① 개인정보의 처리 목적 | ② 개인정보의 처리 및 보유 기간 |
| ③ 개인정보의 제3자 제공에 관한 사항 | ④ 개인정보 처리의 위탁에 관한 사항 |
| ⑤ 정보주체의 권리·의무 및 행사방법에 관한 사항 | |
| ⑥ 처리하는 개인정보의 항목 | ⑦ 개인정보의 파기에 관한 사항 |
| ⑧ 안전성 확보 조치에 관한 사항 | |

12-3. 개인정보 처리방침의 홈페이지 공개 및 이력관리 여부

- ‘개인정보처리방침’을 홈페이지에 공개하고 있으며 변경에 대한 이력관리를 하고 있는지 확인

13 개인정보 보호책임자의 지정 (법 제31조)

□ 세부점검항목(표)

분 야	세부 점검 항목	양호	개선 필요	해당 없음
제31조(개인정보 보호 책임자의 지정)	13-1. 개인정보 보호책임자 지정 여부			

□ 점검 방법 및 평가 기준

13-1. 개인정보 보호책임자 지정 여부

- 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보보호 책임자를 지정하고 있는지 확인

- 교육기관은 다음의 자격 요건에 맞게 지정하고 있는지 확인

< 교육기관 개인정보보호책임자 자격 요건 >

공공 기관		자격 요건
①	시·도교육청	3급 이상 공무원 또는 그에 상당하는 공무원
②	교육지원청	4급 이상 공무원 또는 그에 상당하는 공무원 (과단위 교육지원청은 5급 이상 공무원)
③	초·중·고	교장
④	대학	학무(교무)위원에 상당하는 행정사무를 총괄하는 사람
⑤	그 외의 기관	개인정보 처리 관련 업무를 담당하는 부서의 장

☞ 개인정보파일을 운영하면서 개인정보 보호책임자를 지정하지 않는 사례 있음

14 개인정보파일 등록 및 공개 (법 제32조)

□ 세부점검항목(표)

분 야	세부 점검 항목	양호	개선 필요	해당 없음
제32조(개인정보파일의 등록 및 공개)	14-1. 개인정보파일을 운용하는 경우, 개인정보 보호 종합지원시스템(intra.privacy.go.kr)에 등록 하였으며, 개인정보파일의 보유기간은 타당한가?			

□ 점검 방법 및 평가 기준

14-1. 개인정보파일 등록여부

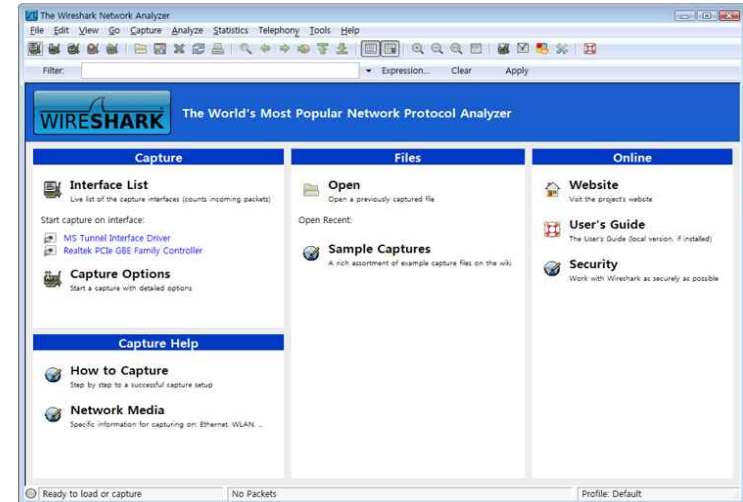
- 기관의 개인정보처리담당자가 운용하고 있는 모든 개인정보파일을 개인정보종합지원시스템(intra.privacy.go.kr)에 등록을 하였는지 확인하고 각 개인정보파일의 보유기간은 타당한지 확인

☞ 보유기간에 대한 근거 없이 영구로 지정하여 보유하고 있는 사례가 있음

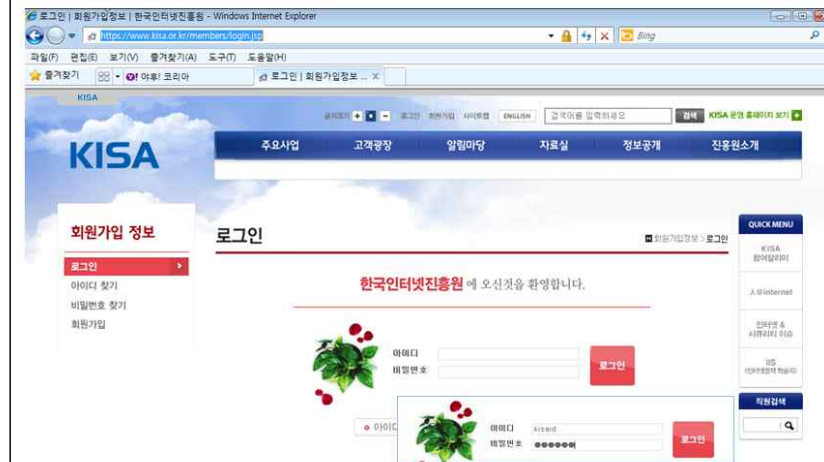
붙임1 네트워크 전송 구간 암호화 여부 검사 방법(wireshark 사용법)

※ WireShark 프로그램은 프리웨어로 인터넷에 검색하여 설치 할 수 있음(출처:KISA)

① WireShark 구동

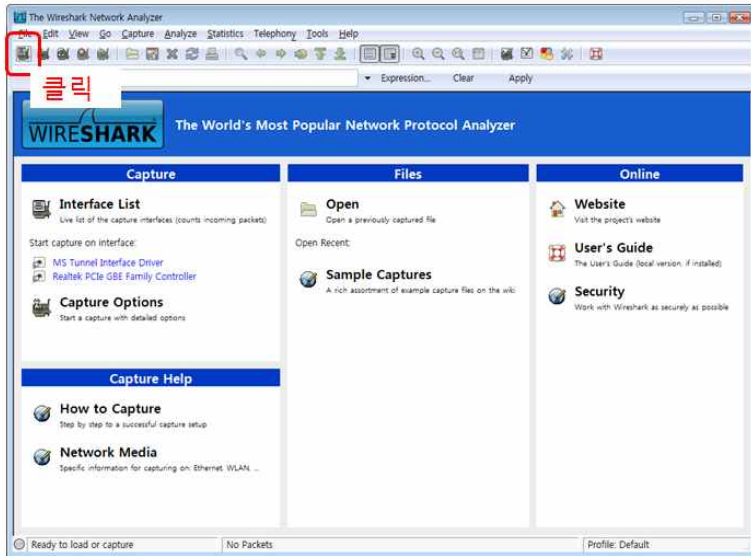


② 점검대상 웹페이지 접속(ex: https://www.kisa.or.kr/members/login.jsp)

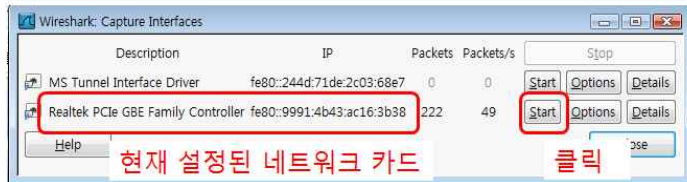


③ 암호화 필요정보 입력 (ex: ID는 kisaaid, PW는 kispw)

③ 패킷캡처 인터페이스 설정



④ 패킷캡처 시작

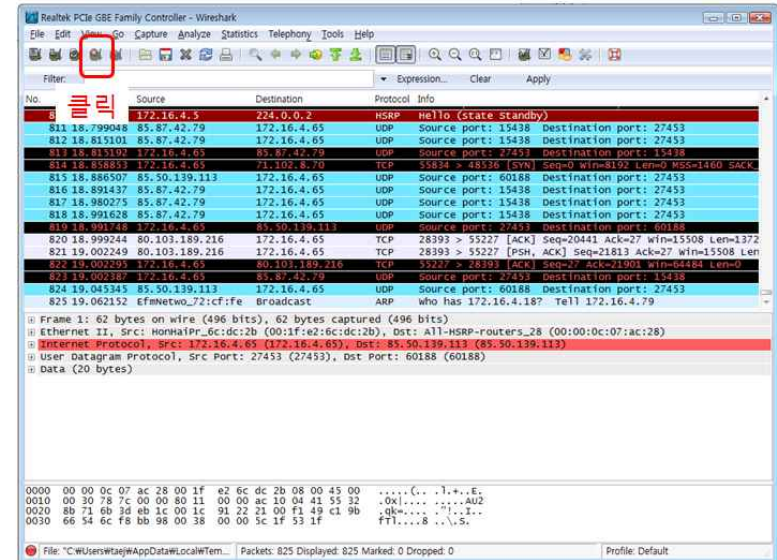


※ packets/s의 수치가 증가하는 것이 현재 설정된 네트워크 카드임

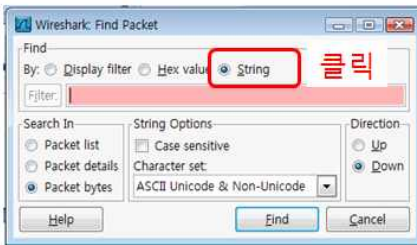
⑤ 점검대상 웹페이지에서 패킷발송(ex: 로그인 버튼 클릭)



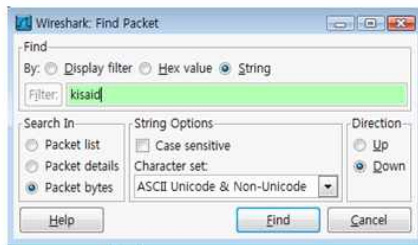
⑥ 캡처된 패킷을 확인 (ex: 로그인 버튼 클릭)



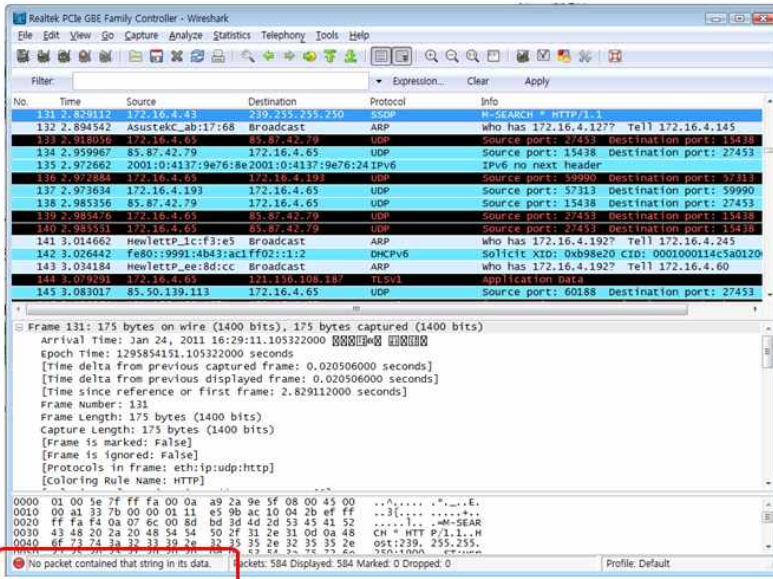
⑦ 캡처된 패킷의 확인화면(⑦)에서 단축키 Ctrl + F 클릭



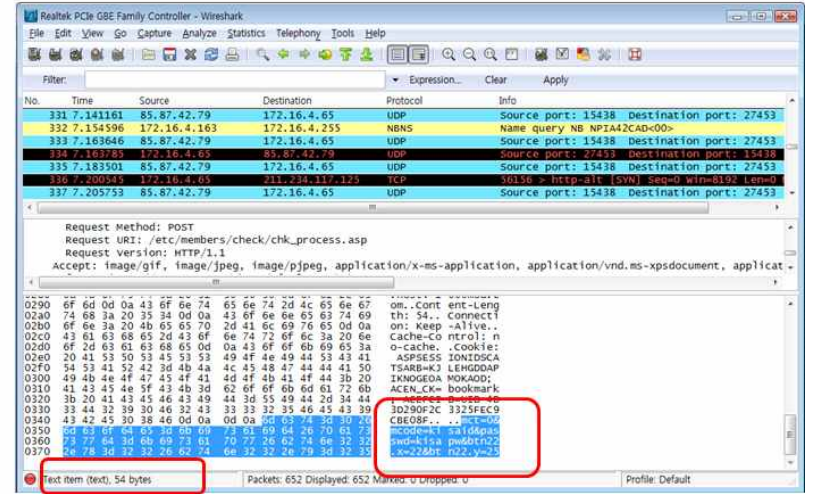
⑧ 암호화 필요 정보 입력 (③의 문자열 입력)



⑨ 암호화 된 정보는 검색이 되질 않음을 확인



⑩ 암호화가 되지 않은 경우 ID(kisaid), PW(kisapw) 확인 가능



6. 강남 대학교 개인정보파일 표준목록

■ 개인정보파일 표준목록

(년. 월. 일. 기준)

파일명	부서명	운영근거	수집항목	수집방법	보유기간
발전기금 기탁자관리	대외교류센터	학교발전기금의 조성 운용 및 회계관리에 관한 규칙 [서식2]	성명, 이메일, 주민번호, 주소, 전화번호, 기부일자, 기부방법, 약정액, 약정형태, 기부금액	서면양식, 홈페이지 약정서	준영구
보건관리	대학진료소	학교보건법 시행령 제32조	성명, 주민번호, 주소, 전화번호, 소속	시스템 연계	10년
교직원관리	교직원지원부	교원자격검정령 시행규칙	성명, 주민번호, 주소, 이메일, 성별, 출신대학, 학번, 학과, 취득학점	오프라인 수집	준영구
사회봉사 관리	글로벌사회공 헌센터	개인정보보호법 제15조	성명, 전화번호, 주소, 이메일, 학번, 학과, 학년, 거주유형, 재학여부	오프라인 수집	탈퇴시 까지
학생상담 관리	학생생활 상담소	개인정보보호법 제15조	성명, 전화번호, 주소, 이메일, 학번, 학과, 학년, 거주유형, 재학여부	오프라인 수집	탈퇴시 까지
어학원생 관리	어학교육원	어학교육원 규정	성명, 전화번호, 소속, 영문이름, 비밀번호, 생년월일, 이메일, 비자유형, 국적, 학교/학년, 보호자정보	홈페이지	5년
연구관리 정보	인사팀 산학협력단	과학기술기본법 시행규칙, [서식1]	성명, 생년월일, 주소, 이메일, 전화번호, 졸업정보, 연구원 직급, 연구 참여 이력, 계좌정보, 연구비 카드정보	시스템 연계, 서면양식, 온라인 수집	준영구
예비군 지원자정보	직장예비군 연대	향토예비군 설치법 시행령 제28조의 2	성명, 주민번호, 주소, 전화번호, 성별, 복무사항, 복무기간, 복무지, 병역처분사항	시스템 연계	준영구
취업통계	취업지원팀	취업관리규정	성명, 이메일, 전화번호, 학번, 학과	시스템 연계	5년
입학지원자 명단	입학전형관리 팀	고등교육법시행 령제34조(입학 전형자료)	성명, 주민번호, 주소, 전화번호, 이메일, 출신고교, 출신대학, 국적, 외국인등록번호	온라인 수집	5년
입학성적 관리	입학전형관리 팀	고등교육법시행 령제34조(입학 전형자료)	수험번호, 성적정보	시스템 연계, 오프라인 수집	5년

파일명	부서명	운영근거	수집항목	수집방법	보유기간
장애학생	장애학생 종합지원센터	장애인활동 지원에 관한 법을 시행령 제30조 2	성명, 주민번호, 학번, 주소, 전화번호, 이메일	시스템 연계	준영구
웹메일 사용자정보	전산정보원	정보화자원 사용규정	성명, 생년월일, 전화번호, 학번, 소속, 아이디, 비밀번호	온라인 수집	1년
홈페이지 회원정보	전산정보원	개인정보보호법 제15조	성명, 주소, 직장주소, 이메일, 전화번호, 생년월일, 아이디, 패스워드	시스템 연계	탈퇴시 까지
통합계정 정보	전산정보원	통합인증서비스 지침	성명, 아이디, 비밀번호, 영문이름, 생년월일, 주소, 이메일, 전화번호, 국적, 직업, 학력	홈페이지	준영구
도서관대출 관리	중앙도서관	도서관운영규정	성명, 학번, 신분, 학과, 주소, 전화번호, FAX, 이메일, 휴복학상태, 퇴학제적사항, 연체료 납부여부	시스템 연계	준영구
정기주차권	안전시설팀	차량교통관리운 영세칙 제7조	성명, 전화번호, 소속, 학년, 학번, 차량명, 차량번호, 차량소유자, 소유자와의 관계	온라인 수집	5년
평생교육 수강생	평생교육원	평생교육법시행 규칙 제4조(학습계좌 운영)	성명, 영문이름, 생년월일, 학력, 주소, 전화번호, 이메일, 수강강좌명, 결제방식 및 결제정보, 이수과목명, 직장번호	서면양식	준영구
학적관리	교무팀	고등교육법시행 령제16조2, 73조	성명, 주민번호, 학번, 학과, 주소, 전화번호, 학위번호, 보호자명, 보호자 전화번호, 보호자주소, 보호자직업	시스템 연계	준영구
성적관리	교무팀	고등교육법시행 령제16조2, 73조	성명, 주민번호, 학번, 학과, 주소, 보호자명, 취득학점, 평점평균	시스템 연계	준영구
졸업관리	교무팀	고등교육법시행 령제16조2, 73조	성명, 주민번호, 학번, 학과, 주소, 전화번호, 학위번호, 보호자명, 보호자 전화번호, 보호자주소, 보호자직업	시스템 연계	준영구
교환학생 관리	대외교류센터 교무팀	고등교육법시행 령제16조2, 73조	성명, 주민번호, 학번, 전화번호, 이메일	시스템 연계, 서면양식	준영구
교원자격증 발급자명부	교직원지원팀	교원자격검정령 시행규칙 서식	성명, 주민번호, 자격증번호, 취급일자	시스템 연계	준영구
학생관리	장학복지팀	학생관리규정	성명, 학과, 생년월일, 전화번호	시스템 연계	5년
기숙사생 관리	심전생활관	심전생활관 규정	성명, 학번, 전화번호, 이메일, 과정구분, 국적, 보호자정보, 주소, 소속, 성적	시스템 연계	5년

개인정보파일 보유기간 책정 기준표

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 개인정보파일 중 영구보존이 필요한 개인정보파일
중영구	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	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

7. 개인정보 처리단계별 준수사항 및 위반시 벌칙사항

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

과태료의 부과기준

1. 일반기준

가. 위반행위의 횟수에 따른 과태료 부과기준은 최근 3년간 같은 위반행위로 과태료를 부과받은 경우에 적용한다. 이 경우 위반행위에 대하여 과태료 부과처분을 한 날과 다시 같은 위반행위를 적발한 날을 각각 기준으로 하여 위반 횟수를 계산한다.

나. 안전행정부장관 또는 관계 중앙행정기관의 장은 다음의 어느 하나에 해당하는 경우에는 제2호에 따른 과태료 부과금액의 2분의 1의 범위에서 그 금액을 감경할 수 있다. 다만, 과태료를 체납하고 있는 위반행위자의 경우에는 그러하지 아니하다.

- 1) 위반행위자가 「질서위반행위규제법 시행령」 제2조의2제1항 각 호의 어느 하나에 해당하는 경우
- 2) 위반행위가 사소한 부주의나 오류로 인한 것으로 인정되는 경우
- 3) 위반행위자가 위법행위로 인한 결과를 시정하였거나 해소한 경우
- 4) 그 밖에 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 과태료를 감경할 필요가 있다고 인정되는 경우

다. 안전행정부장관 또는 관계 중앙행정기관의 장은 다음의 어느 하나에 해당하는 경우에는 제2호에 따른 과태료 부과금액의 2분의 1의 범위에서 그 금액을 가중할 수 있다. 다만, 가중할 사유가 여러 개인 경우라도 법 제75조제1항부터 제3항까지의 규정에 따른 과태료 금액의 상한을 넘을 수 없다.

- 1) 위반의 내용 및 정도가 중대하여 소비자 등에게 미치는 피해가 크다고 인정되는 경우
- 2) 법 위반상태의 기간이 3개월 이상인 경우
- 3) 그 밖에 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 과태료를 가중할 필요가 있다고 인정되는 경우

2. 개별기준

(단위: 만원)

위반행위	근거 법조문	과태료 금액		
		1회 위반	2회 위반	3회 이상 위반
가. 법 제15조제1항을 위반하여 개인정보를 수집한 경우	법 제75조제1항제1호	1000	2000	4000

위반행위	근거 법조문	과태료 금액		
		1회 위반	2회 위반	3회 이상 위반
나. 법 제15조제2항, 제17조제2항, 제18조제3항 또는 제26조제3항을 위반하여 정보주체에게 알려야 할 사항을 알리지 않은 경우	법 제75조제2항제1호	600	1200	2400
다. 법 제16조제2항 또는 제22조제4항을 위반하여 재화 또는 서비스의 제공을 거부한 경우	법 제75조제2항제2호	600	1200	2400
라. 법 제20조제1항을 위반하여 정보주체에게 같은 항 각 호의 사실을 알리지 않은 경우	법 제75조제2항제3호	600	1200	2400
마. 법 제21조제1항을 위반하여 개인정보를 과기하지 않은 경우	법 제75조제2항제4호	600	1200	2400
바. 법 제21조제3항을 위반하여 개인정보를 분리하여 저장·관리하지 않은 경우	법 제75조제3항제1호	200	400	800
사. 법 제22조제1항부터 제3항까지의 규정을 위반하여 동의를 받은 경우	법 제75조제3항제2호	200	400	800
아. 법 제22조제5항을 위반하여 법정대리인의 동의를 받지 않은 경우	법 제75조제1항제2호	1000	2000	4000
자. 법 제24조제2항을 위반하여 정보주체가 주민등록번호를 사용하지 않을 수 있는 방법을 제공하지 않은 경우	법 제75조제2항제5호	600	1200	2400
차. 법 제24조제3항, 제25조제6항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우	법 제75조제2항제6호	600	1200	2400
카. 법 제25조제1항을 위반하여 영상정보처리기기를 설치·운영한 경우	법 제75조제2항제7호	600	1200	2400
타. 법 제25조제2항을 위반하여 영상정보처리기기를 설치·운영한 경우	법 제75조제1항제3호	1000	2000	4000
파. 법 제25조제4항을 위반하여 안내판 설치 등 필요한 조치를 하지 않은 경우	법 제75조제3항제3호	200	400	800
하. 법 제26조제1항을 위반하여 업무 위탁 시 같은 항 각 호의 내용이 포함된 문서에 의하지 않은 경우	법 제75조제3항제4호	200	400	800
거. 법 제26조제2항을 위반하여 위탁하는 업무의 내용과 수탁자를 공개하지 않은 경우	법 제75조제3항제5호	200	400	800

위반행위	근거 법조문	과태료 금액		
		1회 위반	2회 위반	3회 이상 위반
너. 법 제27조제1항 또는 제2항을 위반하여 정보주체에게 개인정보의 이전 사실을 알리지 않은 경우	법 제75조 제3항제6호	200	400	800
더. 법 제30조제1항 또는 제2항을 위반하여 개인정보 처리방침을 정하지 않거나 이를 공개하지 않은 경우	법 제75조 제3항제7호	200	400	800
러. 법 제31조제1항을 위반하여 개인정보 보호책임자를 지정하지 않은 경우	법 제75조 제3항제8호	500		
머. 법 제34조제1항을 위반하여 정보주체에게 같은 항 각 호의 사실을 알리지 않은 경우	법 제75조 제2항제8호	600	1200	2400
버. 법 제34조제3항을 위반하여 조치 결과를 신고하지 않은 경우	법 제75조 제2항제9호	600	1200	2400
서. 법 제35조제3항을 위반하여 열람을 제한하거나 거절한 경우	법 제75조 제2항제10호	600	1200	2400
어. 법 제35조제3항·제4항, 제36조제2항·제4항 또는 제37조제3항을 위반하여 정보주체에게 알려야 할 사항을 알리지 않은 경우	법 제75조 제3항제9호	200	400	800
저. 법 제36조제2항을 위반하여 정정·삭제 등 필요한 조치를 하지 않은 경우	법 제75조 제2항제11호	600	1200	2400
처. 법 제37조제4항을 위반하여 처리가 정지된 개인정보에 대하여 파기 등 필요한 조치를 하지 않은 경우	법 제75조 제2항제12호	600	1200	2400
커. 법 제63조제1항에 따른 관계 물품·서류 등 자료를 제출하지 않거나 거짓으로 제출한 경우 1) 자료를 제출하지 않은 경우 2) 자료를 거짓으로 제출한 경우	법 제75조 제3항제10호	100 200	200 400	400 800
더. 법 제63조제2항에 따른 출입·검사를 거부·방해 또는 기피한 경우	법 제75조 제3항제11호	200	400	800
퍼. 법 제64조제1항에 따른 시정명령에 따르지 않은 경우	법 제75조 제2항제13호	600	1200	2400

8. 표준 개인정보처리 위탁 계약서(안)

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

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

표준 개인정보처리위탁 계약서(안)

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

제1조 (목적) 이 계약은 “갑”이 개인정보처리업무를 “을”에게 위탁하고, “을”은 이를 승낙하여 “을”의 책임아래 성실하게 업무를 완성하도록 하는데 필요한 사항을 정함을 목적으로 한다.

제2조 (용어의 정의) 본 계약에서 별도로 정의되지 아니한 용어는 「개인정보 보호법」 시행령 및 시행규칙, 「개인정보의 안전성 확보조치 기준」(행정자치부 고시 제2016-35호) 및 「표준 개인정보 보호지침」(행정안전부 고시 제2011-45호)에서 정의된 바에 따른다.

제3조 (위탁업무의 목적 및 범위) “을”은 계약이 정하는 바에 따라 () 목적으로 다음과 같은 개인정보 처리 업무를 수행한다.2)

- 1.
- 2.

제4조 (재위탁 제한) ① “을”은 “갑”의 사전 승낙을 얻은 경우를 제외하고 “갑”과의 계약상의 권리와 의무의 전부 또는 일부를 제3자에게 양도하거나 재위탁할 수 없다.
② “을”이 재위탁받은 수탁회사를 선임한 경우 “을”은 당해 재위탁계약서와 함께 그 사실을 즉시 “갑”에 통보하여야 한다.

제5조 (개인정보의 안전성 확보조치) “을”은 「개인정보 보호법」 제24조제3항 및 제29조, 동법 시행령 제21조 및 제30조, 「개인정보의 안전성 확보조치 기준」(행정자치부 고시 제2016-35호)에 따라 개인정보의 안전성 확보에 필요한 관리적·기술적 조치를 취하여야 한다.

제6조 (개인정보의 처리제한) ① “을”은 계약기간은 물론 계약 종료 후에도 위탁업무 수행 목적 범위를 넘어 개인정보를 이용하거나 이를 제3자에게 제공 또는 누설하여

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

서는 안 된다.

② “을”은 계약이 해지되거나 또는 계약기간이 만료된 경우 위탁업무와 관련하여 보유하고 있는 개인정보를 「개인정보 보호법」 시행령 제16조 및 「개인정보의 안전성 확보조치 기준」(행정자치부 고시 제2016-35호)에 따라 즉시 파기하거나 “갑”에게 반납하여야 한다.

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

제7조 (수탁자에 대한 관리·감독 등) ① “갑”은 “을”에 대하여 다음 각 호의 사항을 관리하도록 요구할 수 있으며, “을”은 특별한 사유가 없는 한 이에 응하여야 한다.

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

② “갑”은 “을”에 대하여 제1항 각 호의 사항에 대한 실태를 점검하여 시정을 요구할 수 있으며, “을”은 특별한 사유가 없는 한 이행하여야 한다.

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

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

제8조 (손해배상) ① “을” 또는 “을”의 임직원 기타 “을”의 수탁자가 이 계약에 의하여 위탁 또는 재위탁받은 업무를 수행함에 있어 이 계약에 따른 의무를 위반하거나 “을” 또는 “을”의 임직원 기타 “을”의 수탁자의 귀책사유로 인하여 이 계약이 해지되어 “갑” 또는 개인정보주체 기타 제3자에게 손해가 발생한 경우 “을”은 그 손해를 배상하여야 한다.

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

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

갑	을
○○시 ○○구 ○○동 ○○번지	○○시 ○○구 ○○동 ○○번지
성 명 :	성 명 :
(인)	(인)

3) 「개인정보 안전성 확보조치 기준 고시」(행정자치부 고시 제2016-35호) 및 「개인정보 보호법」 제26조에 따라 개인정보처리자 및 취급자는 개인정보보호에 관한 교육을 의무적으로 시행하여야 한다.

9. 교직원 개인정보보호 서약서 양식표준

개인정보보호 서약서

본인 ()은(는) 업무 중에 알게 된 개인정보 및 업무와 관련된 정보에 대하여 업무 수행중이나 업무 수행 후에도 비밀을 지킬 것을 서약합니다.

또한 본교에서 수집한 개인정보의 보호를 위해 본교에서 정하는 개인정보 내부관리 계획을 준수할 것이며, 적절한 절차 없이 개인정보를 무단으로 조회, 누출하지 않을 것을 서약합니다.

개인정보보호와 관련한 비밀의 준수와 개인정보보호를 위한 법적 준수 기준인 “정보통신망이용촉진 및 정보보호에 관한 법률” 및 “개인정보보호법”에 명시된 모든 조항과 본교의 개인정보 내부관리 계획 등 관련된 모든 조항이 포함된다는 것을 충분히 설명 받고 숙지하였습니다.

만약, 이러한 서약에도 불구하고 업무상 알게 된 사항에 대하여 비밀을 누설하거나 정당한 사유 없이 조회, 유출, 오용할 경우, 형사상 민사상의 법률 조항에 의거하여 제재를 받을 수 있음을 통고 받았으며, 이러한 제재에 대하여 이의를 제기하지 않을 것을 본인의 자의로 서약합니다.

일 시: 201 년 월 일

소 속:

성 명: (인)

10. 개인정보 처리 위탁 계약 보안 서약서 양식

개인정보 처리 위탁(제공) 계약 보안 서약서

_____ (이하 "을"이라 한다)는 강남대학교(이하 "갑"이라 한다)의 개인정보 처리 업무 위탁 업무수행에 따른 개인정보 및 개인정보처리시스템(DBMS)의 안전한 보호를 위해 아래 각 호의 사항을 준수한다.

1. 을은 갑이 위탁한 개인정보 처리 업무 수행 시 개인정보(정보 및 정보시스템)를 안전하게 사용·관리하며, 개인정보의 보호를 위해 다음의 사항을 준수한다.

- 1) 갑의 정보보안 기본지침 및 개인정보보호 관련 법규의 준수
- 2) 개인정보 위탁 업무 처리 시 기술적·관리적 보호 조치
- 3) 위탁 업무 수행 목적 외 개인정보의 처리 금지

-위탁 업무의 목적 :

-위탁 업무의 범위 :

- 4) 업무상 알게 된 개인정보에 관한 비밀 유지
 - 5) 제공받거나 허가받은 개인정보 처리업무 및 처리권한의 제3자 공유 금지
 - 6) 위탁 업무의 종료 시 개인정보 파기 등 의무사항의 이행
 - 7) 위탁 업무의 관련하여 보유하고 있는 개인정보의 관리 현황 점검 및 감독 철저
2. 을은 갑의 업무 수행을 위해 담당하는 직원에 대하여 책임을 진다.
3. 을은 갑의 사전 승인을 받지 못한 프로그램 및 정보기기는 갑의 업무와 관련하여 사용하지 않는다.

4. 을은 갑의 규정 및 관련 법규의 미 준수 또는 관리 소홀로 인해 발생하는 제반 사고에 대한 민·형사상 책임을 진다.

상기사항을 숙지하고 이를 성실히 준수할 것을 서약함.

20 년 월 일

수탁(협력)업체 대표: (서명)