붙임2	한세대학교 개인정보 침해사고 대응 매뉴얼

제1장 총칙

제1조 (목적) 본 지침은 한세대학교(이하 “본 대학”이라 한다)에서 발생하는 개인정보침해사고에 신속하게 대응하기 위한 사고대응 및 처리방법과 이를 위한 사전 준비사항에 대하여 침해사고로 부터의 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 종이문서, 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 총괄책임자) ① 개인정보 총괄책임자는 개인정보침해사고 예방, 처리 및 재발방지의 총괄 관리를 한다.

② 개인정보 총괄책임자는 개인정보 침해사건 발생 시 침해사고 처리책임자를 지정

하고 개인정보침해사고 대응팀을 소집하여 운영한다.

제5조 (개인정보침해사고 대응팀) 개인정보보호 분야별책임자로 구성되며 개인정보 총괄책임자가 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 (개인정보 총괄담당자) 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 개인정보 총괄담당자에게 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 개인정보 총괄담당자는 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 개인정보 총괄담당자는 년 1회 웹사이트의 개인정보 노출 취약점 점검을 시행하고 개인정보총괄책임자에게 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 부서별담당자에게 신고하며 부서별담당자는 개인정보 총괄담당자에게 신고하여야 한다.
② 개인정보침해사고 발생시 고의적으로 신고를 누락 한 경우 개인정보 총괄책임자는 관련자에 대한 처분(징계 등)을 요청 할 수 있다.

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

제14조 (개인정보침해사고 대응팀 구성) ① 개인정보 총괄책임자는 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 총괄책임자가 임의로 침해사고 처리책임자를 지정할 수 있다.
③ 개인정보침해사고 대응팀은 분야별 책임자 중에서 사안에 따라 선정한다.
④ 2, 3등급 침해의 경우 개인정보 총괄책임자는 침해사고처리책임자와 협의하여 개인정보침해사고 대응팀을 구성하지 않을 수 있다.
⑤ 개인정보 총괄책임자는 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 총괄책임자가 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 총괄책임자에게 제출한다.

② 개인정보 총괄책임자는 개인정보침해사고 처리보고서를 검토하고 승인한다.

③ 개인정보 총괄책임자는 개인정보침해 관련자에 대한 처분(징계 등)을 해당부서에 요청할 수도 있다.

④ 개인정보 총괄담당자는 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 총괄책임자에게 제출한다.

② 개인정보 총괄책임자는 개선안을 검토하여 시행 및 변경 여부와 시기를 결정한다.

③ 개인정보 총괄책임자는 필요하다고 판단할 경우 사고의 교훈을 적절한 대상을 지정하여 전파 및 교육을 할 수 있다.

④ 개인정보 총괄책임자는 개선안 시행, 교훈 전파 및 교육 후 그 성과를 검토한다.

제5장 개인정보침해사고의 관리

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

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

제21조 (개인정보침해사고 교육훈련) 개인정보 총괄책임자는 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 개인정보 총괄담당자는 제1항 제2호의 경우 개인정보 유출 사고가 최초 발생한 시점과 알게 된 시점 사이에 시간적 차이가 있는 경우에는 이에 대한 과실유무를 입증하여야 한다.

③ 개인정보 총괄담당자는 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 개인정보 총괄담당자는 정보주체에게 제22조제1항 각 호의 사항을 통지할 때에는 서면, 전자우편, 모사전송, 전화, 휴대전화 문자전송 또는 이와 유사한 방법을 통하여 5일 이내에 정보주체에게 알려야 한다.

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

제24조 (개인정보 유출 보고 절차) ① 개인정보 총괄담당자는 정보주체에 관한 개인정보 유출내용 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 개인정보 총괄담당자는 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

[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, 감봉, 견책, 기타)로 구분
* 비고란에는 처리보고서 문서번호를 기록

[붙임2] 개인정보침해사고 처리보고서

<table>
<tr><td>보고일자</td><td colspan="2"></td><td>문서번호</td><td></td></tr>
<tr><td colspan="5">침해 신고 / 접수 정보</td></tr>
<tr><td>침해등급</td><td colspan="2">□ 1등급 □ 2등급 □ 3등급</td><td>침해대상정보</td><td>□ 일반 개인정보
□ 주민등록번호
□ 계좌번호</td></tr>
<tr><td>접수일시</td><td colspan="2"></td><td>신고일자</td><td></td></tr>
<tr><td>침해사고
처리책임자</td><td colspan="2"></td><td>신고자 연락처</td><td></td></tr>
<tr><td>신고 내용</td><td colspan="4"></td></tr>
<tr><td rowspan="2">대응 과정</td><td>일시</td><td colspan="3">대응활동</td></tr>
<tr><td></td><td colspan="3"></td></tr>
<tr><td>침해 내용</td><td colspan="4">확인된 침해 정보의 세부사항, 규모 및 침해 방법(노출, 외부자 제공, 수집, 접근, 분석, 이용, 내부자 제공, 불법 저장, 불안전한 저장, 파기, 비파기 등 세부사항)</td></tr>
<tr><td>침해 발생 경위</td><td colspan="4"></td></tr>
<tr><td>관련자</td><td colspan="4"></td></tr>
<tr><td>침해 발생 원인</td><td colspan="4"></td></tr>
<tr><td>증거자료</td><td colspan="4"></td></tr>
<tr><td>복구 및
재발방지 조치</td><td colspan="4"></td></tr>
<tr><td>처분</td><td colspan="4"></td></tr>
</table>

[붙임3] 개인정보 침해사실 신고서

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

붙임 :

년 월 일

신고인 : (서명 또는 인)</td></tr>
</table>

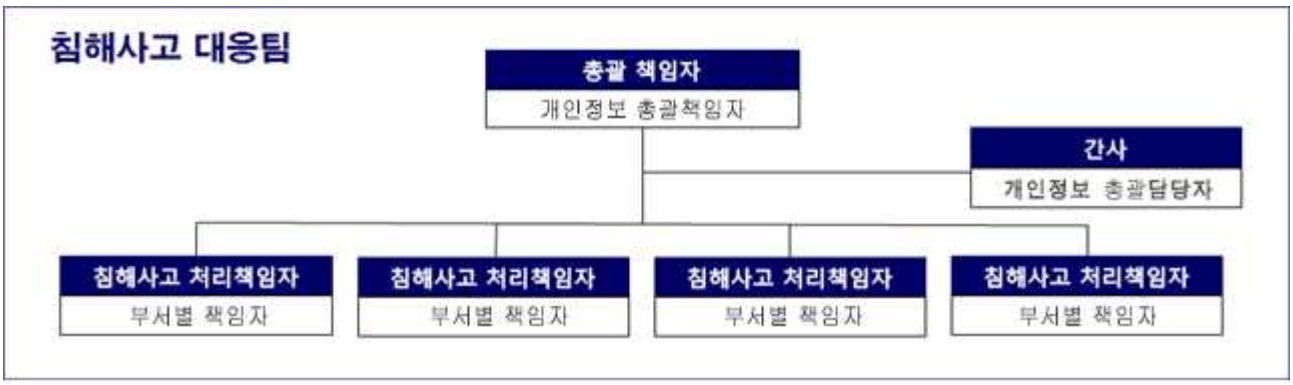
[붙임4]

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 총괄책임자				
	개인정보 취급자				

유출신고(보고) 접수기관	기관명	담당자명	연락처

[붙임5] 침해사고 비상연락망



구분	직책	성명	내선
총괄 책임자 개인정보 총괄책임자	행정처장	김지현	031-450-5005
간사 개인정보 총괄담당자	인사총무 팀장	송기백	031-450-5049
침해사고처리책임자	침해사고 발생한 부서장	OOO	000-0000
부서별 담당자	침해사고 발생한 부서팀장	OOO	000-0000

[별표1] 개인정보침해사고 모의시나리오

구분	행동 요령	행위자	비고
개인정보 침해사고의 발생	o 침해가 발생한 것을 인지한 경우 또는 그러한 침해의 발생이 의심되는 경우 지체없이 개인정보 총괄담당자에게 신고	전직원	홈페이지 개인정보처리방침의 개인정보침해신고서 다운 및 작성
개인정보 침해사고의 **접수**	o 개인정보 총괄담당자는 개인정보침해사고를 접수한 경우 “개인정보 침해사고 관리대장”에 사고 접수를 기록한다. o 개인정보 총괄담당자는 접수 후 지체 없이 개인정보총괄책임자에게 보고한다.	개인정보 총괄담당자	1등급 침해사고의 경우 발생 그 즉시 및 수시로 총장에게 보고
개인정보 침해사고 **대응팀 구성**	o 노출 또는 제공된 정보의 종류에 따라, 발생 부서의 분야별책임자로 침해사고 처리책임자를 지정하고 개인정보침해사고 대응팀을 구성한다.	개인정보 총괄책임자	2,3등급 침해의 경우 개인정보 총괄책임자는 침해사고처리책임자와 협의하여 개인정보침해사고 대응팀을 구성하지 않을 수 있다. 개인정보 총괄담당자는 개인정보가 유출된 경우에는 개인정보 침해 통지 및 조치 결과를 지체 없이 교육부에 공문으로 신고하여야 한다.
개인정보 침해사고의 **분석**	o 침해의 규모, 경위, 방법, 원인 및 관련자를 조사 o 필요시 개인정보침해사고 대응팀 또는 개인정보총괄책임자가 승인한 외부 전문가의 지원을 받아 증거자료를 수집한다. o 개인정보 유출사실을 인지하였을 경우 지체 없이 해당 정보주체에게 관련 사실을 통지한다.	침해사고 처리책임자	
개인정보 침해사고의 대응 및 복구	o 1등급의 경우 침해사고 처리책임자는 해당 개인정보를 파기 또는 회수하기 위한 조치를 취한다. o 2등급의 경우 침해사고 책임자는 해당 개인정보를 파기, 회수 또는 복구하기 위한 조치를 취하거나 정보주체의 사후 동의를 받아 근거를 마련한다. o 3등급의 경우 침해사고 처리책임자는 해	침해사고 처리책임자	

	당 개인정보를 적절히 보호하거나 파기하기 위한 조치를 취한다. o 침해사고 처리책임자는 즉각적 조치가 가능한 경우 재발방지 조치를 취한다.		
개인정보 침해사고의 종료	o 침해사고 처리책임자는 개인정보침해사고 처리보고서를 작성하여 개인정보총괄책임자에게 제출한다. o 개인정보총괄책임자는 개인정보침해사고 처리보고서를 검토하고 승인한다. o 개인정보총괄책임자는 개인정보침해 관련자에 대한 처분(징계 등)을 해당부서에 요청한다. o 개인정보 총괄담당자는 개인정보침해사고 처리보고서를 관리하고 처분(징계 등) 결과를 기록한다.	침해사고 처리책임자 / 개인정보총괄책임자 및 담당자	
개인정보 침해사고 사후분석	o 침해사고 처리책임자는 처리보고서 제출 후 30일 이내 근본원인 분석, 교훈 및 예방을 위한 개선대책을 마련하여 개인정보총괄책임자에게 제출한다.	침해사고 처리책임자	