개인정보침해 및 유출 대응 시행세칙

시행 : 2025.04.01.

제1장 총칙

제1조 (목적) 본 시행세칙은 경희대학교(이하 “본교”라 한다) 「개인정보 내부관리계획」에 의거하여 개인정보침해 및 유출 발생 시 사고대응 및 처리방법과 이를 위한 사전 준비사항을 정의함을 목적으로 한다.

제2조 (근거) 본 시행세칙은 「개인정보 보호법」 및 「개인정보 보호법 시행령」· 「개인정보 처리 방법에 관한 고시」, 「표준 개인정보 보호지침」과 같은 관련 고시 및 지침에 근거한다.

제3조 (용어정의) 본 시행세칙에서 사용되는 용어의 정의는 본교「개인정보 내부관리계획」과 세부절차의 정의를 따른다.

제4조 (적용범위) 본 시행세칙은 해킹, 분실, 도난 등으로 인해 개인정보가 내·외부자에 의하여 유출된 경우에 적용된다.

제2장 개인정보침해 및 유출에 관한 책임

제5조 (개인정보보호책임자) ① 개인정보보호책임자는 개인정보침해 및 유출 예방, 처리 및 재발방지의 총괄 관리 책임을 진다.
② 개인정보보호책임자는 개인정보침해 및 유출 발생 시 개인정보침해 및 유출 처리책임자를 지정하고 개인정보침해 및 유출 대응팀을 소집하여 운영한다.

제6조 (개인정보침해 및 유출 대응팀) ① 개인정보보호조직의 구성원으로 구성되며 개인정보보호책임자가 해당 개인정보침해 및 유출 분석, 대응 및 복구에 필요한 관련자를 지정하여 소집한다. 필요시 업무담당자, 개인정보보호 담당자, 대변인, 외부 전문가 등이 포함될 수 있다.
② 대변인은 개인정보침해 및 유출 대응팀의 입장을 공식적으로 전달하는 역할을 하며, 필요시 개인정보보호책임자가 본교 구성원으로 지정한다.
③ 개인정보침해 및 유출 대응팀은 감사행정원에 법률자문을 구할 수 있다.
④ 본교 개인정보침해 및 유출 대응팀은 [별표3] 개인정보침해 및 유출 대응 업무수행 체계와 같이 구성하여 운영한다.

제7조 (개인정보침해 및 유출 처리책임자) 해당 개인정보침해 및 유출 발생 부서의 부서장으로 지정되며 처리 및 재발방지에 대한 책임을 지고 개인정보침해 및 유출 대응팀과 협력하여 사고를 해결한다.

제8조 (개인정보보호 담당자) ① 개인정보침해 및 유출 신고를 접수하고 본 시행세칙 제10조의 기준에 따라 등급을 분류하여 개인정보침해 및 유출 대응 절차를 개시한다.
② 개인정보침해 및 유출 대응팀의 간사로서 대내외 비상연락망을 관리하고 팀 내 연락 및 조정을 담당한다.
③ 개인정보침해 및 유출 기록을 관리하고 필요시 관련자 및 기관에 보고한다.
④ 필요 시 정보보안에 대한 기술적인 분석을 담당한다.

제9조 (전직원) 본교 소속 내부직원(계약직 등 비정규직 포함)은 개인정보에 대한 침해 또는 유출사고가 발생한 것을 인지한 경우, 지체없이 개인정보보호 담당자에게 신고하여야 한다.

제3장 개인정보침해 및 유출의 분류

제10조 (개인정보침해 및 유출의 분류) 개인정보침해 및 유출은 다음과 같이 3등급으로 분류한다.

1. 1등급 침해는 법적 근거, 규정 또는 본인의 동의 없이 개인정보가 본교 외부의 제3자에게 노출 또는 제공된 것을 말한다.
2. 2등급 침해는 법적 근거, 규정 또는 본인의 동의 없이 개인정보를 수집, 접근, 분석, 이용, 내부자에게 제공, 저장, 파기하는 것을 말한다.
3. 3등급 침해는 안전하지 않은 상태로 개인정보를 저장하거나, 파기해야 할 정보를 파기하지 않는 등 세부 시행세칙의 규정을 위반한 것을 말한다.

<표1>

침해등급	예시	비고
1등급	해킹, 탈취 등에 의한 개인정보 외부 유출 등	
2등급	개인정보취급 권한이 없는 교직원이 개인정보를 취급하는 경우, 개인정보 수집시 동의없이 개인정보를 수집·이용 하는 경우 등	
3등급	주요 개인정보(고유식별번호 등) 암호화 미실시, 개인정보 보유목적 달성 후 미파기, 정보주체 권리행사 대응 미비 등	

제4장 개인정보침해 및 유출 대응절차

제11조 (개인정보침해 및 유출 예방 및 탐지) ① 개인정보보호 담당자는 웹사이트를 통한 개인정보 노출을 예방하기 위하여 개인정보 노출차단 솔루션을 운영하고 월별 현황을 관리한다.

② 개인정보보호 담당자는 분기별로 웹페이지, 붙임파일, 소스코드 및 외부 검색엔진 상의 노출을 점검하고 분기별 현황을 관리한다.

③ 구성원(또는 외부인)이 게시판 등에 자료를 게재할 때 개인정보 노출에 대하여 주의를 환기시키기 위한 경고를 제공하여야 한다.

④ 개인정보보호 담당자는 연 1회 보안취약점 점검을 시행하고 개인정보보호책임자에게 결과를 보고한다.

제12조 (개인정보침해 및 유출의 신고) 본교의 내부직원(계약직 등 비정규직 포함)이 취급하는 개인정보에 대하여 본 시행세칙 제10조에서 정의한 개인정보침해 및 유출이 발생한 것을 인지한 경우 또는 그러한 침해의 발생이 의심되는 경우 지체없이 본교 개인정보보호 담당자에게 신고하여야 한다.

제13조 (개인정보침해 및 유출의 접수) ① 개인정보보호 담당자는 개인정보침해 및 유출을 접수한 경우 [붙임1] “개인정보침해 및 유출 관리대장” 에 사고 접수를 기록한다.

② 개인정보보호 담당자는 접수 후 지체 없이 개인정보보호책임자에게 보고 한다.

③ 개인정보보호 담당자는 개인정보 침해 및 유출사고에 대한 긴급조치가 가능한 경우 지체없이 피해

최소화를 위해 다음 각 호의 조치를 수행한다.

1. 인터넷 홈페이지를 통해 개인정보가 유출된 경우 삭제조치 또는 삭제 요청
2. 오프라인 서류 및 보조저장매체 등이 분실된 경우 조사 및 회수 조치
3. 해킹 등으로 시스템이 탈취되어 개인정보가 유출된 경우 관련 네트워크 경로 차단, 시스템 일시 중지 등의 조치

제14조 (개인정보침해 및 유출 대응체계) ① 개인정보보호책임자는 노출 또는 제공된 정보의 종류에 따라, 발생 부서의 부서장으로 개인정보침해 및 유출 처리책임자를 지정하고 개인정보침해 및 유출 대응팀을 구성한다.

② 발생 부서를 적시할 수 없거나 발생 부서의 부서장이 개인정보침해 및 유출에 연루된 경우 개인정보보호책임자가 임의로 개인정보침해 및 유출 처리책임자를 지정할 수 있다.

③ 2등급 또는 3등급 개인정보침해 및 유출의 경우 개인정보보호책임자는 개인정보침해 및 유출 처리책임자와 협의하여 개인정보침해 및 유출 대응팀을 구성하지 않을 수 있다.

④ 개인정보보호책임자는 필요시 외부 전문가에게 분석을 의뢰할 수 있고 개인정보 유출 인원 등을 확인하여 [별표4] 개인정보 유출 통지방법에 따라 지체 없이 대상자에게 통지한다.

⑤ 개인정보침해 및 유출 대응팀은 필요 시 [별표7] 민원대응 조치에 따라 민원대응팀과 같이 대외적 접촉을 위한 창구를 별도로 마련하여 외부로부터의 개인정보침해 및 유출 관련 질문에 대응 할 수 있다.

⑥ 개인정보침해 및 유출 대응팀은 정보주체의 2차 피해 및 불안 해소를 위한 내용을 개인정보 유출 통지에 포함하여 안내할 수 있다.

⑦ 1천명 이상의 개인정보가 유출된 경우, 민감정보 또는 고유식별정보가 유출된 경우, 개인정보처리시스템 또는 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대한 외부로부터의 불법적인 접근에 의해 개인정보가 유출 등이 된 경우에는 개인정보 침해 통지 및 조치 결과를 지체 없이 개인정보침해 업무를 담당하는 개인정보보호위원회 및 한국인터넷진흥원(KISA)와 같은 전문기관에 신고하여야 한다. 다만, 1건의 개인정보라도 유출된 경우에도 교육부 정보보호팀에 신고하여야 한다.
또한, 천재지변이나 그 밖에 부득이한 사유로 인하여 72시간 이내에 신고하기 곤란한 경우에는 해당 사유가 해소된 후 지체 없이 신고할 수 있으며, 개인정보 유출등의 경로가 확인되어 해당 개인정보를 회수·삭제하는 등의 조치를 통해 정보주체의 권익 침해 가능성이 현저히 낮아진 경우에는 신고하지 않을 수 있다.

⑧ 제7항에 따른 유출 신고는 개인정보보호위원회(한국인터넷진흥원 위탁 운영)의 개인정보 포털 내 개인정보 유출신고 방법에 따른다.

⑨ 개인정보가 분실·도난·유출되었음을 알게 되었을 때에는 [별표4] 개인정보 유출 통지방법을 참고하여 서면등의 방법으로 72시간 이내에 정보주체에게 알려야 하며 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우에는 정보주체가 쉽게 알 수 있도록 본교 홈페이지에 30일 이상 게시하도록 한다.

제15조 (개인정보침해 및 유출의 분석) ① 개인정보침해 및 유출 처리책임자는 침해 사실 여부를 확인하고 사실로 확인될 경우 침해의 규모, 경위, 방법, 원인 및 관련자를 조사한다.

② 개인정보침해 및 유출 처리책임자는 필요한 경우 개인정보침해 및 유출 대응팀 또는 개인정보보호책임자가 승인한 외부 전문가의 지원을 받아 증거자료를 수집한다.

제16조 (개인정보침해·유출의 대응 및 복구) ① 1등급 개인정보침해 및 유출의 경우 개인정보침해 및 유출 처리책임자는 해당 개인정보를 파기 또는 회수하기 위한 조치를 취한다.

② 2등급 개인정보침해의 경우 개인정보침해 및 유출 책임자는 해당 개인정보를 파기, 회수 또는 복구하

기 위한 조치를 취하거나 정보주체의 사후 동의를 받아 근거를 마련한다.
③ 3등급 개인정보침해의 경우 개인정보침해 및 유출 처리책임자는 해당 개인정보를 적절히 보호하거나 파기하기 위한 조치를 취한다.
④ 개인정보침해 및 유출 처리책임자는 즉각적 조치가 가능한 경우 재발방지 조치를 취한다.

제17조 (개인정보침해 및 유출의 종료) ① 개인정보침해 및 유출 처리책임자는 [붙임2] 개인정보침해 및 유출 처리보고서를 작성하여 개인정보보호책임자에게 제출한다.
② 개인정보보호책임자는 개인정보침해 및 유출 처리보고서를 검토하고 승인한다.
③ 개인정보보호책임자는 개인정보침해 및 유출 관련자에 대한 처분(징계 등)을 해당부서에 요청할 수 있다.
④ 개인정보보호 담당자는 개인정보침해 및 유출 처리보고서를 관리하고 처분(징계 등) 결과를 기록한다.

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

제5장 개인정보침해 및 유출의 관리

제19조 (개인정보침해 및 유출의 보고) ① 개인정보보호책임자는 1등급 개인정보침해 및 유출의 경우 발생 즉시 및 수시로 그 진행 현황을 총장에게 보고한다.
② 개인정보보호 담당자는 연간 등급별·유형별 개인정보침해 및 유출 발생 및 처리현황을 개인정보보호책임자에게 보고한다.

제20조 (개인정보침해 및 유출의 현황 관리) 개인정보보호책임자는 개인정보침해 및 유출 현황을 분석하여 추가적인 개선대책이 필요한 경우 개선 대책을 마련하여 시행한다. 개선 대책에는 교육자료 활용 등을 포함할 수 있다.

제21조 (개인정보침해 및 유출 교육훈련) ① 개인정보 보호책임자는 연간 개인정보보호 교육 시 개인정보침해 및 유출사고 관련 내용이 포함되도록 한다.
② 제1항에 따른 교육은 [별표1] 개인정보침해 및 유출 모의시나리오를 활용할 수 있다.

제6장 기타

제22조 (개인정보침해 및 유출 신고자의 보호) ① 개인정보침해 및 유출 신고자의 신분은 개인정보침해 및 유출 대응에 필요한 경우 반드시 필요한 담당자 및 권한자에게만 제공되어야 하며 외부로 노출되어서는 아니 된다.
② 개인정보침해 및 유출 신고자는 어떠한 경우에도 신고로 인해 불이익을 당하는 경우가 없어야 한다.

제23조 (개인정보침해 및 유출 당사자에게 통보) 개인정보침해 및 유출 처리책임자가 개인정보 유출사실을 인지하였을 경우 지체 없이 해당 정보주체에게 관련 사실을 통지한다.

부 칙

본 시행세칙은 2019년 3월 28일부터 시행한다.

부 칙

본 시행세칙은 2021년 7월 13일부터 시행한다.

부 칙

본 시행세칙은 2023년 05월 31일부터 시행한다.

부 칙

본 시행세칙은 2024년 04월 05일부터 시행한다.

부 칙

본 시행세칙은 2025년 04월 01일부터 시행한다.

[붙임1] 개인정보침해 및 유출 관리대장

접수		신고개요	등급	처리유형	종결일자	처리내용	비고
일시	신고자 유형						

* 접수 일시는 신고 접수 일시를 기록
* 신고자 유형은 교원/직원/학생으로 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
* 종결일자는 개인정보침해 및 유출 처리보고서 접수일을 기준으로 기록
* 처리내용은 처분 유형을 사법처리(징역, 벌금, 추징, 재판계류중, 수시중)/ 징계 처분(파면, 해임, 정직, 감봉, 견책)/ 기타로 구분
* 비고란에는 처리보고서 문서번호를 기록

[붙임2] 개인정보침해 및 유출 처리보고서

<table>
<tr><td>보고일자</td><td colspan="2"></td><td>문서번호</td><td></td></tr>
<tr><td colspan="5">개인정보침해 및 유출 신고 / 접수 정보</td></tr>
<tr><td>개인정보침해 및
유출등급</td><td colspan="2">□ 1등급
□ 2등급
□ 3등급</td><td>개인정보침해
및 유출
대상정보</td><td>□ 일반 개인정보
□ 주민번호 등
고유식별정보
□ 계좌번호</td></tr>
<tr><td>접수일시</td><td colspan="2"></td><td>신고일자</td><td></td></tr>
<tr><td>개인정보침해 및
유출 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>개인정보침해 및
유출 내용</td><td colspan="4">확인된 침해 정보의 세부사항, 규모 및 침해 방법(노출, 외부인 제공, 수집, 접근, 분석, 이용, 내부자 제공, 불법 저장, 불안전한 저장, 파기, 비파기 등 세부사항)</td></tr>
<tr><td>개인정보침해 및
유출 발생 경위</td><td colspan="4"></td></tr>
<tr><td>관련자</td><td colspan="4"></td></tr>
<tr><td>개인정보침해 및
유출 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>
</table>

기타	

[붙임3] 개인정보침해 및 유출사실 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>
</table>

위와 같이 개인정보침해 및 유출사실을 신고합니다.

붙임 :

년 월 일

신고인 : (서명 또는 인)

[별표1] 개인정보침해 및 유출 모의시나리오

구분	행동 요령	행위자	비고
개인정보 침해·유출의 **발생**	o 개인정보침해·유출이 발생한 것을 인지한 경우 또는 그러한 개인정보침해·유출의 발생이 의심되는 경우 지체없이 개인정보보호 담당자에게 신고	전직원	
개인정보 침해·유출의 **접수**	o 개인정보보호 담당자는 개인정보침해·유출 신고를 접수한 경우 “개인정보침해 및 유출 관리대장” 에 사고 접수를 기록한다. o 개인정보보호 담당자는 접수 후 지체 없이 개인정보보호책임자에게 보고한다.	개인정보 보호 담당자	1등급 개인정보침해 및 유출의 경우 발생 그 즉시 및 수시로 개인정보보호책임자에게 보고
개인정보 침해 및 유출 **대응팀 구성**	o 노출 또는 제공된 정보의 종류에 따라, 발생 부서의 장으로 개인정보침해 및 유출 처리책임자를 지정하고 개인정보침해 및 유출 대응팀을 구성한다.	개인정보 보호책임자	2등급 또는 3등급 개인정보침해의 경우 개인정보보호책임자는 개인정보침해 및 유출 처리책임자와 협의하여 개인정보침해 및 유출 대응팀을 구성하지 않을 수 있다. 1천명 이상의 개인정보가 유출된 경우에는 개인정보 침해 통지 및 조치 결과를 지체 없이 개인정보침해 업무를 담당하는 정부기관(예: KISA “개인정보침해신고센터” 등)에 신고하여야 한다.
개인정보 침해·유출의 **분석**	o 개인정보침해·유출의 규모, 경위, 방법, 원인 및 관련자를 조사 o 필요시 개인정보침해 및 유출 대응팀 또는 개인정보보호책임자가 승인한 외부 전문가의 지원을 받아 증거자료를 수집한다. o 개인정보 유출사실을 인지하였을 경우 지체 없이 해당 정보주체에게 관련 사실을 통지한다.	개인정보침해 및 유출 처리책임자	

개인정보 침해·유출의 **대응 및 복구**	o 1등급 개인정보침해 및 유출의 경우 개인정보침해 및 유출 처리책임자는 해당 개인정보를 파기 또는 회수하기 위한 조치를 취한다. o 2등급 개인정보침해의 경우 개인정보침해·유출사고 책임자는 해당 개인정보를 파기, 회수 또는 복구하기 위한 조치를 취하거나 정보주체의 사후 동의를 받아 근거를 마련한다. o 3등급 개인정보침해의 경우 개인정보침해 및 유출 처리책임자는 해당 개인정보를 적절히 보호하거나 파기하기 위한 조치를 취한다. o 개인정보침해 및 유출 처리책임자는 즉각적 조치가 가능한 경우 재발방지 조치를 취한다.	개인정보침해 및 유출 처리책임자	
개인정보 침해·유출의 **종료**	o 개인정보침해 및 유출 처리책임자는 개인정보침해 및 유출 처리보고서를 작성하여 개인정보보호책임자에게 제출한다. o 개인정보보호책임자는 개인정보침해 및 유출 처리보고서를 검토하고 승인한다. o 개인정보보호책임자는 필요시 개인정보침해·유출 관련자에 대한 처분(징계 등)을 해당부서에 요청한다. o 개인정보보호 담당자는 개인정보침해 및 유출 처리보고서를 관리하고 처분(징계 등) 결과를 기록한다.	개인정보침해 및 유출 처리책임자 / 개인정보보호책임자 및 담당자	
개인정보 침해·유출 **사후분석**	o 개인정보침해 및 유출사고 처리책임자는 처리보고서 제출 후 30일 이내 근본원인 분석, 교훈 및 예방을 위한 개선대책을 마련하여 개인정보보호책임자에게 제출한다.	개인정보침해 및 유출 처리책임자	

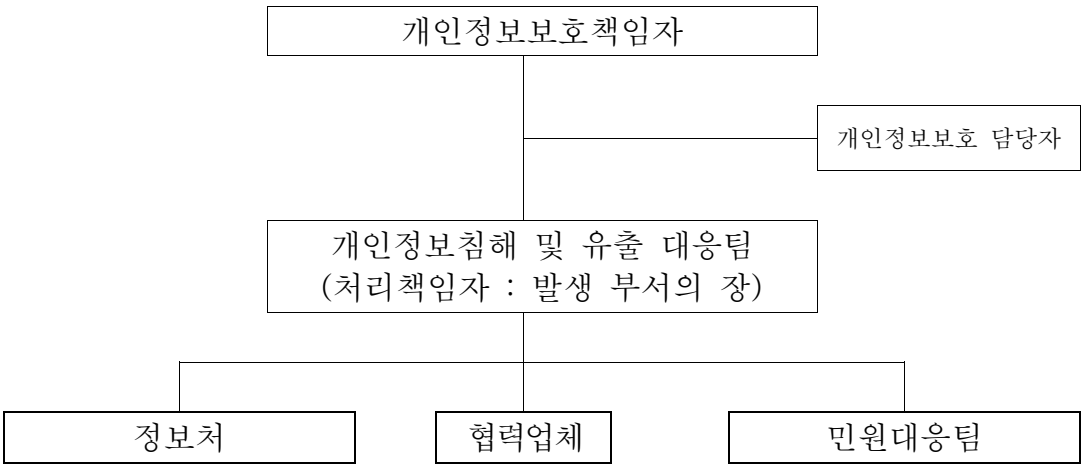
[별표2] 개인정보침해 및 유출 단계별 세부 프로세스

단계	상세 업무	비고
사고인지 및 긴급조치	○ 개인정보 유출 신고 접수 및 사고인지 ○ 개인정보 유출 대응센터 소집 및 유관기관 협조체계 확인 ○ 피해 최소화를 위한 긴급조치 수행 ※ 유출된 개인정보 삭제조치 및 기술지원 요청	[붙임2] [별표3] 참조
↓		
정보주체 유출통지	○ 정보주체에게 개인정보 유출사실 통지(72시간 이내)	[별표4] 참조
↓		
개인정보 유출신고	○ 1천명 이상의 정보주체에 관한 개인정보 유출 시 및 민감정보 또는 고유식별정보가 유출된 경우 개인정보처리시스템 또는 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대한 외부로부터의 불법적인 접근에 의해 개인정보 유출 시 개인정보보호위원회 또는 한국인터넷진흥원(privacy.go.kr)에 유출신고 ○ 단, 1명 이상이라도 교육부 정보보호팀에 신고	[별표6] 참조
↓		
민원대응팀 운영	○ 개인정보 유출 규모 및 성격에 따라 민원대응팀 구성	
↓		
고객민원 대응	○ 2차 피해 방지를 위한 고객 민원 대응 및 고객 불안 해소 조치	
↓		
피해구제 절차	○ 개인정보 유출에 대한 피해구제 절차 안내	
↓		
보안기능 강화	○ 사고 원인 분석 및 보안 강화·기능 개선	
↓		
종료 (결과보고)	○ 개인정보보호책임자에 개인정보침해 및 유출 처리보고서 작성 및 보고	[붙임2] 참조

↓		
재발방지	○ 개인정보 유출 사례 전파 교육 및 개선 대책 시행	

[별표3] 개인정보침해 및 유출 대응 업무수행 체계

❍ 조직체계(개인정보침해 및 유출 대응팀)



❍ 업무분장

조직별	담당자	담당 업무
개인정보보호 책임자		•개인정보침해 및 유출 대응 총괄 지휘
개인정보침해 및 유출 대응팀	발생부서의 장	•개인정보침해 및 유출 인지, 접수, 전파 •개인정보침해 및 유출 대응 절차 수립 •정보주체에게 유출사실 통지 •개인정보보호위원회 또는 전문기관(한국인터넷진흥원)에 유출통지 사실 신고 •사고내용 세부조사(증거자료 수집 등)
정보처	정보기획팀장	•개인정보침해 및 유출 사실 확인, 조사 및 원인 분석 지원 •사고내용 세부조사 지원 •외부요인에 의한 유출의 경우, 유관 기관과 협조하여 사고 처리 지원 •시스템 복구 및 백업(유지보수/협력업체 포함)
개인정보보호 담당자		•개인정보침해 및 유출 관련 대외기관(언론사 등) 대응 •개인정보침해 및 유출 대고객 안내문 문구 최종 검토

조직별	담당자	담당 업무
민원대응팀	발생부서의 장	•고객 개별 통지문 안내에 따른 후속업무(민원 등) 진행 •고객상담센터, 소비자보호 방안 마련(필요시 유관부서와 협조) •온라인 및 오프라인 창구 개설
협력업체	업체별 담당자	•정보시스템 기술적 보호조치 지원

[별표4] 개인정보 유출 통지방법

유출통지 방법

구 분	내 용
통지대상	정보주체
통지방법	○ 서면, 이메일, FAX전송, 전화, 휴대전화 문자전송 또는 이와 유사한 방법 – 다만, 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우, 인터넷 홈페이지에 30일 이상 게시
통지내용	○ 유출된 개인정보의 항목 ○ 유출된 시점과 그 경위 ○ 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보 ○ 개인정보처리자의 대응조치 및 피해 구제절차 ○ 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처
통지시기	유출사실을 발견할 때로부터 72시간 이내

통지연기	○ 개인정보 유출확산방지를 위한 조치가 필요한 경우 연기 가능 – 개인정보가 유출되었을 것으로 의심되는 개인정보처리시스템의 접속권한 삭제·변경 또는 폐쇄 조치 – 네트워크, 방화벽 등 대·내외 시스템 보안점검 및 취약점 보완 조치 – 향후 수사에 필요한 외부의 접속기록 등 보존 조치 – 정보주체에게 유출 관련 사실을 통지하기 위한 유출확인 웹페이지 제작 등의 통지방법 마련 조치 – 기타 개인정보의 유출확산 방지를 위한 필요한 기술적·관리적 조치 ○ 다만, 위 각 항목의 조치를 취한 이후, 정보주체에게 다음 각 항목의 사실만 일차적으로 알리고 추후 확인되는 즉시 알릴 수 있음 – 정보주체에게 유출이 발생한 사실 – 통지내용 중 확인된 사항

[별표5] 개인정보 유출 표준 통지문안(예시)

개인정보 유출 표준 통지문안 (예시)

※ 유출된 항목, 유출된 시점과 경위가 확인되지 않아 통지문에 포함하지 않은 경우 추후 확인되면 반드시 추가 통지

표준 통지문안 예시	부가 설명
귀하의 개인정보는 ○○○시스템에 저장·보관하다가 ○○○○년 ○○월경 해커에 의한 해킹으로 유출되었습니다.	<유출된 시점과 경위> – 유출된 시점과 경위를 상세하게 설명
유출된 개인정보 항목은 이름, 아이디(ID), 비밀번호(P/W), 주민등록번호, 이메일, 연락처 총 6개입니다.	<유출된 항목> – 유출된 항목을 누락 없이 모두 나열
유출 사실을 인지한 후 즉시 해당 IP와 불법접속 경로를 차단하고, 취약점 점검과 보완 조치를 하였습니다. 또한, 유지보수업체 서버에 있던 귀하의 개인정보는 즉시 삭제 조치하였습니다.	< 대응조치> – 예시된 항목 외에도 조치한 내용 설명
혹시 모를 피해를 최소화하기 위하여 귀하의 비밀번호를 변경하여 주시기 바랍니다. 그리고 개인정보 악용으로 의심되는 전화, 메일 등을 받으시거나 기타 궁금하신 사항은 연락주시면 친절하게 안내해 드리고, 신속하게 대응하도록 하겠습니다.	<피해 최소화를 위한 정보주체의 조치방법> – 유출 경위에 따라 정보주체가 할 수 있는 방법을 안내 – 예방 가능한 방법을 모두 안내 (보이스 피싱, 피싱 메일, 불법 TM, 스팸문자 등)
아울러, 피해가 발생하였거나 예상되는 경우에는 아래 담당부서에 신고하시면 성실하게 안내와 상담을 해 드리겠습니다.	<피해 구제절차> – 보상이나 배상이 결정된 경우에는 그 내용을 상세히 기재 – 감독기관 등을 통한 구제절차도 안내

▸ 피해 등 접수 담당부서 : 0000팀 ▸ 피해 등 접수 전화번호 : 031-1234-6789 ▸ 피해 등 접수 e-메일주소 : abcd@khu.ac.kr	<피해 등 신고 접수 담당부서 및 연락처> - 전담처리부서 안내를 원칙으로 하되, 대량 유출로 일시적으로 콜센터 등 다른 부서를 지정한 경우 해당 부서를 안내

[별표6] 개인정보 유출 신고기관 연락처

□ **개인정보 유출 신고**

기 관 명	전화번호	인터넷사이트
개인정보 보호위원회	-	https://www.privacy.go.kr/ (개인정보포털)
한국인터넷 진흥원	118 (Fax:02-405-5229)	
교육부 정보보호팀	044-203-6505	-

□ **관련기관 연락처**

기 관 명	전화번호	인터넷사이트
대검찰청 사이버범죄 수사단	1301	http://www.spo.go.kr/minwon
경찰청 사이버수사국	182	https://ecrm.police.go.kr/minwon/main

[별표7] 민원대응 조치

❍ 개인정보침해 및 유출 대응팀은 오프라인 창구를 개설
❍ 전화, 메일, 홈페이지 등 한 가지 이상의 채널을 선택하여 단일화된 민원대응 창구 구축

구분	채널	상세 내용
오프라인	OO관 OO처 사무실	상황에 따라 변동될 수 있음
온라인 中 택 1	전화	02-000-0000
	메일	privacy@khu.ac.kr
	홈페이지	https://www.khu.ac.kr

❍ 민원대응팀은 유관부서와 협의하여 피해자 구제방안, 수사 진행상황 등에 대한 외부 질의 답변 방향 결정
❍ 협의 방안을 토대로 민원대응 매뉴얼 작성 및 배포
❍ 민원대응 전담 인력·회선 확보 및 대응 매뉴얼 교육
❍ 대외적 접촉창구는 민원대응팀으로 단일화하여 홈페이지에 공지하고 타 팀에서 외부로부터 개인정보 유출관련 질문을 받으면 최대한 민원대응팀으로 연결
❍ 기본적으로 민원대응팀을 통해서 1차 민원 대응을 하고, 다음과 같은 경우 해당 부서에서 응대

문의별	담당부서
유출 확인 문의 대응	OO 팀
피해구제 관련 문의 대응	OO 팀
기타 문의	OO 팀

❍ 유출 규모와 상황을 고려하여 원활한 민원 처리를 위해 통신사와 통신회선 증설 및 인터넷회선 확충과 관련된 계약수립