개인정보 침해사고 대응지침

2020. 2

국제대학교

제1장 총칙

제1조 (목적) 이 지침은 「국제대학교 개인정보 침해사고 대응지침(이하 "대응지침" 이라 한다)」개인정보침해사고 발생 시 사고대응 및 처리방법과 이를 위한 사전 준비사항을 목적으로 한다.

제2조 (적용범위) 본 지침의 적용범위는 세부지침의 적용 범위를 따른다.

제3조 (용어정의) 본 지침에서 사용되는 용어의 정의는 세부지침의 정의를 따른다.

제2장 개인정보 침해사고에 관한 책임

제4조 (개인정보보호책임자) ① 개인정보보호책임자는 개인정보침해사고 예방, 처리 및 재발방지의 총괄 관리 책임을 진다.

② 개인정보보호책임자는 개인정보침해사건 발생 시 침해사고 처리책임자를 지정하고 개인정보침해사고 대응팀을 소집하여 운영한다.

제5조 (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.

③ 개인정보침해기록을 관리하고 필요시 관련자 및 기관에 보고한다.

제6조 (침해사고처리책임자) 침해사고 처리책임자는 침해사고 발생 부서의 분야별 책임자로 지정되며 침해사고처리 및 재발방지에 대한 책임을 지고 침해사고대응팀과 협력하여 사고를 해결한다.

제7조 (침해사고대응팀) 침해사고 대응팀은 개인정보보호책임자, 개인정보

보호담당자, 침해사고처리책임자로 구성되며 개인정보보호책임자가 해당 침해사고 분석, 대응 및 복구에 필요한 관련자를 지정하여 소집한다. 필요시 업무담당자, 대변인, 규제개혁법무담당관, 외부 전문가 등이 포함될 수 있다.

제8조 (전 교직원) 국제대학교(본교, 부속 및 부설기관)의 교직원(계약직 등 비정규직 포함)은 개인정보에 대한 침해가 발생한 것을 인지한 경우, 지체 없이 개인정보보호담당자에게 신고하여야 한다.

제3장 침해사고의 분류

제9조 (개인정보침해의 분류) 개인정보침해사고는 다음과 같이 3등급으로 분류한다.

1등급	법적 근거, 규정 또는 본인의 동의 없이 개인정보가 국제대학교 외부의 제3자에게 노출 또는 제공
2등급	법적 근거, 규정 또는 본인의 동의 없이 개인정보를 수집, 접근, 분석, 이용, 내부자에게 제공, 저장, 파기
3등급	안전하지 않은 상태로 개인정보를 저장하거나, 파기해야 할 정보를 파기하지 않는 등 세부지침의 규정을 위반한 것

제4장 침해사고 대응절차

제10조 (개인정보침해 예방 및 탐지) ① 개인정보보호담당자는 홈페이지, 붙임파일, 소스코드 및 외부 검색엔진 상의 노출을 점검하고 현황을 관리한다.

② 홈페이지 게시판 등에 자료를 게재할 때 개인정보 노출에 대하여 주의를 환기시키기 위한 경고를 제공하여야 한다.

③ 개인정보보호담당자는 홈페이지의 개인정보 노출 취약점 점검을 시행하고 개인정보보호책임자에게 결과를 보고한다.

제11조 (개인정보침해의 신고) 국제대학교(본교, 부속 및 부설기관)의 교직원(계약직 등 비정규직 포함)이 취급하는 개인정보의 침해가 발생한 것을 인지한 경우 또는 그러한 침해의 발생이 의심되는 경우 지체없이 개인정보보호담당자에게 신고하여야 한다.

국제대학교 홈페이지	⇒	개인정보처리방침	⇒	개인정보침해 사실신고서 다운로드[붙임1]	⇒	신고서작성 및 제출(정보지원센터)

제12조 (개인정보침해사고의 접수) 개인정보보호담당자는 개인정보침해사고를 접수한 경우 개인정보 침해사고 관리대장[붙임2]에 사고 접수를 기록하고, 지체 없이 개인정보보호책임자에게 보고 한다.

제13조 (개인정보침해 대응체계) ① 개인정보보호책임자는 노출 또는 제공된 정보의 종류에 따라, 발생 부서 및 학과의 분야별책임자를 침해사고처리책임자로 지정하고 침해사고 대응팀을 구성한다.

② 발생 부서를 적시할 수 없거나 담당 분야별책임자가 침해사고에 연루된 경우 개인정보보호책임자가 임의로 침해사고 처리책임자를 지정할 수 있다.

③ 2등급 또는 3등급 침해의 경우 개인정보보호책임자는 침해사고처리책임자와 협의하여 침해사고대응팀을 구성하지 않을 수 있다.

④ 개인정보보호책임자는 필요시 외부 전문가에게 분석을 의뢰할 수 있다.

⑤ 1천명 이상의 개인정보가 유출된 경우에는 개인정보 침해 통지 및 조치결과를 지체 없이 행정안전부장관 또는 전문기관(한국정보화진흥원, 한국인터넷진흥원)에 신고하여야 한다.

제14조 (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 침해사고대응팀 또는 개인정보보호

책임자가 승인한 외부 전문가의 지원을 받아 증거자료를 수집한다.

제15조 (침해사고의 대응 및 복구) ① 1등급 침해의 경우 침해사고 처리책임자는 해당 개인정보를 파기 또는 회수하기 위한 조치를 취한다.

② 2등급 침해의 경우 침해사고 책임자는 해당 개인정보를 파기, 회수 또는 복구하기 위한 조치를 취하거나 정보주체의 사후 동의를 받아 근거를 마련한다.

③ 3등급 침해의 경우 침해사고 처리책임자는 해당 개인정보를 적절히 보호하거나 파기하기 위한 조치를 취한다.

④ 침해사고 처리책임자는 즉각적 조치가 가능한 경우 재발방지 조치를 취한다.

제16조 (침해사고의 종료) ① 침해사고 처리책임자는 개인정보침해사고 처리보고서[붙임3]를 작성하여 개인정보보호책임자에게 제출한다.

② 개인정보보호책임자는 개인정보침해사고 처리보고서를 검토하고 승인한다.

③ 개인정보보호책임자는 개인정보침해 관련자에 대한 처분(징계 등)을 해당 부서에 요청한다.

④ 개인정보보호담당자는 개인정보침해사고 처리보고서를 관리하고 처분(징계 등) 결과를 기록한다.

제17조 (침해사고 사후분석) ① 침해사고 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 개인정보 침해사고의 관리

제18조 (개인정보침해사고의 보고) ① 개인정보보호책임자는 1등급 사고의 경우 발생 즉시 및 수시로 그 진행 현황을 총장에게 보고한다.

② 개인정보보호담당자는 등급별.유형별 침해사고 발생 및 처리현황을 개인정보보호책임자에게 보고한다.

제19조 (개인정보침해사고의 현황 관리) 개인정보보호책임자는 개인정보침해사고 현황을 분석하여 추가적인 개선대책이 필요한 경우 개선 대책을 마련하여 시행한다. 개선 대책에는 교육자료 활용 등을 포함할 수 있다.

제20조 (개인정보침해사고 교육훈련) ① 개인정보보호책임자는 전 교직원에게 개인정보침해사고의 유형과 보고 방법을 교육하여야 한다.

② 개인정보보호책임자는 개인정보침해사고 시나리오를 마련하여 모의훈련을 실시하여야 한다.

제6장 기타

제21조 (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.

제22조 (개인정보침해 당사자에게 통보) 침해사고 처리책임자 개인정보 유출사실을 인지하였을 경우 지체 없이 해당 정보주체에게 관련 사실을 통지한다.

[붙임1] **개인정보 침해사실 신고서**

<table>
<tr><td rowspan="3">신고인</td><td colspan="2">성명</td><td></td></tr>
<tr><td rowspan="2">연락처</td><td>휴대폰</td><td></td></tr>
<tr><td>email</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 개인정보침해사실을 신고 합니다

년 월 일

신고인 : (서명 또는 인)</td></tr>
</table>

[붙임2] **개인정보침해사고 관리대장**

접수		신고개요	등급	처리유형	종결일자	처리내용	비고
일시	신고자 유형						

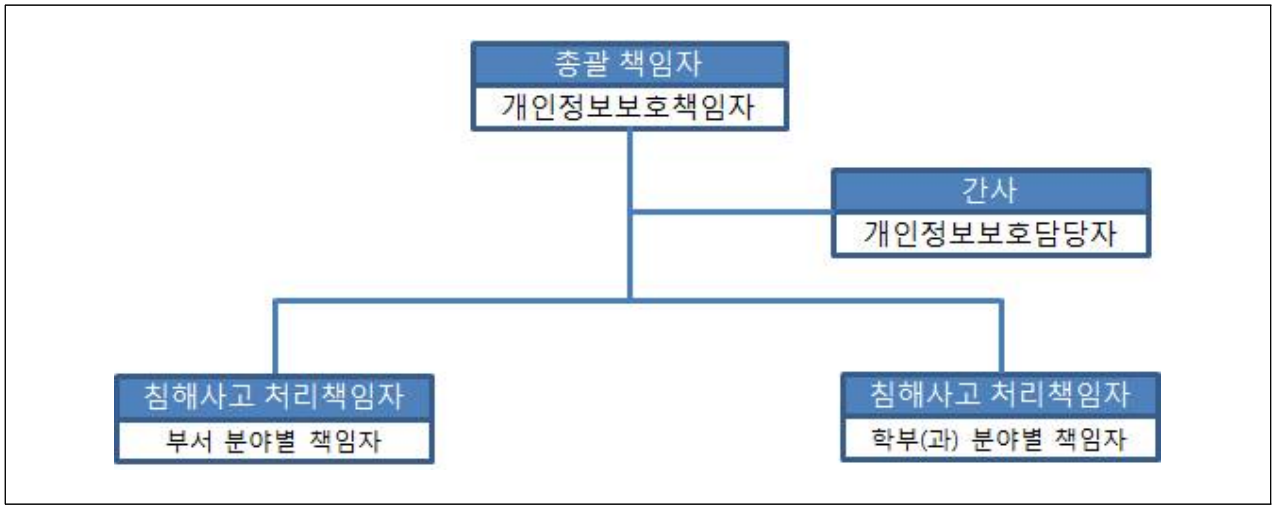
* 접수 일시는 사고 접수 일시를 기록
* 신고자 유형은 교직원/학생/일반으로 구분
* 신고 개요는 신고 내용을 기록
* 등급은 1/2/3 등급으로 구분
* 처리유형은 사실 확인 중/ 상담 및 자료제공/ 타기관 이송/ 위법성 통보/ 수사 의뢰/ 법위반 확인 불가/ 기타(징계위원회 회부)로 구분
* 종결일자는 개인정보침해사고 처리보고서 접수일을 기준으로 기록
* 처리내용은 처분 유형을 사법처리(징역, 벌금, 추징, 재판계류중, 수시중)/ 징계 처분(파면, 해임, 정직, 감봉, 견책, 기타)로 구분
* 비고란에는 처리보고서 문서번호를 기록

[붙임3] **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
☐ 주민번호
☐ 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>

[붙임4] **침해사고 비상연락망**

□ 침해사고 대응팀 조직도



□ 침해사고 처리책임자

부서	책임자
행정부서	각 행정부서장
학과	각 학과장
부속기관	각 부속기관장
부설기관	각 부설기관장
법인	산학협력단장
연구기관	각 연기기관장

[별표1] 개인정보침해사고 모의시나리오

구분	행동 요령	행위자	비고
개인정보 침해사고의 발생	o 침해가 발생한 것을 인지한 경우 또는 그러한 침해의 발생이 의심되는 경우 지체없이 개인정보보호담당자에게 신고	전교직원	국제대학교 홈페이지 ⇒ 개인정보처리방침 ⇒ 개인정보침해사실신고서 다운로드 ⇒ 신고서 작성 및 제출
개인정보 침해사고의 접수	o 개인정보보호담당자는 개인정보침해사고를 접수한 경우 “개인정보 침해사고 관리대장”에 사고 접수를 기록한다. o 개인정보보호담당자는 접수 후 지체 없이 개인정보보호책임자에게 보고한다.	개인정보 보호담당자	1등급 침해사고의 경우 발생 그 즉시 및 수시로 총장에게 보고
개인정보 침해사고 대응팀 구성	o 노출 또는 제공된 정보의 종류에 따라, 발생 부서의 분야별책임자를 침해사고 처리책임자로 지정하고 개인정보침해사고 대응팀을 구성한다.	개인정보 보호책임자	2등급 또는 3등급 침해의 경우 개인정보보호책임자는 침해사고 처리책임자와 협의하여 개인정보침해사고 대응팀을 구성하지 않을 수 있다. 1천명 이상의 개인정보가 유출된 경우에는 개인정보 침해 통지 및 조치 결과를 지체 없이 행정안전부장관 또는 전문기관(한국정보화진흥원, 한국인터넷진흥원)에 신고하여야 한다.
개인정보 침해사고의 분석	o 침해의 규모, 경위, 방법, 원인 및 관련자를 조사 o 필요시 개인정보침해사고 대응팀 또는 개인정보보호책임자가 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 1등급 침해의 경우 침해사고 처리책임자는 해당 개인정보를 파기 또는 회수하기 위한 조치를 취한다. o 2등급 침해의 경우 침해사고 책임자는 해당 개인정보를 파기, 회수 또는 복구하기 위한 조치를 취하거나 정보주체의 사후 동의를 받아 근거를 마련한다.	침해사고 처리책임자	

	o 3등급 침해의 경우 침해사고 처리책임자는 해당 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 개인정보보호책임자에게 제출한다. o 개인정보보호책임자는 개인정보침해사고 처리보고서를 검토하고 승인한다. o 개인정보보호책임자는 개인정보침해 관련자에 대한 처분(징계 등)을 해당부서에 요청한다. o 개인정보보호담당자는 개인정보침해사고 처리보고서를 관리하고 처분(징계 등) 결과를 기록한다.	침해사고 처리책임자 / 개인정보보호책임자 및 담당자	
개인정보 침해사고 사후분석	o 침해사고 처리책임자는 처리보고서 제출 후 30일 이내 근본원인 분석, 교훈 및 예방을 위한 개선대책을 마련하여 개인정보보호책임자에게 제출한다.	침해사고 처리책임자	

[별표2] 개인정보침해사고 대응절차