



세명대학교

개인정보 유출등 사고 대응 매뉴얼



2024. 03.

세명대학교
[학술정보원 전산정보팀]

1. 개요

1.1 목적	1
1.2 법적 근거	1
1.3 용어 정의	1
1.4 단계별 프로세스	2
1.5 유출등 대응 업무수행 체계	3

2. 개인정보 유출등 사고 대응 조치 및 피해 구제 방법

2.1 유출등 통지·조회 절차	5
2.2 유출등 신고 절차 및 방법	7
2.3 정보주체 민원 대응 조치	9
2.4 정보주체 불안 해소 조치	9
2.5 피해자 구제 조치	9

3. 개인정보 유출등 원인별 보호 조치

3.1 해킹	10
3.2 내부자 유출	10
3.3 이메일 오발송	11
3.4 개인정보 노출	11

4. 개인정보 유출등 사고 재발방지 조치

4.1 유출등 원인 보완 및 재발방지 조치 계획 수립·이행	12
4.2 재발방지 교육 및 사례 전파	12

【참고자료】

[붙임 1] 개인정보 유출등 신고서(양식)	13
[붙임 2] 개인정보 유출등 신고 조치확인서(양식)	15
[붙임 3] 개인정보 유출등에 따른 2차 피해유형 및 대응요령	21
[붙임 4] 교육부 개인정보보호 포털 유출 신고 절차	24
[붙임 5] 유관기관 관련 연락처	29

개인정보 유출등 대응 절차(요약)

1. 개인정보 유출등 대응 체계 구축

개인정보 유출등 사고 대응팀	개인정보 보호책임자	개인정보 유출등 대응 총괄 지휘, 개인정보 유출등 사고 대응팀 구성·운영
	개인정보 보호담당자	정보주체에게 개인정보 유출 통지, 교육부 또는 개인정보위에 개인정보 유출 신고
	정보보호 담당자	교육부 및 과기정통부에 침해사고 신고, 사고경위 분석, 시스템 복구 등 침해대응
	담당·지원 부서	정부, 언론사, 이용자 민원 대응, 이용자 피해구제 분쟁조정 기구 안내

2. 피해 최소화 및 긴급 조치

유형	대응 방안
해킹	시스템 분리/차단 조치, 로그 등 증거자료 확보, 유출 원인 분석, 정보주체 및 개인정보취급자 비밀번호 변경 등
내부자	유출 경로 확인, 유출에 활용된 컴퓨터/USB/이메일/출력물 등 확보, 취급자의 접근권한 확인, 비정상 접근 경로 차단 등
이메일	발송 이메일 즉시 회수, 수신자에게 오발송 메일 삭제 요청, 대용량 메일 서버 운영자에게 파일 삭제 요청, 파일 전송시 암호화 등
노출	검색엔진 : 노출된 개인정보 삭제 요청, 로봇(크롤링 등)배제 규칙 적용 등 시스템 오류 : 소스 코드, 서버 설정 등 원인 파악 및 수정 등

3. 개인정보 유출등 통지 및 신고

근거법률	개인정보 보호법		교육부 개인정보 보호지침
	제34조(개인정보 유출 등의 통지·신고)		제13조(개인정보 유출등의 신고)
유출 통지	규모	1명 이상	
	시점	72시간 이내(유출등이 되었음을 알게 되었을 때)	
	방법	홈페이지, 서면 등의 방법으로 개별 통지	
	항목	① 유출등이 된 개인정보의 항목, ② 유출등이 된 시점과 그 경위 ③ 유출등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법, ④ 개인정보처리자의 대응조치 및 피해구제 절차, ⑤ 피해 신고·상담 부서 및 연락처 등	
유출 신고	규모	① 1천명 이상 ② 1명 이상 민감정보, 고유식별정보 유출 등 ③ 외부로부터의 불법적인 접근에 의한 개인정보 유출 등	1명 이상
	시점	72시간 이내(유출등이 되었음을 알게 되었을 때)	
	기관	개인정보보호위원회 또는 한국인터넷진흥원 (privacy.go.kr)	교육부 또는 한국교육학술정보원 (privacy.moe.go.kr)

4. 피해 구제 및 재발 방지

정보주체 피해 구제	<ul style="list-style-type: none"> - 홈페이지 등을 통한 유출여부 조회 기능 제공 - 유출로 인한 피해 신고, 접수, 상담, 문의 등 각종 민원대응 방안 마련 - 유출 대응 현장 혼란 최소화 방안 강구 - 보이스피싱 등 2차 피해 방지를 위한 유의 사항 안내 - 피해 보상 계획 마련 및 관련 제도 안내 등
재발 방지 대책 마련	<ul style="list-style-type: none"> - 개인정보 유출 원인 등에 대한 개선방안 마련 - 취급자 대상 개인정보보호 교육 실시 - 홈페이지 취약점 제거 등 개인정보 안전조치 강화 등

1 개요

1.1 목적

- ‘세명대학교 개인정보 유출등 사고 대응 매뉴얼’은 ‘개인정보 보호법’ 및 동법 시행령, 관련 지침 따라 개인정보 유출등 사고에 대하여 신속하고 체계적인 대응을 목적으로 한다.

1.2 법적 근거

- 개인정보 보호법 및 시행령
- 개인정보의 안전성 확보조치 기준(개인정보보호위원회고시)
- 표준 개인정보 보호지침(개인정보보호위원회고시)
- 교육부 개인정보 보호지침(교육부훈령)

1.3 용어 정의

개인정보 유출의 개념

표준 개인정보 보호지침 제25조(개인정보의 유출등) 개인정보의 분실·도난·유출(이하 "유출등"이라 한다)은 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고 개인정보가 해당 개인정보처리자의 관리·통제권을 벗어나 제3자가 그 내용을 알 수 있는 상태에 이르게 된 것을 말한다.

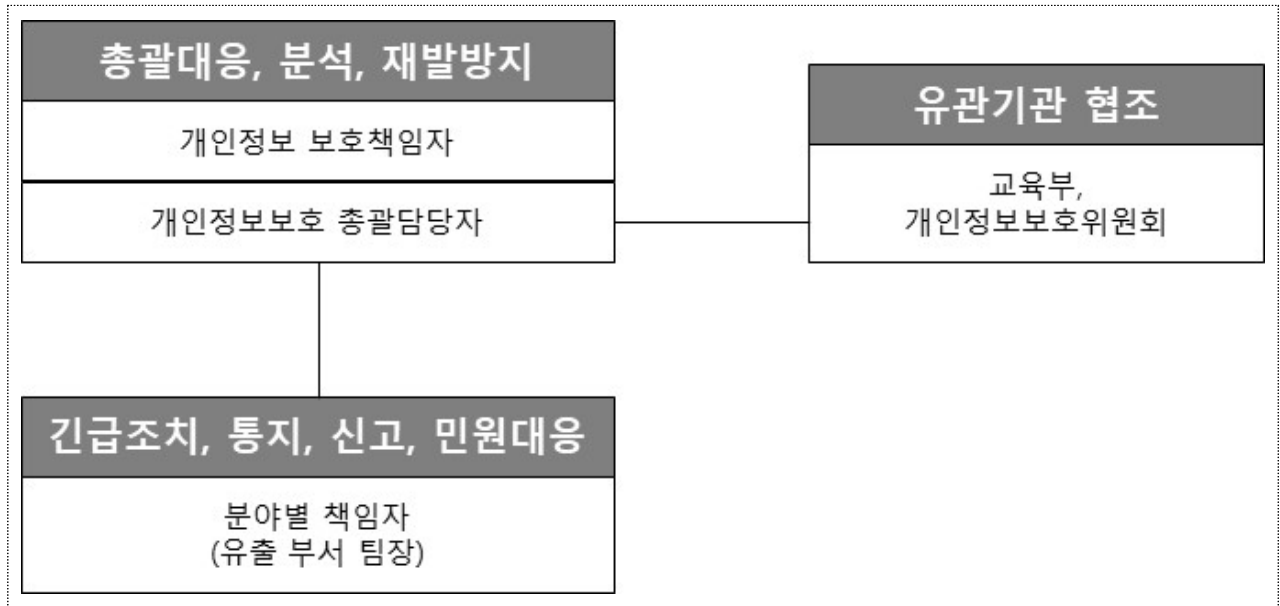
용어	정의
유출등 사고 대응팀	• 개인정보 유출등 사고 발생에 따른 사고의 분석, 처리지원, 사후 복구, 사후 예방조치 등을 주요 업무로 하는 개인정보보호 담당부서를 말함
개인정보 보호책임자	• 개인정보 보호법 제31조에 근거하여 개인정보 처리 업무를 총괄하는 자 • 개인정보 보호담당자를 임명하여 유출등 사고 발생 시 본 절차에 따라 대응토록 함
개인정보 보호담당자	• 개인정보 보호책임자의 지정을 받아 개인정보 보호업무를 수행하는 자
분야별 책임자	• 개인정보 보호책임자의 지휘·감독을 받아 각 업무부서의 개인정보 처리에 관한 업무를 총괄해서 책임지거나 업무처리를 최종적으로 결정하는 자를 말함
분야별 담당자	• 개인정보보호 분야별 책임자의 지정을 받아 개인정보 보호업무를 수행하는 자
개인정보취급자	• 개인정보를 처리하는 업무를 담당하는 자로서 직접 개인정보에 관한 업무를 담당하는 자와 그 밖에 업무상 필요에 의해 개인정보에 접근하여 처리하는 모든 자를 말함

1.4 단계별 프로세스(업무 절차)

단계	상세 업무	비고
사고인지 및 긴급조치	<ul style="list-style-type: none"> ○ 개인정보 유출등 사고 인지 및 신고 접수 <ul style="list-style-type: none"> - 유출등 사고 발생이 의심되는 경우, 지체없이 개인정보 보호담당자에게 신고 ○ 개인정보 보호담당자는 사고 내용 등에 대해 개인정보 보호책임자에게 보고 ○ 유출등 사고 대응반 소집 및 유관기관 협조체계 확인 ○ 피해 최소화를 위한 긴급조치 수행 <ul style="list-style-type: none"> - 유출등이 된 개인정보 비공개 또는 삭제 조치 - 유출등 접속 경로 차단, 취약점 점검·보완 등 긴급조치, 재발방지 조치 등 	
↓		
정보주체 유출등 통지	<ul style="list-style-type: none"> ○ 정보주체에게 개인정보 유출등 사실 통지(72시간 이내) <ul style="list-style-type: none"> - 유출등이 된 개인정보의 항목, 유출등이 된 시점과 그 경위, 피해 구제절차 등 	세부내용 2.1 참고
↓		
개인정보 유출등 신고	<ul style="list-style-type: none"> ○ 1명 이상의 개인정보 유출등 발생 시 교육부(privacy.moe.go.kr)에 유출 신고 ○ ①천명 이상 유출등이 발생하거나, ②민감정보·고유식별정보 1건 이상 또는 ③외부로부터의 불법적인 접근에 의해 1건 이상 유출등 발생 시 교육부 및 개인정보보호위원회(한국인터넷진흥원, privacy.go.kr)에 유출 신고 	세부내용 2.2 참고
↓		
사고분석	<ul style="list-style-type: none"> ○ 유출등 사고 대응반의 조사 및 분석 <ul style="list-style-type: none"> - 사고 원인 분석, 유출등 규모 확인, 사고 원인에 대한 조치 등 	
↓		
민원대응	<ul style="list-style-type: none"> ○ 민원대응을 위한 별도의 온·오프라인 창구 개설·운영 <ul style="list-style-type: none"> - 피해자 구제방안, 수사 진행상황 등에 대한 답변 방향 결정 및 응대 - 2차 피해 방지를 위한 조치방법 안내 등 고객 불안 해소 조치 및 피해구제 절차 안내 	세부내용 2.3~2.5 참고
↓		
유출등 사고 결과보고	<ul style="list-style-type: none"> ○ 개인정보 유출등 사고 결과보고서 작성 및 보고 	
↓		
개선 및 이행점검	<ul style="list-style-type: none"> ○ 개인정보 유출등 사고 사례 전파 교육 및 개선 대책 시행 (재발방지) 	

1.5 유출등 대응 업무수행 체계

○ 조직체계



○ 업무분장

조직	역할	담당 업무
개인정보보호 책임자	총괄지휘	<ul style="list-style-type: none"> 유출등 사고 대응 총괄 지휘
개인정보 보호담당자	총괄대응	<ul style="list-style-type: none"> 유출등 사고 관련사항 개인정보 보호책임자에게 보고 유출등 사고 인지, 접수, 전파 유출등 사고 대응 절차 수립 유출등 사고 조사 결과 유출부서에 통보
	분석	<ul style="list-style-type: none"> 유출등 사고 확인, 조사 및 원인 분석 사고내용 세부조사 및 결과보고
	재발방지	<ul style="list-style-type: none"> 개인정보 유출등 사고 사례 전파 교육 및 안내
분야별책임자	긴급조치	<ul style="list-style-type: none"> 피해 최소화를 위한 긴급조치 수행 ※ 유출등 개인정보 삭제조치 및 기술지원 요청
	유출통지	<ul style="list-style-type: none"> 정보주체에게 유출등 사실 통지(72시간 이내)
	유출신고	<ul style="list-style-type: none"> 교육부 또는 개인정보보호위원회(전문기관)에 유출등 통지 신고(72시간 이내)
	민원대응	<ul style="list-style-type: none"> 유출등 사실 통지문 안내에 따른 후속업무(민원 상담 등) 유출등 사고 관련 대외기관(언론사 등) 대응 개인정보 유출에 대한 피해구제 절차 안내

○ 비상연락망

- 개인정보 유출등 사고 대응팀

조직별	담당자	전화번호
개인정보보호책임자	학술정보원장	043-649-7000
개인정보 보호담당자	전산정보팀장	043-649-7101
분야별책임자	부서별 팀장	
분야별담당자	각 부서 개인정보 보호담당자	

- 협력업체/유지보수업체

업체명	담당 시스템	담당자	전화번호	이메일
(주)트루인테크놀로지스	DBMS시스템	권일용 사원	010-8389-6838	iykwon@truin.kr
(주)트루인테크놀로지스	DB접근제어	전호근 사원	010-9778-7748	hgjeon@truin.kr
(주)트루인테크놀로지스	DB서버	임종석 책임	010-2745-8572	jslim@truin.kr
케이엘정보통신(주)	스토리지	김광일 과장	010-9370-5230	kikim@klic.co.kr
(주)유아이에스	웹서버	조경호 이사	010-6475-0882	khcho@uistech.co.kr
(주)엔엔소프트	그룹웨어	한승빈 대리	010-2043-9067	ho8263@nnsoft.co.kr
(주)케이사인	SSO	신지원 주임	010-2236-0210	support93@ksign.com
(주)케이닷컴	네트워크시스템	김희준 이사	010-6416-4137	hjkim@k-dat.com
(주)엔에스솔루션	방화벽	김민중 주임	010-5185-2842	mjkim@nssolution.co.kr
(주)솔버아이티	웹방화벽	김병선 차장	010-3425-3114	bskim@s-it.kr

2 개인정보 유출등 사고 대응 조치 및 피해 구제 방법

2.1 유출등 통지·조회 절차

- 분야별책임자(유출등 부서의 팀장)는 유출등 인원 등을 확인하여 유출등 통지 방법에 따라 개인정보 유출등 통지문(예시)을 참고하여 정보주체들에게 유출등 통지

근거법률		개인정보 보호법	교육부 개인정보 보호지침
		제34조(개인정보 유출등 등의 통지·신고)	제13조(개인정보 유출등의 신고)
유출 통지	규모	1명 이상	
	시점	72시간 이내(유출등이 되었음을 알게 되었을 때)	
	방법	홈페이지, 서면 등의 방법으로 개별 통지	
	항목	① 유출등이 된 개인정보의 항목, ② 유출등이 된 시점과 그 경위 ③ 유출등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법, ④ 개인정보처리자의 대응조치 및 피해구제 절차, ⑤ 피해 신고·상담 부서 및 연락처 등	
유출 신고	규모	① 1천명 이상 ② 1명 이상 민감정보, 고유식별정보 유출 등 ③ 외부로부터의 불법적인 접근에 의한 개인정보 유출 등	1명 이상
	시점	72시간 이내(유출등이 되었음을 알게 되었을 때)	
	기관	개인정보보호위원회 또는 한국인터넷진흥원 (privacy.go.kr)	교육부 또는 한국교육학술정보원 (privacy.moe.go.kr)

- 수탁사업자가 수탁 업무를 처리하는 과정에서 개인정보가 유출등이 된 경우 즉시 위탁자에게 보고하도록 표준 개인정보처리위탁 계약서에 명시하고, 수탁 사업자로부터 보고 받은 시점에서 지체 없이 유출 통지
- 1명 이상 개인정보 유출등이 되었음을 알게 되었을 때에는 서면 등의 방법으로 72시간 이내에 유출등 통지 항목 5개를 정보주체에게 안내
 - 정보주체의 연락처를 알 수 없는 경우 인터넷 홈페이지에 통지항목 5개를 30일 이상 게시하는 것으로 정보주체 유출등 통지 의무를 갈음할 수 있음
- 정보주체가 개인정보 유출등 여부 등을 확인가능 하도록 별도의 홈페이지 등을 제공
 - ※ 개인정보 유출등 결과는 전체 공지가 아닌 핸드폰 인증 등을 통해 정보주체가 개별 본인 확인 후 개인정보 유출등 결과 조회 지원

개인정보 유출등 통지문(예시)

통지문(예시)	작성 준수사항
<p>개인정보 유출 사실을 통지해 드리며, 깊이 사과드립니다.</p>	
<p>❶ 고객님의 개인정보는 ○○○○년 ○○월 ○○일 해커에 의한 홈페이지 내 약성코드가 삽입되어 ○○건이 유출된 것으로 확인되었습니다. 유출된 정확한 일시는 에서 현재 수사가 진행 중이며, 확인되면 추가로 알려 드리도록 하겠습니다.</p>	<p>❶ 개인정보 유출 등이 발생한 시점과 확인한 유출 건수를 누구나 이해할 수 있게 상세하게 설명 <small>☞ 잘못된 사례: '회원정보 일부' 등</small></p>
<p>❷ 유출된 개인정보 항목은 이름, 아이디(ID), 비밀번호(P/W), 이메일, 휴대전화번호 총 5개 항목입니다.</p>	<p>❷ 유출된 개인정보 항목은 누락없이 모두 나열하여야 함 <small>☞ 잘못된 사례: '등'으로 생략하거나, 회사전화 번호, 집전화번호를 '전화번호'로 통칭</small></p>
<p>❸ 유출 사실을 인지한 후 해당 약성코드는 즉시 삭제하였으며, 해커가 접속한 해당 IP와 우회 접속한 IP를 차단하고, 추가적인 홈페이지 취약점 점검과 보완 조치를 하였습니다. 더불어 침입방지시스템을 추가 도입하여 24시간 모니터링을 수행하고 있습니다.</p>	<p>❸ 개인정보처리자 등의 대응조치 내용 접속경로 차단 등 예시된 항목 외에도 망분리, 방화벽 설치, 개인정보 암호화, 인증 등 접근통제, 시스템 모니터링 강화 등 조치한 사항을 설명</p>
<p>❹ 이번 사고로 인해 유출된 개인정보를 이용하여 웹사이트 명의도용, 보이스피싱, 파밍 등 2차 피해의 우려가 있으므로 혹시 모를 피해를 막기 위하여 고객님의 비밀번호를 변경하여 주시기 바랍니다.</p>	<p>❹ 이용자가 취할 수 있는 조치 방법 유출된 개인정보, 경로 등에 따라 발생할 수 있는 피해를 추정하여 가능한 피해예방 조치를 모두 안내(예: 보이스피싱, 피싱메일, 불법TM, 스팸문자 등)</p>
<p>❺ 비밀번호 변경하기</p>	<p>❺ 이용자의 비밀번호 변경페이지로 연결</p>
<p>❻ 개인정보 악용으로 의심되는 전화, 메일 등을 받으시거나 기타 궁금하신 사항은 아래 피해 등 접수 담당부서로 연락해주시기 바랍니다.</p> <p>▶ 피해 등 접수 담당부서: ○○○○팀 (000-123-0000) ▶ 피해 등 접수 e-메일: ○○○○@oooo.co.kr</p> <p style="text-align: right;">○○○교육기관</p>	<p>❻ 이용자가 상담 등을 접수할 수 있는 부서 및 연락처 전담처리부서 안내를 원칙으로 하되, 대량 유출로 일시적으로 콜센터 등 다른 부서를 지정한 경우 해당 부서를 안내</p>
<p>❼ 개인정보 유출 여부 조회하기</p>	<p>❼ 이용자가 자신의 개인정보 유출여부를 조회할 수 있도록 절차를 마련</p>

2.2 유출등 신고 절차 및 방법

○ 유출등 신고 절차



○ 유출등 신고 방법

구분	내용
신고 대상	<ul style="list-style-type: none"> ▶ 개인정보가 1천명 이상 유출등이 됐거나, 민감정보·고유식별정보 및 외부로부터의 불법적인 접근에 의해 1건이라도 유출이 된 경우는 교육부 및 개인정보위(또는 한국인터넷진흥원)에 신고 ▶ 1명 이상 유출등이 된 경우 교육부에 신고
신고 시기	<ul style="list-style-type: none"> ▶ 유출등이 되었음을 알게 된 후 72시간 이내 ※ 유출등의 경로가 확인되어 해당 개인정보를 회수·삭제하는 등의 조치를 통해 정보주체의 권익 침해 가능성이 현저히 낮아진 경우에는 신고하지 않을 수 있음
신고 방법	<ul style="list-style-type: none"> ▶ 교육부(privacy.moe.go.kr) 및 개인정보보호위원회(privacy.go.kr) 홈페이지를 통해 유출등 신고서 제출 ※ 부득이한 경우 전자우편 등을 통해 개인정보 유출등 신고서 제출
신고 내용	<ul style="list-style-type: none"> ▶ 기관명, 통지여부, 유출등이 된 개인정보 항목·규모, 유출등 시점·경위, 유출등 피해 최소화 대책·조치 및 결과, 정보주체가 할 수 있는 피해 최소화 방법 및 구제절차, 담당부서·담당자 연락처 등 ※ 정보주체에 대한 유출등 통지 결과 및 피해 최소화를 위한 긴급 조치 내용이 포함되도록 해야 함
신고 양식	<ul style="list-style-type: none"> ▶ [붙임 1] 개인정보 유출등 신고서 (양식)

※ 조치결과는 교육부 개인정보 보호지침 제14조(개인정보의 유출등 조사)에 따라 [붙임 2] 개인정보 유출등 신고 조치확인서 작성 및 제출(moeprivacy@keris.or.kr)

개인정보 유출등 신고서 작성 방법

유출등 신고서 양식	작성 방법
① 유출등이 된 개인정보 항목	<ul style="list-style-type: none"> - 유출등이 된 개인정보 항목을 모두 기재해야 하며, ‘등’과 같이 일부 생략하거나 휴대전화 번호와 집 전화번호를 ‘전화번호’로 기재하여서는 안됨 - 유출등이 된 개인정보의 모든 항목을 적어야 하며, 유출 등 규모도 현 시점에서 파악된 내용을 모두 작성
② 유출등이 된 시점과 그 경위	<ul style="list-style-type: none"> - 유출등 시점, 인지시점을 명확히 구분하여 날짜 및 시간 모두 작성해야 하며, 유출등 경위와 인지경위를 포함
③ 정보주체가 취할 수 있는 피해 최소화 조치	<ul style="list-style-type: none"> - 개인정보 유출등으로 발생 가능한 스팸 문자, 보이스피싱, 금융사기와 같은 2차적인 피해 방지를 위해 이용자가 할 수 있는 조치를 기재(예: 비밀번호 변경 등)
④ 개인정보처리자 대응조치 및 피해 구제절차	<ul style="list-style-type: none"> - 유출등 사실을 안 후 긴급히 조치한 내용과 향후 이용자의 피해구제를 위한 계획 및 절차를 기재 ex) 경찰에 신고, 일시적 홈페이지 로그인 차단(홈페이지 해킹일 경우) 등
⑤ 정보주체가 피해 신고·상담 등을 접수할 수 있는 부서 및 연락처	<ul style="list-style-type: none"> - 실제 신고 접수 및 상담이 가능한 전담 처리부서와 해당 담당자 연락처를 기재
⑥ 기타	<ul style="list-style-type: none"> - 유출등이 된 기관명, 사업자번호, 사업자 주소, 웹사이트 주소 등 기재

2.3 정보주체 민원 대응 조치

- 분야별책임자(부서별 팀장)는 유관부서(개인정보 보호담당자 등)와 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 민원대응반으로 단일화하여 홈페이지(semyung.ac.kr)에 공지하고 타 팀에서 외부로부터 개인정보 유출등 관련 질문을 받으면 최대한 민원대응반으로 연결

2.4 정보주체 불안 해소 조치

- 홈페이지(semyung.ac.kr)에 유출등 피해 최소화를 위해 현재 기관에서 실시하고 있는 노력에 대한 사항 공지(1일 1회 이상 업데이트)
- 비밀번호 등 유출등 시 비밀번호 변경 등을 할 수 있도록 유출등 통지 시 함께 안내
 - ※ 불법스팸대응센터(☎118, spam.kisa.or.kr)를 통하여 불법스팸신고 및 차단등을 구체적으로 안내

[개인정보 유출등 항목별 2차 피해 예방을 위한 안내사항]

항목	세부 안내 사항
아이디, 비밀번호 유출	- 비밀번호 변경 안내
다량의 개인정보 유출	- 보이스피싱 등 2차 피해 예방 안내

- (정보주체 요청이 있을 시) 회원 탈퇴 방법 안내 및 정보주체의 개인정보 삭제 조치

2.5 피해자 구제 조치

- 정보주체에게 개인정보 유출등 피해에 대한 피해구제, 상담 등을 문의 할 수 있음을 안내
- 개인정보를 유출등 당한 사람은 누구든지 개인정보 분쟁조정위원회에 분쟁조정을 신청할 수 있음을 안내(「개인정보 보호법」 제43조제1항)
- 정보주체는 개인정보처리자가 이 법을 위반한 행위로 손해를 입으면 개인정보처리자에게 손해배상을 청구할 수 있음을 안내

3 개인정보 유출등 원인별 보호 조치

3.1 해킹

- 개인정보가 유출이 된 사실을 알게 된 경우에는 개인정보 추가 유출 방지를 위한 대책을 마련하고 피해를 최소화할 수 있는 조치를 강구하여야 함
 - 유출된 시스템 분리·차단 조치, 관련 로그 등 증거자료 확보, 유출 원인 분석, 이용자 및 개인정보취급자 비밀번호 변경* 등 기술적 보호조치 강화, 시스템 변경, 기술지원 의뢰 및 복구 등과 같은 긴급 조치를 시행하여야 함
 - * 일방향 암호화되지 않은 비밀번호가 유출되었거나, 해커 등이 이용자의 비밀번호를 알고 있다고 판단되는 경우에는 이용자가 비밀번호를 변경하지 않으면 이용할 수 없도록 하고, 일방향 암호화된 비밀번호가 유출된 경우에도 비밀번호 변경을 유도하여 추가 피해 예방 방지
 - 사고원인 조사 등 조치가 완료된 이후에는 개인정보 유출의 직·간접적인 원인을 즉시 제거하고, 미비한 보호조치 부분을 파악하기 위한 취약점 점검·개선 조치 등을 수행하여야 함

3.2 내부자 유출

- 개인정보 유출자가 개인정보처리시스템에 접속한 이력 및 개인정보 열람·다운로드 등 내역을 확인하여야 함
- 개인정보 유출자의 개인정보처리시스템에 대한 접근·접속 경로 등을 확인하고, 비정상적인* 접속인 경우 접속경로를 확인하여 차단하여야 함
 - * 비인가된 개인정보 처리, 대량의 개인정보에 대한 조회·정정·다운로드·삭제·출력 등
- 개인정보취급자의 개인정보처리시스템 접속계정, 접속권한, 접속기록 등을 검토하여 추가적인 유출 여부를 확인하여야 함
- 개인정보 유출에 활용된 단말기(PC, 스마트폰 등)와 매체(USB, 이메일, 출력물 등)를 회수하고, 필요시 수사기관 등과 협조하여 유출된 개인정보를 회수하기 위한 모든 방법을 강구하여야 함

3.3 이메일 오발송

- 이메일 회수가 가능한 경우에는 즉시 회수 조치하고, 불가능한 경우에는 이메일 수신자에게 오발송 메일의 삭제를 요청*하여야 함
 - * 삭제 요청시 가능한 삭제되었음을 확인할 수 있는 증빙자료 첨부를 같이 요청 (예: 삭제전 목록화면과 삭제후 목록화면을 받음)
- 메일서버 외 첨부파일서버(대용량 메일 등)를 이용하는 경우 첨부파일서버 운영자에게 관련 파일의 삭제를 요청하여야 함

3.4 개인정보 노출

- (외부 검색엔진을 통한 노출의 경우) 노출된 사업자의 웹페이지 삭제를 검토하고, 검색엔진에 노출된 개인정보 삭제를 요청하여야 하며, 필요시 로봇배제 규칙*을 적용하여 외부 검색엔진의 접근을 차단하여야 함
 - * 홈페이지 공개 원칙에 벗어나지 않는 범위 내에서 로봇배제 적용 필요
- (관리자 페이지에 접속하여 노출된 경우) 관리자의 접속 IP를 제한하고, 소스코드를 수정하여 사용자 인증 절차를 추가하여야 함
- (개인정보취급자 부주의로 인한 노출의 경우) 게시글 및 첨부파일 내 개인정보 노출 부분을 삭제 또는 마스킹 처리하여 필요한 경우 다시 게시하여야 함
- (상용 오피스 취약점으로 노출된 경우) S/W버전은 항상 최신버전*으로 이용하며 홈페이지 첨부파일 탑재 시 엑셀 문서는 PDF 등으로 변환**하여 탑재
 - * 엑셀2003 이하에서는 외부링크 취약점이 존재하여 엑셀2007 이상 버전 사용(관련문서: 교육부 교육정보화과-4027(2017.08.04.))
 - ** 엑셀은 OLE개체, 열·행·시트 숨김, 치환함수, 피벗테이블 등의 다양한 기능으로 사용자가 인지하지 못하는 개인정보 등 노출 발생 가능성 높음

4 개인정보 유출등 사고 재발방지 조치

4.1 유출 원인 보완 및 재발방지 조치 계획 수립·이행

- 개인정보 유출등 원인별 긴급 보호조치를 취한 이후 보완대책 점검 및 보완 실시
- 중장기 보완대책을 위해 재발방지 계획을 수립하고 수립된 계획에 따라 이행 실시*

* 개인정보의 안전성 확보조치 기준(개인정보보호위원회고시 제2023-6호)에 따라 개인정보보호 책임자가 내부관리계획의 이행실태를 연 1회 이상 점검

4.2 재발방지 교육 및 사례 전파

- 기관내 구성원 재발방지 교육 실시
 - 개인정보 유출등과 관련된 부서내 모든 취급자는 필수적으로 재발방지 교육 실시
- 개인정보 유출등 사례를 내부공지 등을 통해 기관내 구성원에게 사례를 전파*
 - * 사례전파 시 또 다른 개인정보 유출등이 발생하지 않도록 주의 필요
 - 사례 전파의 구성(예시)

구분	구성 내용
사고 개요	<ul style="list-style-type: none"> • 0년 0월 0일 개인정보 취급자가 홈페이지 게시판 관리 중 개인정보가 포함된 파일을 게시판에 탑재함 • 개인정보가 포함된 파일(엑셀)을 00으로부터 0년 0월 0일 인지하여 해당파일 삭제 조치함 • 개인정보 00건, 포함된 개인정보 항목은 00을 포함한 총 00개가 유출됨
사고 처리 절차	<ul style="list-style-type: none"> • 정보주체에게 유출통지를 하였으며, 홈페이지에 관련 내용을 탑재하여 전파 • 피해 구제 방안 등 정보주체 민원 대응반 구축 • 재발방지대책(교육 등)을 수립
기관 보완 조치 내용	<ul style="list-style-type: none"> • 개인정보 취급자 대상 개인정보 교육 실시 • 개인정보 웹 필터링 시스템 도입으로 개인정보 파일 검출 • 기관 개인정보 체계 강화를 위한 홍보자료 및 사례 전파 실시
향후 기관의 보완 방향	<ul style="list-style-type: none"> • 개인정보 필터링 시스템 등 개인정보 체계 강화를 위한 시스템 구축 • 매년 개인정보 취급자 대상 개인정보 교육 실시
관련 변경 지침	<ul style="list-style-type: none"> • 내부관리 계획 수립 시 개인정보 유출 재발방지 계획 포함

붙임1 **개인정보 유출등 신고서(양식)**

개인정보 유출등 신고서

기관명					
유출등이 된 개인정보 항목 및 규모					
유출등이 된 시점과 그 경위					
유출등 피해 최소화를 위해 정보주체가 할 수 있는 방법 등					
개인정보처리자의 대응 조치 및 피해 구제절차					
정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처					
유출등 신고(보고) 담당자		성명	부서	직위	연락처
	개인정보 보호책임자				
	담당자 (취급자)				

유출등 신고 접수기관	기관명	담당자명	연락처

개인정보 유출등 신고서(작성 사례)

기관명	교육 고등학교				
유출등이 된 개인정보 항목 및 규모	<ul style="list-style-type: none"> 유출규모: 1,150명(중복제거 후 1,100명) - 교육부 신고(2024.3.22. 13:00), 개인정보위 신고여부(2024.3.22. 12:00) 유출항목: 이름, ID, 비밀번호, 주소, 핸드폰번호, 이메일 				
유출등이 된 시점과 그 경위	<ul style="list-style-type: none"> 사고발생 인지경위(인지시점 포함) <ul style="list-style-type: none"> - 2024.3.21 10:00 월별 개인정보처리시스템 접속로그 점검 시 특정 IP로부터 다량의 개인정보 다운로드 기록 확인 - 2024.3.21 11:00 개인정보처리시스템의 로그 확인 결과 알 수 없는 개인정보 압축 파일 발견 - 2024.3.21 12:00 IP Table, NAC 등을 확인하여 개인정보를 다운로드한 특정 IP의 PC(용역업체 개인 PC) 확인 유출 시점 및 경위 <ul style="list-style-type: none"> - 2024.3.4 20:00 용역업체 A씨는 개인정보처리시스템에 접속하여 다량의 개인정보파일을 생성 후 PC로 다운로드 - 2024.3.4 21:00 PC내 보안 솔루션(NAC 등)에 의하여 상용 이메일 접근 불가 확인 후 개인 이메일 서버로 파일 전송 				
유출등 피해 최소화를 위해 정보주체가 할 수 있는 방법 등	<ul style="list-style-type: none"> 정보주체가 할 수 있는 피해최소화 방법 <ol style="list-style-type: none"> ① 2차 피해 방지를 위하여 개인정보 유출 여부 조회(학교 홈페이지 등) ② 유출사고 발생 후 홈페이지 로그인시 개인정보 유출에 따른 비밀번호 변경 사고발생 후 조치사항 <ol style="list-style-type: none"> ① 기관 개인정보 유출사고 대응 매뉴얼에 따라 유출사고 대응반 구축 ② 개인정보 유출 접수 창구 및 민원 대응 창구 구축 ③ 유출 항목 및 발생 상황 인지 후 유출 통지문 작성 및 관련 내용 통지, 교육부 개인정보 유출 신고 ④ 유출 원인에 따른 개인정보처리시스템에 대한 접근권한 관리체계 강화 ⑤ 재발방지 대책을 위한 보안강화 계획(안) 수립 				
정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처	<ol style="list-style-type: none"> ① 2차 피해 접수를 위한 피해 접수 담당 창구 운영(02-124-2345, abcd@efgf.co.kr) ② 개인정보 유출 관련 개인정보 분쟁조정 신청 창구 안내(1833-6972) 				
정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처		성명	부서	직위	연락처
	개인정보 보호책임자	김영희	총무과	총무과장	044-123-1234
	개인정보 취급자	홍길동	총무과	담당자	044-123-1234
유출 신고 접수기관	기관명	담당자명		연락처	
	한국교육학술정보원 및 00시도교육청	김철수		044-234-5678	

붙임2 **개인정보 유출등 신고 조치확인서(양식)**

개인정보 유출등 신고 조치확인서(양식)

※ 6하 원칙에 따라 사실 관계를 명확하게 작성(moeprivacy@keris.or.kr로 제출).

기관명		00학교													
정보주체 통지 여부	통지일시	2024.00.00. 12:00													
	통지방법	(예시) 전화, 이메일, 서면, 팩스, 홈페이지 공개* 등 * 정보주체의 연락처를 알 수 없는 경우													
	필수통지 항목	<table border="1"> <thead> <tr> <th>필수 통지 항목 5가지</th> <th>포함 여부 확인(O, X)</th> </tr> </thead> <tbody> <tr> <td>① 유출등이 된 개인정보의 항목</td> <td>○ 또는 X</td> </tr> <tr> <td>② 유출등이 된 시점과 및 그 경위</td> <td>○ 또는 X</td> </tr> <tr> <td>③ 피해 최소화를 위한 정보주체가 할 수 있는 방법</td> <td>○ 또는 X</td> </tr> <tr> <td>④ 기관의 대응조치 및 피해구제 절차</td> <td>○ 또는 X</td> </tr> <tr> <td>⑤ 피해 신고·상담 부서 및 연락처 등</td> <td>○ 또는 X</td> </tr> </tbody> </table>		필수 통지 항목 5가지	포함 여부 확인(O, X)	① 유출등이 된 개인정보의 항목	○ 또는 X	② 유출등이 된 시점과 및 그 경위	○ 또는 X	③ 피해 최소화를 위한 정보주체가 할 수 있는 방법	○ 또는 X	④ 기관의 대응조치 및 피해구제 절차	○ 또는 X	⑤ 피해 신고·상담 부서 및 연락처 등	○ 또는 X
		필수 통지 항목 5가지	포함 여부 확인(O, X)												
① 유출등이 된 개인정보의 항목		○ 또는 X													
② 유출등이 된 시점과 및 그 경위		○ 또는 X													
③ 피해 최소화를 위한 정보주체가 할 수 있는 방법		○ 또는 X													
④ 기관의 대응조치 및 피해구제 절차		○ 또는 X													
⑤ 피해 신고·상담 부서 및 연락처 등	○ 또는 X														
(예시) 이메일, 팩스, 홈페이지 공개 등 내용 이미지 캡처 등 증빙자료 포함															
발생(인지) 일자	2024.00.00.														
발생(인지) 경로	(예시) - 2024.00.00 00:00 KISA에서 통보 - 정보주체가 해당 학과에 신고, ECSC 사고 신고, 민원인 신고 등														

유출등 사실 인지 이후 후속 조치 경과 (유출등 피해 최소화 대책·조치 및 결과)	<p>개인정보 유출등 발생시 아래 사항 준수</p> <ol style="list-style-type: none"> 개인정보 유출등 대응 매뉴얼 구비 <ul style="list-style-type: none"> ※ 법령에 기반하여 최신화 되어있는지 확인 및 개선, 유출등 발생시 매뉴얼대로 즉시 신고 등 대응 유출등 원인 보완 및 재발방지 조치계획 수립·이행 개인정보취급자(전직원) 대상 사례 전파 및 재발방지 교육 <ul style="list-style-type: none"> ※ 개인정보보호 관련 전직원 교육 실시, 특히 신규 직원은 업무 투입 전 개인정보보호 기본 교육 실시 후 투입 그 밖의 개인정보의 유출등 방지를 위해 필요하다고 판단되는 사항 		
	<p>(예시)</p> <ul style="list-style-type: none"> - 2024.00.00 00:00 해당 게시글 삭제 - 2024.00.00 00:00 정보주체에게 메일, 문자로 안내 - 2024.00.00 00:00 홈페이지취약점 점검 수행 - 2024.00.00 00:00 홈페이지에 유출 건 내용 게시 - 2024.00.00 00:00 재발방지대책 수립 - 2024.00.00 00:00 전직원 대상 개인정보 관련 교육 - 개인정보 파일 삭제, 오발송된 이메일 회수, 사례전파, 교육실시 등 증빙자료 포함 		
교육부 신고 일시 (1명 이상 유출등)	2024. 0. 00. 12:00	[교육부 신고] 유출등 통지 및 조치 결과를 지체 없이 상급기관을 경유하여 교육부에 신고(교육부 개인정보보호 포털(privacy.moe.go.kr))	
개인정보보호위원회 신고 일시 (1천명 이상, 민감정보·고유식별정보, 외부로부터의 불법적인 접근으로 유출등)	2024. 0. 00. 12:00	[교육부 및 개인정보보호위원회 신고] 유출등 통지 및 조치 결과를 지체 없이 상급기관을 경유하여 교육부에 신고하고(교육부 개인정보보호 포털, 개인정보보호위원회(또는 한국인터넷진흥원, www.privacy.go.kr)에 신고	
유출등이 된 개인정보	규모(명)	00명	(중복제거) 00명
	항목	이름, 핸드폰번호 ,,,,	
유출등이 된 시점과 그 경위	<p>(예시)</p> <ul style="list-style-type: none"> - 2024.00.00 00:00 메일 잘못 발송, 실수로 개인정보 파일 첨부함 - 2024.00.00 00:00 유출 확인 		

<p>정보주체가 할 수 있는 피해 최소화 방법 및 구제 절차</p>	<p>(예시) 피해구제 절차 안내 등</p>
<p>진행 사항 또는 향후 계획</p>	<p>(예시) 자체 내부 감사 수행, 상위기관 현장 컨설팅 수행, 개인정보보호위원회 점검 예정 등</p>

※ 유출등 신고 후 1주일 이내 조치 확인서를 작성하여 교육부 개인정보보호 포털- 유출신고 내역을 수정하여 제출하거나 메일(moeprivacy@keris.or.kr)로 반드시 제출

개인정보 유출등 신고 조치 확인서(작성 사례)

※ 6하 원칙에 따라 사실 관계를 명확하게 작성(moeprivacy@keris.or.kr로 제출).

기관명	교육 고등학교												
정보주체 통지 여부	통지일시	2024. 3. 22. (화) 13:00											
	통지방법	이메일 및 유선 전화											
	필수통지 항목	<table border="1"> <thead> <tr> <th>필수 통지 항목 5가지</th> <th>포함 여부 확인(O, X)</th> </tr> </thead> <tbody> <tr> <td>① 유출등이 된 개인정보의 항목</td> <td>○</td> </tr> <tr> <td>② 유출등이 된 시점과 및 그 경위</td> <td>○</td> </tr> <tr> <td>③ 피해 최소화를 위한 정보주체가 할 수 있는 방법</td> <td>○</td> </tr> <tr> <td>④ 기관의 대응조치 및 피해구제 절차</td> <td>○</td> </tr> <tr> <td>⑤ 피해 신고·상담 부서 및 연락처 등</td> <td>○</td> </tr> </tbody> </table> <p style="text-align: center;">개인정보 유출 사실을 통지해 드리며, 깊이 사과드립니다.</p> <p>고객님의 개인정보는 2023년 3월 4일 00용역업체 직원에 의하여 외부 유출된 사실을 확인하였고, 2차 피해 예방을 위해 경찰청에 즉시 조사를 의뢰하여 수사진행 중입니다.</p> <p>유출된 개인정보 항목은 이름, 아이디(ID), 비밀번호(P/W), 이메일, 핸드폰번호, 주소 총 6개 항목입니다.</p> <p>유출 사실을 인지한 후 즉시 접속 경로를 차단하고, 취약점 점검과 보완 조치를 완료 하였습니다.</p> <p>현재까지 확인한 바로는 경찰청에서 00용역업체 직원이 외부로 유출된 개인정보는 제3자에게 2차 전달하거나 판매하지 않는 것으로 확인 되었습니다.</p> <p>혹시 모를 피해를 최소화하기 위하여 00시스템과 동일한 ID 및 비밀번호를 사용하고 있는 웹사이트가 있다면, 귀하의 계정정보(ID/비밀번호)를 변경하여 주시기 바랍니다.</p> <p>아울러 피해가 발생하였거나 기타 궁금하신 사항은 아래 담당부서에 신고하시면 성실하게 안내와 상담을 해 드리고, 필요한 조치를 거쳐 손해 배상 등의 구제절차를 진행하도록 하겠습니다.</p> <p>앞으로 해당 서비스에 대한 보안 및 개인정보보호 조치 강화 등 개인정보에 대한 관리체계를 개선하고, 향후 다시는 이와 유사한 사례가 발생하지 않도록 최선의 노력을 다하겠습니다.</p> <p>귀하게 실례를 끼쳐 드리게 되어 거듭 진심으로 사과 드립니다.</p> <p>▶ 피해 등 접수 담당부서: 0000팀(00-0000-0000) ▶ 피해 등 접수 메일:0000@0000.kr</p> <p style="text-align: right;">00교육기관 000</p>	필수 통지 항목 5가지	포함 여부 확인(O, X)	① 유출등이 된 개인정보의 항목	○	② 유출등이 된 시점과 및 그 경위	○	③ 피해 최소화를 위한 정보주체가 할 수 있는 방법	○	④ 기관의 대응조치 및 피해구제 절차	○	⑤ 피해 신고·상담 부서 및 연락처 등
필수 통지 항목 5가지	포함 여부 확인(O, X)												
① 유출등이 된 개인정보의 항목	○												
② 유출등이 된 시점과 및 그 경위	○												
③ 피해 최소화를 위한 정보주체가 할 수 있는 방법	○												
④ 기관의 대응조치 및 피해구제 절차	○												
⑤ 피해 신고·상담 부서 및 연락처 등	○												

발생(인지) 일자	2024.3.21.	
발생(인지) 경로	<ul style="list-style-type: none"> - 2024.3.21 10:00 월별 개인정보처리시스템 접속로그 점검 시 특정 IP로부터 다량의 개인정보 다운로드 기록 확인 - 2024.3.21 10:30 정보보안 솔루션(방화벽, IPS 등) 로그 분석 결과 외부 해킹 공격은 없음 - 2024.3.21 11:00 개인정보처리시스템의 로그 확인 결과 알 수 없는 개인정보 압축 파일 발견 - 2024.3.21 12:00 IP Table, NAC 등을 확인하여 개인정보를 다운로드한 특정 IP의 PC(용역업체 개인 PC) 확인 - 2024.3.21 13:00 해당 PC 점검 및 유출 내용 확인 	
유출등 사실 인지 이후 후속 조치 경과 (유출등 피해 최소화 대책·조치 및 결과)	<ul style="list-style-type: none"> - 2024.3.21. 12:00 기관 개인정보 유출사고 대응 매뉴얼에 따라 유출사고 대응반 구축 - 2024.3.21. 13:30 개인정보 유출 접수 창구 및 민원 대응 창구 구축 - 2024.3.21. 14:00 유출 항목 및 발생 상황 인지 후 유출 통지문 작성 및 관련 내용 통지, 개인정보보호위원회 및 교육부 개인정보 유출 신고 - 2024.3.21. 14:30 유출 원인에 따른 개인정보처리시스템에 대한 접근권한 관리체계 강화 - 2024.3.21. 15:00 유출 피해 최소화를 위해 추가 확인 정보 공지 및 관련 내용 현행화 실시 - 2024.3.21. 15:30 재발방지 대책을 위한 보안강화 계획(안) 수립 <ul style="list-style-type: none"> 1) 보안 솔루션 도입 2) 전 직원대상 사례 전파 교육 및 개인정보 교육 3) 모든 개인정보처리시스템 대상 안전성 확보 조치 방안 점검 	
교육부 신고 일시 (1명 이상 유출등)	2024. 3. 22. 14:00	[교육부 신고] 유출 통지 및 조치 결과를 지체 없이 상급기관을 경유하여 교육부에 신고(교육부 개인정보보호 포털(privacy.moe.go.kr))
개인정보보호위원회 신고 일시 (1천명 이상, 민감정보·고유식별정보, 외부로부터의 불법적인 접근으로 유출등)	2024. 3. 22. 14:00	[교육부 및 개인정보보호위원회 신고] 유출 통지 및 조치 결과를 지체 없이 상급기관을 경유하여 교육부에 신고하고(교육부 개인정보보호 포털, 개인정보보호위원회(또는 한국인터넷진흥원, www.privacy.go.kr)에 신고
유출등이 된 개인정보	규모(명)	1,150명 (중복제거) 1,100명(학생 600명, 학부모 200명, 교직원 300명)
	항목	이름, ID, 비밀번호, 주소, 핸드폰번호, 이메일
유출등이 된 시점과 그 경위	<ul style="list-style-type: none"> - 2024.3.4 20:00 용역업체 A씨는 개인정보처리시스템에 접속하여 다량의 개인정보파일을 생성 후 PC로 다운로드 - 2024.3.4 21:00 PC내 보안 솔루션(NAC 등)에 의하여 상용 이메일 접근 불가 확인 후 개인 이메일 서버로 파일 전송 	

<p>정보주체가 할 수 있는 피해 최소화 방법 및 구제절차</p>	<ul style="list-style-type: none"> ▪ 정보주체가 할 수 있는 피해최소화 방법 ① 2차 피해 방지를 위하여 개인정보 유출 여부 조회(학교 홈페이지 등) ② 유출사고 발생 후 홈페이지 로그인시 개인정보 유출에 따른 비밀번호 변경 ▪ 피해자 구제절차 ① 2차 피해 접수를 위한 피해 접수 담당 창구 운영 (02-124-2345, abcd@efgf.co.kr) ② 개인정보 유출 관련 개인정보 분쟁조정 신청 창구 안내(1833-6972)
<p>진행사항 또는 향후계획</p>	<ul style="list-style-type: none"> ① 개인정보 파일 운영 강화를 위한 보안 솔루션 도입(DLP, DRM 등) ② 용역업체(유지보수 등)가 접속할 수 있는 별도의 계정 생성 ③ 개인정보취급자 대상 개인정보보호 교육 강화 ④ 모든 개인정보처리시스템 대상 개인정보 보호법 등 관련 법률에 따라 개인정보 안전성 확보 조치 이행사항 확인 및 관련 내용 점검

※ 유출등 신고 후 1주일 이내 조치 확인서를 작성하여 교육부 개인정보보호 포털-유출신고 내역을 수정하여 제출하거나 메일(moeprivacy@keris.or.kr)로 반드시 제출

붙임3

개인정보 유출등에 따른 2차 피해유형 및 대응요령

	피해종류	활용된 개인정보 주요항목	개인정보 악용 절차	이용자 대응요령
	온라인 사기쇼핑	주민등록번호, 카드번호, 유효기간 등	① 카드번호, 유효기간으로 온라인 결제가 가능한 국내외 홈쇼핑 사이트에 접속 ② 홈쇼핑 홈페이지, ARS를 통한 온라인 사기 결제·주문	<ul style="list-style-type: none"> • 신용카드 정지 및 재발급 신청 ※ 신고기관 : 각 카드사, 한국소비자원 소비자상담센터(☎1372) 등
금전적	명의도용을 통한 통신서비스 가입	이름, 주소, 주민등록번호 등	① 유출된 개인정보를 이용하여 휴대전화, 인터넷전화 등 가입 ※ 통신서비스 가입 시 본인확인절차가 있으므로 주민등록증 위조 등 추가적인 불법 행위 수반이 예상됨 ② 불법 가입한 전화번호로 스팸을 발송하여 금전적 이익을 취득함 ※ 명의를 도용당한 사람은 서비스 이용제한을 당하거나 명의도용 소명절차를 밟는 등 피해를 당함	<ul style="list-style-type: none"> • 한국정보통신진흥협회(KAIT)의 명의도용방지서비스(M-Safer)를 통한 불법 통신서비스 신규가입 여부 확인 ※ 신고기관 : 통신민원조정센터(msafer.or.kr) ※ 명의도용방지서비스(M-Safer) : 통신서비스 신규가입시 이메일·문자로 가입여부 통보
	명의도용을 통한 신용카드 복제	이름, 신용카드 번호, 유효기간 등	① 유출된 개인정보를 이용하여 신용카드 불법 복제 ※ 특수장비를 이용하여 카드번호, 유효기간, 이름 등으로 복제 가능 ② 불법 복제된 카드를 국내외에서	<ul style="list-style-type: none"> • 신용카드 정지 및 재발급 신청, 이용내역 통지 서비스 가입 ※ 신고기관 : 각 카드사, 경찰, 금융감독원(☎1332)

	피해종류	활용된 개인정보 주요항목	개인정보 악용 절차	이용자 대응요령
			<p>활용하여 상품 결제 등에 악용 ※ 국내외 POS단말기의 경우 마그네틱 부분만을 이용하여 결제 가능</p>	
	스미싱	휴대전화번호	<p>① '정보유출 확인 안내' 등 금융기관을 사칭하는 문자메시지에 악성코드(인터넷주소)를 삽입하여 발송 ② 금융기관 사칭 메시지를 받은 피해자가 인터넷주소(URL)를 클릭하면 악성코드에 감염되어 소액결제 피해 및 개인·금융정보 탈취</p>	<ul style="list-style-type: none"> 수상한 문자메시지 삭제 및 메시지 상 링크 클릭하지 않기 또는 카드사 공지 전화번호 확인 ※ 신고기관 : 카드사, 경찰, 불법스팸대응센터(☎118)
비금전적	보이스피싱	신용카드번호, 휴대전화, 집전화번호, 집주소 등	<p>① 경찰, 금융감독당국 또는 금융회사 직원을 사칭하여 전화 ② 금융관련 업무 목적 사칭을 통한 개인정보·금융정보 탈취(비밀번호, 보안카드번호 등) ③ 유출된 금융사를 사칭, 개인정보 유출 확인을 빙자하여 ARS를 통해 계좌번호/비밀번호 등 금융정보 입력 요청</p>	<ul style="list-style-type: none"> 수상한 전화 거부 및 각 카드사에서 공지한 전화번호 확인 ※ 신고기관 : 카드사, 경찰, 불법스팸대응센터(☎118)
	명의도용을 통한 온라인회원 가입	이름, 이메일, 연락처 등	<p>① 유출된 개인정보를 이용하여 웹사이트 가입 ※ 일부 홈페이지의 경우 이름,</p>	<ul style="list-style-type: none"> e프라이버시 클린서비스(www.eprivacy.go.kr)를 활용한 해당 사이트 탈퇴 요청 ※ 신고기관 : 경찰, 불법스팸대응센터(☎118)

	피해종류	활용된 개인정보 주요항목	개인정보 악용 절차	이용자 대응요령
			<p>이메일, 연락처만으로 회원가입 가능</p> <p>② 명의도용을 통해 본인도 모르는 수십여개의 웹사이트 가입하여 개인정보 불법 이용</p>	<p>※ 국내 사이트로 주민번호 사용 내역이 있는 경우만 가능하며, 주민번호 미사용시 서비스 불가</p>
	<p>휴대전화/이메일 스팸발송</p>	<p>휴대전화 번호, 이메일 주소 등</p>	<p>① 유출된 개인정보를 이용해 불특정 다수에게 스팸 발송</p> <p>※ 유출된 모든 휴대전화, 이메일로 도박 등 스팸 무작위 발송 가능</p> <p>※ 신용정보, 연소득 등 활용 대출 스팸 발송, 자동차 보유여부를 활용한 보험 스팸 발송 등 특정유형의 개인에 대한 타겟 마케팅 가능</p> <p>② 휴대전화, 이메일 서비스 이용자는 원치 않는 홍보·마케팅 광고 수신</p>	<ul style="list-style-type: none"> • 지능형 스팸차단서비스를 이용한 스팸 차단, 수신 스팸 적극 신고 ※ 신고기관 : 카드사, 경찰, 불법스팸대응센터(☎118) ※ 지능형 스팸차단서비스 : 발신·회신번호 등 발송패턴을 분석하여 스팸을 차단해주는 서비스
	<p>사회공학적인 기법을 활용한 악성코드 유포메일 발송</p>	<p>이메일주소 등</p>	<p>① 해커가 특정 대상을 목표로 스팸/피싱 시도용 첨부파일이 포함되어 있거나 연결을 유도 URL이 포함된 이메일 발송</p> <p>② 수신자들이 이메일에 포함된 첨부파일 및 URL을 클릭</p> <p>③ 해커가 수신자의 PC를 장악하여 기밀 및 개인정보를 빼냄</p>	<ul style="list-style-type: none"> • 의심가는 이메일을 받은 경우 함부로 열람하지 않고 바로 삭제 • 사용자 PC의 바이러스 백신을 항상 최신버전으로 유지 및 정기적 검사 수행 ※ 신고기관 : 경찰, 불법스팸대응센터(☎118)

붙임4 | 교육부 개인정보보호 포털 유출등 신고 절차

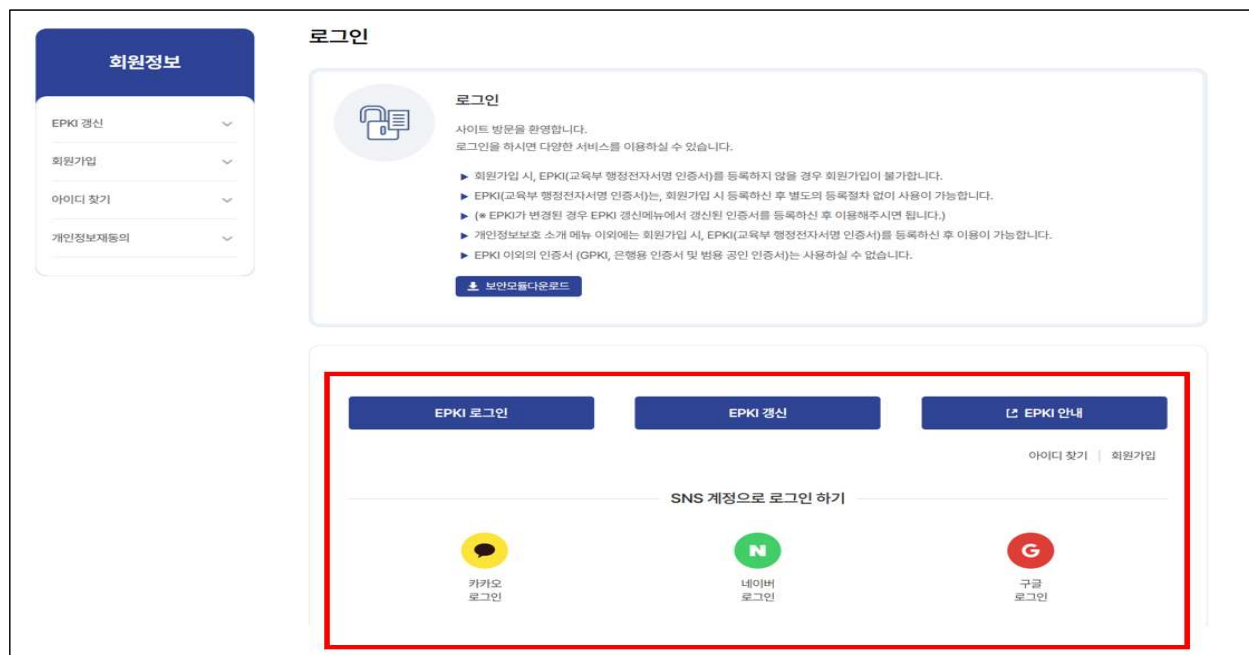
□ 유출등 신고 절차

[1단계] 교육부 개인정보보호 포털(https://privacy.moe.go.kr) 사이트 접속 →

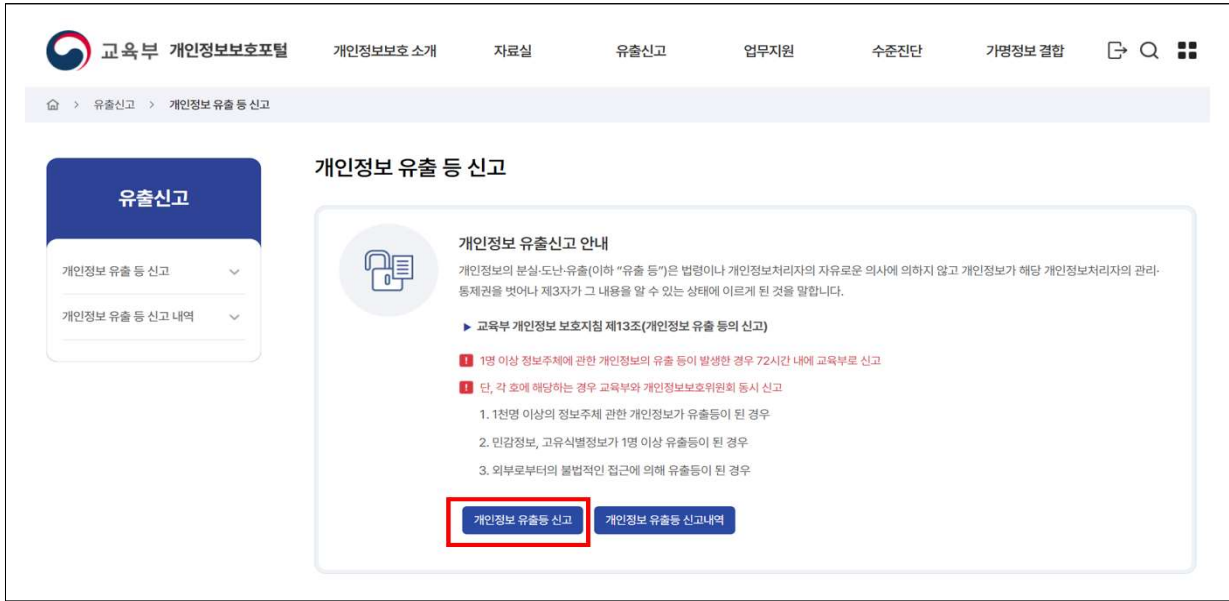
① [개인정보 유출 등 신고] 선택



[2단계] EPKI 로그인 및 SNS(카카오톡, 네이버, 구글) 계정으로 로그인 실시

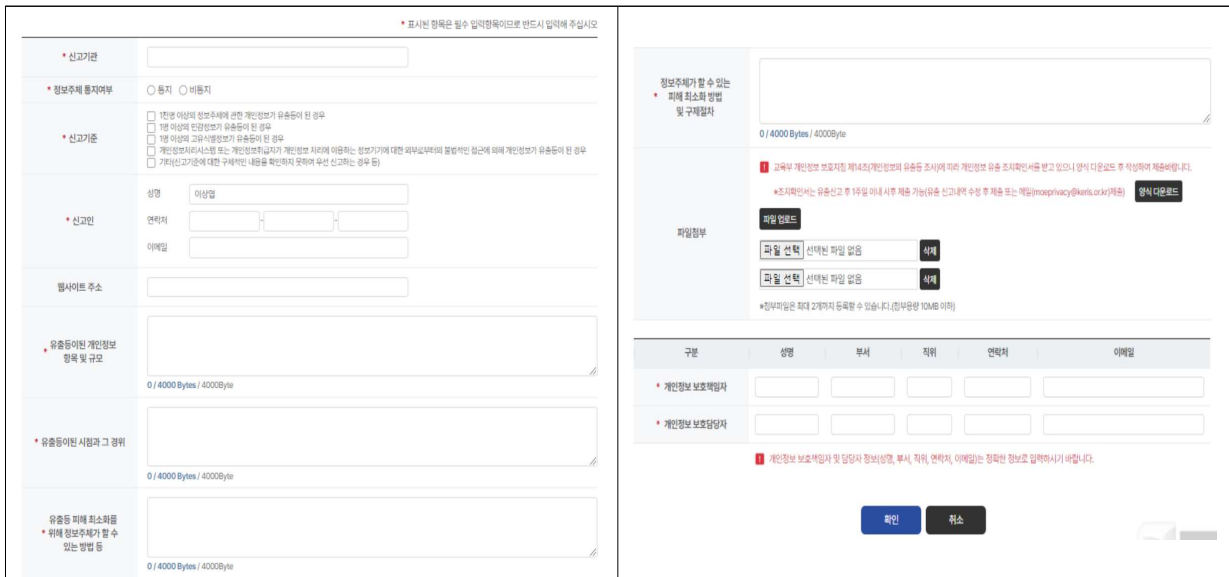


[3단계] ① [개인정보 유출 등 신고] 선택



[4단계] ① [유출신고 관련 내용 작성] → ② [확인] 완료

※ 유출 등 신고서 내용은 정확한 정보(이메일, 연락처 등)로 입력하여 작성



[5단계] 교육부 개인정보 보호지침 제13조에 따른 개인정보 유출 등 신고서(붙임 1)를 첨부파일로 제출

※ 개인정보 유출 등 신고 완료 후 1주일 이내 개인정보 유출 등 신고 조치 확인서(붙임2)를 작성 후 교육부 개인정보보호 포털-유출신고 내역 수정하여 제출하거나 메일(moeprivacy@keris.or.kr)로 전달

□ 유출등 신고내역 수정(조치 확인서 제출 등) 절차

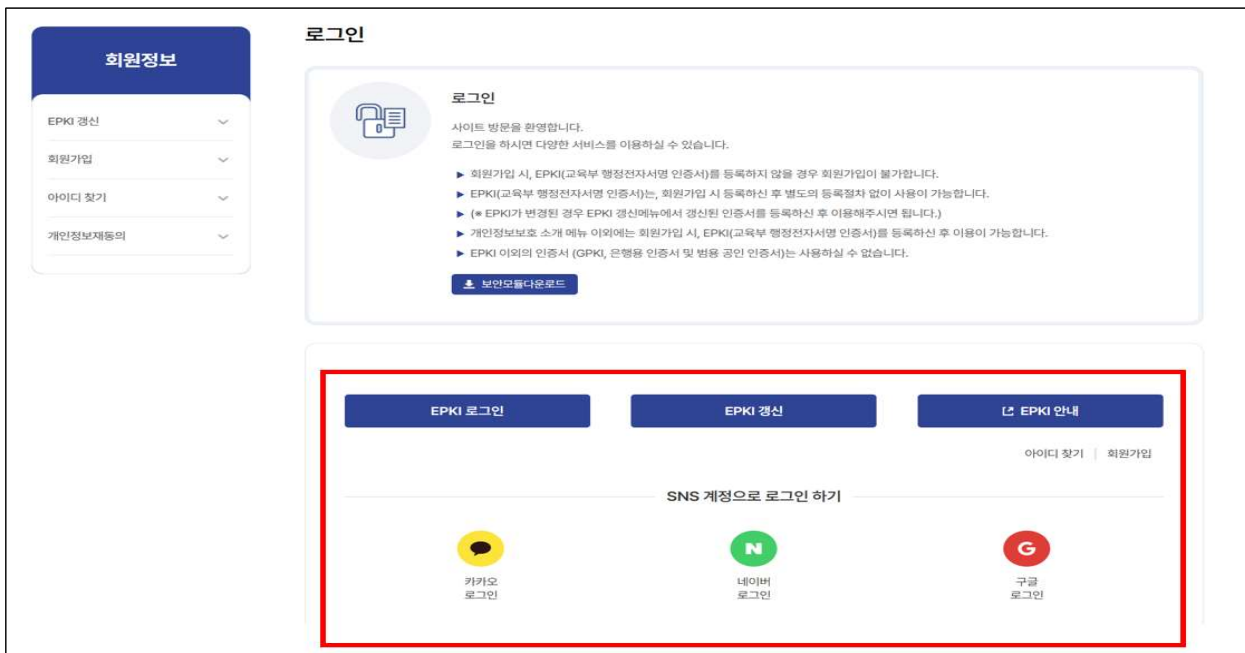
[1단계] 교육부 개인정보보호 포털(<https://privacy.moe.go.kr>) 사이트 접속 →

① [개인정보 유출 등 신고] 선택

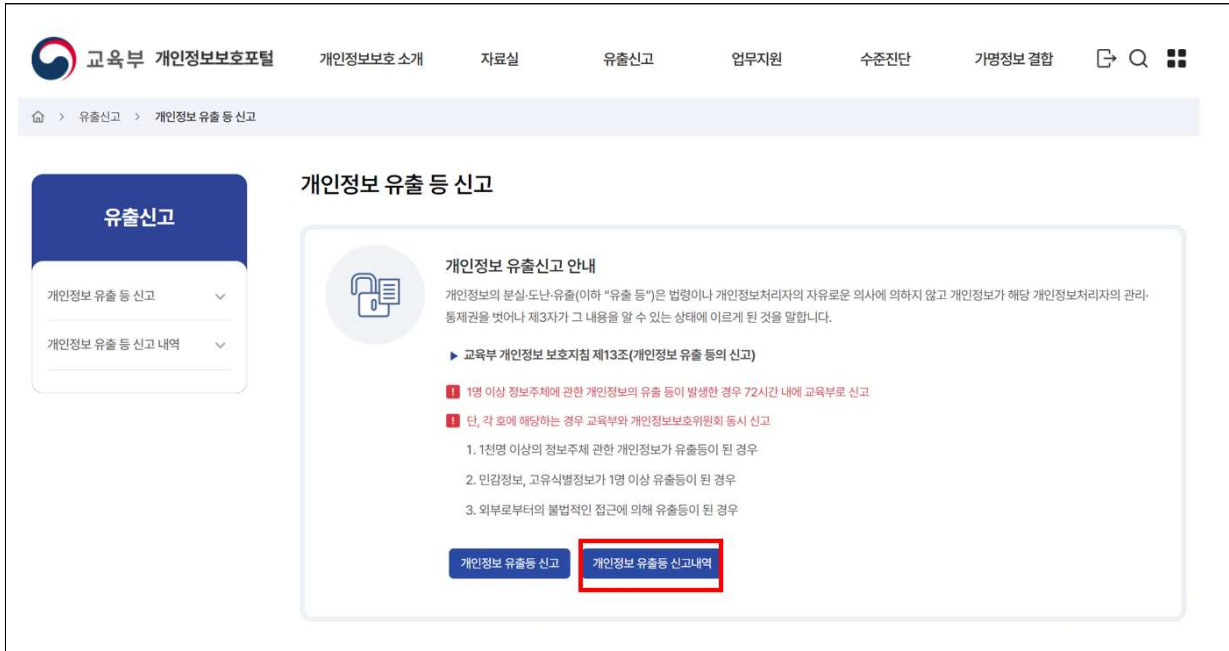


[2단계] EPKI 로그인 및 SNS(카카오, 네이버, 구글) 계정으로 로그인 실시

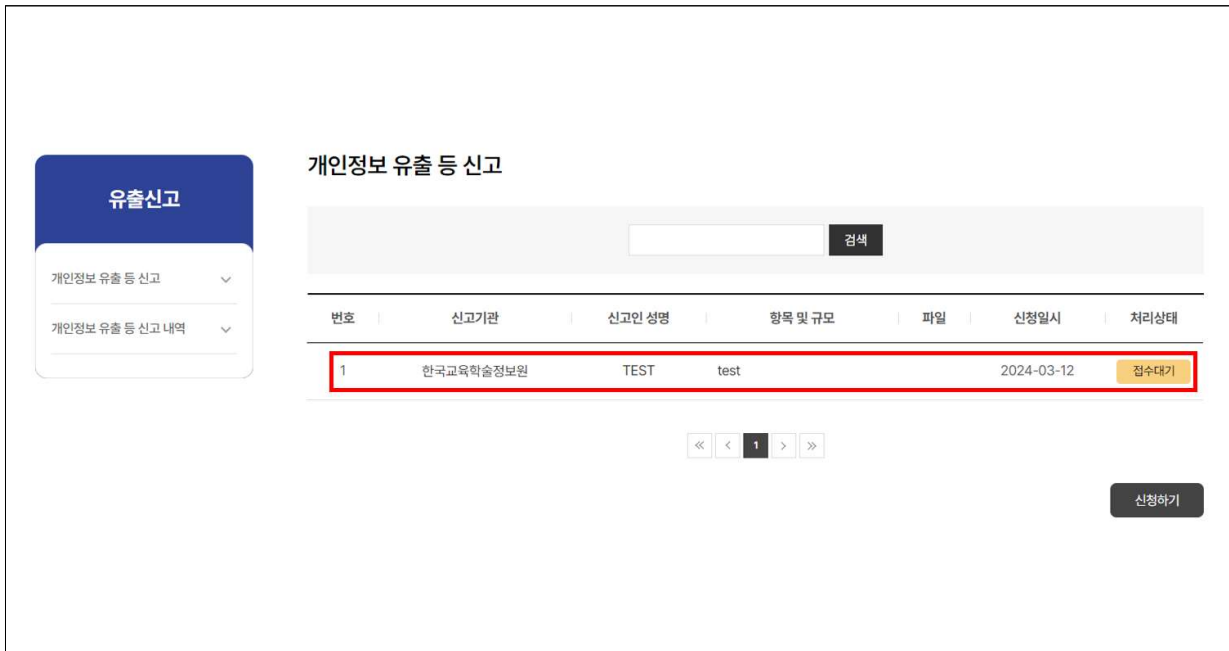
※ 개인정보 유출등 신고한 계정과 동일 계정으로 로그인(동일한 계정 아닐 경우 수정 불가)



[3단계] ① [개인정보 유출 등 신고내역] 선택



[4단계] ① 유출 등 신고 내역 확인 후 수정할 유출 등 신고 내역 선택



[5단계] ① [수정] 선택 후 내용 수정

유출신고

개인정보 유출 등 신고

개인정보 유출 등 신고 내역

개인정보 유출 등 신고

* 신고기관	한국교육학술정보원
* 정보주체 통지여부	통지
* 신고기준	1천명 이상의 정보주체에 관한 개인정보 유출등이 된 경우
* 신고인	성명 TEST 연락처 010-1234-1234 이메일 abcd@keris.or.kr
웹사이트 주소	moe.privacy.go.kr
* 유출된 개인정보의 항목 및 규모	test
* 유출된 시점과 그 경위	test
* 유출피해 최소화 대책, 조치 및 결과	test
정보주체가 할 수 있는 * 피해 최소화 방법 및 구제절차	test
파일첨부	

분류	성명	부서	직위	연락처	이메일
* 개인정보보호 책임자	TEST	test	test	test	test
* 개인정보보호 담당자	test	test	test	test	test

수정
삭제
목록

[6단계] ① 유출등 신고 내역 수정 후 [확인] 선택

* 표시된 항목은 필수 입력항목이므로 반드시 입력해 주십시오

* 신고기관	한국교육학술정보원
* 정보주체 통지여부	<input checked="" type="radio"/> 통지 <input type="radio"/> 비통지
* 신고기준	<input checked="" type="checkbox"/> 1천명 이상의 정보주체에 관한 개인정보 유출등이 된 경우 <input type="checkbox"/> 1천 이상 10만 이하의 정보주체에 관한 개인정보 유출등이 된 경우 <input type="checkbox"/> 1천 이상 10만 이하의 정보주체에 관한 개인정보 유출등이 된 경우 <input type="checkbox"/> 개인정보처리시스템 또는 개인정보취급자가 개인정보 처리에 사용하는 정보기기에 대한 외부물건의 불법적인 접근에 의해 개인정보가 유출등이 된 경우 <input type="checkbox"/> 기타(신고기준에 대한 구체적인 내용을 확인하지 못하여 우선 신고하는 경우 등)
* 신고인	성명 TEST 연락처 010 - 1234 - 1234 이메일 abcd@keris.or.kr
웹사이트 주소	moe.privacy.go.kr
* 유출된 개인정보 항목 및 규모	test <small>4 / 4000 Bytes / 4000Byte</small>
* 유출된 시점과 그 경위	test <small>4 / 4000 Bytes / 4000Byte</small>

유출등 피해 최소화 * 위해 정보주체가 할 수 있는 방법 등	test <small>4 / 4000 Bytes / 4000Byte</small>																		
정보주체가 할 수 있는 * 피해 최소화 방법 및 구제절차	test <small>4 / 4000 Bytes / 4000Byte</small>																		
파일첨부	<div style="font-size: x-small; color: red;"> * 교육부 개인정보 보호지침 제14조(개인정보의 유출등 조치)에 따라 개인정보 유출 조치확인서를 받고 있으니 양식 다운로드 후 작성하여 제출하십시오. * 조치확인서는 유출신고 후 1주일 이내 사유 제출 가능(유출 신고내역 수정 후 제출 또는 책임(moeprivacy@keris.or.kr)을) </div> <div style="text-align: right; margin-top: 5px;"> 파일 업로드 양식 다운로드 </div> <div style="font-size: x-small; color: gray; margin-top: 5px;"> *첨부파일은 최대 2개까지 등록할 수 있습니다. (첨부파일용 10MB 이하) </div>																		
	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 15%;">구분</th> <th style="width: 15%;">성명</th> <th style="width: 15%;">부서</th> <th style="width: 15%;">직위</th> <th style="width: 15%;">연락처</th> <th style="width: 15%;">이메일</th> </tr> </thead> <tbody> <tr> <td>* 개인정보 보호책임자</td> <td>TEST</td> <td>test</td> <td>test</td> <td>test</td> <td>test</td> </tr> <tr> <td>* 개인정보 보호담당자</td> <td>test</td> <td>test</td> <td>test</td> <td>test</td> <td>test</td> </tr> </tbody> </table> <div style="font-size: x-small; color: red; margin-top: 5px;"> * 개인정보 보호책임자 및 담당자 정보(성명, 부서, 직위, 연락처, 이메일)는 정확한 정보로 입력하시기 바랍니다. </div>	구분	성명	부서	직위	연락처	이메일	* 개인정보 보호책임자	TEST	test	test	test	test	* 개인정보 보호담당자	test	test	test	test	test
구분	성명	부서	직위	연락처	이메일														
* 개인정보 보호책임자	TEST	test	test	test	test														
* 개인정보 보호담당자	test	test	test	test	test														

확인
취소

※ 개인정보 유출등 신고서(붙임1), 개인정보 유출 신고 조치 확인서(붙임2)를 작성하여 붙임파일로 제출

붙임5**유관기관 관련 연락처** 개인정보 유출등 신고

기 관 명	전화번호	인터넷사이트
교육부	-	https://privacy.moe.go.kr/ (교육부 개인정보보호 포털)
개인정보보호위원회 (한국인터넷진흥원)	118	https://privacy.go.kr/ (개인정보보호 포털)

 관련기관 연락처

기 관 명	전화번호	인터넷사이트
대검찰청	1301	https://www.spo.go.kr/
경찰청	182	https://ecrm.cyber.go.kr