교육분야 개인정보 유출사고 대응 매뉴얼

2023. 5.

교육부

KERIS 한국교육학술정보원

1. 개요

2. 개인정보 유출사고 대응 조치 및 피해 구제 방법

3. 개인정보 유출 원인별 보호 조치

4. 개인정보 유출사고 재발방지 조치

【참고자료】

❍ 본 매뉴얼은 「개인정보 보호법」의 적용을 받는 개인정보처리자를 대상으로 합니다.

적용대상

업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통해 개인정보를 처리하는 교육기관의 모든 개인정보처리자

교육기관 즉, 교육부(소속기관 포함), 교육청(직속기관 포함), 교육지원청, 초·중·고(각급학교 포함), 대학, 국·공립대학병원, 교육부 산하 공공기관이 대상입니다.

❍ 본 매뉴얼은 「표준 개인정보 보호지침」(개인정보보호위원회 고시 제2020-1호, 2020.8.11.) 제29조(개인정보 유출 사고 대응 매뉴얼 등)에 따라,

- 유출사고 발생 시 신속한 대응과 그 피해를 최소화하기 위한 최소한의 사항을 안내하고 있습니다.

관계법령

표준 개인정보 보호지침

제29조(개인정보 유출 사고 대응 매뉴얼 등) ① 다음 각 호의 어느 하나에 해당하는 개인정보처리자는 유출 사고 발생 시 신속한 대응을 통해 피해 발생을 최소화하기 위해 「개인정보 유출 사고 대응 매뉴얼」을 마련하여야 한다.

1. 법 제2조제6호에 따른 공공기관
2. 그 밖에 1천명 이상의 정보주체에 관한 개인정보를 처리하는 개인정보처리자

② 제1항에 따른 개인정보 유출 사고 대응 매뉴얼에는 유출 통지·조회 절차, 영업점·인터넷 회선 확충 등 민원 대응조치, 현장 혼잡 최소화 조치, 불안 해소조치, 피해자 구제조치 등을 포함하여야 한다.

③ 개인정보처리자는 개인정보 유출에 따른 피해복구 조치 등을 수행함에 있어 정보주체의 불편과 경제적 부담을 최소화할 수 있도록 노력하여야 한다.

❍ 따라서 각 교육기관은 본 매뉴얼을 조직의 특성 및 환경에 맞게 보완하여 사용하시기 바랍니다.

1 개요

1.1 목적

❍ ‘개인정보 유출사고 대응 매뉴얼’은 교육기관이 ‘개인정보 보호법’ 및 동법 시행령, 관련 지침 따라 개인정보 유출 사고에 대한 신속하고 체계적인 대응을 목적으로 한다.

※ 관련근거 : 표준 개인정보 보호지침 제29조(개인정보 유출 사고 대응 매뉴얼 등)

1.2 법적 근거

❍ 개인정보 보호법 및 시행령

❍ 표준 개인정보 보호지침

❍ 개인정보의 안전성 확보조치 기준

❍ 교육부 개인정보 보호지침

1.3 적용 범위 및 용어 정의

❍ 해킹, 분실, 도난 등으로 인해 개인정보가 내·외부자에 의하여 유출된 경우에 적용된다.

o 단 1건만 유출되어도 정보주체에 대한 통지 등 의무를 이행하고 교육부에 신고하여야 하며, 1천명 이상 유출된 경우 교육부 및 개인정보보호위원회(한국인터넷진흥원)에 신고 o 유출된 정보(예: 비밀번호, 계좌번호 등)가 암호화되어 있어도 개인정보 보호법 기준 개인정보 유출에 해당함

용 어	정 의
유출	• 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고, 정보주체의 개인정보에 대하여 개인정보처리자가 통제를 상실하거나 또는 권한 없는 자의 접근을 허용한 것 ☞ 표준 개인정보 보호지침(개인정보보호위원회 제2020-1호) 제25조
유출사고	• 비인가 된 접근, 정보시스템의 오남용, 비인가 된 시스템 사용 또는 사용자의 계정 도용, 악성코드 유입 및 실행 등으로 발생한 개인정보 유출사고
유출사고 대응팀	• 개인정보 유출사고 발생에 따른 사고의 분석, 처리지원, 사후 복구, 사후 예방 조치 등을 주요 업무로 하는 개인정보보호 담당부서를 말함
개인정보 보호책임자	• 개인정보 보호법 제31조에 근거하여 개인정보 처리 업무를 총괄하는 자 • 개인정보 보호담당자를 임명하여 유출사고 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

가이드

개인정보 유출의 개념

표준 개인정보보호지침 제25조(개인정보의 유출) 개인정보의 유출은 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고, 정보주체의 개인정보에 대하여 개인정보처리자가 **통제를 상실**하거나 **권한 없는 자의 접근을 허용한 것**으로서 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, 기타 저장 매체가 권한이 없는 자에게 잘못 전달된 경우
4. 기타 권한이 없는 자에게 개인정보가 전달된 경우

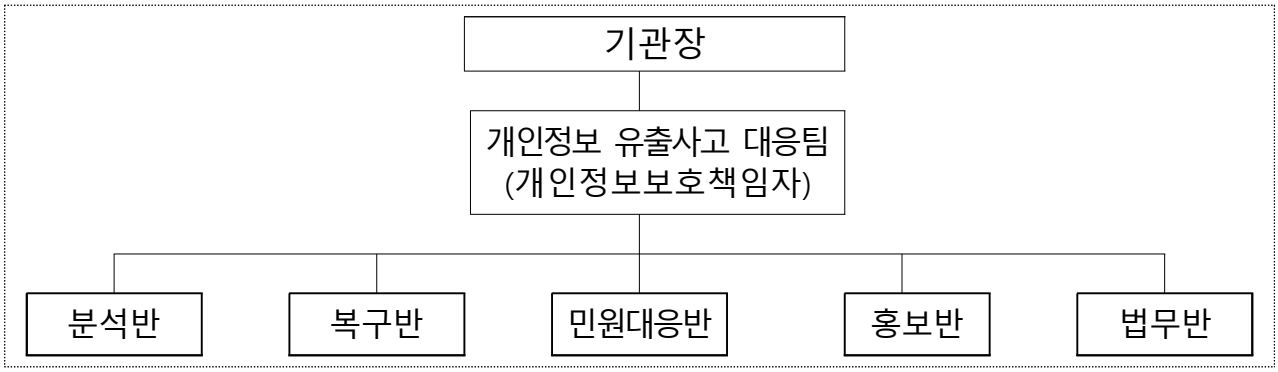
1.4 단계별 프로세스(업무 절차)

o 기관의 개인정보 처리 형태에 따라 조직체계, 업무분장, 비상연락체계가 상이하므로 본 양식을 참고하여 작성(다음 예시가 의무사항은 아님)

단계	상세 업무	비고
사고인지 및 긴급조치	○ 개인정보 유출사고 신고 접수 및 사고인지 ○ 유출사고 대응센터 소집 및 유관기관 협조체계 확인 ○ 피해 최소화를 위한 긴급조치 수행 ※ 유출된 개인정보 삭제조치 및 기술지원 요청	
↓		
정보주체 유출통지	○ 정보주체에게 개인정보 유출사실 통지(5일 이내)	세부내용 2.1 참고
↓		
개인정보 유출신고	○ 1명 이상의 개인정보 유출시 교육부(privacy.moe.go.kr)에 유출 신고 ○ 1천명 이상의 개인정보 유출시 교육부 및 개인정보보호위원회(한국인터넷진흥원, privacy.go.kr)에 유출 신고	세부내용 2.2 참고
↓		
민원대응	○ 개인정보 유출사고 규모 및 성격에 따라 민원대응반 구성 ○ 2차 피해 방지를 위한 민원 대응 및 불안 해소 조치	세부내용 2.4~2.5 참고
↓		
피해구제 절차	○ 개인정보 유출에 대한 피해구제 절차 안내	세부내용 2.6 참고
↓		
보안기능 강화	○ 사고 원인 분석 및 보안 강화·기능 개선	
↓		
결과 보고	○ 기관장 및 이사회에 개인정보 유출사고 결과보고서 작성 및 보고	
↓		
재발방지	○ 개인정보 유출사고 사례 전파 교육 및 개선 대책 시행	

1.5 유출 대응 업무수행 체계

❍ 조직체계(예시)



❍ 업무분장

조직	담당 업무
기관장	• 유출 대응 관련 방향성 제시 등 의사 결정
개인정보보호 책임자	• 유출사고 대응 총괄 지휘 및 유출사고 대응 팀 구성·운영
개인정보 유출사고 대응팀	• 유출사고 인지, 접수, 전파 • 유출사고 대응 절차 수립 • 정보주체에게 유출사실 통지 • 개인정보보호위원회(전문기관)에 유출통지 사실 신고
분석반	• 유출 사실 확인, 조사 및 원인 분석 • 사고내용 세부조사
복구반	• 외부요인에 의한 유출의 경우, 유관 기관과 협조하여 사고 처리 지원 • 시스템 복구 및 백업(유지보수/협력업체 포함)
민원대응반 (온라인, 오프라인)	• 개별 통지문 안내에 따른 후속업무(민원 등) 진행 • 상담센터, 소비자보호 방안 마련(필요시 유관부서와 협조)
홍보반	• 유출사고 관련 대외기관(언론사 등) 대응 • 유출사고 안내문 문구 최종 검토
법무반	• 법률상 대응방안, 의사결정 사항 등 정책적 판단사항 검토 및 결정 • 유출사고 관련 수사기관 경과사항 대응 및 대책반 공유

❍ 비상연락망

- 개인정보 유출사고 대응팀

조직별	담당자	전화번호	이메일
개인정보보호책임자	성함, 직책 명시	02-000-0000 (010-000-0000)	OOO@ooo.kr
총괄대응본부	○○팀장	02-000-0000 (010-000-0000)	OOO@ooo.kr
분석반	○○팀장	02-000-0000 (010-000-0000)	OOO@ooo.kr
복구반	○○팀장	02-000-0000 (010-000-0000)	OOO@ooo.kr
민원대응반	○○팀장	02-000-0000 (010-000-0000)	OOO@ooo.kr
홍보반	○○팀장	02-000-0000 (010-000-0000)	OOO@ooo.kr
법무반	○○팀장	02-000-0000 (010-000-0000)	OOO@ooo.kr

- 협력업체/유지보수업체

업체명	담당 시스템	담당자	전화번호	이메일
ㅇㅇ기업	ㅇㅇ시스템	성함, 직책 명시	00-000-0000 (010-000-0000)	OOO@ooo.kr
ㅇㅇ기업	ㅇㅇ시스템	성함, 직책 명시	00-000-0000 (010-000-0000)	OOO@ooo.kr
ㅇㅇ기업	ㅇㅇ시스템	성함, 직책 명시	00-000-0000 (010-000-0000)	OOO@ooo.kr
ㅇㅇ기업	ㅇㅇ시스템	성함, 직책 명시	00-000-0000 (010-000-0000)	OOO@ooo.kr
ㅇㅇ기업	ㅇㅇ시스템	성함, 직책 명시	00-000-0000 (010-000-0000)	OOO@ooo.kr

2 개인정보 유출사고 대응 조치 및 피해 구제 방법

2.1 유출 통지·조회 절차

가이드

o 개인정보처리자는 개인정보 보호법 제34조제1항에 따른 통지 절차를 마련하고 이에 대한 내용을 기술
o 개인정보처리자는 1천명 이상 정보주체의 개인정보 유출 사고 발생 시 당국에 대한 신고 관련 절차를 마련하고 이에 대한 내용을 기술
o 개인정보처리자는 정보주체가 홈페이지 등을 통해 자신의 개인정보가 유출되었는지 확인할 수 있는 절차를 만들고 이에 대한 내용을 기술
o (개인정보 처리 업무 위탁 시) 1차적인 유출 신고 및 통지 의무는 위탁자에게 있으므로, 유출사고 발생 시 수탁자와의 대응 절차를 마련하고 이에 대한 내용을 기술

❍ 총괄대응본부는 유출 인원 등을 확인하여 [붙임 1] 유출 통지 방법에 따라 [붙임 2] 표준 개인정보 유출 통지 문항 (예시)을 참고하여 정보주체들에게 유출 통지

- 통지 항목 : ①유출된 개인정보의 항목, ②유출 시점과 그 경위, ③피해 최소화를 위한 정보주체의 조치방법, ④기관의 대응조치 및 피해구제 절차, ⑤피해 신고 접수 담당부서 및 연락처

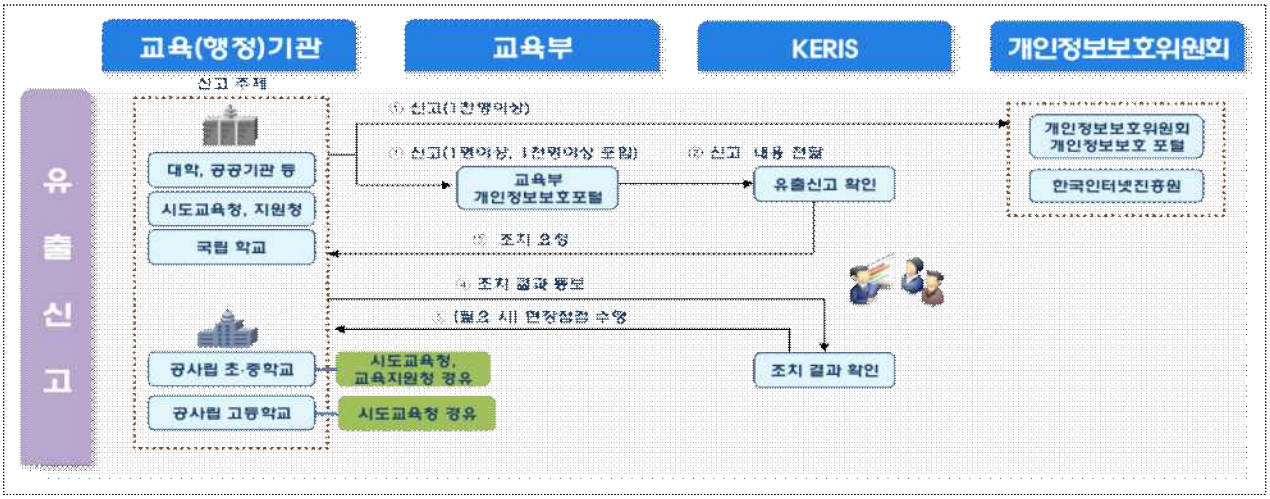
❍ 수탁사업자가 수탁 업무를 처리하는 과정에서 개인정보가 유출된 경우 즉시 위탁자에게 보고하도록 위·수탁계약서에 명시하고, 수탁사업자로부터 보고 받은 시점에서 지체 없이 유출 통지

❍ 1천명 이상 유출 시에는 홈페이지에 필수 유출통지 5개 항목을 7일 이상 공지하고, 정보주체가 유출 여부를 확인할 수 있는 별도 페이지(http://ooo.com/119) 제공

- 개인정보 유출 결과는 전체 공지가 아닌 아이핀(I-PIN), 핸드폰 인증 등을 통해 정보주체가 개별 본인 확인 후 개인정보 유출 결과 조회 지원

2.2 유출 신고 절차 및 방법

❍ 유출 신고 절차



※ 유출 건수가 500건 이상인 경우 유출 규모, 방법 등 사안의 경중에 따라 교육부 현장 특별점검 실시

❍ 유출 신고 방법

구분	내용
신고대상	▶ 1천명 이상 유출된 경우에는 교육부에 보고하고 개인정보보호위원회(또는 한국인터넷진흥원)에 신고 ▶ 1명 이상 유출된 경우 상급기관을 경유하여 교육부에 보고 ※ 공·사립 초등학교·중학교는 교육지원청, 교육청, 교육부에 보고 ※ 고등학교, 교육지원청, 교육청 직속기관 등은 교육청, 교육부에 보고 ※ 국립학교, 대학, 교육청, 공공기관 등은 교육부에 보고
신고시기	▶ 5일 이내(정보주체에 대한 통지 및 조치결과 신고)
신고방법	▶ 교육부(privacy.moe.go.kr) 및 개인정보보호위원회(privacy.go.kr) 홈페이지를 통해 유출 사고 보고 및 신고서 제출 ※ 부득이한 경우 전자우편, 팩스 공문 등을 통해 유출사고 보고 및 신고서 제출 ▶ 시간적 여유가 없거나 특별한 사정이 있는 경우 상급기관과 교육부에 동시에 보고하며 유출신고서를 제출
신고내용	▶ 기관명, 통지여부, 유출된 개인정보 항목·규모, 유출 시점·경위, 유출피해 최소화 대책·조치 및 결과, 정보주체가 할 수 있는 피해 최소화 방법 및 구제절차, 담당부서·담당자 연락처 등 ※ 정보주체에 대한 유출 통지 결과 및 피해 최소화를 위한 조치 결과가 포함되도록 해야 함
신고양식	▶ [붙임 3] 개인정보 유출 신고서 (양식)

※ 교육부 개인정보 보호지침 제53조의2(개인정보의 유출조사)제2항에 따라 [붙임4] 개인정보 유출신고 조치확인서 작성

2.3 현장 혼잡 최소화 조치

가이드

o 물리적으로 개인정보가 소실되거나 운영 중인 개인정보가 유출당했을 경우, 해당 현장 혼잡 최소화를 위한 절차를 마련하고 이에 대한 내용을 기술

❍ 총괄대응본부는 O층 OO회의실에 오프라인 창구를 개설

- 전화, 메일, 홈페이지, SNS 등 한 가지 이상의 채널을 선택하여 단일화된 민원대응 창구를 구축

구분	채널	상세 내용
오프라인	3층 00회의실	
온라인 中 택 1	전화	02-000-0000
	메일	privacy@ooo.ooo
	홈페이지	https://ooo.ooo
	SNS	#OOOO

❍ 복구반은 유출된 시스템의 이용을 제한하고 별도의 임시 시스템 구축을 통하여 기관의 업무 혼잡 방지

❍ 분석반은 대외 수사 기관에 협조할 수 있는 전담 인력 구성 및 대응

❍ 시스템 오류 등 서비스 장애로 인한 정보주체의 민원 발생 시 유관부서와 협의하여 해결

2.4 정보주체 민원 대응 조치

가이드

o 개인정보처리자는 정보주체 민원을 처리할 수 있는 체계를 만들고 이에 대한 내용을 기술

- ❍ 민원대응반은 유관부서(총괄대응본부, 법무반)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 사내 및 대민 OOO 홈페이지(http://ooo.com)에 공지하고 타 팀에서 외부로부터 개인정보 유출관련 질문을 받으면 최대한 민원대응반으로 연결
- ❍ 기본적으로 민원대응반을 통해서 1차 민원 대응을 하고, 다음과 같은 경우 해당 부서에서 응대

문의별	담당부서
유출 확인 문의 대응	OO 팀 or OO반
피해구제 관련 문의 대응	OO 팀 or OO반
기타(OOO)	OO 팀 or OO반

2.5 정보주체 불안 해소 조치

가이드

o 개인정보처리자는 정보주체가 유출된 개인정보로 인한 불안을 해소할 수 있는 체계를 마련하고 이에 대한 내용을 기술

- ❍ OOO홈페이지(http://ooo.com)에 유출 피해 최소화를 위해 현재 기관에서 실시하고 있는 노력에 대한 사항 공지(1일 1회 업데이트)

❍ 비밀번호, 신용카드번호 등 유출 시 비밀번호 변경, 카드 재발급 등을 할 수 있도록 유출 통지 시 함께 안내

※ 보이스피싱, 문자피싱 등 금융사기 예방을 위한 차단신청 기능(voice.anti-phishing.or.kr, sms.anti-phishing.or.kr)등을 구체적으로 안내

[개인정보 유출 항목별 2차 피해 예방을 위한 안내사항]

구분	세부 안내 사항
아이디, 비밀번호 유출	- 비밀번호 변경 안내
카드번호 유출	- 카드 재발급 절차 안내
다량의 개인정보 유출	- 보이스피싱 등 2차 피해 예방 안내

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

2.6 피해자 구제 조치

가이드

o 개인정보처리자는 정보주체가 피해를 구제할 수 있는 절차를 마련하고, 이에 대한 내용을 기술

❍ 정보주체에게 개인정보 유출 피해에 대한 피해구제, 상담 등을 문의 할 수 있음을 안내

❍ 개인정보를 유출당한 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 유출 원인별 보호 조치

3.1 해킹

❍ 개인정보가 유출된 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 외부 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 유출사고 재발방지 조치

4.1 유출원인 보완 및 재발방지 조치 계획 수립·이행

❍ 개인정보 유출 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 제2020-2호)에 따라 개인정보보호 책임자가 내부관리계획의 이행실태를 연 1회 이상 점검·관리할 때 같이 점검 실시 권고

4.2 재발방지 교육 및 사례 전파

❍ 기관내 구성원 재발방지 교육 실시

- 개인정보 유출과 관련된 부서내 모든 취급자는 필수적으로 재발방지 교육 실시

❍ 개인정보 유출 사례를 내부공지 등을 통해 기관내 구성원에게 사례를 전파*

* 사례전파 시 또 다른 개인정보 유출이 발생하지 않도록 주의 필요

- 사례 전파의 구성(예시)

구분	구성 내용
사고 개요	• 0년 0월 0일 개인정보 취급자가 홈페이지 게시판 관리 중 개인정보가 포함된 파일을 게시판에 탑재함 • 개인정보가 포함된 파일(엑셀)을 00으로부터 0년 0일 0일 인지하여 해당파일 삭제 조치함 • 개인정보 00건, 포함된 개인정보 항목은 00을 포함한 총 00개가 유출됨
사고 처리 절차	• 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	• 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	• 개인정보 필터링 시스템 등 개인정보 체계 강화를 위한 시스템 구축 • 매년 개인정보 취급자 대상 개인정보 교육 실시
관련 변경 지침	• 내부관리 계획 수립 시 개인정보 유출 재발방지 계획 포함

붙임1 **유출 통지 방법**

유출 통지 방법

구분	내용
통지대상	▶정보주체
통지방법	▶ 서면, 전자우편, FAX전송, 전화, 휴대전화 문자전송 또는 이와 유사한 방법 ▶ 위의 통지방법과 동시에 홈페이지 공개 가능 - 단, 통지 및 조치 후에도 1천명 이상의 개인정보가 유출된 경우에는 서면 동의 방법과 함께 인터넷 홈페이지에 7일 이상 통지내용을 게재
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 알게 되었을 때에는 지체없이(5일 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 보완조치 - 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 ▶ 개인정보처리자는 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

붙임2 표준 개인정보 유출 통지 문안(예시)

□ 부가설명 란에 **필수사항은 < >, 참고사항은 ( )**로 표기하였음
□ 필수사항이 확인되지 않아 통지문에 포함하지 않은 경우 추후 확인되면 반드시 추가 통지
□ 아래 예시를 참고하여 유출 상황에 적합하게 내용을 변경하여 활용

표준 통지문안 예시	부가 설명
개인정보 유출 사실을 통지해 드리며, 깊이 사과드립니다.	**< 제목 >** - '유출 통지'문구 포함
귀하의 개인정보 보호를 위해 최우선으로 노력하여 왔으나, 불의의 사고로 귀하의 소중한 개인정보가 유출되었음을 알려드리며, 이에 대하여 진심으로 사과를 드립니다.	(사과문) - 유출 통지 사실 알림 - 사과문을 먼저 표현
귀하의 개인정보는 20ㅇㅇ년 ㅇ월 ㅇ일 000시스템 장애처리를 위한 데이터 분석 과정에서 유지보수업체로 전달되었고, 유지보수업체는 자체 서버에 저장·보관하다가 안전한 조치를 다하지 못해 20ㅇㅇ년 ㅇ월경 해커에 의한 해킹으로 유출되었습니다. 유출된 정확한 일시는 대구지방경찰청에서 현재 수사가 진행중이며, 확인되면 추가로 알려 드리도록 하겠습니다.	**<유출된 시점과 경위>** - 유출된 시점과 경위를 누구나 이해할 수 있게 상세하게 설명 - '귀하', '고객님' 등으로 유출된 정보주체 명시 ※ 부적합한 표현 : 일부 고객, 회원 정보의 일부 등 - 추가 확인된 사항은 반드시 추가로 통지
유출된 개인정보 항목은 이름, 아이디(ID), 비밀번호(P/W), 이메일, 연락처로 총 6개입니다.	**<유출된 항목>** - 유출된 항목을 누락 없이 모두 나열 ※ '등'으로 생략하거나, '회사 전화번호' 및 '집 전화번호'를 합쳐서 '전화번호'로 표시 안됨
유출 사실을 인지한 후 즉시 해당 IP와 불법접속 경로를 차단하고, 취약점 점검과 보완 조치를 하였습니다. 또한, 유지보수업체 서버에 있던 귀하의 개인정보는 즉시 삭제 조치하였습니다.	**<개인정보처리자의 대응조치>** - 접속경로 차단 등 예시된 항목 외에도 망 분리, 방화벽, 개인정보 암호화, 인증 등 접근통제, 시스템 모니터링 강화 등의 조치한 내용 설명

붙임3 **개인정보 유출 신고서(양식)**

개인정보 유출 신고서(양식)

<table>
<tr><td>기관명</td><td colspan="5"></td></tr>
<tr><td>정보주체에의
통지 여부</td><td colspan="5"></td></tr>
<tr><td>유출된 개인정보의
항목 및 규모</td><td colspan="5"></td></tr>
<tr><td>유출된 시점과
그 경위</td><td colspan="5"></td></tr>
<tr><td>유출피해 최소화
대책·조치 및 결과</td><td colspan="5"></td></tr>
<tr><td>정보주체가 할 수
있는 피해 최소화
방법 및 구제절차</td><td colspan="5"></td></tr>
<tr><td rowspan="3">담당부서·담당자 및
연락처</td><td></td><td>성명</td><td>부서</td><td>직위</td><td>연락처</td></tr>
<tr><td>개인정보
보호책임자</td><td></td><td></td><td></td><td></td></tr>
<tr><td>개인정보
취급자</td><td></td><td></td><td></td><td></td></tr>
</table>

유출신고접수기관	기관명	담당자명	연락처

개인정보 유출 신고서(작성 사례)

<table>
<tr><td>기관명</td><td colspan="5">교육 고등학교</td></tr>
<tr><td>정보주체에의
통지 여부</td><td colspan="5">▪ 통지일자: 2023. 3. 22. (화)
▪ 통지방법: 이메일 및 유선 전화
▪ 통지대상: 정보주체 1,100명(학생 600명, 학부모 200명, 교직원 300명)</td></tr>
<tr><td>유출된 개인정보의
항목 및 규모</td><td colspan="5">▪ 유출규모: 1,150명(중복제거 후 1,100명)
- 교육부 신고여부(○), 개인정보위 신고여부(○), 홈페이지 공개여부(○)
▪ 유출항목: 이름, ID, 비밀번호, 주소, 핸드폰번호, 이메일</td></tr>
<tr><td>유출된 시점과
그 경위</td><td colspan="5">▪ 사고발생 인지경로
- 2023.3.21 10:00 월별 개인정보처리시스템 접속로그 점검 시 특정 IP로부터 다량의 개인정보 다운로드 기록 확인
- 2023.3.21 11:00 개인정보처리시스템의 로그 확인 결과 알 수 없는 개인정보 압축 파일 발견
- 2023.3.21 12:00 IP Table, NAC 등을 확인하여 개인정보를 다운로드한 특정 IP의 PC(용역업체 개인 PC) 확인
▪ 유출 시점 및 경위
- 2023.3.4 20:00 용역업체 A씨는 개인정보처리시스템에 접속하여 다량의 개인정보파일을 생성 후 PC로 다운로드
- 2023.3.4 21:00 PC내 보안 솔루션(NAC 등)에 의하여 상용 이메일 접근 불가 확인 후 개인 이메일 서버로 파일 전송</td></tr>
<tr><td>유출피해 최소화
대책・조치 및 결과</td><td colspan="5">▪ 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
▪ 사고발생 후 조치사항
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</td></tr>
<tr><td>정보주체가 할 수
있는 피해 최소화
방법 및 구제절차</td><td colspan="5">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)</td></tr>
<tr><td rowspan="3">담당부서・담당자 및
연락처</td><td></td><td>성명</td><td>부서</td><td>직위</td><td>연락처</td></tr>
<tr><td>개인정보
보호책임자</td><td>김영희</td><td>총무과</td><td>총무과장</td><td>044-123-1234</td></tr>
<tr><td>개인정보
취급자</td><td>홍길동</td><td>총무과</td><td>담당자</td><td>044-123-1234</td></tr>
</table>

유출신고접수기관	기관명	담당자명	연락처
	한국교육학술정보원 및 00시도교육청	김철수	044-234-5678

붙임4 **개인정보 유출신고 조치확인서(양식)**

개인정보 유출신고 조치확인서(양식)

※ 6하 원칙에 따라 사실 관계를 명확하게 작성하여 주십시오.

<table>
<tr><td colspan="2">기관명</td><td>00학교</td></tr>
<tr><td rowspan="3">정보주체
통지 여부</td><td>통지일자</td><td>2023.00.00.</td></tr>
<tr><td>통지방법</td><td>(예시) 전화, 이메일, 서면, 팩스 등</td></tr>
<tr><td>필수통지
항목</td><td>
<table>
<tr><th>필수 통지 항목 5가지</th><th>포함 여부 확인(O, X)</th></tr>
<tr><td>① 유출된 개인정보의 항목</td><td>O 또는 X</td></tr>
<tr><td>② 유출 시점과 및 그 경위</td><td>O 또는 X</td></tr>
<tr><td>③ 피해 최소화를 위한 정보주체의 조치방법</td><td>O 또는 X</td></tr>
<tr><td>④ 기관의 대응조치 및 피해구제 절차</td><td>O 또는 X</td></tr>
<tr><td>⑤ 피해 신고 접수 담당부서 및 연락처</td><td>O 또는 X</td></tr>
</table>
(예시) 이메일 내용 이미지 캡쳐 등 증빙자료 포함
</td></tr>
<tr><td colspan="2">발생(인지) 일자</td><td>2023.00.00.</td></tr>
<tr><td colspan="2">발생(인지) 경로</td><td>(예시)
- 2023.00.00 00:00 KISA에서 통보
- 정보주체가 해당 학과에 신고, ECSC 사고 신고, 민원인 신고 등</td></tr>
<tr><td colspan="2">조치 일자</td><td>2023.00.00.</td></tr>
</table>

<table>
<tr><td>유출사실 인지 이후
후속 조치
(유출피해 최소화
대책・조치 및 결과)</td><td colspan="3">개인정보 유출 시 아래 사항 준수
1. 개인정보 유출 대응 매뉴얼 구비
※ 법령에 기반하여 최신화 되어있는지 확인 및 개선, 유출 시 매뉴얼대로 즉시 신고 등 대응
2. 유출원인 보완 및 재발방지 조치계획 수립·이행
3. 개인정보취급자(전직원) 대상 사례 전파 및 재발방지 교육
※ 개인정보보호 관련 전직원 교육 실시, 특히 신규 직원은 업무 투입 전 개인정보보호 기본 교육 실시 후 투입
4. 그 밖의 개인정보의 유출 방지를 위해 필요하다고 판단되는 사항

(예시)
- 2023.00.00 00:00 해당 게시글 삭제
- 2023.00.00 00:00 정보주체에게 메일, 문자로 안내
- 2023.00.00 00:00 홈페이지취약점 점검 수행
- 2023.00.00 00:00 00홈페이지에 유출 건 내용 게시
- 2023.00.00 00:00 재발방지대책 수립
- 2023.00.00 00:00 전직원 대상 개인정보 관련 교육
- 개인정보 파일 삭제, 오발송된 이메일 회수, 사례전파, 교육실시 등 증빙자료 포함</td></tr>
<tr><td colspan="2">신고 일자</td><td colspan="2">2023.00.00.</td></tr>
<tr><td rowspan="2">유출된
개인정보</td><td>규모(명)</td><td>00명</td><td>(중복제거) 00명</td></tr>
<tr><td>항목</td><td colspan="2">이름, 핸드폰번호 ,,,,,</td></tr>
<tr><td colspan="2">유출된 시점과
그 경위</td><td colspan="2">(예시)
- 2023.00.00 00:00 메일 잘못 발송, 실수로 개인정보 파일 첨부함
- 2023.00.00 00:00 유출 확인</td></tr>
</table>

<table>
<tr><td>교육부 신고 여부
(1명 이상 유출시)</td><td>○ 또는 X</td><td rowspan="3">(1명 이상인 경우)
유출 통지 및 조치 결과를 지체 없이 상급기관을 경유하여 교육부에 보고(교육부 개인정보보호 포털(privacy.moe.go.kr))

(1천명 이상인 경우)
유출 통지 및 조치 결과를 지체 없이 상급기관을 경유하여 교육부에 보고하고(교육부 개인정보보호 포털), 개인정보보호위원회(또는 한국인터넷진흥원, www.privacy.go.kr)에 신고

※1천명 이상 개인정보가 유출된 경우 개별 통지와 함께 유출된 사실을 인터넷 홈페이지에 7일 이상 게재</td></tr>
<tr><td>개인정보보호위원회
신고 여부
(1천명 이상 유출시)</td><td>○ 또는 X</td></tr>
<tr><td>홈페이지 공지 여부 및
공지 기간
(1천명 이상 유출)</td><td>(예시)
- 00홈페이지 00게시판에 공지
- 공지기간 : 2023.00.00~00.00.

- 공지사항 내용 이미지 캡쳐 등 증빙자료 포함</td></tr>
<tr><td>정보주체가 할 수 있는
피해 최소화 방법 및
구제절차</td><td colspan="2">(예시) 피해구제절차 안내 등</td></tr>
<tr><td>진행사항 또는
향후계획</td><td colspan="2">(예시)
자체 내부 감사 수행, 상위기관 현장 컨설팅 수행, 개인정보보호위원회 점검 예정 등</td></tr>
</table>

개인정보 유출신고 조치 확인서(작성 사례)

※ 6하 원칙에 따라 사실 관계를 명확하게 작성하여 주십시오.

<table>
<tr><td colspan="2">기관명</td><td>교육 고등학교</td></tr>
<tr><td rowspan="3">정보주체
통지 여부</td><td>통지일자</td><td>2023. 3. 22. (화)</td></tr>
<tr><td>통지방법</td><td>이메일 및 유선 전화</td></tr>
<tr><td>필수통지
항목</td><td>
<table>
<tr><th>필수 통지 항목 5가지</th><th>포함 여부 확인(O, X)</th></tr>
<tr><td>① 유출된 개인정보의 항목</td><td>O</td></tr>
<tr><td>② 유출 시점과 및 그 경위</td><td>O</td></tr>
<tr><td>③ 피해 최소화를 위한 정보주체의 조치방법</td><td>O</td></tr>
<tr><td>④ 기관의 대응조치 및 피해구제 절차</td><td>O</td></tr>
<tr><td>⑤ 피해 신고 접수 담당부서 및 연락처</td><td>O</td></tr>
</table>
개인정보 유출 사실을 통지해 드리며,
깊이 사과 드립니다.

고객님의 개인정보는 2023년 3월 4일 00용역업체 직원에 의하여 외부 유출된 사실을 확인하였고, 2차 피해 예방을 위해 경찰청에 즉시 조사를 의뢰하여 수사진행 중입니다.

유출된 개인정보 항목은 이름, 아이디(ID), 비밀번호(P/W), 이메일, 핸드폰번호, 주소 총 6개 항목입니다.

유출 사실을 인지한 후 즉시 접속 경로를 차단하고, 취약점 점검과 보완 조치를 완료 하였습니다.

현재까지 확인한 바로는 경찰청에서 00용역업체 직원이 외부로 유출된 개인정보는 제3자에게 2차 전달하거나 판매하지 않는 것으로 확인 되었습니다.

혹시 모를 피해를 최소화하기 위하여 00시스템과 동일한 ID 및 비밀번호를 사용하고 있는 웹사이트가 있다면, 귀하의 계정정보(ID/비밀번호)를 변경하여 주시기 바랍니다.

아울러 피해가 발생하였거나 기타 궁금하신 사항은 아래 담당부서에 신고하시면 성실하게 안내와 상담을 해 드리고, 필요한 조치를 거쳐 손해배상 등의 구제절차를 진행하도록 하겠습니다.

앞으로 해당 서비스에 대한 보안 및 개인정보보호 조치 강화 등 개인정보에 대한 관리체계를 개선하고, 향후 다시는 이와 유사한 사례가 발생하지 않도록 최선의 노력을 다하겠습니다.

귀하께 실례를 끼쳐 드리게 되어 거듭 진심으로 사과 드립니다.

▶ 피해 등 접수 담당부서: 0000팀(00-0000-0000)

▶ 피해 등 접수 메일:0000@0000.kr

00교육기관 000
</td></tr>
</table>

<table>
<tr><td colspan="2">발생(인지) 일자</td><td colspan="3">2023.3.21.</td></tr>
<tr><td colspan="2">발생(인지) 경로</td><td colspan="3">- 2023.3.21 10:00 월별 개인정보처리시스템 접속로그 점검 시 특정 IP로부터 다량의 개인정보 다운로드 기록 확인
- 2023.3.21 10:30 정보보안 솔루션(방화벽, IPS 등) 로그 분석 결과 외부 해킹 공격은 없음
- 2023.3.21 11:00 개인정보처리시스템의 로그 확인 결과 알 수 없는 개인정보 압축 파일 발견
- 2023.3.21 12:00 IP Table, NAC 등을 확인하여 개인정보를 다운로드한 특정 IP의 PC(용역업체 개인 PC) 확인
- 2023.3.21 13:00 해당 PC 점검 및 유출 내용 확인</td></tr>
<tr><td colspan="2">조치 일자</td><td colspan="3">2023.3.21.</td></tr>
<tr><td colspan="2">유출사실 인지 이후 후속 조치
(유출피해 최소화 대책・조치 및 결과)</td><td colspan="3">- 2023.3.21. 12:00 기관 개인정보 유출사고 대응 매뉴얼에 따라 유출사고 대응반 구축
- 2023.3.21. 13:30 개인정보 유출 접수 창구 및 민원 대응 창구 구축
- 2023.3.21. 14:00 유출 항목 및 발생 상황 인지 후 유출 통지문 작성 및 관련 내용 통지, 개인정보보호위원회 및 교육부 개인정보 유출 신고
- 2023.3.21. 14:30 유출 원인에 따른 개인정보처리시스템에 대한 접근권한 관리체계 강화
- 2023.3.21. 15:00 유출 피해 최소화를 위해 추가 확인 정보 공지 및 관련 내용 현행화 실시
- 2023.3.21. 15:30 재발방지 대책을 위한 보안강화 계획(안) 수립
1) 보안 솔루션 도입
2) 전 직원대상 사례 전파 교육 및 개인정보 교육
3) 모든 개인정보처리시스템 대상 안전성 확보 조치 방안 점검</td></tr>
<tr><td colspan="2">신고 일자</td><td colspan="3">2023.3.22.</td></tr>
<tr><td rowspan="2">유출된 개인정보</td><td>규모(명)</td><td>1,150명</td><td colspan="2">(중복제거) 1,100명(학생 600명, 학부모 200명, 교직원 300명)</td></tr>
<tr><td>항목</td><td colspan="3">이름, ID, 비밀번호, 주소, 핸드폰번호, 이메일</td></tr>
<tr><td colspan="2">유출된 시점과 그 경위</td><td colspan="3">- 2023.3.4 20:00 용역업체 A씨는 개인정보처리시스템에 접속하여 다량의 개인정보파일을 생성 후 PC로 다운로드
- 2023.3.4 21:00 PC내 보안 솔루션(NAC 등)에 의하여 상용 이메일 접근 불가 확인 후 개인 이메일 서버로 파일 전송</td></tr>
<tr><td colspan="2">교육부 신고 여부
(1명 이상 유출시)</td><td>○</td><td rowspan="3">(1명 이상인 경우)
유출 통지 및 조치 결과를 지체 없이 상급기관을 경유하여 교육부에 보고(교육부 개인정보보호 포털(privacy.moe.go.kr))

(1천명 이상인 경우)</td></tr>
<tr><td colspan="2">개인정보보호위원회 신고 여부
(1천명 이상 유출시)</td><td>○</td></tr>
<tr><td colspan="2">홈페이지 공지 여부 및 공지 기간</td><td>- 학교 홈페이지 공지사항 게시판에 공지
- 공지기간 : 2023.3.22.~4.1.</td></tr>
</table>

<table>
<tr>
<td>(1천명 이상 유출시)</td>
<td>
개인정보 유출 사실을 통지해 드리며,
깊이 사과 드립니다.

고객님의 개인정보는 2023년 3월 4일 00용역업체 직원에 의하여 외부 유출된 사실을 확인하였고, 2차 피해 예방을 위해 경찰청에 즉시 조사를 의뢰하여 수사진행 중입니다.

유출된 개인정보 항목은 이름, 아이디(ID), 비밀번호(P/W), 이메일, 핸드폰번호, 주소 총 6개 항목입니다.

유출 사실을 인지한 후 즉시 접속 경로를 차단하고, 취약점 점검과 보완 조치를 완료 하였습니다.

현재까지 확인한 바로는 경찰청에서 00용역업체 직원이 외부로 유출된 개인정보는 제3자에게 2차 전달하거나 판매하지 않는 것으로 확인 되었습니다.

혹시 모를 피해를 최소화하기 위하여 00시스템과 동일한 ID 및 비밀번호를 사용하고 있는 웹사이트가 있다면, 귀하의 계정정보(ID/비밀번호)를 변경하여 주시기 바랍니다.

아울러 피해가 발생하였거나 기타 궁금하신 사항은 아래 담당부서에 신고하시면 성실하게 안내와 상담을 해 드리고, 필요한 조치를 거쳐 손해배상 등의 구제절차를 진행하도록 하겠습니다.

앞으로 해당 서비스에 대한 보안 및 개인정보보호 조치 강화 등 개인정보에 대한 관리체계를 개선하고, 향후 다시는 이와 유사한 사례가 발생하지 않도록 최선의 노력을 다하겠습니다.

귀하께 실례를 끼쳐 드리게 되어 거듭 진심으로 사과 드립니다.

▶ 피해 등 접수 담당부서: 0000팀(00-0000-0000)

▶ 피해 등 접수 메일:0000@0000.kr

00교육기관 000
</td>
<td>유출 통지 및 조치 결과를 지체 없이 상급기관을 경유하여 교육부에 보고하고(교육부 개인정보보호 포털), 개인정보보호위원회(또는 한국인터넷진흥원, www.privacy.go.kr)에 신고

※1천명 이상 개인정보가 유출된 경우 개별 통지와 함께 유출된 사실을 인터넷 홈페이지에 7일 이상 게재</td>
</tr>
<tr>
<td>정보주체가 할 수 있는 피해 최소화 방법 및 구제절차</td>
<td colspan="2">▪ 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)</td>
</tr>
<tr>
<td>진행사항 또는 향후계획</td>
<td colspan="2">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</td>
</tr>
</table>

붙임5 **사고대응 흐름도**


유출 사고 발생
신고/접수
보안부서
협업부서
IT 부서
보고(보안조치 사항)
보고(사실관계 등)
보고(시스템 사항)
총괄 대응 본부
1차 보고
개인정보 보호 책임자
소집
유출사고 대응센터
2차 보고
개인정보 보호 책임자
분석
복구
민원 대응
홍보
법무
대응방안 적용
문제 공유 및 교육/ 재발 방지 대책 마련

붙임6 개인정보 유출에 따른 2차 피해유형 및 대응요령

	피해종류	활용된 개인정보 주요항목	개인정보 악용 절차	이용자 대응요령
금전적	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	• 신용카드 정지 및 재발급 신청 ※ 신고기관 : 각 카드사, 한국소비자원 소비자 상담센터(☏1372) 등
	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	• 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	• 신용카드 정지 및 재발급 신청, 이용내역 통지 서비스 가입 ※ 신고기관 : 각 카드사, 경찰, 금융감독원(☏1332)

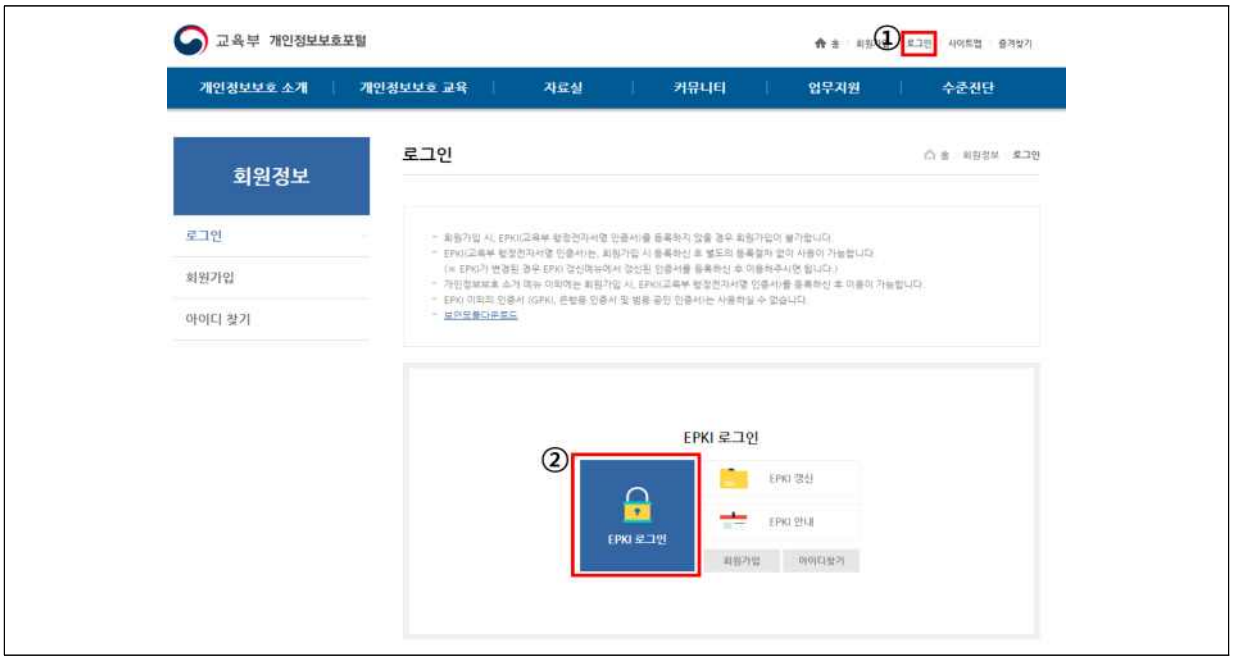
	피해종류	활용된 개인정보 주요항목	개인정보 악용 절차	이용자 대응요령
			활용하여 상품 결제 등에 악용 ※ 국내외 POS단말기의 경우 마그네틱 부분만을 이용하여 결제 가능	
	스미싱	휴대전화번호	① '정보유출 확인 안내' 등 금융기관을 사칭하는 문자메시지에 악성코드(인터넷주소)를 삽입하여 발송 ② 금융기관 사칭 메시지를 받은 피해자가 인터넷주소(URL)를 클릭하면 악성코드에 감염되어 소액결제 피해 및 개인·금융정보 탈취	• 수상한 문자메시지 삭제 및 메시지 상 링크 클릭하지 않기 또는 카드사 공지 전화번호 확인 ※ 신고기관 : 카드사, 경찰, 불법스팸대응센터(☏118)
비금전적	보이스피싱	신용카드번호, 휴대전화, 집전화번호, 집주소 등	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	• 수상한 전화 거부 및 각 카드사에서 공지한 전화번호 확인 ※ 신고기관 : 카드사, 경찰, 불법스팸대응센터(☏118)
	명의도용을 통한 온라인회원 가입	이름, 이메일, 연락처 등	① 유출된 개인정보를 이용하여 웹사이트 가입 ※ 일부 홈페이지의 경우 이름,	• 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
			이메일, 연락처만으로 회원가입 가능 ② 명의도용을 통해 본인도 모르는 수십여개의 웹사이트 가입하여 개인정보 불법 이용	※ 국내 사이트로 주민번호 사용 내역이 있는 경우만 가능하며, 주민번호 미사용시 서비스 불가
	휴대전화/이메일 스팸발송	휴대전화 번호, 이메일 주소 등	① 유출된 개인정보를 이용해 불특정 다수에게 스팸 발송 ※ 유출된 모든 휴대전화, 이메일로 도박 등 스팸 무작위 발송 가능 ※ 신용정보, 연소득등 활용 대출 스팸 발송, 자동차 보유여부를 활용한 보험 스팸 발송 등 특정유형의 개인에 대한 타겟 마케팅 가능 ② 휴대전화, 이메일 서비스 이용자는 원치 않는 홍보·마케팅 광고 수신	• 지능형 스팸차단서비스를 이용한 스팸 차단, 수신 스팸 적극 신고 ※ 신고기관 : 카드사, 경찰, 불법스팸대응센터(☏118) ※ 지능형 스팸차단서비스 : 발신·회신번호 등 발송패턴을 분석하여 스팸을 차단해주는 서비스
	사회공학적 기법을 활용한 악성코드 유포메일 발송	이메일주소 등	① 해커가 특정 대상을 목표로 스팸/피싱 시도용 첨부파일이 포함되어 있거나 연결을 유도 URL이 포함된 이메일 발송 ② 수신자들이 이메일에 포함된 첨부파일 및 URL을 클릭 ③ 해커가 수신자의 PC를 장악하여 기밀 및 개인정보를 빼냄	• 의심가는 이메일을 받은 경우 함부로 열람하지 않고 바로 삭제 • 사용자 PC의 바이러스 백신을 항상 최신버전으로 유지 및 정기적 검사 수행 ※ 신고기관 : 경찰, 불법스팸대응센터(☏118)

붙임7 교육부 개인정보보호 포털 유출신고 절차

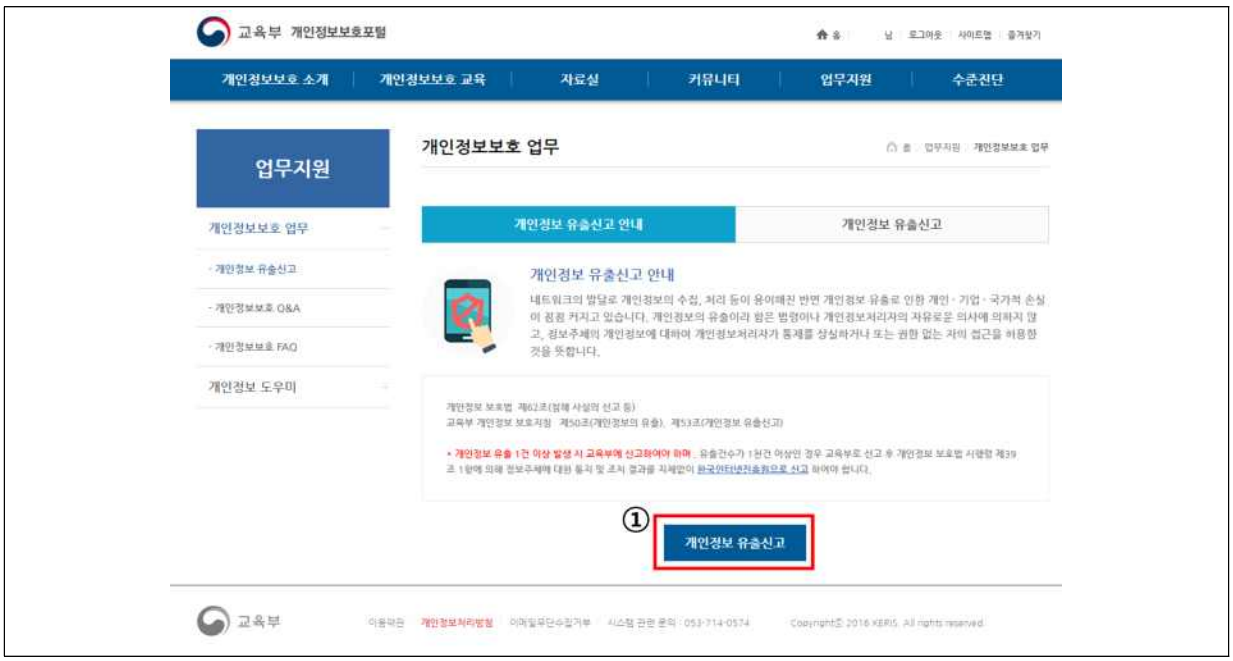
[1단계] 교육부 개인정보보호 포털(https://privacy.moe.go.kr) 사이트 접속 → ① [로그인] → ② [EPKI 로그인] 선택

※ 회원가입이 되어 있지 않은 경우, 회원가입 메뉴를 통하여 회원가입 진행

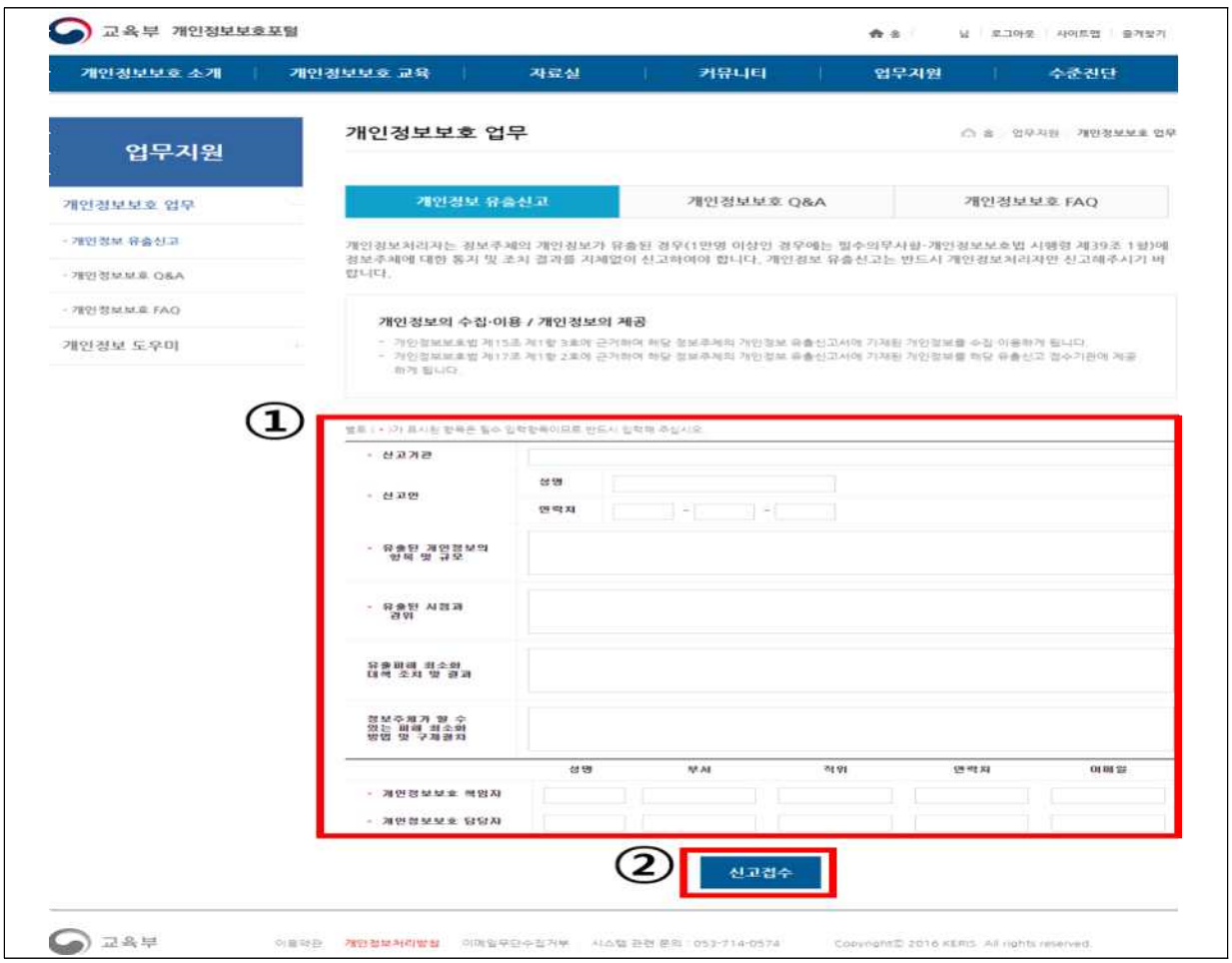


[2단계] ① [업무지원] → ② [개인정보보호 업무] 선택

[3단계] ① [개인정보 유출신고] 선택



[4단계] ① [유출신고 관련 내용 작성] → ② [신고접수] 완료



붙임8 유관기관 관련 연락처

□ 개인정보 유출 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