전라북도교육청장수도서관
개인정보보호 내부관리 계획(개정)

2022. 1.

전라북도교육청장수도서관
Jeollabukdo Office of Education Jangsu Public Library

목 차

제1장 총 칙

제1조(목적) 전라북도교육청장수도서관(이하 “본 기관”) 개인정보 내부 관리계획은 「개인정보 보호법」제29조와 같은 법 시행령 제30조 그리고 ‘개인정보의 안전성 확보조치 기준’에 따라 개인정보를 처리함에 있어서 개인정보가 분실・도난・유출・위조・변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적・관리적 및 물리적 안전조치에 관한 사항을 정하는 것을 목적으로 한다.

제2조(용어 정의) 개인정보 내부 관리계획에서 사용하는 용어의 뜻은 다음과 같다.

1. "개인정보"란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.

1의2. “가명처리”란 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것을 말한다.

2. "처리"란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.
3. “정보주체”란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
4. “개인정보파일”이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.
5. “개인정보처리자”란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.
6. “개인정보 보호책임자”란 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지는 자로서 영 제32조제2항에 해당하는 자를 말한다.

6의2. “개인정보 보호담당자”란 기관의 실질적인 개인정보 보호업무를 담당하는 자로 개인정보 처리자가 지정한 자를 말한다.

7. “개인정보취급자”란 개인정보처리자가 고용하는 임직원, 파견근로자, 시간제근로자 등을 말한다.
8. “개인정보처리시스템”이란 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템을 말한다.
9. “위험도 분석”이란 개인정보 유출에 영향을 미칠 수 있는 다양한 위험요소를 식별・평가하고 해당 위험요소를 적절하게 통제할 수 있는 방안 마련을 위한 종합적으로 분석하는 행위를 말한다.
10. “비밀번호”란 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터 또는 정보통신망 등에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.
11. “정보통신망”이란 「전기통신기본법」제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집・가공・저장・검색・송신 또는 수신하는 정보통신체계를 말한다.
12. “가상사설망”이란 인터넷과 같은 공중망(Public Network)을 마치 전용선으로 사설망(Private network)을 구축한 것처럼 사용할 수 있는 망을 말한다.
13. “공개된 무선망”이란 불특정 다수가 무선접속장치(AP)를 통하여 인터넷을 이용할 수 있는 망을 말한다.
14. “모바일 기기”란 무선망을 이용할 수 있는 PDA, 스마트폰, 태블릿PC 등 개인정보 처리에 이용되는 휴대용 기기를 말한다.
15. “바이오정보”란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.
16. “보조저장매체”란 이동형 하드디스크, USB메모리, CD(Compact Disk), DVD(Digital Versatile Disk) 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 용이하게 연결・분리할 수 있는 저장매체를 말한다.
17. “내부망”이란 물리적 망분리, 접근 통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.
18. “접속기록”이란 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무내역에 대하여 개인정보 취급자 등의 계정, 접속일시, 접속지 정보(접속한 자의 PC, 모바일기기 등 단말기 정보 또는 서버의 IP주소 등), 처리한 정보주체 정보, 수행업무(수집, 생성, 연계, 연동, 기록, 저장, 보유 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기 등) 등을 전자적으로 기록한 것을 말한다. 이 경우 “접속”이란 개인정보처리시스템과 연결되어 데이터 송신 또는 수신이 가능한 상태를 말한다.
19. “관리용 단말기”란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리시스템에 직접 접속하는 단말기를 말한다.

제3조(적용 범위) 본 기관이 개인정보를 처리하거나 본 기관의 개인정보 처리 업무를 위탁받아 처리하는 수탁자에게는 본 개인정보 내부 관리계획이 적용된다.

제2장 내부 관리계획의 수립 및 시행

제4조(내부 관리계획의 수립 및 승인) ① 개인정보 보호책임자는 개인정보 보호와 관련한 법령 및 규정 등을 준수할 수 있도록 내부 의사결정 절차를 통하여 내부 관리계획을 수립하여야 한다.

② 개인정보 보호책임자는 내부 관리계획의 각 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부 관리계획을 수정하여야 하며, 그 이력을 보관·관리하여야 한다.

③ 개인정보 보호책임자는 연 1회 이상으로 내부 관리계획의 이행 실태를 점검·관리하고 그 결과에 따라 적절한 조치를 취하여야 한다.

제5조(내부 관리계획의 공표) ① 개인정보 보호책임자는 제4조에 따라 승인된 내부 관리계획을 모든 교직원 및 관련자에게 알림으로써 이를 준수하도록 하여야 한다.
② 내부 관리계획은 전 직원이 언제든지 열람할 수 있는 방법으로 비치하거나 제공하여야 한다.

제3장 개인정보 보호책임자의 역할 및 책임

제6조(개인정보 보호책임자의 지정) ① 본 기관은 「개인정보 보호법」제31조와 같은 법 시행령 제32조 및 교육부 개인정보 보호지침(이하 "지침") 제21조에 따라 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자를 도서관장으로 정한다.

제7조(개인정보 보호책임자의 역할 및 책임) ① 개인정보 보호책임자는 다음 각 호의 업무를 수행한다.
1. 개인정보 보호 계획의 수립 및 시행
2. 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
3. 개인정보 처리와 관련한 불만의 처리 및 피해 구제
4. 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
5. 개인정보 보호 교육 계획의 수립 및 시행
6. 개인정보파일의 보호 및 관리 감독
7.「개인정보 보호법」제30조에 따른 개인정보 처리방침의 수립·변경 및 시행
8. 개인정보 보호 관련 자료의 관리
9. 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기

② 개인정보 보호책임자는 제1항의 업무를 수행함에 있어서 필요한 경우 개인정보의 처리 현황, 처리 체계 등에 대하여 수시로 조사하거나 관계 당사자로부터 보고를 받을 수 있다.
③ 개인정보 보호책임자는 개인정보 보호와 관련하여 이 법 및 다른 관계 법령의 위반 사실을 알게 된 경우에는 즉시 개선조치 보고하여야 한다.

제8조(개인정보취급자의 역할 및 책임) ① 개인정보취급자는 본 기관의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자를 말한다.
② 개인정보취급자는 개인정보를 처리함에 있어서 개인정보가 안전하게 관리될 수 있도록 동 계획은 물론, 개인정보 보호와 관련한 법령 및 규정 등을 준수하여야 한다.

제4장 개인정보 보호 교육

제9조(개인정보 보호책임자의 교육) ① 본 기관은 개인정보 보호책임자를 대상으로 연 1회 이상 개인정보 보호와 관련된 교육을 실시한다.

제10조(개인정보취급자의 교육) ① 개인정보 보호책임자는 개인정보의 적정한 취급을 보장하기 위하여 다음 각 호의 사항을 정하여 개인정보취급자에게 필요한 개인정보 보호 교육 계획(연간 개인정보보호 추진 계획에 포함 가능)을 수립하고 실시하여야 한다.
1. 교육 목적 및 대상
2. 교육 내용
3. 교육 일정 및 방법

② 개인정보 보호책임자는 제4장에 따라 개인정보 보호 교육을 실시한 결과 또는 이를 입증할 수 있는 관련 자료 등을 기록·보관하여야 한다.

제5장 기술적 안전조치

제11조(접근 권한의 관리) ① 본 기관은 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.

② 본 기관은 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하여야 한다.

③ 본 기관은 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.

④ 본 기관은 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자 별로 사용자계정을 발급하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

⑤ 본 기관은 개인정보처리시스템, 인터넷 홈페이지 등에 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 다음 각 호의 사항을 적용하여야 한다.

1. 문자, 숫자의 조합·구성에 따라 최소 8자리 또는 10자리 이상의 길이로 구성
   - 최소 8자리 이상 : 두 종류 이상의 문자를 이용하여 구성한 경우
     ※ 문자 종류 : 알파벳 대문자와 소문자, 특수문자, 숫자
   - 최소 10자리 이상 : 하나의 문자종류로 구성한 경우
     ※ 단, 숫자로만 구성할 경우 취약할 수 있음
2. 비밀번호는 추측하거나 유추하기 어렵도록 설정
   - 동일한 문자 반복(aaabbb, 123123 등), 키보드 상에서 나란히 있는 문자열(qwer 등), 일련번호(12345678 등), 가족이름, 생일, 전화번호 등은 사용하지 않음
3. 비밀번호가 제3자에게 노출되었을 경우 지체 없이 새로운 비밀번호로 변경해야 함

⑥ 본 기관은 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 한다.

제12조(접근통제) ① 본 기관은 정보통신망을 통한 인가되지 않은 내·외부자의 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 조치를 하여야 한다.

1. 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol)주소 등으로 제한하여 인가받지 않은 접근을 제한
2. 개인정보처리시스템에 접속한 IP(Internet Protocol)주소 등을 분석하여 불법적인 개인정보 유출 시도 탐지 및 대응

② 본 기관은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다.

③ 본 기관은 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치를 하여야 한다.

④ 본 기관은 고유식별정보를 처리하는 인터넷 홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점을 점검하고 필요한 보완 조치를 하여야 한다.

⑤ 본 기관은 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 하여야 한다.

⑥ 본 기관에서 별도의 개인정보처리시스템을 이용하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 제1항을 적용하지 아니할 수 있으며, 이 경우 업무용 컴퓨터 또는 모바일 기기의 운영체제(OS : Operating System)나 보안프로그램 등에서 제공하는 접근 통제 기능을 이용할 수 있다.

⑦ 본 기관은 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.

제13조(개인정보의 암호화) ① 본 기관은 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

② 본 기관은 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화(해쉬함수)하여 저장하여야 한다.

③ 본 기관은 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.

④ 본 기관은 내부망에 고유식별정보를 저장하는 경우 암호화 한다. 다만, 개인정보보호법 제33조에 따른 개인정보 영향평가의 대상이 되는 경우 해당 개인정보 영향평가의 결과 및 위험도 분석 결과에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.

⑤ 본 기관은 제1항, 제2항, 제3항, 또는 제4항에 따라 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.

⑥ 본 기관은 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다.

⑦ 본 기관은 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

제14조(접속기록의 보관 및 점검) ① 본 기관은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 다음 각 호의 항목을 포함하여 최소 1년 이상 보관·관리하여야 한다. 다만, 5만명 이상의 정보주체에 관하여 개인정보를 처리하거나, 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다.

1. 개인정보취급자 식별 정보(ID 등 계정정보)
2. 접속 일시(날짜 및 시간)
3. 접속지 정보(접속자의 단말기 정보 또는 IP 주소)
4. 처리한 정보주체 정보(정보주체의 이름, ID 등)
5. 수행 업무(열람, 수정, 삭제, 인쇄, 입력 등)

② 본 기관은 개인정보의 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 특히, 개인정보를 다운로드한 것이 발견되었을 경우에는 내부 관리계획으로 정하는 바에 따라 그

사유를 반드시 확인하여야 한다.

③ 본 기관은 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.

제15조(악성프로그램 등 방지) ① 본 기관은 악성프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다.

1. 보안 프로그램의 자동 업데이트 기능을 사용하거나, 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지
2. 악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 즉시 이에 따른 업데이트를 실시
3. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치

제16조(관리용 단말기의 안전조치) 본 기관은 개인정보 유출 등 개인정보 침해사고 방지를 위하여 관리용 단말기에 대해 다음 각 호의 안전조치를 하여야 한다.

1. 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치
2. 본래 목적 외로 사용되지 않도록 조치
3. 악성프로그램 감염 방지 등을 위한 보안조치 적용

제6장 관리적 안전조치

제17조(개인정보 보호조직 구성 및 운영) ① 본 기관은 개인정보의 안전한 처리를 위하여 다음 각 호의 사항을 포함하는 개인정보보호 조직을 구성하고 운영하여야 한다.

1. 개인정보 보호책임자 : 도서관장
2. 개인정보보호 담당자 : 개인정보보호 업무 담당자
3. 개인정보취급부서 : 개인정보를 처리하는 각 실·과

② 개인정보취급부서에서는 개인정보보호 조직과 충분히 협의, 조정하여 개인정보를 처리하여야 한다.

③ 개인정보보호 조직은 제7조에 따른 업무를 수행하여야 하며, 그 밖에 개인정보의 안전성 확보를 위하여 본 기관이 필요하다고 판단되는 사항을 수행할 수 있다.

제18조(개인정보 유출 사고 대응) ① 본 기관은 개인정보의 유출 사고 발생 시 신속한 대응을 통해 피해 발생을 최소화하기 위해 개인정보 유출 사고 대응 계획을 수립하고 시행하여야 한다.

② 제1항에 따른 개인정보 유출 등 침해사고 대응 매뉴얼에는 긴급조치, 유출 통지·조회 및 신고 절차, 고객 민원 대응조치, 현장 혼잡 최소화 조치, 피해자 불안 해소조치, 피해자 구제조치 등을 포함하여야 한다.

③ 본 기관은 개인정보 유출 등 침해사고에 따른 피해복구 조치 등을 수행함에 있어 정보주체의 불편과 경제적 부담을 최소화할 수 있도록 노력하여야 한다.

제19조(수탁자에 대한 관리 및 감독) ① 본 기관은 제3자에게 개인정보의 처리 업무를 위탁하는 경우에는 다음 각 호의 사항을 준수하여야 한다.

1. 위탁업무의 목적 및 범위
2. 위탁업무 기간
3. 재위탁 제한에 관한 사항
4. 위탁업무 수행 목적 외 개인정보 처리 금지에 관한 사항
5. 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
6. 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항
7. 정보주체의 권리 보장에 관한 사항
8. 개인정보의 파기에 관한 사항
9. 수탁자가 준수해야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

② 본 기관은 개인정보의 처리 업무를 위탁하는 경우 인터넷 홈페이지에 위탁하는 업무의 내용과 수탁자를 지속적으로 공개하여야 한다.

③ 본 기관은 개인정보의 처리 업무를 위탁하는 경우 다음 각 호의 사항을 정하여 수탁자를 교육하고 수탁자가 개인정보를 안전하게 처리하는지 감독하여야 한다.

1. 교육 및 감독 대상
2. 교육 및 감독 내용
3. 교육 및 감독 일정, 방법

④ 본 기관은 제3항에 따라 수탁자를 교육하고 감독한 결과에 대한 기록을 남기고 문제점이 발견된 경우에는 필요한 보안조치를 하여야 한다.

제7장 물리적 안전조치

제20조(물리적 안전조치) ① 본 기관은 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 한다.

② 본 기관은 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.

③ 본 기관은 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안대책을 마련하여야 한다. 다만, 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 이를 적용하지 아니할 수 있다.

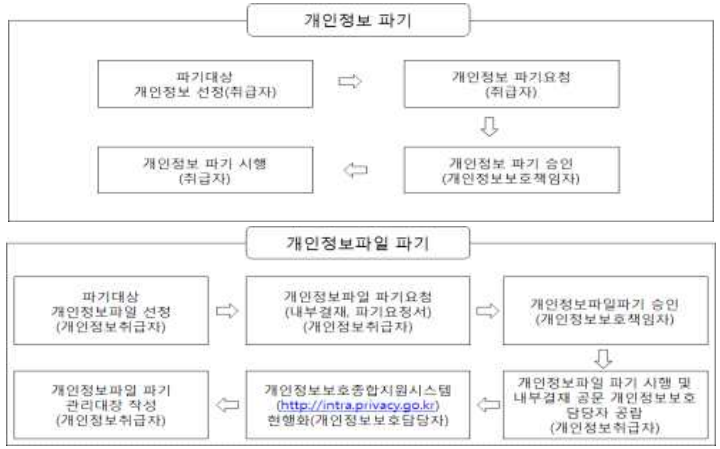
제21조(개인정보의 파기) ① 본 기관은 개인정보를 파기할 경우, 다음 각 호 중 어느 하나의 조치를 하여야 한다.

1. 완전파괴(소각·파쇄 등)
2. 전용 소자장비를 이용하여 삭제
3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

② 본 기관은 개인정보의 일부만을 파기하는 경우, 제1항의 방법으로 파기하는 것이 어려울 때에는 다음 각 호의 조치를 하여야 한다.

1. 전자적 파일 형태인 경우 : 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독
2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 해당 부분을 마스킹, 천공 등으로 삭제

③ 개인정보(파일) 파기 절차



제8장 그 밖에 개인정보 보호를 위하여 필요한 사항

제22조(개인정보의 목적 외 이용·제공) ① 본 기관은 원칙적으로 개인정보를 당초 수집 목적의 범위를 초과하여 이용하거나 제공하지 않는다. 다만, 다음 각 호의 어느 하나에 해당되는 경우에는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다.

1. 정보주체의 별도 동의를 받은 경우
2. 다른 법률의 특별한 규정
3. 명백히 정보주체 또는 제3자의 생명, 신체, 재산의 이익에 필요한경우
4. 삭제<2020. 2. 4.>
5. 개인정보를 목적 외 로 이용하거나 제3자에게 제공하지 않으면 다른 법률에서 정하는 소관업무 수행 불가한 경우로 보호위원회의심의·의결을 거친 경우
6. 조약, 국제협정 이행을 위해 외국 정부 등 제공에 필요한 경우
7. 범죄수사와 공소의 제기 및 유지를 위하여 필요한 경우
8. 법원의 재판업무 수행을 위하여 필요한 경우
9. 형(刑)및 감호, 보호처분의 집행을 위하여 필요한 경우

② 본 기관은 개인정보의 목적 외 이용·제공에 관한 업무절차, 방법, 제한, 안전성 확보조치 방안, 관리대장 기록·관리 방안 및 사실의 공개 등은 개인정보 목적 외 이용·제공 절차서에 따른다.

제23조(개인영상정보처리기기의 설치·운영) ① 본 기관은 교육부 개인정보 보호지침에 따라 영상정보처리기기를 설치·운영하고 이 지침의 준수 여부에 대한 자체점검을 실시하여 다음 해 3월 31일까지 그 결과를 행정안전부장관에게 통보하고 시행령 제34조제3항에 따른 시스템에 등록하여야 한다. 이 경우 다음 각 호의 사항을 고려하여야 한다.

1. 영상정보처리기기의 운영·관리 방침에 열거된 사항
2. 관리책임자의 업무 수행 현황
3. 영상정보처리기기의 설치 및 운영 현황
4. 개인영상정보 수집 및 이용·제공·파기 현황
5. 위탁 및 수탁자에 대한 관리·감독 현황
6. 정보주체의 권리행사에 대한 조치 현황
7. 기술적·관리적·물리적 조치 현황
8. 영상정보처리기 설치·운영의 필요성 지속 여부 등

② 본 기관은 제1항에 따른 영상정보처리기기 설치·운영에 대한 자체점검을 완료한 후에는 그 결과를 홈페이지 등에 공개하여야 한다.

제24조(가명정보의 처리) ① 본 기관은 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리 할 수 있으며, 가명정보를 제3자에게 제공하는 경우에는 특정 개인을 알아보기 위하여 사용될 수 있는 정보를 포함하지 않는다.

② 본 기관은 가명처리 할 경우 관련 가이드라인에서 제시하는 기준을 만족하도록 처리 한다.

[별첨1] 개인정보 유출 사고 대응 매뉴얼

개인정보 유출 사고 대응 매뉴얼

1 개요

1.1 목적

❍ '개인정보 유출 사고 대응 매뉴얼'은 교육(행정)기관이 '개인정보보호법' 및 동법 시행령, 시행규칙, 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

❍ 개인정보보호법 및 시행령, 시행규칙
❍ 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 유출 된 경우 교육부 및 개인정보보호위원회(한국인터넷진흥원)에 신고
o 유출된 정보(예: 비밀번호, 계좌번호 등)가 암호화되어 있어도 정보주체 통지 의무 이행

용 어	정 의
침해	• 법적 근거, 규정 또는 본인 동의에 의하지 않고 이루어지는 개인정보의 수집, 저장, 이용 및 제공, 파기행위 일체 ☞ 개인정보가 유출되지 않은 접근 시도를 포함
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
침해·유출사고 (침해사고)	• 비인가 된 접근, 정보시스템의 오남용, 비인가 된 시스템 사용 또는 사용자의 계정 도용, 악성코드 유입 및 실행 등으로 발생한 개인정보 침해·유출사고
침해·유출사고 대응팀 (침해사고 대응팀)	• 개인정보 침해·유출사고 발생에 따른 사고의 분석, 처리지원, 사후 복구, 사후 예방조치 등을 주요 업무로 하는 개인정보보호 담당부서를 말함
개인정보 보호책임자	• 개인정보보호법 제31조에 의거 개인정보보호 업무를 총괄 • 개인정보 보호담당자를 임명하여 침해·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.

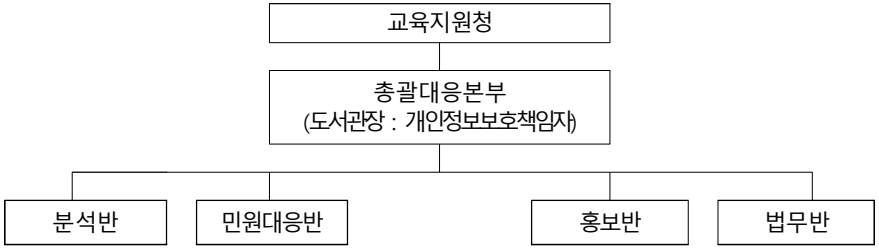
1. 개인정보가 포함된 서면, 이동식 저장장치, 휴대용 컴퓨터 등을 분실하거나 도난당한 경우
2. 개인정보가 저장된 데이터베이스 등 개인정보처리시스템에 정상적인 권한이 없는 자가 접근한 경우
3. 개인정보처리자의 고의 또는 과실로 인해 개인정보가 포함된 파일 또는 종이문서, 기타 저장 매체가 권한이 없는 자에게 잘못 전달된 경우
4. 기타 권한이 없는 자에게 개인정보가 전달된 경우

1.4 단계별 프로세스(업무 절차)

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



❍ 업무분장

조직별	담당	담당 업무
총괄대응본부	개인정보 보호책임자	• 유출사고 대응 총괄 지휘
	개인정보보호 담당자	• 유출사고 인지, 접수, 전파 • 유출사고 대응 절차 수립 • 정보주체에게 유출사실 통지 • 개인정보보호위원회(전문기관)에 유출통지 사실 신고
분석반	정보 담당자	• 유출 사실 확인, 조사 및 원인 분석 • 사고내용 세부조사
민원대응반 (온라인, 오프라인)	민원담당	• 개별 통지문 안내에 따른 후속업무(민원 등) 진행 • 상담센터, 소비자보호 방안 마련(필요시 유관부서와 협조)
홍보반	개인정보보호 담당자	• 유출사고 관련 대외기관(언론사 등) 대응 • 유출사고 안내문 문구 최종 검토
법무반	교감	• 법률상 대응방안, 의사결정 사항 등 정책적 판단사항 검토 및 결정 • 유출사고 관련 수사기관 경과사항 대응 및 대책반 공유
개인정보 취급자 및 전직원		• 개인정보 유출 시 정보보호 부서에 신고 및 업무 협조 사항 이행

2 개인정보 유출사고 대응 조치 및 피해 구제 방법

2.1 유출 통지·조회 절차

가이드

o 개인정보처리자는 개인정보보호법 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 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 통지 신고 절차

❍ 유출 신고 절차

❍ 유출통지 신고방법

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, 도교육청, 교육부에 보고 ※ 고등학교, 교육지원청, 교육청 직속기관 등은 도교육청, 교육부에 보고 ※ 국립학교는 교육부에 보고
신고시기	▶ 5일 이내(정보주체에 대한 통지 및 조치결과 신고)
신고방법	▶ 전자우편, 팩스, 공문, 인터넷 사이트*를 통해 유출사고 보고 및 신고서 제출 * 교육부 : privacy.moe.go.kr 개인정보보호위원회(또는 한국인터넷진흥원) : privacy.go.kr ▶ 시간적 여유가 없거나 특별한 사정이 있는 경우 상급기관과 교육부에 동시에 보고하며, 전화, 전자우편**을 통해 보고와 유출신고서를 제출 ** 전자우편 주소 : privacyleak@keris.or.kr
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)

2.3 현장 혼잡 최소화 조치

가이드

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

❍ 총괄대응본부는 사무실 오프라인 창구를 개설

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

구분	채널
오프라인	사무실 (상황에 따라 창구 변경 가능)
온라인 中 택 1 (상황 발생 시 선택)	전화
	메일
	홈페이지
	SNS

❍ 분석반은 대외 수사 기관에 협조 할 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 홈페이지에 공지하고 타 부서에서 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	사무실
피해구제 관련 문의 대응	
기타	

2.5 정보주체 불안 해소 조치

가이드

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

- ❍ 홈페이지에 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(www.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
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 침해·유출 피해에 대한 피해구제, 상담 등을 문의 할 수 있음을 안내
- ❍ 개인정보를 침해당한 사람은 누구든지 개인정보 분쟁조정위원회에 분쟁조정을 신청할 수 있음을 안내(「개인정보보호법」 제43조제1항)
- ❍ 정보주체는 개인정보처리자가 이 법을 위반한 행위로 손해를 입으면 개인정보처리자에게 손해배상을 청구할 수 있음을 안내

3 개인정보 유출 원인별 보호 조치

3.1 해킹

❍ 해킹 등 침해사고 발생으로 인해 개인정보가 유출된 사실을 알게 된 경우에는 개인정보 추가 유출 방지를 위한 대책을 마련하고 피해를 최소화할 수 있는 조치를 강구하여야 함

- 추가 유출 방지를 위해 시스템 일시정지, 이용자 및 개인정보취급자 비밀번호 변경*, 유출 원인 분석, 기술적 보안조치 강화, 시스템 변경, 기술지원 의뢰 및 복구 등과 같은 긴급조치를 시행하여야 함

  * 일방향 암호화되지 않은 비밀번호가 유출된 경우에는 비밀번호를 변경하지 않으면 이용할 수 없도록 하고, 일방향 암호화된 비밀번호가 유출된 경우에도 비밀번호 변경을 유도하여 추가 피해 예방에 노력하여야 함

- 개인정보 유출의 직접·간접적인 원인을 즉시 제거하고, 미비한 보호조치 부분을 파악하여 보완하여야 함

3.2 내부자 유출

❍ 개인정보 유출자가 개인정보처리시스템에 접속한 이력 및 개인정보 열람·다운로드 등 내역을 확인하여야 함

❍ 개인정보 유출자의 개인정보처리시스템에 대한 접근형태가 정상인지 비정상인지 여부를 확인하고, 비정상적*인 접속인 경우 우회경로를 확인하여 접속을 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, 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

** 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 교육을 실시

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

* 사례전파시 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

〔붙임 1〕

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

〔붙임 2〕

표준 개인정보 유출 통지 문안(예시)

□ 부가설명 란에 **필수사항은 < >, 참고사항은 ( )**로 표기하였음
□ 필수사항은 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, 회원정보의 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

〔붙임 3〕

개인정보 유출 신고서(양식)

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 보호책임자				
	개인정보 취급자				

유출신고접수기관	기관명	담당자명	연락처

〔붙임 4〕

개인정보 유출신고 조치 확인서(양식)

※ 6하 원칙에 따라 사실 관계를 명확하게 작성하여 주십시오.

기관명		00학교
정보주체 통지 여부	통지일자	0000.00.00.
	통지방법	(예시) 전화, 이메일, 서면, 팩스 등
	필수통지 항목	필수 통지 항목 5가지 / 포함 여부 확인(O, X) ① 유출된 개인정보의 항목 / O 또는 X ② 유출 시점과 및 그 경위 / O 또는 X ③ 피해 최소화를 위한 정보주체의 조치방법 / O 또는 X ④ 기관의 대응조치 및 피해구제 절차 / O 또는 X ⑤ 피해 신고 접수 담당부서 및 연락처 / O 또는 X (예시) 이메일 내용 이미지 캡쳐 등 증빙자료 포함
발생(인지) 일자		0000.00.00.
발생(인지) 경로		(예시) - 0000.00.00 00:00 KISA에서 통보 - 정보주체가 해당 학과에 신고, ECSC 침해사고, 민원인 신고 등
조치 일자		0000.00.00.

유출사실 인지 이후 후속 조치 (유출피해 최소화 대책・조치 및 결과)	**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) - 0000.00.00 00:00 해당 게시글 삭제 - 0000.00.00 00:00 정보주체에게 메일, 문자로 안내 - 0000.00.00 00:00 홈페이지취약점 점검 수행 - 0000.00.00 00:00 00홈페이지에 유출 건 내용 게시 - 0000.00.00 00:00 재발방지대책 수립 - 0000.00.00 00:00 전직원 대상 개인정보 관련 교육 - 개인정보 파일 삭제, 오발송된 이메일 회수, 사례전파, 교육실시 등 증빙자료 포함		
신고 일자	0000.00.00.		
유출된 개인정보	규모(명)	00명	(중복제거) 00명
	항목	이름, 핸드폰번호 ,,,,,	
유출된 시점과 그 경위	(예시) - 0000.00.00 00:00 메일 잘못 발송, 실수로 개인정보 파일 첨부함 - 0000.00.00 00:00 유출 확인		
교육부 신고 여부 (1명 이상 유출시)	ㅇ 또는 X	(1명 이상인 경우) 유출 통지 및 조치 결과를 지체 없이 상급기관을 경유하여 교육부에 보고(교육부 개인정보보호 포털(privacy.moe.go.kr))	
개인정보보호위원회	ㅇ 또는 X		

신고 여부 (1천명 이상 유출시)		(1천명 이상인 경우) 유출 통지 및 조치 결과를 지체 없이 상급기관을 경유하여 교육부에 보고(교육부 개인정보보호 포털(privacy.moe.go.kr))
홈페이지 공지 여부 및 공지 기간 (1천명 이상 유출)	(예시) - 00홈페이지 00게시판에 공지 - 공지기간 : 0000.00.00~00.00. - 공지사항 내용 이미지 캡쳐 등 증빙자료 포함	※1천명 이상 개인정보가 유출된 경우 개별 통지와 함께 유출된 사실을 인터넷 홈페이지에 7일 이상 게재
정보주체가 할 수 있는 피해 최소화 방법 및 구제절차	(예시) 피해구제절차 안내 등	
진행사항 또는 향후계획	(예시) 자체 내부 감사 수행, 상위기관 현장 컨설팅 수행, 개인정보보호위원회 점검 예정 등	

[붙임 5]

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	• 신용카드 정지 및 재발급 신청, 이용내역 통지 서비스 가입 ※ 신고기관 : 각 카드사, 경찰, 금융감독원(☏1332)

	피해종류	활용된 개인정보 주요항목	개인정보 악용 절차	이용자 대응요령
			② 불법 복제된 카드를 국내외에서 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	• e프라이버시 클린서비스(www.eprivacy.go.kr)를 활용한 해당 사이트 탈퇴 요청

	피해종류	활용된 개인정보 주요항목	개인정보 악용 절차	이용자 대응요령
			※ 일부 홈페이지의 경우 이름, 이메일, 연락처만으로 회원가입 가능 ② 명의도용을 통해 본인도 모르는 수십여개의 웹사이트 가입하여 개인정보 불법 이용	※ 신고기관 : 경찰, 불법스팸대응센터(☏118) ※ 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)

[붙임 6]

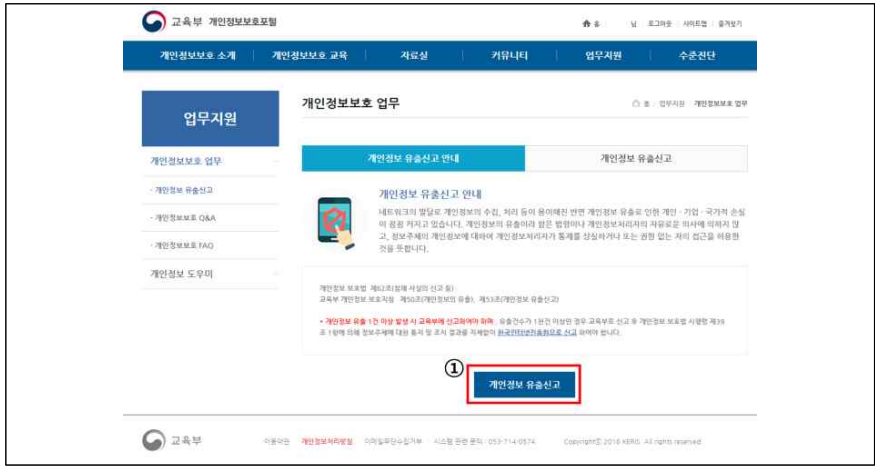
교육부 개인정보보호 포털 유출신고 절차

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

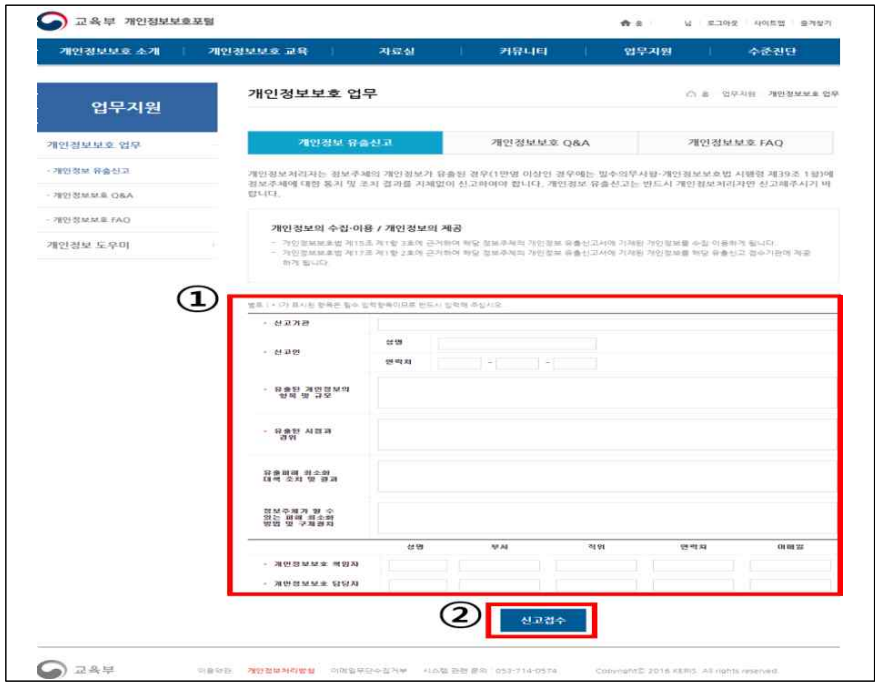
※ 회원가입이 되어 있지 않은 경우, 회원가입 메뉴를 통하여 회원가입 진행

[2단계] ① [업무지원] → ② [개인정보보호 업무] 선택

[3단계] ① [개인정보 유출신고] 선택



[4단계] ① [유출신고 관련 내용 작성] → ② [신고접수] 완료



〔붙임 7〕

□ 개인정보 유출 신고

기 관 명	전화번호	인터넷사이트
교육부	-	https://privacy.moe.go.kr/ (교육부 개인정보보호 포털)
전라북도교육청	239-3434	
개인정보보호위원회	118 (Fax:02-2100-3008)	https://privacy.go.kr/ (개인정보보호 포털)
한국인터넷진흥원	118	

□ 관련기관 연락처

기 관 명	전화번호	인터넷사이트
대검찰청 과학수사부 사이버수사과	1301	http://www.spo.go.kr/
경찰청 사이버수사국	182	http://ecrm.cyber.go.kr/

[별첨2] 개인정보 내부 관리계획 이행실태 점검표

개인정보 내부 관리계획 이행실태 점검표

점검항목	점검결과 (○,×)	세부 점검 방법
개인정보 보호책임자 지정 및 역할 수행		1. 개인정보 보호책임자 지정 여부 - 내부 관리계획 및 개인정보처리방침에 개인정보 보호책임자 지정유무
		▫ **이행실적 및 증빙자료** *ex) "개인정보보호 개인정보처리방침 변경 수립" (○○학교-34(0000.00.00.)* *※ 증빙할 수 있는 공문 제목 및 번호 기재 또는 증빙 사진*
		2. 역할수행 여부 - 개인정보 보호책임자가 내부 관리계획에 지정된 역할을 적절하게 수행하고 있는지 여부
		▫ **이행실적 및 증빙자료** - 하위 점검 항목들을 수행한 것으로 증빙을 갈음함
개인정보 취급자 교육 실시		1. 개인정보 보호 교육 계획 수립 - 교육목적 및 대상, 교육내용, 교육일정 및 방법을 포함한 교육 계획 수립 여부
		▫ **이행실적 및 증빙자료** *ex) "0000년 교직원 개인정보보호 교육 실시 계획" (○○학교-56(0000.00.00.)*
		2. 개인정보 보호 교육 실시 - 개인정보취급자를 대상으로 개인정보 보호 교육의 실시 여부
		▫ **이행실적 및 증빙자료** *ex) "0000년 교직원 개인정보보호 교육 실시 결과" (○○학교-78(0000.00.00.)*
접근권한 관리		○ 나이스, k-에듀파인 권한 부여대장의 관리 - 개인정보처리시스템에 접근 권한을 최소한의 범위로 부여여부 - 전보, 퇴직 인사이동 시 권한 변경 및 말소 여부(홈페이지, 메신저 등) - 사용자별 접속 계정 발급 및 공유금지의 이행여부
		▫ **이행실적 및 증빙자료** *ex) "0000년 0학기 나이스 권한 부여 내역" (○○학교-90(0000.00.00.)*
접근통제 및 단말기 안전조치		1. 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통해 공개·유출되지 않도록 업무용PC, 모바일 기기 등에 접근통제 조치(비밀번호 설정 등) 여부 2. 일정시간 이상 업무처리 하지 않을 경우 자동으로 시스템 접속 차단(업무용PC 화면보호기 비밀번호 설정) 여부
		▫ **이행실적 및 증빙자료** *ex) "0000년 0월 사이버 보안진단결과 등록" (○○학교-101(0000.00.00.) → 매월실시*
암호화		○ 업무용PC에 주민등록번호 저장 시 PC개인정보보호시스템(Privacy-i)을 통한 암호화 실시 여부
		▫ **이행실적 및 증빙자료** *ex) PC개인정보보호시스템 관리자 보고서 개인정보 처리 현황 자료*
접속기록 보관 및 점검		○ 별도 운영하는 개인정보처리시스템이 있을 경우 접속기록 점검 및 보관 여부 - 운영하는 개인정보처리시스템이 없을 경우 "해당없음" 표기
악성프로그램 방지		○ 업무용PC에 백신 소프트웨어 설치 운영 및 다음사항 준수 여부 1. 자동업데이트 사용(최신 상태 유지) 2. 악성 프로그램 관련 경보 발령 또는 사용 중인 응용 프로그램, 운영체제 보안 업데이트 공지 시 즉시 업데이트 실시 3. 악성프로그램 발견 시 즉시 삭제 조치 등 ※ 내PC지키미 매월 실시(100점 유지)
		▫ **이행실적 및 증빙자료** *ex) "0000년 0월 사이버 보안진단결과 등록" (○○학교-101(0000.00.00.) → 매월실시*
수탁자에 대한 관리 및 감독		○ 개인정보 처리 업무를 위탁하는 경우 준수사항 이행 여부 1. 위탁계약서 작성 2. 위탁사항 공개 3. 수탁업체 교육 및 관리 감독 여부
		▫ **이행실적 및 증빙자료** *ex) 개인정보처리 표준 위탁 계약서, 업체 교육 결과, 개인정보 파기 확인서, 개인정보처리 방침 위탁사항 공개 자료 등*
물리적 안전조치		1. 전산실, 평가실 등 개인정보 보관 장소의 물리적 통제 절차 수립 ex) 통제구역 지정, 출입자대장 관리, 잠금장치 설정 등 2. 개인정보 포함 서류, 휴대용 저장매체를 잠금장치가 있는 안전한 장소에 보관 여부
		▫ **이행실적 및 증빙자료** *ex) 통제 구역 및 상시 출입자 지정(○○학교-105(0000.00.00.), 잠금장치 설정 사진*
파기 수행		○ 개인정보 파기 시 절차 준수 여부 1. 처리목적 달성, 보유기간 경과 시 즉시 파기 2. 파기 기록·관리 3. 재생 및 복구 불가능한 방법으로 파기 여부 ※ 위 3가지 내용 포함 한 내부결재 공문
		▫ **이행실적 및 증빙자료** *ex) 개인정보 파기(○○학교-10(0000.00.00.)*
영상정보 처리기기 운영·관리		1. 영상정보처리기기 운영·관리방침 수립 및 홈페이지 공개 여부 (개인정보처리방침에 포함 가능) 2. CCTV안내판 설치 여부(눈에 잘 띄는 곳) - 설치목적 및 장소, 촬영범위 및 시간, 관리책임자 성명 또는 직책 및 연락처, 위탁의 경우 수탁자 및 연락처 3. 개인영상정보 관리 대장 작성 여부 - 열람·이용·제공 및 주기적 자동 파기 사항 기록 4. 안전한 물리적 보관 시설 또는 잠금 장치 설치 여부 5. 영상정보처리기기 운영 현황 등록·관리 여부 (매년 3월 개인정보보호종합지원시스템-intra.privacy.go.kr)
		▫ **이행실적 및 증빙자료** *ex) 영상정보처리기기 운영·관리 방침 홈페이지 공개 화면, CCTV 안내판 설치 사진, 개인영상정보 관리대장, CCTV 상황실 또는 잠금 장치 설치 사진, 영상정보처리기기 현황 등록 자료 등*

※ 개인정보 보호책임자는 「교육부 개인정보 보호지침」 제35조에 따라 연 1회 이상 내부 관리계획의 이행 실태를 점검·관리해야 함.

[별첨3] 개인정보보호 교육 계획 및 결과(참고용)

0000년 개인정보보호 교육 계획

□ 개요

개인정보의 안전한 관리 및 운용을 위해 개인정보보호 관련 규정 및 변경 사항, 안전조치 요령, 침해 사고 시 대응방안 등 체계적인 교육 실시

※ 관련근거 : 개인정보보호법 제28조제2항 (개인정보취급자에 대한 정기적인 교육 실시), 개인정보보호법 제31조제2항제5호 (개인정보 보호 교육계획의 수립 및 시행)

□ 교육대상 및 범위

교육 범위	책임자	담당자	취급자/일반직원
o 개인정보보호 관련 법·제도 현황	○	○	○
o 개인정보보호 규칙	○	○	○
o 개인정보 침해유형·대응 및 피해구제	○	○	○
o 개인정보 보안관리 방안	○	○	○
o 업무 수행 시 의무사항 및 벌칙	○	○	○
o 개인정보 보호책임자 역할	○		
o 개인정보 담당자 역할		○	
o 개인정보 취급자 역할			○
o 개인정보취급자에 대한 의무사항			○
o 목적 외 이용·제공 절차 및 대장 관리	○	○	○
o 기술적·관리적·물리적 보호조치 사항	○	○	○

□ 교육 내용

교육대상	중점 교육내용	추진일정	방법
책임자	· 개인정보보호 업무 총괄·조정자로서 관리 역량 제고	연1회 (0월)	· 외부참여 ※ CPO 워크숍 등
담당자	· 개인정보보호 총괄 실무자로서 개인정보 보호 전문성 강화	연1회 (0월)	· 외부참여 또는 자체교육 ※ 내·외부 강사 및 온라인 교육 등
취급자 (일반직원)	· 개인정보 수집·이용에서 파기까지 단계별 조치사항 교육 · 개인정보보호 규정, 개인정보보호법에 의한 요구사항	연1회 (0월)	· 외부참여 또는 자체교육 ※ 내외부 강사 및 온라인 교육 등
영상정보처리기기 운영자	· 영상정보처리기기 설치·운영을 위한 법제도적 요구사항	연1회 (0월)	
수탁사 (용역사업)	· 개인정보의 기술적·관리적 보호조치, 고의적인 개인정보 유출 및 사고 방지 등	연1회 (0월)	

※ 내부사정 또는 내부교육 추진 일정에 따라 변경 될 수 있음

□ 향후 계획

o 개인정보보호 교육계획에 따라 교육 실시(연중)

교육대상	주요 교육 내용	1/4			2/4			3/4			4/4		
		1	2	3	4	5	6	7	8	9	10	11	12
책임자 (CPO)	· 개인정보보호 업무 총괄·조정자로서 관리 역량 제고						O O						
담당자	· 개인정보보호 총괄 실무자로서 개인정보보호 전문성 강화				O O								
취급자 (일반직원)	· 개인정보 수집·이용에서 파기까지 단계별 조치사항 교육										O O		
영상정보처리기기 운영자	· 영상정보처리기기 설치·운영을 위한 법제도적 요구사항				O O								
수탁사 (용역사업)	· 개인정보의 기술적·관리적 보호조치, 고의적인 개인정보 유출 및 사고 방지 등			O O									

※ 교육 추진 일정은 변경 될 수 있음

☞ 교육 자료는 전라북도교육청 누리집 미래인재과 > 업무마당 > 정보보호 (https://www.jbe.go.kr/boho) > 개인정보보호 > 자료실 참고

0000년 개인정보보호 교육 결과

□ 목적

개인정보의 안전한 관리 및 운용을 위해 개인정보보호 관련 규정 및 변경 사항, 안전조치 요령, 침해 사고 시 대응방안 등 체계적인 교육 실시

□ 교육 내용

- 개인정보보호 관련 법·제도 현황
- 개인정보보호 규칙
- 개인정보 침해 유형·대응 및 피해구제 사례 소개
- 개인정보 보안관리 방안
- 업무수행 시 의무사항 및 벌칙
- 개인정보 보호책임자 역할
- 개인정보 담당자 역할
- 개인정보 취급자 역할
- 목적 외 이용·제공 절차 및 관리대장 운영에 관한 사항
- 개인정보의 기술적·관리적·물리적 보호조치에 관한 사항 등

□ 교육 결과

교육일자	대상	대상인원	참석 인원	비율	비고
0000. 0. 0.	*책임자*	*1*	*1*	*100%*	*이수증*
0000. 0. 0.	*담당자*	*1*	*1*	*100%*	
0000. 0. 0.	*취급자*	*50*	*50*	*100%*	*등록부*

□ 교육 등록부

o 교육명 : 개인정보보호 교육

o 일 시 : OOOO. O. O. OO:OO~OO:OO

o 장 소 : OOOO

o 강 사 :

구분	소속	이름	서명
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			

[별첨4] 수탁사 대상 개인정보보호 교육·관리감독 계획 및 결과(참고용)

「OOO」 용역 수탁자 대상 개인정보보호 교육 및 관리·감독 계획

□ 개 요

개인정보의 안전한 관리 및 운용을 위해 수탁사의 개인정보취급 인력에 대한 **개인정보보호 교육 및 관리·감독 실시**

□ 위탁 현황

○ 수탁기관 :
○ 계약기간 :
○ 위탁내용 :

□ 교육 계획

○ 교육시기 : 연 1회 이상
○ 교육대상 : 개인정보를 취급하는 인력
○ 교육방법 : 온라인 교육 또는 집합 교육
○ 교육내용
- 개인정보보호 관련 법·제도 현황
- 개인정보 침해 유형 및 피해구제 사례 소개
- 개인정보 보안관리 방안
- 업무수행 시 의무사항 및 벌칙
- 위탁업무 수행 목적 외 개인정보의 처리금지에 관한 사항
- 개인정보의 기술적·관리적·물리적 보호조치에 관한 사항 등

□ 관리 · 감독 계획

○ 수탁사 자체점검 : 월 1회 실시
○ 위탁사 방문점검 : 연 1회 이상
○ 점검내용 : 수탁업체 보안 점검표에 따라 점검

※ 점검시는 '수탁업체 개인정보 관리 실태 점검표(붙임2)' 활용

「OOO」 용역 수탁자 대상 개인정보보호 교육 및 관리·감독 결과

□ OOO 용역 현황

❍ 위탁내용 :
❍ 수탁기관 :
❍ 계약기간 :

□ 개인정보 관련 수탁자 교육 실시

❍ 일 시 :
❍ 장 소 :
❍ 교육 결과

대상	대상인원	참석 인원	비율	비고
(주)00회사	*5*	*5*	*100%*	*참석 결과표*

❍ 교육내용
- 개인정보보호 관련 법·제도 현황
- 개인정보 침해 유형 및 피해구제 사례 소개
- 개인정보 보안관리 방안
- 업무수행 시 의무사항 및 벌칙
- 위탁업무 수행 목적 외 개인정보의 처리금지에 관한 사항
- 개인정보의 기술적·관리적·물리적 보호조치에 관한 사항 등

❍ 교육사진

<교육사진>

□ 개인정보 관리 실태 점검 실시

❍ 점검일시 :
❍ 점검내용 : 수탁업체 개인정보 관리 실태 점검표에 따라 점검
❍ 점 검 자 :

※ [붙임1~4] 자료 참고

[붙임1] 교육 참석 결과표

개인정보보호 교육 참석 결과표

☐ 회의명 : 개인정보보호 교육

☐ 일　시 : OOOO. O. O. OO:OO~OO:OO

☐ 장　소 : OOOO

구분	소속	이름	서명
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			

[붙임2] 수탁업체 관리 실태 점검표

수탁업체 개인정보 관리 실태 점검표

기관명		점검기간	
개인정보파일명		점검일	
사업명		점검자	(인)
용역책임자(사업자)			

연번	점검항목	결과	비고
1	개인정보 보호책임자는 지정되어 있는가?		
2	개인정보 보호 교육계획을 수립하여 시행하고 있는가?		
3	재 위탁을 하거나 위탁 목적 외로 개인정보를 활용하지는 않는가?		
4	개인정보가 관리되는 PC, 시스템에 비인가 프로그램(P2P, 웹하드 등의) 접속을 차단하는가?		
5	개인정보에 접근할 수 있는 접근자를 제한하고, 개인정보 취급에 따른 이력관리를 수행하는가?		
6	고유식별정보에 대하여 암호화 조치를 수행하는가?		
7	개인정보파일 및 해당 개인 정보에 접근하는 PC 및 시스템에 비밀번호를 설정하여 관리하는가?		
8	개인정보 취급 과정에서 발생한 출력물 및 임시파일을 즉시 삭제하는가?		

※ 결과: O, X, 해당없음으로 표시

※ 위탁 업무의 특성을 반영하여 점검항목을 추가 및 수정하여 사용

[붙임3] 보안서약서(업체용)

개인정보 보안서약서

본인은 20○○년 ○○월 ○○일부로 전라북도교육청장수도서관 개인정보 취급위탁 업무수행에 따른 개인정보 및 개인정보처리시스템의 안전한 보호를 위해 아래 각 호의 사항을 준수한다.

1. 정보보호 규정 및 개인정보보호 관련 법규의 준수
2. 업무상 알게 된 개인정보에 관한 비밀 유지
3. 제공받은 목적 외 이용 및 제공 금지
4. 제공받거나 허가받은 개인정보 취급업무 및 취급권한의 제3자 공유 금지
5. 개인정보의 처리 목적 달성 후 파기
6. 관련 법규의 미 준수 또는 관리소홀로 인해 발생한 개인정보 사고에 대한 책임 부담
7. 업무 수행하는 직원에 대한 책임
8. 사전 승인을 받지 못한 프로그램 및 정보기기 사용 불가

위 서약내용을 위반한 행위로 인한 손해 시 고의 또는 과실이 없음을 입증하지 아니하면 민·형사상의 책임을 면할 수 없음을 확인합니다.

※ 관련 규정
가. 개인정보보호법 28조
나. 표준개인정보보호지침 17조

년 월 일

서약자 소속
직위(급)
성명 (인)

전라북도교육청장수도서관장 귀하

[붙임4] 파기확인서(업체용_사업종료시)

개인정보 파기확인서

본인은 20○○년 ○○월 ○○일부로 전라북도교육청장수도서관 개인정보 취급위탁 업무수행이 종료됨에 따라 제공받은 모든 개인정보를 파기하였음을 확인합니다.

위 정보를 파기하지 않아 발생되는 손해에 대해서 고의 또는 과실이 없음을 입증하지 아니하면 관계법규에 의거 민·형사상의 책임을 면할 수 없음을 확인합니다.

※ 관련 규정
가. 개인정보보호법 제26조
나. 개인정보보호법 시행령 제28조
다. 표준개인정보보호지침 제10조

년 월 일

확인자 소속
직위(급)
성명 (인)

전라북도교육청장수도서관장 귀하

[별첨5] 표준 개인정보처리위탁 계약서

표준 개인정보처리위탁 계약서

전라북도교육청장수도서관(이하 “위탁자”이라 한다)과 △△△(이하 “수탁자”이라 한다)는 “위탁자”의 개인정보 처리업무를 “수탁자”에게 위탁함에 있어 다음과 같은 내용으로 본 업무위탁계약을 체결한다.

제1조 (목적) 이 계약은 “위탁자”가 개인정보처리업무를 “수탁자”에게 위탁하고, “수탁자”는 이를 승낙하여 “수탁자”의 책임아래 성실하게 업무를 완성하도록 하는데 필요한 사항을 정함을 목적으로 한다.

제2조 (용어의 정의) 본 계약에서 별도로 정의되지 아니한 용어는「개인정보 보호법」, 같은 법 시행령,「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시 제2021-2호) 및「표준 개인정보 보호지침」(개인정보보호위원회 고시 제2020-1호)에서 정의된 바에 따른다.

제3조 (위탁업무의 목적 및 범위) “수탁자”는 계약이 정하는 바에 따라 (_____) 목적으로 다음과 같은 개인정보 처리 업무를 수행한다.[1)]

1.
2.
3.

제4조 (위탁업무 기간) 이 계약서에 의한 개인정보 처리업무의 기간은 다음과 같다.

계약 기간 : 년 월 일 ~ 년 월 일

제5조 (재위탁 제한) ① “수탁자”는 “위탁자”의 사전 승낙을 얻은 경우를 제외하고 “위탁자”와의 계약상의 권리와 의무의 전부 또는 일부를 제3자에게 양도하거나 재위탁할 수 없다.

② “수탁자”가 다른 제3의 회사와 수탁계약을 할 경우에는 “수탁자”는 해당 사실을 계약 체결 7일 이전에 “위탁자”에게 통보하고 협의하여야 한다.

제6조 (개인정보의 안전성 확보조치) “수탁자”는「개인정보 보호법」제23조제2항 및 제24조제3항 및 제29조, 같은 법 시행령 제21조 및 제30조, 「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시 제2021-2호)에 따라 개인정보의 안전성 확보에 필요한 관리적·기술적 조치를 취하여야 한다.

1) 각호의 업무 예시 : 고객만족도 조사 업무, 회원가입 및 운영 업무, 사은품 배송을 위한 이름, 주소, 연락처 처리 등

제7조 (개인정보의 처리제한) ① “수탁자”는 계약기간은 물론 계약 종료 후에도 위탁업무 수행 목적 범위를 넘어 개인정보를 이용하거나 이를 제3자에게 제공 또는 누설하여서는 안 된다.

② “수탁자”는 계약이 해지되거나 또는 계약기간이 만료된 경우 위탁업무와 관련하여 보유하고 있는 개인정보를 「개인정보 보호법」시행령 제16조 및「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시 제2021-2호)에 따라 즉시 파기하거나 “위탁자”에게 반납하여야 한다.

③ 제2항에 따라 “수탁자”가 개인정보를 파기한 경우 지체없이 “위탁자”에게 그 결과를 통보하여야 한다.

제8조 (수탁자에 대한 관리·감독 등) ① “위탁자”는 “수탁자”에 대하여 다음 각 호의 사항을 감독할 수 있으며, “수탁자”는 특별한 사유가 없는 한 이에 응하여야 한다.

1. 개인정보의 처리 현황
2. 개인정보의 접근 또는 접속현황
3. 개인정보 접근 또는 접속 대상자
4. 목적외 이용·제공 및 재위탁 금지 준수여부
5. 암호화 등 안전성 확보조치 이행여부
6. 그 밖에 개인정보의 보호를 위하여 필요한 사항

② “위탁자”는 “수탁자”에 대하여 제1항 각 호의 사항에 대한 실태를 점검하여 시정을 요구할 수 있으며, “수탁자”는 특별한 사유가 없는 한 이행하여야 한다.

③ “위탁자”는 처리위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 1년에 1회 이상 “수탁자”를 교육할 수 있으며, “수탁자”는 이에 응하여야 한다.[2)]

④ 제1항에 따른 교육의 시기와 방법 등에 대해서는 “위탁자”는 “수탁자”와 협의하여 시행한다.

제9조 (정보주체 권리보장) ① “수탁자”는 정보주체의 개인정보 열람, 정정·삭제, 처리 정지 요청 등에 대응하기 위한 연락처 등 민원 창구를 마련해야 한다.

제10조 (개인정보의 파기) ① “수탁자”는 제4조의 위탁업무기간이 종료되면 특별한 사유가 없는 한 지체 없이 개인정보를 파기하고 이를 “위탁자”에게 확인받아야 한다.

제11조 (손해배상) ① “수탁자” 또는 “수탁자”의 임직원 기타 “수탁자”의 수탁자가 이 계약에 의하여 위탁 또는 재위탁 받은 업무를 수행함에 있어 이 계약에 따른 의무를 위반하거나 “수탁자” 또는 “수탁자”의 임직원 기타 “수탁자”의 수탁자의 귀책사유로 인하여 이 계약이 해지되어 “위탁자” 또는 개인정보주체 기타 제3자에게 손해가 발생

2)「개인정보 안전성 확보조치 기준 고시」(개인정보보호위원회 고시 제2021-2호) 및「개인정보 보호법」제26조에 따라 개인정보처리자 및 취급자는 개인정보보호에 관한 교육을 의무적으로 시행하여야 한다.

한 경우 “수탁자”는 그 손해를 배상하여야 한다.

② 제1항과 관련하여 개인정보주체 기타 제3자에게 발생한 손해에 대하여 “위탁자”가 전부 또는 일부를 배상한 때에는 “위탁자”는 이를 “수탁자”에게 구상할 수 있다.

본 계약의 내용을 증명하기 위하여 계약서 2부를 작성하고, “위탁자”와 “수탁자”가 서명 또는 날인한 후 각 1부씩 보관한다.

20 . . .

위탁자	수탁자
주 소 : 전북 장수군 장수읍 호비로 58	주 소 :
기관(회사)명 : 전라북도교육청장수도서관	기관(회사)명 :
대표자 성명 : (인)	대표자 성명 : (인)