개인정보 내부 관리계획

2023. 3.

설천중 · 고등학교
교육정보부

[제 · 개정이력]

순번	구분	시행일자	제정·개정 주요내용	작성자	관련대호
1	제정	2018. 9. 20.	**개인정보보호 내부 관리계획 제정**	김00	설천고등학교 -6874(2018.9.20.)
2	개정 (1차)	2019. 11. 5.	**1. 개인정보의 안전성 확보 조치 기준 개정 사항 반영** (행정안전부 고시 2019-47호, 2019.6.7.) - 접속 기록 항목 추가(처리한 정보 주체 정보) - 접속기록 보관 기간 차등적 연장 (6개월 이상→ 최소 1년 이상) - 접속기록 점검에 관한 사항 개선 · 접속기록 점검 주기 단축 (반기별 1회 이상→월 1회 이상) · 개인정보를 다운로드 한 경우 그 사유 반드시 확인 (신설) **2. 내부관리계획의 수립 및 이행실태 점검에 관한 사항 추가** **3. 접근권한 관리 개인정보 취급자 비밀번호 변경 주기 축소** **(반기별 1회→분기별 1회)** **4. 개인정보 침해사고 시 행안부 신고 인원 변경** **(1만명→1천명)**	한00	설천고등학교 -8111(2019.11.5.)
3	개정 (2차)	2020. 3. 9.	**오·탈자 수정**	오00	설천고등학교 -1475(2020.3.9.)
4	개정 (3차)	2021. 4. 1.	**1. 개인정보보호법 개정안(2020.8.5.시행) 반영** - 제2조 "가명정보" 정의 추가, "접속기록" 정의 수정 - 제28조제1항제4호 삭제 **2. 제5조 내부관리계획 변경시 공지 추가** **3. 제8조 개인정보 취급자의 역할 명시** **4. 제11조 비밀번호 노출 시 즉시 변경 추가** **5. 제17조 개인정보 보호조직 구성 및 운영 변경**	백00	설천중학교 -1746 (2021.0.0.)
5	개정 (4차)	2022. 3. 7.	1. 법적 의무사항 및 권장사항 분류 2. 제1조(목적) '제2019-47호' 내용 삭제 3. 제2조(용어 정의) 6의2, 6의3 신설 및 7 수정 4. 제5조(내부 관리계획의 공표)제2항 수정 5. 제6조(개인정보 보호책임자의 지정) 수정 6. 제8조(개인정보취급자의 역할 및 책임) 수정 7. 제11조(접근 권한의 관리)제5항제1호~제3호 수정 8. 제12조(접근통제)제8항 삭제 9. 제13조(개인정보의 암호화)제4항 수정 10. 제14조(접속기록의 보관 및 점검)제4항 삭제 11. 제17조(개인정보 보호조직 구성 및 운영)제1항 수정 12. 제18조(개인정보 유출 사고 대응)제1항~제3항 수정 13. 제19조(수탁자에 대한 관리 및 감독)제1항제8호~제9호 신설 14. 제21조(개인정보의 파기)제1항 수정 15. 제22조(개인정보의 목적 외 이용·제공)제2항 수정 16. 영상정보처리기기의 설치 및 운영·관리 규정 삭제 17. 제23조(개인영상정보처리기기의 설치·운영) 신설 18. 제24조(가명정보의 처리) 신설 19. [별지1] 개인정보 내부 관리계획 이행실태 점검표 삭제	길00	

목 차

제1장 총 칙

제1조(목적) 설천중·고등학교 개인정보 내부 관리계획은「개인정보 보호법」제29조와 같은 법 시행령 제30조 그리고 '개인정보의 안전성 확보조치 기준'(제2020-2호)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. "개인정보보호 업무 분야별책임자"(이하 "분야별책임자"라 한다)란 업무를 위하여 개인정보파일을 처리하는 부서의 장으로 개인정보 보호책임자가 지정한 자를 말한다.

6의3. "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. "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.

10. “정보통신망”이란 「전기통신기본법」제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말한다.
11. “공개된 무선망”이란 불특정 다수가 무선접속장치(AP)를 통하여 인터넷을 이용할 수 있는 망을 말한다.
12. “모바일 기기”란 무선망을 이용할 수 있는 PDA, 스마트폰, 태블릿PC 등 개인정보 처리에 이용되는 휴대용 기기를 말한다.
13. “바이오정보”란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.
14. “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.
15. “내부망”이란 물리적 망분리, 접근 통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.
16. “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.
17. “관리용 단말기”란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리시스템에 직접 접속하는 단말기를 말한다.

제3조(적용 범위) 설천중·고등학교가 개인정보를 처리하거나 설천중·고등학교의 개인정보처리 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 이행실태를 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 설천중·고등학교는 「개인정보 보호법」 제31조와 같은 법 시행령 제32조 및 교육부 개인정보보호지침(이하 "지침") 제21조에 따라 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자를 교장으로 정하며, 지침 제24조에 따라 분야별 책임자는 각 부서의 장으로 한다.

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 설천중·고등학교의 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 준수한다.

제4장 개인정보 보호 교육

제9조(개인정보 보호책임자의 교육) ① 설천중·고등학교는 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 계획을 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 설천중·고등학교는 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.

② 설천중·고등학교는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하여야 한다.

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

④ 설천중·고등학교는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자 별로 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

⑤ 설천중·고등학교는 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 지체없이 새로운 비밀번호로 변경해야 함

⑥ 설천중·고등학교는 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 설천중·고등학교는 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 설천중·고등학교는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다.

③ 설천중·고등학교는 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 한다.

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

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

⑥ 설천중·고등학교에서 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 설천중·고등학교는 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.

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

② 설천중·고등학교는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 않도록 일방향 암호화(해쉬함수)하여 저장하여야 한다.

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

④ 설천중·고등학교가 내부망에 고유식별정보를 저장하는 경우에는 암호화한다. 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 설천중·고등학교는 제1항, 제2항, 제3항, 또는 제4항에 따라 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.

⑥ 설천중·고등학교는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어(도교육청에서 구축한 PC개인정보보호시스템) 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

제14조(접속기록의 보관 및 점검) ① 설천중·고등학교는 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 개인정보시스템의 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 설천중·고등학교는 개인정보의 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월별로 1회 이상 점검하여야 한다. 특히, 개인정보를 다운로드한 것이 발견되었을 경우에는 그 사유를 반드시 확인하여야 한다.

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

제15조(악성프로그램 등 방지) ① 설천중·고등학교는 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) ① 설천중·고등학교는 개인정보 유출 등 개인정보 침해사고 방지를 위하여 관리용 단말기에 대해 다음 각 호의 안전조치를 하여야 한다.

1. 인가받지 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 설천중·고등학교는 개인정보의 안전한 처리를 위하여 다음과 같이 개인정보 보호조직을 구성하고 운영하여야 한다.

1. 개인정보 보호책임자 : 교장
2. 개인정보 보호담당자 : 개인정보보호 업무 담당자
3. 개인정보 취급부서 : 개인정보를 처리하는 각 부서

② 개인정보 취급부서에서는 개인정보 보호조직과 충분히 협의, 조정하여 개인정보를 처리하여야 한다.

③ 개인정보 보호조직은 제7조에 따른 업무를 수행하며, 그 밖에 개인정보의 안전성 확보를 위하여 필요하다고 판단되는 사항을 수행할 수 있다.

제18조(개인정보 유출 사고 대응) ① 설천중·고등학교는 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 설천중·고등학교는 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 설천중·고등학교는 제3자에게 개인정보의 처리 업무를 위탁하는 경우에는 다음 각 호의 내용이 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. 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항
8. 개인정보의 파기에 관한 사항
9. 수탁자가 준수해야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

② 설천중·고등학교는 개인정보의 처리 업무를 위탁하는 경우 인터넷 홈페이지에 위탁하는 업무의 내용과 수탁자를 지속적으로 공개하여야 한다.

③ 설천중·고등학교는 개인정보의 처리 업무를 위탁하는 경우 다음 각 호의 사항을 정하여 수탁자를 교육하고 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.

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

④ 설천중·고등학교는 제3항에 따라 수탁자를 교육하고 감독한 결과에 대한 기록을 남기고 문제점이 발견된 경우에는 필요한 보안조치를 하여야 한다.

제7장 물리적 안전조치

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

② 설천중·고등학교는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.

③ 설천중·고등학교는 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 설천중·고등학교는 개인정보를 파기할 경우, 다음 각 호 중 어느 하나의 조치를 하여야 한다.

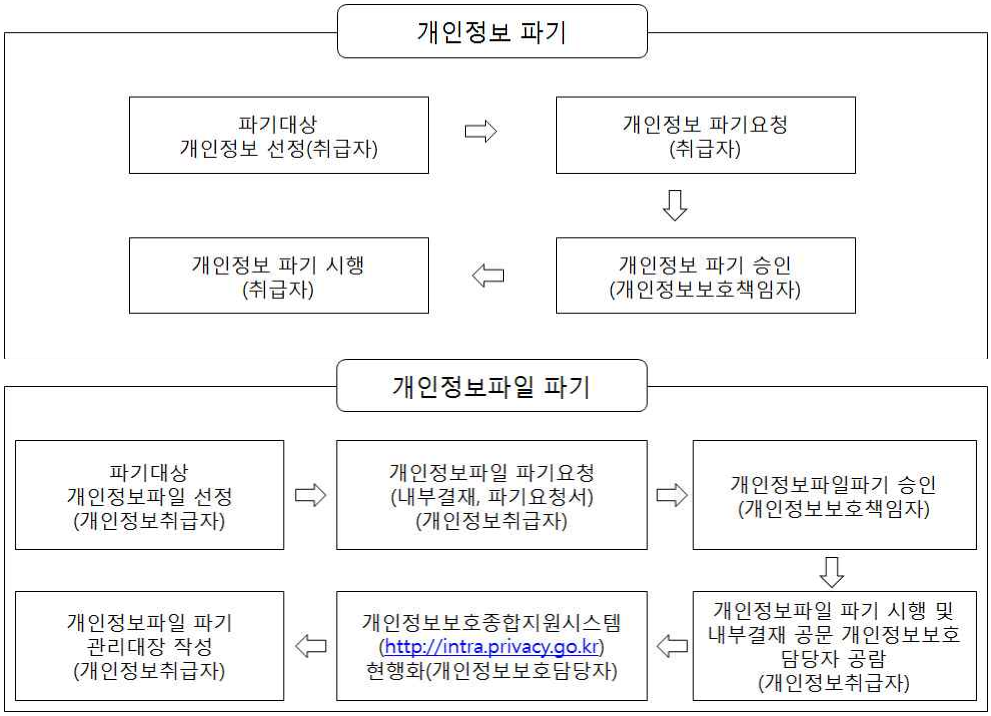
1. 완전파괴(소각·파쇄 등)
2. 전용 소자장비를 이용하여 삭제
3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

② 설천중·고등학교는 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 설천중·고등학교는 개인정보 파기에 관한 사항을 기록·관리하며, 파기의 시행 및 확인은 개인정보 보호책임자의 책임하에 수행한다.

④ 개인정보(파일) 파기 절차



제8장 그 밖에 개인정보 보호를 위하여 필요한 사항

제22조(개인정보의 목적 외 이용·제공) ① 설천중·고등학교는 원칙적으로 개인정보를 당초 수집 목적의 범위를 초과하여 이용하거나 제공하여서는 아니 된다. 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 필요한 경우
4. 개인정보를 목적 외로 이용하거나 제3자에게 제공하지 않으면 다른 법률에서 정하는 소관업무 수행 불가한 경우로 보호위원회의심의·의결을 거친 경우
5. 조약, 국제협정 이행을 위해 외국 정부 등 제공에 필요한 경우
6. 범죄수사와 공소의 제기 및 유지를 위하여 필요한 경우
7. 법원의 재판업무 수행을 위하여 필요한 경우
8. 형(刑)및 감호, 보호처분의 집행을 위하여 필요한 경우

② 설천중·고등학교는 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 설천중·고등학교는 교육부 개인정보 보호 지침에 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 설천중·고등학교는 제1항에 따른 영상정보처리기기 설치·운영에 대한 자체점검을 완료한 후에는 그 결과를 홈페이지 등에 공개하여야 한다.

제24조(가명정보의 처리) ① 설천중·고등학교는 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 설천중·고등학교는 가명처리할 경우 관련 가이드라인에서 제시하는 기준을 만족하도록 처리한다.

[별지 1]

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** 예) "개인정보보호 개인정보처리방침 변경 수립" (설천중학교-00(2022.00.00.) → 증빙할 수 있는 공문 제목 및 번호 기재 또는 증빙사진 첨부
		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 수립여부
		□ **이행실적 및 증빙자료** 예) "2020년 교직원 개인정보보호 교육 실시 계획" (설천중학교-00(2022.00.00.)
		2. 개인정보 보호 교육 실시 - 개인정보취급자를 대상으로 개인정보 보호 교육의 실시 여부
		□ **이행실적 및 증빙자료** 예) "2020년 교직원 개인정보보호 교육 실시 결과" (설천중학교-00(2022.00.00.)
접근권한 관리		• 나이스, 에듀파인, 업무관리 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** 예) "2020년 1학기 나이스 권한 부여 내역" (설천중학교-00(2022.00.00.) "2020년 9월 사이버 보안진단결과 등록" (설천중학교-00(2022.00.00.) → 매월실시
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** 예) "2020년 9월 사이버 보안진단결과 등록" (설천중학교-00(2022.00.00.)→ 매월실시
암호화		○ 업무용PC에 주민등록번호 저장 시 PC개인정보보호시스템(Privacy-i)을 통한 암호화 실시 여부
		□ **이행실적 및 증빙자료** 예) PC개인정보보호시스템 관리자 보고서 개인정보 처리 현황 캡쳐 화면 등

점검항목	점검결과 (○,×)	세부 점검 방법
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 예) “2020년 9월 사이버 보안진단결과 등록” (설천중학교-00(2022.00.00.) → 매월실시
수탁자에 대한 관리 및 감독		개인정보 처리 업무를 위탁하는 경우 준수사항 이행 여부(위탁 업무 없는 경우 “해당없음”) 1. 위탁계약서 작성 2. 위탁사항 공개 3. 수탁업체 교육 및 관리 감독 여부
		□ 이행실적 및 증빙자료 예) 개인정보처리 표준 위탁 계약서, 업체 교육 결과, 개인정보 파기 확인서, 개인정보처리 방침 위탁사항 공개화면 캡쳐 등
물리적 안전조치		1. 전산실, 평가실 등 개인정보 보관 장소의 물리적 통제 절차 수립 예) 통제구역 지정, 출입자대장 관리, 잠금장치 설정 등 2. 개인정보 포함 서류, 휴대용 저장매체의 잠금장치가 있는 안전한 장소에 보관 여부
		□ 이행실적 및 증빙자료 예) 통제 구역 및 상시 출입자 지정(설천중학교-00(2022.00.00.), 잠금장치 설정 사진 등
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 예) 개인정보 파기(설천중학교-00(2022.00.00.)
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*