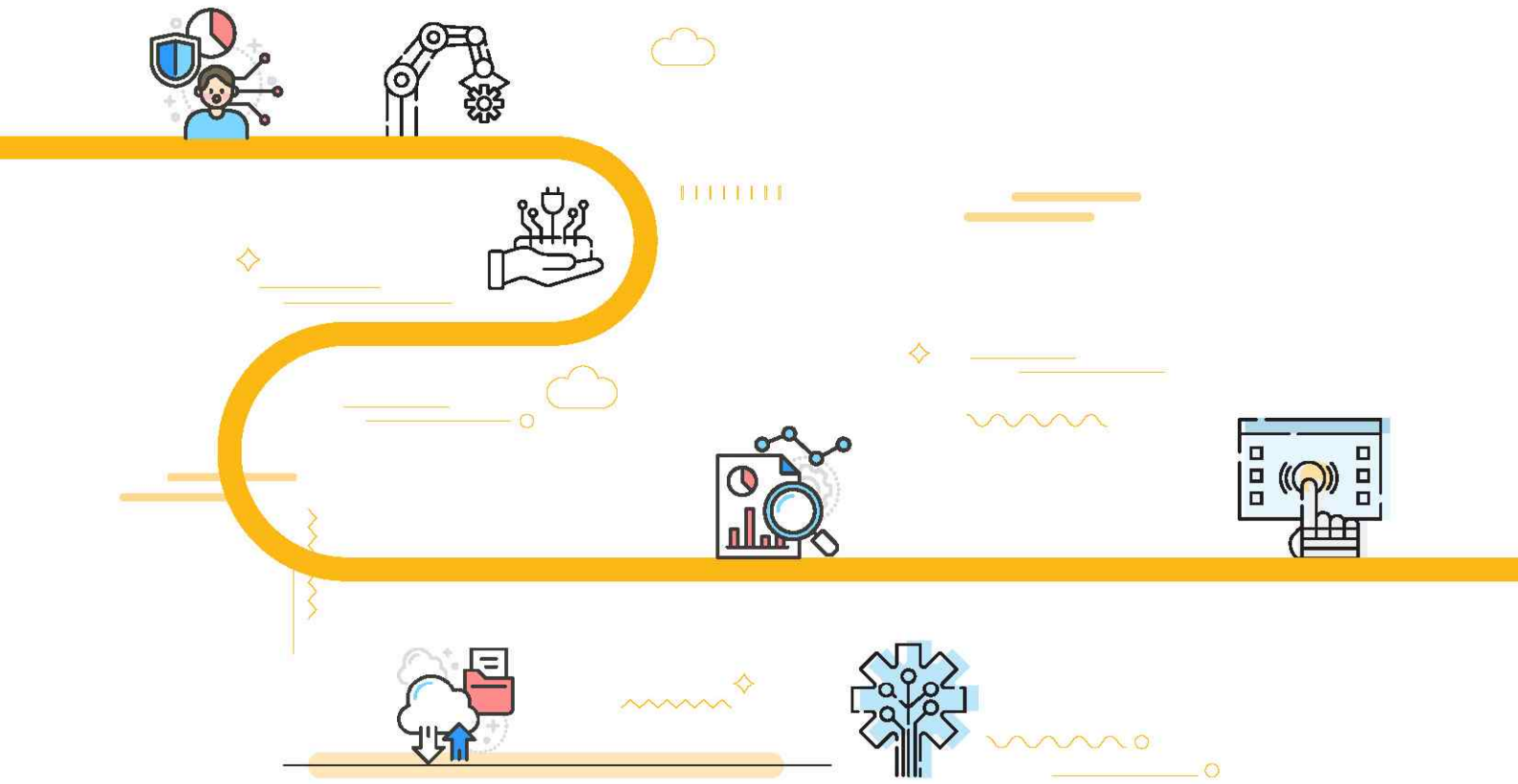
다양성이 꽃피는
공존의 혁신미래교육

청렴 서울교육

정보보안 도움자료



서울특별시교육청
SEOUL METROPOLITAN OFFICE OF EDUCATION

목 차

각급학교 정보보안 기본 이행 사항

구분	기본 이행 사항	시기	근거
기본 활동	■ 학교 정보보안담당관 및 업무담당자 지정 - 정보보안담당관: 정보보안업무를 담당하는 부장 또는 교감 중 임명 - 정보보안담당관의 주요 역할 • 정보통신실, 정보통신망 현황자료 등에 관한 보안관리 총괄 • 정보보안 교육 총괄 • '사이버보안진단의 날 운영' 등 교내 정보보안 업무 지도·감독	학년초	정보보안 기본지침 제5조
	■ 정보보안 추진 계획 수립 - 각급학교는 별도의 계획수립 없이 「서울특별시교육청 정보보안 업무 추진 계획」을 따를 수 있음. 단, 학교별 보안대책이 필요한 경우 별도 수립	학년초	정보보안 기본지침 제6조
	■ 소속 전 직원 대상 정보보호 교육 실시 - (방법) 자체 교육(개인별 온라인 교육 이수 가능) - (중점내용) • 사이버보안진달의 날(내PC지키미 점검, 개인정보파일 암호화 등) • 개인 단말기(PC, 노트북, 스마트패드 등) 보안 준수 사항 ☞ 개별사용자는 본인이 사용하는 단말기 관련 책임이 있음 • 이메일 이용 시 유의사항(발신 불명, 의심 메일 즉시 완전 삭제 등) • 개인정보 처리 유의사항 등 - 교육 결과 관련 내부결재, 교육자료, 출석부 또는 온라인이수증 등 증빙 자료는 기관 자체 보관 ■ 정보보안 담당자 교육 이수 - 교육청 주관 담당자 연수 참석 또는 온라인 교육센터 이용(연간 15시간 이상)	연1회 이상	정보보안 기본지침 제9조 개인정보 보호법 제28조
	■ 사이버보안진단의 날 운영 - (일자) 매월 세번째 수요일 - (중점내용) • 내PC지키미 실행 후 점검항목 안전조치(업무망 100점, 교육망 75점 이상) • PC 내 개인정보파일 암호화 • 홈페이지에 비공개 업무자료 및 개인정보 노출 여부 점검 • 기타 학교 자체 정보보안 활동	매월	정보보안 기본지침 제10조, 제68조 개인정보 보호법 제24조

구분	기본 이행 사항	시기	근거
정보 통신망 보안	■ 업무망(교사망), 교육망, 무선망, 기타망 분리 운영 - 각각 별도의 스위치 장비로 물리적 분리 운영 ■ 학교 네트워크 구성도 비공개 대상 정보로 지정·관리	상시	정보보안 기본지침 제40조
	■ 업무와 관련 없는 인터넷(게임·음란·도박 등) 사용 제한 - 필요 시 교육지원청으로 서비스 허용 신청서 공문으로 요청	상시	정보보안 기본지침 제47조
정보 시스템 보안	■ 정보시스템(서버, 네트워크장비, 무선장비, PC, 노트북 등) 관리 - 정보시스템 관리자 지정·운영 - 정보시스템 관리대장 작성 및 현행화	상시	정보보안 기본지침 제48조
	■ 휴대용 저장매체(전산장비 포함) 외부 반출·입 관리 - 정보시스템 외부 반출·입 시(외부 수리 포함) 대장 관리 - 외부 회의, 출장으로 반출 시 비공개 중요 자료 삭제 확인하고, 반입 시 악성코드 감염 여부 확인	상시	정보보안 기본지침 제49조, 제76조
	■ 불용 PC 하드디스크 업무자료 삭제(포맷) - 디지털·혁신미래교육과에서 추진하는 불용PC 수거로 처리 ☞ 보안각서 및 삭제결과 등을 반드시 확인 - 저장매체 물리적 파괴 또는 디가우징 자체 처리 ☞ 교육연구정보원 인프라운영과로 사전 협의 후 공문 제출	사안 발생시	정보보안 기본지침 제59조
PC 보안	■ 단말기에 대한 보안대책 준수(학교장이 별도 정할 수 있음) - CMOS·로그온·자료 암호화 비밀번호의 정기적 변경 사용 - 단말기 작업을 일정 시간 이상 중단 시 비밀번호 등을 적용한 화면보호 조치 - 최신 백신 소프트웨어 설치 - 운영체제 및 응용프로그램에 대한 최신 보안패치 유지 - 출처, 유통경로 및 제작자가 불분명한 응용프로그램의 사용 금지 - 신뢰할 수 있는 인터넷사이트 활용, 파일 다운로드 시 최신 백신 소프트웨어로 검사 후 활용 - 업무상 불필요한 프로그램 설치 금지 및 공유 폴더 삭제 - 웹브라우저를 통해 서명되지 않은 액티브-X 등이 다운로드·실행되지 않도록 보안 설정	상시	정보보안 기본지침 제71조, 제72조

구분	기본 이행 사항	시기	근거
통제 구역 관리	■ 보호지역(제한구역 및 통제구역) 지정 및 관리 - 전산실(주전산기 설치구역) 통제구역으로 지정 - CCTV 통제실 등 제한구역으로 지정 - 보호지역 표지 부착, 잠금장치 설정, 관리책임자 지정  - 통제구역 출입자 관리(「출입통제대장」 비치하여 기록유지)	상시	정보보안 기본지침 제84조 교육부 보안업무 규정 시행세칙 제60조 ~62조
정보화 용역 사업 관리	■ 정보화 용역사업(PC 유지보수 등) 보안관리 - (사업시작)참여인력용 보안서약서, (사업종료) 대표자용 확약서 징구 - 용역 참여인력 대상 정보보안 교육 실시 - 계약서(과업지시서)에 보안 관련 특약사항 포함(준수사항, 누출금지정보 목록 등) - 개인정보 처리 위탁 시 표준개인정보처리위탁 계약서 작성	상시	정보보안 기본지침 제13조, 제25조, 제26조, 제49조
디지털 복합기 관리	■ 디지털복합기(하드디스크 내장형) 보안 - 기본 비밀번호 변경 후 사용(유지보수 업체 또는 제조사 문의) - 복합기에 스캔문서가 저장되지 않도록 설정 - 복합기 폐기·양여 또는 외부 반출 시 저장 자료 완전 삭제	상시	정보보안 기본지침 제88조
권한 관리	■ 정보시스템(나이스, K-에듀파인, 홈페이지 등) 권한관리 철저 - 관리자가 인사이동, 보직변경, 퇴직 등 변동사항 발생 시 신속히 권한 회수(정보시스템별 권한관리 지침 참고) - 정보시스템 접근권한 적절성 점검(연2회 이상)	상시	정보보안 기본지침 제73조
기타	■ 기본 이행 사항에 명시하지 않은 사항은 서울특별시교육청 정보보안 기본지침(2022.5.개정) 준용	상시	

정보보안 업무
세부 내용

1 정보보안담당관 지정

관련 근거

▸ 서울특별시교육청 정보보안 기본지침(2022.5.) 제5조(정보보안담당관 운영)

업무시기

▸ 정보보안담당관 변경시(인사이동)

주요내용

❑ **정보보안담당관 지정**

- 정보보안담당관 임명: 학교장이 정보보안 업무를 담당하는 부장 또는 교감 중에서 임명

※ 정보보안담당관 변경 시 내부결재 득한 후 자체 보관

❑ **학교 정보보안담당관의 기본 활동**

- **정보통신실, 정보통신망 현황자료 등에 관한 보안관리 총괄**
- **정보보안교육 총괄 및 '사이버보안진단의 날' 시행**
- **해당 기관의 정보보안업무 감독**
- **부서 분임정보보안담당관 업무 감독**
- **그 밖에 정보보안과 관련한 사항**

참고

▸ 정보보안담당관 임명 및 관리 체계 수립 기안문(예시)

예시 **정보보안담당관 임명 및 관리 체계 수립 기안문**

다양성이 꽃피는 공존의 혁신미래교육

○○○학교

수신자 내부결재

(경유)

제목 ○○○학교 정보보안담당관 임명 및 관리 체계 수립

1. 관련

가. 서울특별시교육청 보안업무 시행 지침

나. 서울특별시교육청 정보보안 기본지침 제5조(정보보안담당관 운영)

2. 202○학년도 ○○○학교의 정보보안담당관을 임명하고, 효율적이고 체계적으로 정보보안 업무를 추진하기 위해 다음과 같이 관리 체계를 수립하고자 합니다.

구분	소속부서	이름	주요역할
(필수) **정보보안담당관**	**교감 또는 정보부장**	○○○	**정보보안 업무 총괄**
(필수) 정보보안담당자	○○○부	○○○	정보보안 업무 실무 총괄
(선택) 부서분임 정보보안담당관	○○○부	○○○	○○부 정보보안 관리
	○○○부	○○○	○○부 정보보안 관리
	○○○부	○○○	○○부 정보보안 관리

끝.

★ 교장

협조자

시행 ○○학교-0000 (0000. 00. 00.) 접수 ( )

우 00000 서울특별시 ○○○○○○ / http://www.

전화 02-000-0000 /전송 02-000-0000 / ○○○@○○○ / 비공개(7)

2 정보보안 교육

관련 근거

▸ 서울특별시교육청 정보보안 기본지침(2022.5.) 제9조(정보보안교육)

업무시기

▸ 상시(연 1회 이상)

주요내용

❑ **정보보호 교육 계획 수립**(개인정보보호 교육 포함 수립 가능)

❑ **정보보호(정보보안 및 개인정보보호) 교육 이행**

- 개인정보 보호책임자(교장): 개인정보보호위원회, 교육부, 교육청 교육 참석 또는 서울특별시교육청교육연수원 온라인 이수
- **정보보안담당자: 연간 15시간 이상 이수**
- **전 직원**: 연 1회 이상(온라인 교육 포함)
- **수탁자**: 정보화사업 용역 위탁 계약 시 참여인력 대상 교육
- **교육 결과 입증 자료 자체 보관(수료증, 출석부, 교육사진, 교육자료 등)**

☞ 교육 실시 후 입증자료를 포함하여 내부결재

※ 정보보호 온라인 교육 관련 사이트

① 서울시교육청교육연수원 https://www.seti.go.kr
② 교육부 정보보호교육센터 https://sec.keris.or.kr
③ 개인정보 포털(수탁자교육용): https://www.privacy.go.kr

참고

▸ 정보보호(정보보안 및 개인정보보호) 교육 계획 기안문(예시)
▸ 정보보호(정보보안 및 개인정보보호) 교육자료(예시)
▸ 정보보호(정보보안 및 개인정보보호) 교육 결과 보고 기안문(예시)

예시

정보보호(정보보안 및 개인정보 보호) 교육 계획 기안문

다양성이 꽃피는 공존의 혁신미래교육

○○○학교

수신자 내부결재
(경유)
제목 202○년도 정보보호(정보보안 및 개인정보보호) 교육 계획(안)

1. 관련
   가. 서울특별시교육청 정보보안 기본지침 제9조(정보보안교육)
   나. 교육부 개인정보 보호지침 제32조(개인정보보호교육)

2. 정보보호 침해 사고 예방과 경각심 제고를 위해 (법정의무)정보보안 및 개인정보보호 교육 계획을 다음과 같이 수립·추진하고자 합니다.

대상	교육내용	교육시기	방법	기준
개인정보보호책임자 (교장)	책임자의 역할과 인식 제고	상반기	온라인교육개별이수 또는 교육청 교육 참석	연1회 이상
정보보안담당자	정보보안담당자 역할 및 주요 업무 내용 등	상반기	교육청 교육 참석	연15시간 이상
개인정보보호담당자	개인정보보호 담당자 역할 및 주요 업무 내용 등			
전 직원 (개인정보 취급자) * 기간제, 강사 포함	•정보보안 수칙(단말기 보안, 사이버보안진단의 날 등) •업무처리 단계별 개인정보 처리 •개인정보 유·노출시 처리 절차 및 예방 교육 등	2020.0.00.	자체교육 또는 온라인교육개별이수	연1회 이상
정보화사업 용역업체 (개인정보 수탁기관)	•수탁자 안전조치의무 준수 •누출금지정보 및 유출금지 •작업장소 보안 준수사항 •개인정보 안전조치의무 준수 등	사업착수 시	자체교육	참여인력별

끝.

★ 교장

협조자

시행 ○○학교-0000 (0000. 00. 00.) 접수 ( )

우 00000 서울특별시 ○○○○○○ / http://www.

전화 02-000-0000 /전송 02-000-0000 / ○○○@○○○ / 비공개(7)

교내 전직원 정보보안 및 개인정보보호 교육 자료

○○○부(20○○.○○.○○.)

[정보보안 교육]

1. 사이버보안진단의 날(매월 세 번째 수요일)

○ 내PC지키미, PC개인정보관리프로그램 실행하여 점검 후 취약점 모두 조치

점검 대상	프로그램	조치 기준	참고
① 내PC지키미	(AhnLab ESA)	10개 항목 (엄무망:100점, 학생망:75점)	부서 공용PC 포함
② 개인정보파일 (주민등록번호)관리	(AhnLab Privacy Management 5.0)	법적근거 없는 고유식별정보 삭제, 주민등록번호 100% 암호화 조치	법적근거 없거나, 보유기간 경과한 파일 즉시 삭제

※ 고유식별정보: 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호
⇒ 법적 근거 없는 고유식별정보 즉시 삭제
⇒ 고유식별정보는 상시 암호화 저장하여 보관

○ 홈페이지(학교 자체 운영 웹사이트 포함) 게시 자료 점검

- 메뉴(게시판)별 담당자는 비공개 업무자료 및 개인정보가 노출되어 있는지 점검
- 게시판에서 공개기한이 지났거나 불필요한 게시글 정비

2. PC 보안 관리

(정보보안 기본지침 제72조)
개별사용자는 기관에서 지급받은 단말기(PC, 노트북, 스마트패드 등) 사용과 관련한 일체의 보안관리 책임이 있으며, 다음 보안사항을 준수해야 합니다.

○ 비밀번호 설정

① 부팅(CMOS) 시	② 윈도우 로그온 시	③ 화면보호기
		
단말기 메인보드 바이오스에서 설정	윈도우 시작 시 로그온 화면	10분 이상 미사용시 화면보호 설정

④ 중요자료, 개인정보파일 등	처리방법
주민등록번호 포함된 개인정보파일	법령근거 없다면 ☞ 즉시 삭제 있다면 ☞ 개인정보관리프로그램 암호화( ) 또는 개별 프로그램 파일 암호화
개인정보 포함 파일, 중요자료 파일 등	개별 프로그램 파일 암호화 ☞ 한글-저장하기-문서암호 설정 ☞ 엑셀-저장하기-도구:일반옵션-암호 설정 ※ 프로그램 버전에 따라 설정방법은 다를 수 있음

- 비밀번호는 **문자, 숫자, 특수문자 등을 조합하여 복잡하게 설정하고, 주기적으로 변경**

○ **'컴퓨터이름'을 실사용자 이름으로 변경**
- 보안사고 발생 시 신속하게 피해자를 식별하여 사고대응을 하기 위해 PC사용자 이름 상시 현행화

○ 매월 **'내PC지키미' 프로그램을 활용해서 최소한의 PC 보안진단 및 조치** 실시
- 운영체제 및 한글프로그램의 최신버전으로 보안 패치
- 백신 최신버전으로 업데이트 등

○ **랜섬웨어 피해 예방 수칙**(인터넷 이용 관련 보안사항)
- 출처가 **불분명한 이메일 첨부파일**이나 **웹사이트(URL) 열람 자제, 신뢰할 수 없는 사이트에서 파일 다운로드 및 실행 주의**

  ※ 유튜브 동영상 다운로드 시 랜섬웨어 발생 사고 빈번히 발생, 각별한 주의 필요
- 인터넷 파일 공유·메신저·대화방 프로그램 등 **업무상 불필요한 프로그램의 설치 금지 및 공유 폴더 삭제**
- 인터넷에서 **자료 다운로드 시 컴퓨터 바이러스 감염여부를 최신 백신 프로그램으로 확인 점검 후 활용**
- 웹브라우저를 통해 **서명되지 않은 액티브-X 등이 다운로드·실행되지 않도록 보안 설정**
- 개인별 **중요 업무자료는 정기적으로 오프라인 백업**

※ 랜섬웨어란?
시스템을 잠그거나 데이터를 암호화하여 사용할 수 없도록 한 뒤, 이를 인질로 삼아 금전을 요구하는 악성 프로그램

※ 랜섬웨어 사고발생 시 조치(사고 발견시 즉시 수행)
감염 장비 랜선 분리, 포맷금지 ⇒ 학교 정보보안담당관에 신고 ⇒ 상위기관에 즉시 침해사고 신고
(랜섬웨어 공격자와 기관 · 직원의 개별적인 금전거래 금지)

○ 외부 수리, 회의, 출장 등으로 전산장비(노트북, 태블릿PC 등) 반·출입 시 비공개 자료 유출 주의
- 반출 시 **비공개 중요자료 삭제 여부 확인**하며, 반입 시 **악성코드 감염 여부 확인**
- **'휴대용 저장매체(전산장비 포함) 반·출입 관리대장' 작성 관리**

  ※ PC 등 정보화기기를 폐기, 재활용, 외부수리하는 경우 내부에 저장되어 있는 개인정보가 노출되는 사례가 많으므로 반드시 삭제 조치(대규모 개인정보 유출 가능)

3. 휴대용 저장매체 보안 관리

○ 대상 매체: USB메모리, SD카드, 외장형 하드디스크 등

○ 휴대용 저장매체는 관리대장(일반용, 비밀용)에 등록하여 관리
- 일반용
  - 업무관련 일반자료
  - 휴대용 저장매체 관리대장(일반용) 작성
  - 보관 장소: **개인서랍, 캐비닛 등에 안전하게 보관**

- 비밀용
  - 비밀등급별 각각 휴대용 저장매체를 마련하고 하나의 휴대용 저장매체에는 동일등급의 자료만 보관
  - 휴대용 저장매체 관리대장(비밀용) 작성
  - 보관 장소: **이중 캐비닛 또는 금고**

- 휴대용 저장매체(전산장비 포함) **반·출입 시 '반·출입 관리대장' 작성 관리**
  - 반출 시 비공개 중요자료 삭제 여부 확인하며, 반입 시 악성코드 감염 여부 확인

- 휴대용 저장매체 불용처리 확인서
  - 휴대용 저장매체를 불용 처리하거나 재사용할 경우 '불용처리 확인서'를 작성하여 정보보안담당관의 확인을 받아야 함

4. 디지털복합기 보안관리

- 복합기에 **작업문서(복사, 스캔자료 등)가 저장되지 않도록 설정**하고 **저장 여부 점검**
- 최신 펌웨어로 업데이트하고, 복합기 관리자 패스워드 주기적으로 변경

5. 홈페이지 등 게시자료 보안

- 부서에서 홈페이지 등에 업무자료를 게시하고자 할 경우 자료 내용을 **사전 검토하여 비공개 업무자료가 게시되지 않도록 주의**
- 비공개 업무자료가 무단 게시되었는지 정기적으로 점검하고 발견 즉시 삭제조치

6. 학교 자체 운영 SNS(유튜브, 인스타그램, 카카오스토리 등) 보안 관리

- 계정관리
  - **공유 사용 금지**하며, **미사용 계정은 즉시 삭제**
  - 비밀번호는 숫자·문자·특수 등 혼합하여 **복잡하게 설정**하고, **주기적으로 변경**

- 보안기능 설정 및 점검
  - OTP 또는 생체인증 등 **2단계 인증 설정**
  - 접속 단말기 설정 및 해외 로그인 차단 등 **추가 보안기능 설정**
  - 관리단말기는 OS·백신 최신 업데이트 적용 여부 점검 등

7. 재택근무 시 개인 PC를 업무에 사용하는 경우 보안 관리

- 운영체제 및 응용프로그램의 최신 보안 업데이트 실시
- 백신 보안패치 최신 업데이트 및 주기적 바이러스 검사
- 가정의 인터넷 공유기를 최신SW로 업데이트하고 공유기 비밀번호 설정
- 개인영업장(카페, 식당 등)에 설치된 **사설 와이파이, 공용PC를 이용한 재택근무 자제**

[개인정보 보호 교육]

1. 〈전 직원이 꼭 숙지해야 할〉 우리 학교 개인정보 내부 관리 계획

❍ 문서번호: *OOO학교-OOO(2023.00.00.)* ☞ 전직원 공람처리 완료

〈개인정보 내부 관리계획 주요 내용〉

- 개인정보 보호 조직에 관한 구성 및 운영
- 개인정보의 기술적·물리적 안전조치
- 개인정보 보호 교육
- 개인정보 처리의 위탁 및 수탁자 관리·감독
- 개인정보의 목적 외 이용 및 제3자 제공
- 개인정보 파기계획 및 절차
- 개인정보 유출 등 신고체계

2. 개인정보 침해 사례 및 유의사항

[유의사항①] 필요 최소한의 개인정보 처리

침해 사례	❍ 사생활 침해 우려가 있는 개인정보*를 정보주체의 동의 없이 수집 (* 학부모의 직업, 학력, 주거형태 등) ❍ 법령의 근거 없는 업무 처리(홍보영상 촬영, 졸업앨범, 우유급식, 스쿨뱅킹 등) 시 정보주체(학생, 학부모, 교직원) 동의 없이 수집 · 이용
유의 사항	❍ 정보주체의 **사생활 침해를 최소화하는 방법**으로 개인정보를 처리 ☞ 개인정보보호 원칙 준수 ❍ 필요 최소 정보 외의 개인정보 수집에 동의하지 않는다는 이유로 부당한 불이익 금지 ❍ 법령의 근거 없는 정보주체(학생, 학부모, 교직원) 개인정보 수집·이용 시 반드시 동의 ❍ 학년초 일괄로 동의서를 받을 시 업무목적 별로 동의사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고 각각 동의를 받아야 함 ❍ (만14세 미만 아동의 개인정보 처리) **법정대리인의 동의 필수**

[유의사항②] 고유식별정보, 민감정보 처리 제한

침해 사례	❍ 법률 근거 없이 주민등록번호가 포함된 자료를 요구 ☞ 주민등록번호 수집 법정주의 위반
유의 사항	❍ 고유식별정보*, 민감정보**는 **원칙적으로 처리 금지** ❍ 처리 시 반드시 법적근거 또는 별도 동의 필수이며, **저장 시 암호화 조치** * 고유식별정보 : 주민등록번호, 운전면허번호, 여권번호, 외국인등록번호 ** 민감정보 : 사상, 신념, 노동조합·정당의 가입 및 탈퇴, 정치적 견해, 건강, 성생활, 유전정보, 범죄경력, 인종, 개인을 알아볼 목적으로 생성한 생체정보 등 ❍ **주민등록번호는 처리 시 법적근거 필수, 저장 시 암호화 필수**

〔유의사항③〕 제3자 제공 및 목적 외 이용 · 제공

침해 사례	❍ 학사업무를 위해 수집한 학생의 개인정보를 별도의 동의절차 없이 홍보·마케팅 용도로 목적 외 이용 ❍ 학사업무를 위해 수집한 학생의 개인정보를 별도 동의 또는 법률의 근거 없이 제3자에게 제공 ❍ 민원인이 교원의 개인 휴대폰번호를 요구하여, 해당교원의 동의 없이 휴대폰번호를 제공 ❍ 반 편성 정보를 알리는 과정에서 성적 등이 포함된 자료를 강당 벽면에 게시 ❍ 교직원 집주소, 이메일 정보가 포함된 파일을 학교 홈페이지에 탑재 ❍ 학생 신상정보를 단체SNS를 통해 타 학생, 학부모에게 공개 ❍ 여러명의 개인정보가 포함된 파일을 이메일을 통하여 다수의 사용자에게 일괄 발송 ❍ 연말정산 관련 확인 자료를 메신저를 통해 전직원에게 전달 ❍ 공문서 첨부파일에 주민등록번호, 휴직사유(질병명) 등 타인의 고유식별정보, 민감정보 및 사생활 침해 우려 개인정보가 포함된 문서를 일괄 단체발송
유의 사항	❍ **법령의 근거 없는 정보주체(학생, 학부모, 교직원) 개인정보 제공 시 반드시 동의** ❍'공공기관'의 경우 감사, 범죄 수사, 공소 제기 및 유지 등을 위하여 정보주체의 동의 없이 개인정보를 제공할 수 있으나, **종합적인 상황을 고려하여 개인정보의 이용 없이는 목적을 달성할 수 없고 개인 사생활을 침해하지 않는 등 제한적으로 개인정보를 제공**하여야 함 ❍ 홈페이지, 게시판, 단체SNS 등에 **개인정보가 게시되지 않도록 주의** ❍ 홈페이지 게시판 첨부파일 탑재 시 **엑셀문서 탑재 지양(PDF 변환 게시 권고)** * 정보가 없음을 육안으로 확인했음에도 엑셀의 다양한 기능으로 개인정보 유출위험 ❍ 공문서에 고유식별정보(주민등록번호 등), 민감정보(병력, 건강 등)는 **'비공개 6호', '직원열람 제한(영구)' 을 지정하여 업무관련자 외에는 열람제한** ❍ 사생활 침해 우려 개인정보를 다수에게 발송해야 하는 경우 **개인별로 메일 발송**

〔유의사항④〕 개인정보 안전조치 미흡

침해 사례	❍ 개인정보가 포함된 인쇄물을 이면지로 재활용 ❍ 개인정보가 포함된 파일 암호화 미조치 ❍ 책상 위, 책꽂이 등 노출된 장소에 개인정보 포함 자료를 비치하여 유출 우려
유의 사항	❍ 개인정보의 보유기간 경과, 처리목적을 달성한 경우, 별도의 보관 기간이 규정되어 있지 않다면, **지체 없이(5일 이내) 파기** * 공공기록물에 해당하는 경우 기록물 폐기절차에 따라 별도 폐기 ❍ **고유식별정보, 민감정보** 및 **중요 개인정보 파일 암호화 조치** ❍ 개인정보는 책상 서랍 등 **안전한 장소에 보관 후 잠금장치 확인** 철저

3. 개인정보 처리 단계별 주요 내용

개인정보 개념 및 원칙

○ 개인정보의 개념

- 살아있는 개인*에 관한 정보**로서 특정 개인을 알아볼 수 있는 정보로, 해당 정보만으로는 특정 개인을 식별할 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함

*개인: 생존하는 사람에 해당(법인이나 단체는 포함되지 않음)
**정보: 정보의 종류·형태를 구분하지 않음(문자, 음성, 부호, 영상 등)

- 가명처리함으로써 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보(가명정보)

○ 개인정보 보호의 원칙

- 명확한 수집 목적이 필요
- 적법하고 정당한 수집

※ 법률에 의하거나, 계약의 체결·이행, 정보주체에게 고지하여 동의를 받아 수집

- 목적에 필요한 최소한의 개인정보만 수집
- 처리 목적 내에서 적합하게 처리, 목적 외 활용 금지
- 수집한 개인정보는 정보주체의 권리침해 가능성 등을 고려하여 안전하게 보관
- 개인정보 처리사항 공개 및 열람청구권 등 정보주체의 권리보장
- 정보주체의 사생활 침해 최소화 방법으로 처리
- 가능한 경우에는 익명으로, 익명처리로 목적을 달성할 수 없는 경우에는 가명으로 처리
- 목적 달성 및 보존 기간이 사라진 개인정보는 지체 없이 파기

개인정보 수집 · 이용(법 제15조)

○ 동의가 필요한지 여부 확인

- **정보주체의 동의를 받지 않는 경우**
  - 법률에 특별한 규정이 있거나 법령상 의무 준수
  - 공공기관이 법령 등에서 정하는 소관업무 수행
  - 정보주체와의 계약 체결 및 이행
  - 급박한 생명, 신체, 재산의 이익 보호
  - 개인정보처리자의 정당한 이익 달성
- **정보주체의 동의를 받는 경우 “최소한으로 적법하게”**
  - 필수/선택 항목을 엄격하게 구분하여 수집
  - 목적에 필요한 최소한의 개인정보 수집

※ 동의 받을 때 의무 고지사항

- 수집·이용 목적
- 수집 항목
- 보유·이용 기간
- 동의 거부 권리 및 동의 거부 시 불이익 내용

☞ 수집 위반 시 5천만원 이하 과태료

○ 개인정보 동의 받는 방법(법 제22조)

- 동의서에 특히 명확히 표시해야 하는 항목(시행령 제17조)
  - 재화나 서비스의 홍보 및 판매 연락을 할 수 있다는 사실
  - 민감정보, 고유식별번호(여권번호, 운전면허번호, 외국인등록번호)
  - 개인정보의 보유 및 이용 기간
  - 개인정보 제공받는 자 및 제공받는 자의 이용 목적

※ 중요사항 표시 방법

- 글씨는 9포인트 이상으로 하되 다른 내용보다 20% 이상 크게
- 다른 색의 글씨, 굵은 글씨 또는 밑줄 등 사용하여 명확히 드러나게
- 중요한 내용이 많은 경우는 별도 요약 제시

☞ 위반 시 1천만원 이하 과태료

○ 민감정보 및 고유식별번호 처리 제한(법 제23조, 제24조)

- 원칙적으로는 처리 금지
- 처리 가능한 경우
  - 별도 동의 얻은 경우
  - 법령에서 처리를 요구하거나 허용한 경우

☞ 위반 시 5년 이하의 징역 또는 5천만원 이하의 벌금

민감정보	고유식별정보
- 사상, 신념 - 노동조합·정당의 가입 및 탈퇴, 정치적 견해 - 건강, 성생활 등의 정보, 유전정보 - 범죄경력(전과·수형기록등) - 개인의 신체적, 생리적, 행동적 특징에 관한 정보 - 인종이나 민족에 관한 정보	- 주민등록번호 *(동의 받아도 처리 불가)* - 운전면허번호 - 여권번호 - 외국인등록번호

분실 · 도난 · 유출 · 위조 · 변조 또는 훼손되지 않도록
암호화 등 안전성 확보 조치

개인정보 위탁

〈업무 위탁 예시〉
- 개인정보가 포함된 자료의 출력을 출판사·인쇄소에 맡기는 경우
- 학생증·졸업앨범 등의 외주 제작, 방과후 교육을 외부업체에 위탁
- 졸업여행, 현장학습 등 여행사를 통한 보험 가입
- 외부업체의 홈페이지 웹호스팅 등

○ 개인정보 위탁 시 단계별 수행사항

구분	수행사항
계약 전	• 위탁할 업무 범위 구분 → 수탁자 선정 → 처리범위의 명확화 • 개인정보 처리위탁 문서 작성 (표준 개인정보처리 위탁 계약서 또는 특약사항)
계약 후	• 홈페이지 개인정보처리방침에 위탁에 관한 사항 공개 (위탁업무 내용, 수탁자 정보) • 수탁자 교육: 교육 계획 → 이행* → 결과 보고 * 위탁자 및 제3자 전문가의 집합·온라인 교육, 수탁자의 자체 교육 모두 가능 • 수탁자 안전조치의무 준수 여부 등 점검 : 점검 계획 → 이행** → 결과 보고 ** 자료제출 요구, 현장방문, 원격점검 등 다양한 수단 활용 가능
계약 종료 후	• 수탁자의 개인정보 파기(반환)을 통한 개인정보 불법 처리 유통 방지 - 수탁자는 위탁자 요청 시 즉시 반환하며, 개인정보의 무결성 및 완전성 보장 - 위탁자는 수탁자의 개인정보 파기 여부 확인 후 개인정보 파기 확인서 징구

○ 위탁 계약서 필수 기재 사항

- 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
- 개인정보의 기술적·관리적 보호조치에 관한 사항
- 위탁업무의 목적 및 범위
- 재위탁제한에 관한 사항
- 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
- 위탁업무와 관련하여 보유하고 있는 개인정보의 관리·감독에 관한 사항
- 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

☞ 손해배상책임 발생 시, 수탁자는 개인정보처리자의 소속직원으로 간주

○ 개인정보 처리 위탁 VS 제3자 제공

구분	개인정보처리위탁	제3자 제공
관련조항	법 제26조	법 제17조, 제18조
이전목적	제공하는 자의 이익/목적	제공받는 자의 이익
예측 가능성	정보주체가 사전 예측 가능	정보주체가 사전 예측 곤란
이전 방법	위탁사실 공개	제공목적 등 고지 후 정보주체의 동의 획득
관리·감독의무	위탁자	제공받는 자
손해배상책임	위탁자 부담	제공받는 자 부담
예시	• 방과후 교육을 외부업체에 위탁 • 졸업앨범 제작 • 직원 교육을 위해 위탁업체에 직원 명단 제공 • 사설알림서비스	• 경찰에 수사자료 제공 • 법원의 재판업무 수행 • 감사기관 등에 감사자료로 제출 • 마케팅 회사에 제공

개인정보 파기

○ 개인정보의 파기(법 제21조)

- 보유기간 경과, 목적 달성 등 지체 없이(5일 이내) 파기. 다만, 다른 법령에 따라 보존하여야 하는 경우는 보존
- 개인정보 파기 시 복구 또는 재생되지 않도록 조치
- 다른 법령에 따라 보존하여야 하는 경우 다른 개인정보와 분리하여 저장·관리
- 개인정보처리자는 개인정보의 파기에 관한 사항을 대장에 기록 관리하고 반드시 개인정보 보호책임자는 파기 결과 확인

○ 학교에서의 개인정보 파기

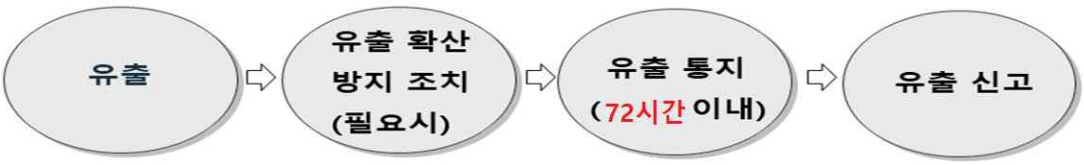
- 대상: 학기 초, 학기 중 수집한 각종 개인정보, 학생기초 자료조사서, 홈페이지 회원정보 등
- 파기절차

파기 계획 수립	⇨	파기 수행	⇨	파기 완료 보고
내부결재, 책임자 승인		담당자 파기 또는 개인정보보호 담당자 수합 또는 부서별 파기 등		내부결재, 책임자 승인

- 각급학교 표준개인정보파일 중 “홈페이지 회원정보”는 추가로 「개인정보파일 파기관리대장」에 기록(파기사유: 회원정보 부분파기)

개인정보 유출 시 대응방안 (`23.9.15.개정)

○ 유출 대응 절차



○ 유출 통지 항목

- 유출된 개인정보의 항목
- 유출된 시점과 그 경위
- 정보주체가 피해를 최소화할 수 있는 방안
- 개인정보처리자의 대응조치 및 피해 구제절차
- 피해 발생 시 신고 등을 접수할 수 있는 담당부서 및 연락처

○ 유출 신고

- 유출 신고 : 1건 이라도 유출시 유출내용 및 조치결과를 72시간 이내에 신고
  - 방법 : 상급기관에 공문 보고(개인정보 유출신고서 첨부)하고 교육부 ‘개인정보 유출 신고센터’(https://privacy.moe.go.kr)에 직접 신고
- 개인정보보호위원회 또는 인터넷진흥원(https://privacy.go.kr)에 추가 신고
  ①1천명 이상 유출 ②민감정보 또는 고유식별정보 유출 ③해킹

예시 정보보호(정보보안 및 개인정보보호) 교육 결과 보고 기안문(일괄)

다양성이 꽃피는 공존의 혁신미래교육

○○○학교

수신자 내부결재

(경유)

제목 202○년도 정보보호(정보보안 및 개인정보보호) 교육 결과 보고

1. 관련

가. 「개인정보 보호법」제28조(개인정보취급자에 대한 감독)

나. 0000년 정보보호(정보보안 및 개인정보 보호) 교육 계획(○○○학교-000, 2000.00.00.)

2. 202○년도 정보보호(정보보안 및 개인정보 보호) 교육 실시 결과를 다음과 같이 보고합니다.

구분	교육일시	대상자	참석자	결과 (이수율)	비고
개인정보 보호 책임자 (교장)	2000.00.00.	1명	1명	100%	교육연수원 CPO교육 온라인 수강
정보보안 및 개인정보보호 담당자	2000.00.00.	1명	1명	100%	교육청 담당자 교육 이수
개인정보 취급자 (전직원)	2000.00.00.	00명	00명	00%	0월 월례조회시 자체교육 실시
정보화사업 용역업체 (개인정보 수탁기관)	2000.00.00.	00명	00명	00%	수탁기관: 00업체

붙임 1. 교육참석 서명부(이수증) 1부.

2. 교육자료 1부. 끝.

★ 교장

협조자

시행 ○○학교-0000 (0000. 00. 00.) 접수 ( )

우 00000 서울특별시 ○○○○○○ / http://www.

전화 02-000-0000 /전송 02-000-0000 / ○○○@○○○ / 비공개(7)

예시 정보보호(정보보안 및 개인정보보호) 교육 결과 보고 기안문(개별)

다양성이 꽃피는 공존의 혁신미래교육

○○○학교

수신자 내부결재

(경유)

제목 202○년도 정보보호(정보보안 및 개인정보보호) 교육 결과 보고

1. 관련

가. 「개인정보 보호법」제28조(개인정보취급자에 대한 감독)

나. 0000년 정보보호(정보보안 및 개인정보 보호) 교육 계획(○○○학교-000, 2000.00.00.)

2. 202○학년도 (법정의무)정보보안 및 개인정보보호 교육 실시 결과를 다음과 같이 보고합니다.

가. 교육대상: 전 직원(개인정보 취급자)

나. 교육일시: 20○○.○.○○. 00:00 ~ 00:00

다. 교육방법: 집합교육(○○○) 또는 온라인교육 개별이수

라. 교육참석 현황(서명부 참조)

대상	참석자	참석율
○○명	○○명	○○%

붙임 1. 교육참석 서명부 또는 온라인 이수증 스캔본 1부.
2. 교육자료 1부. 끝.

★ 교장

협조자

시행 ○○학교-0000 (0000. 00. 00.) 접수 ( )

우 00000 서울특별시 ○○○○○○ / http://www.

전화 02-000-0000 /전송 02-000-0000 / ○○○@○○○ / 비공개(7)

3 사이버보안진단의 날 운영

관련 근거

▸ 서울특별시교육청 정보보안 기본지침(2022.5.) 제10조(사이버보안진단의 날)

업무시기

▸ 매월 세 번째 수요일

주요내용

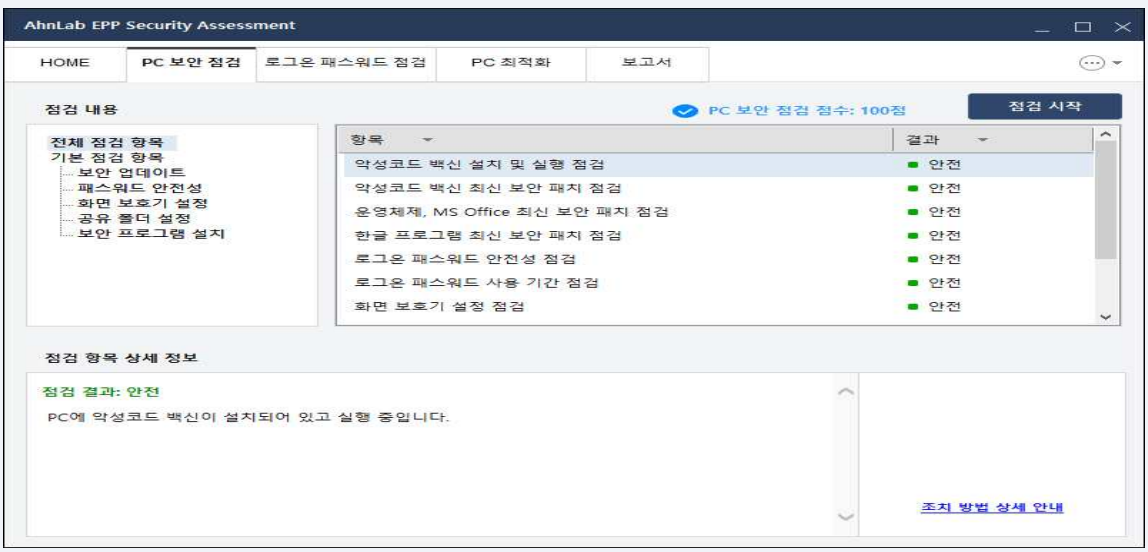
❑ **사이버보안진단의 날 지정·운영: 매월 세 번째 수요일**

❑ **내PC지키미 설치·실행**

- 교내 전체 PC 내PC지키미 Agent 설치: 업무망(자동설치), 학생망(수동설치)
- 기준: 업무망(교사망) 100점, 학생망 75점 이상

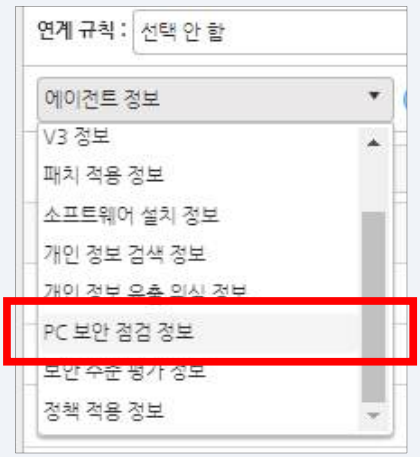
연번	점검 항목	점수	비고
1	악성코드 백신 설치 및 실행 점검	10	
2	악성코드 백신 최신 보안 패치 점검	10	
3	운영 체제, MS Office 최신 보안 패치 점검	20	
4	한글 프로그램 최신 보안 패치 점검	10	
5	로그온 패스워드 안전성 점검	10	학생망 제외 가능
6	로그온 패스워드 사용 기간 점검	10	〃
7	화면 보호기 설정 점검	5	〃
8	사용자 공유 폴더 설정 점검	10	
9	USB 자동 실행 설정 점검	5	
10	미사용 ActiveX 프로그램 점검	10	

※ 내PC지키미 실행 화면

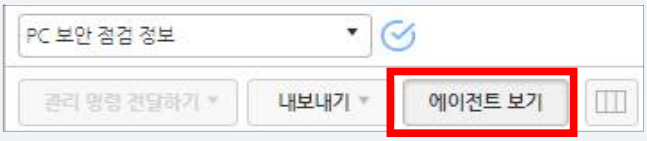


❑ **소속 기관 개인별 내PC지키미 진단결과 확인 방법(관리자)**

1. 이클린 포털(https://sen.go.kr/eclean/) 접속 후 관할 교육지원청 선택
2. Ahnlab EPP 관리자 페이지 접속 후 [관리>에이전트 현황] 메뉴 선택
3. 왼쪽 그룹창에서 '교사망(또는 학생망)' 선택
4. '에이전트 정보'를 'PC 보안 점검 정보'로 변경

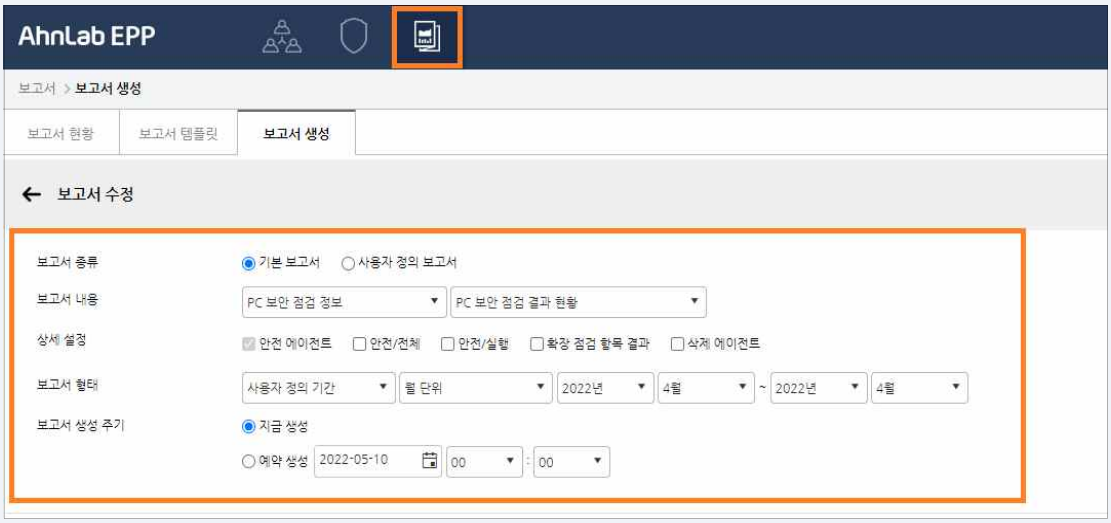


5. [에이전트 보기] 버튼 선택

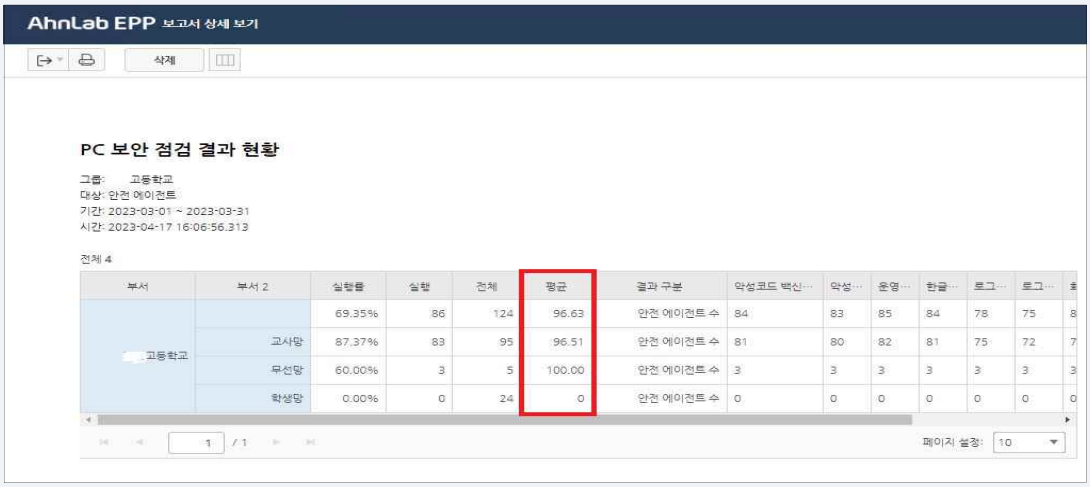


❑ **보고서 생성 및 확인 방법**

1. [보고서>보고서 생성] 메뉴 선택 후 [추가] 버튼 클릭
2. 보고서종류(**기본보고서**), 보고서내용(**PC보안 점검 정보-PC보안 점검 결과 현황**), 보고서형태(**사용자정의기간-해당 월**), 보고서생성주기(**지금생성**) 선택



3. '대상설정-그룹' 항목에서 '학교명' 클릭
4. '보고서이름' 입력 후 [확인] 버튼 클릭 ※ 보고서 생성까지 1~2분 소요
5. 생성된 보고서 확인



❑ PC내 개인정보파일 정비 및 중요 데이터 암호화

- 개별 점검 후 파일 삭제 또는 암호화 처리 **※ 주민등록번호 포함 파일은 암호화 의무**
- 개인정보파일 **암호화 미조치 파일이 있는 경우** 메시지 발생 ☞ 즉시 처리

대상파일	처리방법	비고
고유식별번호 (주민등록번호 등) 포함된 파일	법령근거 없다면 ☞ **삭제** 또는 생년월일로 대체 법령근거 있다면 ☞ 개인정보관리프로그램 **암호화**() **또는** 개별 프로그램 파일 암호화	보유 기간 종료 또는 이용 목적이 달성된 경우 즉시(5일 이내) **삭제**
개인정보 포함 파일, 중요자료 파일 등	**개별프로그램 파일 암호화** ☞ **한글**-저장하기-문서암호 설정 ☞ **엑셀**-저장하기-도구:일반옵션-암호 설정 ※ 프로그램 버전에 따라 설정방법은 다를 수 있음	

❑ 홈페이지 등에 게시자료 점검

- 비공개 업무자료 및 개인정보 노출 여부 점검
- 공개기한이 지났거나 불필요한 게시글 정비 등

❑ 기타 학교에서 필요한 보안취약점 개선

참고

▸ EPP 관리자 매뉴얼 ☞ 이클린 포털(https://sen.go.kr/eclean/)에서 다운로드

4 정보통신망 보안

관련 근거

- 서울특별시교육청 정보보안 기본지침(2022.5.) 제40조(내부망 · 인터넷망 분리)
- 서울특별시교육청 정보보안 기본지침(2022.5.) 제43조(무선랜 보안)
- 서울특별시교육청 정보보안 기본지침(2022.5.) 제47조(인터넷 사용제한)
- 서울특별시교육청 정보보안 기본지침(2022.5.) 제69조(정보통신망 현황자료 관리)

업무시기

- 상시

주요내용

❑ 네트워크 관리

- 업무망(교사망), 학생망, 무선망, 기타(서비스)망 분리

※ 각각 별도의 스위치 장비로 물리적 분리

❑ 정보통신망 현황 자료 관리

- 정보통신망 구성 현황(IP주소 할당현황 포함), 정보시스템 운용 현황: 비공개 대상 정보로 지정·관리

※ 보안사고 발생 시 IP추적을 위해 구성도, PC이름, IP 등 정비 필요

- 네트워크 구성도 현행화

❑ 무선랜 이용

- 업무망(교사망)을 통한 무선랜 이용 금지
- 정보시스템 관리대장에 무선장비 포함하여 작성(5. 정보시스템 보안 참고)

❑ 인터넷 사용 제한

- 사이버공격 등으로부터 정보통신망과 정보시스템의 정상적인 운영 보장을 위함
- 업무와 관련이 없는 인터넷 이용차단(게임·음란·도박 등)
- 교육 및 업무를 위하여 필요한 경우 교육지원청에 '서비스 허용 요청서'를 공문으로 요청

참고

- 정보시스템 원격접속 및 서비스 허용 절차
- 원격 접속 허용 요청서(서식)
- 서비스 허용 요청서(서식)

절차 정보시스템 원격접속 및 서비스 허용 절차

1. 정보시스템 원격접속 허용

○ **(기본 원칙) 불가피한 경우**를 제외하고 **원격접속 금지**

○ **(허용 시간)** 관련 시스템**관리자 근무시간 내**로 제한하는 등 보안대책을 마련

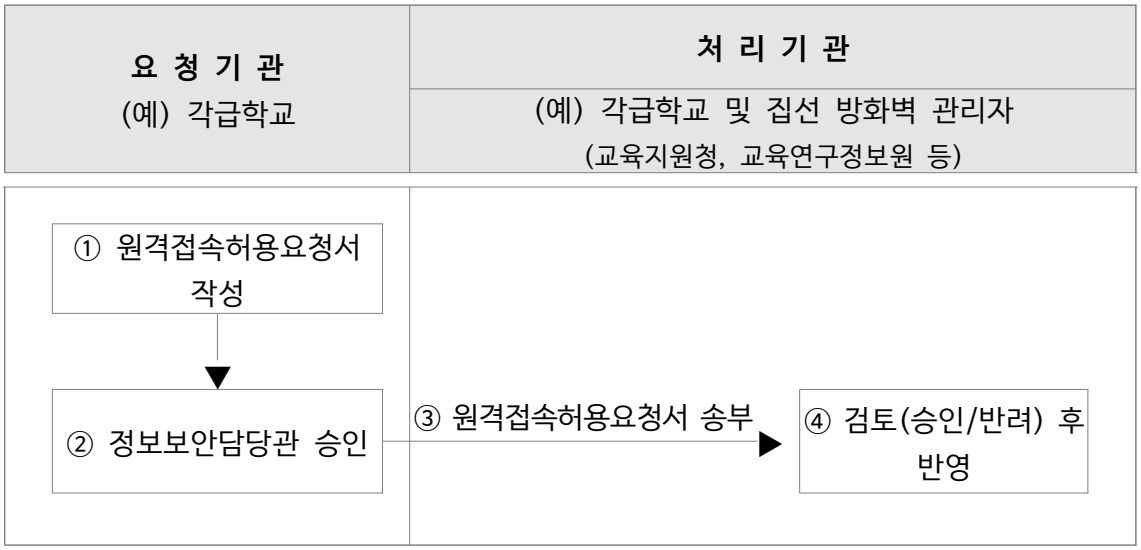
○ **(처리 절차)**

① **원격접속 허용 요청서[붙임1]** 작성 및 **부서 승인** (업무 담당자)

② **기관 정보보안담당관 승인**

③ 집선교육지원청 또는 교육연구정보원으로 **①의 요청서 제출**

④ 요청서 검토 후 **정보(보호)시스템 설정 변경** (집선 정보(보호)시스템 관리자)



2. 서비스 허용

○ **(기본 원칙) 불가피한 경우**를 제외하고 **접속 금지**

○ **(허용 원칙) 불가피하게** 교육이나 업무에 반드시 필요한 경우

- 불가피하게 교육이나 업무에 반드시 필요한 사유의 **입증책임은 신청기관 부담**
- 게임·음란·도박 및 불법 유해차단사이트 요청 금지

○ **(처리 절차) 요청 서식[붙임2]**을 제외하고, **원격 접속 허용 절차와 동일**

서식 정보시스템 원격 접속 허용 요청서

원격 접속 허용 요청서

신청기관(부서)		
담당자	검토자	책임자

승인부서		
담당자	팀장	부장

※신청자는 굵은 선 안에만 기록

신청자	소속(부서)		직급		성명	
사 용 기 간				긴급연락처		
사 유						
등 록 구 분		☐ 신규		☐ 변경	☐ 삭제	

접근대상(사용자 PC 등)		대상장비(서버 등)		
사용자명(소속)	접근IP	장비IP	접근포트	접근계정

작업 내용			
처 리 일 자		처 리 자	(서명)
처 리 내 역			

■ 본 시스템과 관련하여 직·간접적으로 알게 된 모든 정보를 엄격히 보호하고 준수하며 위반 시 민·형사상 책임과 관계법규에 의한 조치에 따를 것을 서약합니다.

신청일자 : . . . 신청자 : (서명)

※ 신청서는 교육청 담당자와 사전 협의 후 작성하여 제출
※ 접근대상 및 대상장비는 필요할 경우 행을 추가하거나 별도 첨부 가능

서식 서비스 허용 요청서

서비스 허용 요청서

신청기관(부서)		
담당자	검토자	책임자

승인부서		
담당자	팀장	부장

※신청자는 굵은 선 안에만 기록

신청자	소속(부서)		직급		성명	
사 용 기 간				긴급연락처		
사 유						
등 록 구 분		☐ 신규 ☐ 변경 ☐ 삭제				

접근대상		대상서비스	
사용자명(소속)	접근IP	서비스명	도메인(또는 IP)

처 리 일 자		처 리 자	(서명)
처 리 내 역			

■ 본 시스템과 관련하여 직·간접적으로 알게 된 모든 정보를 엄격히 보호하고 준수하며 위반 시 민·형사상 책임과 관계법규에 의한 조치에 따를 것을 서약합니다.

신청일자 : . . . 신청자 : (서명)

※ 신청서는 교육청 담당자와 사전 협의 후 작성하여 제출
※ 접근대상 및 대상장비는 필요할 경우 행을 추가하거나 별도 첨부 가능

5 정보시스템 보안

관련 근거

- 서울특별시교육청 정보보안 기본지침(2022.5.) 제48조(정보시스템 보안책임)
- 서울특별시교육청 정보보안 기본지침(2022.5.) 제49조(정보시스템 유지보수)
- 서울특별시교육청 정보보안 기본지침(2022.5.) 제59조(저장매체 불용처리)
- 서울특별시교육청 정보보안 기본지침(2022.5.) 제76조(휴대용 저장매체 보안)
- 서울특별시교육청 정보보안 기본지침 [부록3] USB메모리 등 휴대용 저장매체 보안관리지침

업무시기

- 상시

주요내용

❑ 정보시스템 관리

- 정보시스템(PC·서버·네트워크장비·정보통신기기 등)에 대한 관리자 및 관리책임자 지정·운영
- 정보시스템 관리대장 작성 및 현행화

※ 관리대상: 서버, 네트워크 장비(방화벽, 스위치 등 스쿨넷 임대장비 포함), 무선장비, PC, 노트북 등

❑ 정보시스템 외부 반출·입 관리

- 정보시스템 외부 반출·입 시(외부 수리 포함) 반출·입 대장 관리
- 휴대용 저장매체(전산장비포함) 반출·입 대장 서식을 참고하여 작성
- 외부 회의, 출장으로 반출 시 비공개 중요 자료 삭제 확인하고, 반입 시 악성코드 감염 여부 확인

❑ 저장매체 불용 처리

- 저장매체 외부수리·교체·반납·양여·폐기·불용 처리 시 저장 자료 삭제
- 삭제대상: PC·노트북·서버·복합기 등에 장착된 HDD, SSD 등의 저장 매체
- 저장매체 불용 시 삭제방법: 다음 분류에 따른 기준 이상으로 삭제
- 비밀·대외비를 저장한 저장매체는 소각·파쇄·용해 등의 방법으로 완전 파괴 필요

저장 자료 / 저장 매체	공개 자료	비공개 자료	대외비 자료	비밀 자료
자기테이프 플로피디스크	자체 판단	물리적 파괴	물리적 파괴	물리적 파괴
광디스크 (CD · DVD 등)	자체 판단	물리적 파괴	물리적 파괴	물리적 파괴
반도체메모리 (SSD · USB 등)	포맷 또는 삭제	물리적 파괴	물리적 파괴	물리적 파괴
하드디스크	포맷 또는 삭제	디가우징 또는 완전삭제 S/W	물리적 파괴	물리적 파괴

※ 물리적파괴: 소각·파쇄·용해 등의 방법으로 완전파괴

※ 디가우징: 강력한 자기장을 이용해 하드디스크에 저장된 데이터를 물리적으로 복구 불가능하게 삭제

❑ **저장자료 삭제 확인**

- 저장매체에 저장된 자료의 삭제를 외부업체에 의뢰 시 정보보안담당관 입회하여 삭제 절차·방법 준수여부 등을 확인·감독하여야 함(내부결재, 삭제 시 사진 등 증적자료 별도 관리)
- 정보시스템 도입·임차 시 교환·반출·반납을 대비하여 저장자료 완전삭제 방법 등 보안조치 방안을 계약서에 포함

[디지털·혁신미래교육과에서 추진하는 불용PC 수거로 처리하고자 할 경우]

☞ 보안각서 및 삭제 결과 등을 반드시 확인

[저장매체를 물리적 파괴 또는 디가우징 처리하고자 할 경우]

☞ 처리절차

- 저장매체 파쇄 요청서를 첨부하여 교육연구정보원 인프라운영과로 공문 제출
- 사전 협의된 일시에 대상 저장 매체를 소지하여 인프라운영과로 방문
- 신청문의: 교육연구정보원 교육정보화부 인프라운영과(02-3019-8184)

※ 관련공문: PC를 포함한 정보시스템 불용처리 시 데이터 완전삭제 철저
(교육연구정보원 정보보호과-1149, 2020.5.11.)

참고

- 정보시스템 관리대장(예시)
- 휴대용 저장매체(전산장비포함) 반출ㆍ입 대장(서식)
- 전자정보 저장매체 파쇄 요청 절차
- 전자정보 저장매체 파쇄 요청 기안문(예시)

예시 정보시스템(IP 포함) 관리대장(예시1)

작성일자 :　　관리자확인 :　　(인)

연번	소속	취급자성명	종류 (서버·PC 등)	제조사	모델명	관리번호	도입일자	IP	설치장소
1	○○부	○○○	스위치			○○초-시스템-1	○○○○.○.○.	10.xx6.xxx.xxx	정보통신실
2	○○부	○○○	스위치			○○초-시스템-2	○○○○.○.○.	10.xx6.xxx.xxx	컴퓨터 교육실
3	○○부	○○○	PC			○○초-업무용PC-1	○○○○.○.○.	10.xx6.xxx.xxx	1-1반
4	○○부	○○○	PC			○○초-업무용PC-2	○○○○.○.○.	10.xx6.xxx.xxx	1-2반
5	○○부	○○○	PC			○○초-교육용PC-1	○○○○.○.○.	10.xx6.xxx.xxx	컴퓨터 교육실
6	○○실	○○○	태블릿			○○초-테블릿PC-1~30	○○○○.○.○.	10.xx6.xxx.xxx	컴퓨터 교육실

※ PC, 노트북, 프린터, 서버, 네트워크 장비 등

[작성방법]

- **정보시스템 관리대장의 관리방식(수기 또는 전자), 기재 항목 등은 학교 실정에 따라 자율적으로 운영하며, 항상 최신화 자료로 유지**
- 취급자: 장비의 유지관리 책임 또는 취급자
- 관리번호: “기관(학교)명” + “용도” + “장비 전체 일련번호” (학교에서 자율적으로 부여)
- 관리자확인(인): 각급기관의 장이 지정한 정보시스템 관리자 확인(내부결재 시 생략 가능)

※ 정보시스템 관리대장은 비공개 업무자료로 관리

예시 정보시스템(IP 포함) 관리대장(예시2)

작성일자 :　　관리자확인 :　　(인)

관리번호	부서명(설치장소)	사용자(관리자)		형태	제조회사	모델명	OS	CPU	RAM	IP	구입시기	모니터		기기변경내역		비 고
		직위	성명									형태	크기	시기	내 역	
1	교장실	교장	홍OO	데스크탑	삼보	DB-P70	Win10	i7, 2.1GHz	16GB	55	2020.11.	LCD	20“			
2	행정실	실장	김OO	데스크탑	레드스톤	LX-L30	Win10	i3 2.4GHz	4GB	66	2018. 2.	LCD	24“	2020.05	램8G로 교체, LCD(24“) 교체	
3	제1교무실	교감	강OO	데스크탑	에이텍	D-P60	Win10	i3 3.6GHz	8GB	47	2019.12.	LCD	19“	2022.01	SSD 설치	
4	연구부	부장	고OO	노트북	루검즈	CN5300	Win10	i5, 2.6GHz	8GB	77	2020. 3.	LCD	20“			
…	…	…		…	…	…	…	…	…	…	…					

※ 정보시스템 관리대장의 관리방식(수기 또는 전자), 기재 항목 등은 학교 실정에 따라 자율적으로 운영하며, 항상 최신화 자료로 유지

휴대용 저장매체(전산장비 포함) 반출·입 대장

〈 관리자 : 4급 김유○ 〉

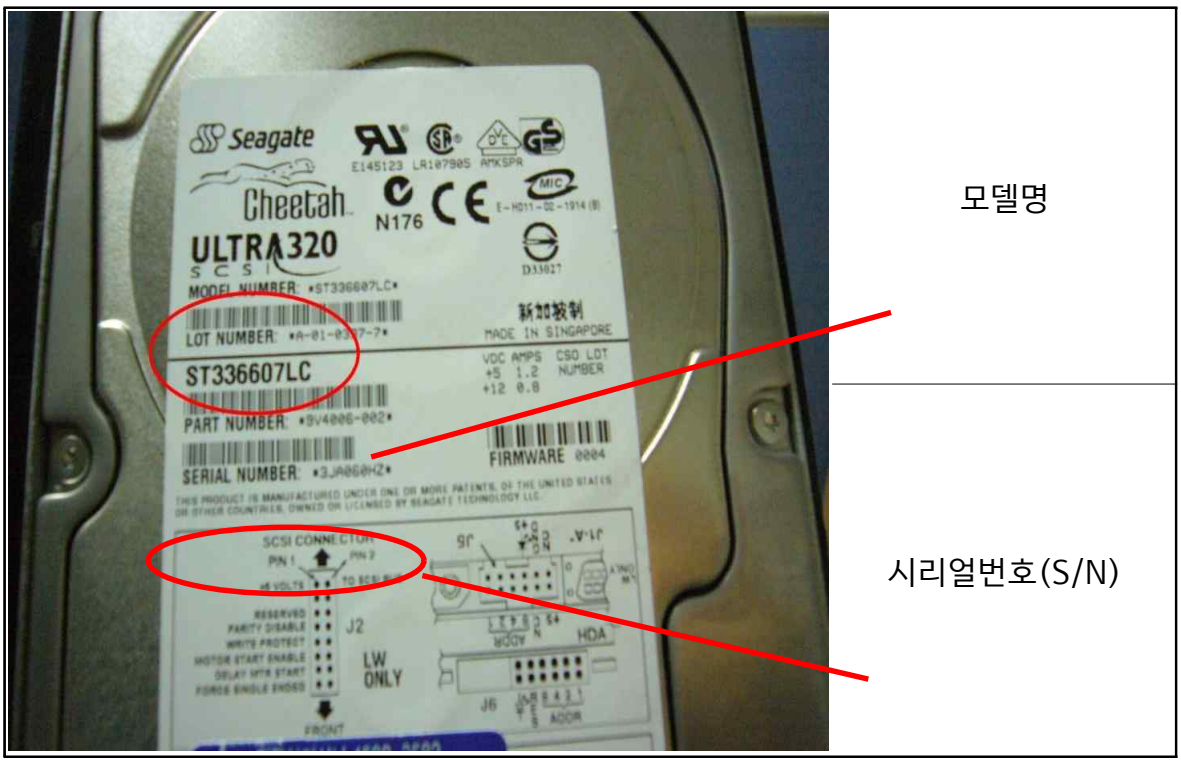
장비명	관리번호 (시리얼번호)	사용자	용도	비공개 중요 자료 완전 삭제 확인 악성코드 감염 여부 확인	반출입 일시 (입·출 구분)	확인 ***친필서명***
USB	총무-일반-01 (610-RUCW-61659)	6급 홍길동	국회 제출	홍길동	2016.03.08.10:00(출)	김유신
				나보안	2016.03.08.18:00(입)	김유신
CD	총무-일반-03 (4589-KK-4585)	6급 유관순	행자부 회의참석	유관순	2016.05.08.10:00(출)	김유신
				나보안	2016.05.08.18:00(입)	김유신
노트북PC	s111-001-113 (5004829800055)	6급 유관순	세미나 발표	유관순	2017.12.1 13:00 (출)	김유신
				나보안	2017.12.1 19:00 (입)	김유신
USB	총무-일반-005 (610-RUFU-61747)	6급 홍길자	재택근무	*홍길자*	2022.12.1 18:00(출)	김유신
				나보안	2022.12.2 10:00(입)	김유신

절차 전자정보 저장매체 파쇄 요청 절차

1. 파쇄대상 저장매체 파악
2. 하드디스크의 경우 가이드를 반드시 제거(하드디스크 자체만 파쇄가능)

가이드 등이 장착된 상태(제거요망)	가이드 등이 모두 제거된 상태 (파쇄가능 상태)
	

3. 전자정보 저장매체 파쇄 요청서 작성, **작성 예시 참조**
   - 파쇄 요청서 작성 시 고유번호는 아래 이미지를 참조하여 작성
   - CD, LTO 테이프, DVD 등 고유번호가 없는 매체는 관리번호 기재



4. 작성된 문서를 첨부하여 전자정보 저장매체 파쇄 요청 공문을 서울특별시교육청교육연구정보원 -교육정보화부-**인프라운영과**로 제출(작성 예시 참조)
   ※ **방문일시는 사전에 협의(인프라운영과 ☎02-2230-8527)**
5. 지정된 일시에 종합전산센터(학교보건진흥원 3층)에 **소거할 저장매체**를 소지하고 방문
6. 인프라운영과 직원 입회하에 저장매체 파쇄 실시

예시 전자정보 저장매체 파쇄 요청 기안문

다양성이 꽃피는 공존의 혁신미래교육

○○○학교

수신자 서울특별시교육청교육연구정보원(교육정보화부 인프라운영과장)

(경유)

제목 전자정보 저장매체 파쇄 요청

1. 관련: 서울특별시교육청 정보보안 기본지침 제59조(저장매체 불용처리)
2. 위 호와 관련하여 아래와 같이 전자정보 저장매체 파쇄를 요청합니다.
   가. 방문일시: 20○○.○.○○. 00:00 ~ 00:00
   ※ 담당자와 협의 후 결정
   나. 대상수량: 하드디스크 ○○개, 자기테이프 ○○개
   다. 방 문 자: ○○○

붙임 전자정보 저장매체 파쇄 요청서 1부. 끝.

○○ 학교장

★ 교장

협조자

시행 ○○학교-0000 (0000. 00. 00.) 접수 ( )

우 00000 서울특별시 ○○○○○○ / http://www.

전화 02-000-0000 /전송 02-000-0000 / ○○○@○○○ / 비공개(7)

[붙임]

전자정보 저장매체 파쇄 요청서

처리기관		
담당자	팀장	과장

번호	매체 형태	고유번호 (모델명/시리얼번호)	최종 사용자명	사 유	비고
1	*하드디스크*	*ST336607LC/3JA060HZ*	*홍길순*	*불용처리*	
2	*자기 테이프*	*LTO4/A00016L4*	*홍길산*	*불용처리*	
3	*하드디스크*	*MX4707EW/KA4674STW*	*이몽룡*	*고장*	
4		이 하 여 백			
5					
6					
7					
8					
9					
10					
11					
유의 사항	*○ 파쇄가능 저장매체* *- 서버용 하드디스크(2.5인치, 3.5인치,5.25인치)* *- LTO 테이프 미디어* *- CD, DVD, BLU-RAY 등의 디스크 미디어* *- DAT 등 소형 테이프 미디어* *○ 고유번호는 Serial Number 또는 모델명, 관리번호도 가능* *○ 최종 사용자가 없는 경우 최종 관리자로 작성* *○ 사유는 불용 또는 고장 등으로 작성 필*				

■ 소자매체수량에 맞게 번호를 늘려 작성

신청자	신청일자	*2023. . .*				
	소속기관	*○○**학교***	직급 (직위)	*○○○*	성명	*홍길동(서명)*

6 단말기(PC, 노트북 등) 보안

관련 근거

- 서울특별시교육청 정보보안 기본지침(2022.5.) 제71조(개별사용자 보안)
- 서울특별시교육청 정보보안 기본지침(2022.5.) 제72조(단말기 보안)

업무시기

- 상시

주요내용

❑ **개별사용자:** PC 등 정보시스템을 사용하거나 정보통신망에 접속하는 행위와 관련하여 스스로 보안책임을 져야함

❑ **단말기에 대한 보안 대책 준수(학교장이 별도로 정할 수 있음)**

- CMOS·로그온·자료 암호화 비밀번호의 정기적 변경 사용
- 단말기 작업을 10분 이상 중단 시 비밀번호 등을 적용한 화면보호 조치
- 최신 백신 소프트웨어 설치
- 운영체제 및 응용프로그램에 대한 최신 보안패치 유지
- 출처, 유통경로 및 제작자가 불분명한 응용프로그램의 사용 금지
- 신뢰할 수 있는 인터넷사이트 활용, 파일 다운로드 시 최신 백신 소프트웨어로 검사 후 활용
- 업무상 불필요한 프로그램 설치 금지 및 공유 폴더 삭제
- 웹브라우저를 통해 서명되지 않은 액티브-X등이 다운로드·실행되지 않도록 보안 설정
- PC, 노트북 등을 기관 외부로 반출 혹은 반입 시 휴대용 저장매체 반출·입 대장에 기록

❑ **PC보안시스템**

프로그램명	적용대상		기능	설치방법
	교사망	학생망		
통합PC보안관리(EPP)	○	○	PC지키미, 패치, 백신, 개인정보 관리	교사망PC **(자동설치)** 학생망PC **(수동 설치)**
지능형위협탐지시스템(APT) (1권역: , 2권역)	○	○	지능형 위협 프로그램 탐지·차단	
유해매체차단시스템 (PC보안케어)		○	유해 동영상 및 파일 실행 차단	

※ 1권역: 동부, 서부, 북부, 강동송파, 강서양천, 성동광진, 성북강북

※ 2권역: 남부, 중부, 강남서초, 동작관악

❑ EPP 관리자 페이지

● 접속 방법
- 이클린사이트 접속
http://www.sen.go.kr/eclean
☞ 소속 지원청 클릭
☞ EPP 관리자 페이지 바로가기 클릭

● 접속 실패 시 참고사항
- 접속 가능 PC: 학교 당 2개(2개 IP만 접속 허용)
- 접속 보안: 로그인 5회 실패 시 10분간 접속 차단(로그인 인증 보류)
※ 관리계정 및 접속 IP 확인은 관할 교육지원청에 문의

● 주요 기능
- 내PC지키미 현황 조회 및 점검보고서 생성 (기준: 교사망 100점, 학생망 75점 이상)
⇒ 메뉴: 보고서 → 보고서 생성 → PC보안점검정보 → PC보안 점검결과 현황
- 개인정보 보유 조회 및 보고서 생성 (기준: 개인정보파일 안전조치(암호화) 100%)
⇒ 메뉴: 보고서 → 보고서 생성 → 개인정보검색 → 개인정보검색현황, 개인정보처리현황

참고

▸ EPP 관리자 매뉴얼 ☞ 이클린 포털(https://sen.go.kr/eclean/)에서 다운로드

7 통제구역 관리

관련 근거

- 교육부 보안업무규정 시행세칙 제60조,제61조,제62조
- 서울특별시교육청 정보보안 기본지침(2022.5.) 제84조(정보통신시설 보호대책)

업무시기

- 상시

주요내용

❑ 전산실 통제구역 지정

- 통제구역: 보안장비 설치 구역, 전산실(주전산기 설치 구역)
- 통제구역 표시 및 관리책임자 표지 부착, 잠금장치 설치

통제구역	통제구역 (15Cm × 30Cm) 또는 【통제구역】 비인가자는 출입을 금함
관리책임자	(예시) ○○ 구역관리책임자 / 정 / 부 (3cm × 9cm)

※ 정보통신실 등 정보통신시설 및 장소는「보안업무규정」제34조에 따른 보호지역으로 지정·관리하여야 함

❑ 통제구역 출입통제 대장 관리

- 보안장비, 네트워크 장비 유지보수업체 정기점검 방문 시 반드시 대장에 기재
- 통제구역인 전산실을 성적처리, 방송실 등과 공동사용 시 별도 출입통제 조치 필요

※ 전산실에 상시 근무자가 있을 경우 통제구역 출입관리가 어려워 전산실/사무실 분리

- 교육부 보안업무규정 시행세칙 별지 제14호

***(서식)* 통제구역 출입통제대장**

연월일	출입시간 퇴실시간	용무	출입자		입회자		비고 (서명)
			소속 (주소)	성명	직급	성명	

참고

- 교육부 보안업무규정 시행세칙 별지 제14호(통제구역 출입통제대장)

8 디지털복합기 관리

관련 근거

▸ 서울특별시교육청 정보보안 기본지침(2022.5.) 제88조(디지털복합기 보안)

업무시기

▸ 상시

주요내용

❑ **도입**

- 복합기 내 저장매체가 있거나 장착이 가능한 경우 자료유출을 방지하기 위하여 자료 완전 삭제 또는 디스크암호화 기능이 탑재된 제품 도입(CC인증 제품)

  ※ 학교는 필수 아님

- 복합기 폐기·양여 또는 외부 반출 시 저장된 자료 완전 삭제
- 기본 비밀번호 변경 후 사용: 변경 방법은 유지보수 업체 및 제조사에 문의
- 복합기 설치·운용 시 보안대책
  - 암호화 저장 기능이 있는 경우 해당 기능 사용
  - 정기적으로 저장된 작업 내용(출력, 스캔 등) 완전 삭제
  - 공유 저장소 사용 제한 및 접근 제어
  - 고정 IP주소 설정 및 불필요한 서비스 제거

❑ **국내 CC인증 제품 확인 방법**

① IT보안인증사무국 홈페이지(https://www.itscc.kr) 접속
② [인증제품목록]에서 검색창의 제품유형 - '디지털 복합기' 선택
③ 인증보고서에 '완전삭제' 항목 또는 '데이터 암호화' 부분 확인

❑ **국제 CC인증 제품 확인 방법**

① CCRA 홈페이지(https://www.commoncriteriaportal.org/) 접속
② [CERTIFIED PRODUCTS] 항목에서 'Multi-function Devices' 선택- Security Target에서 확인

9 휴대용 저장매체(USB 등) 관리

관련 근거

▸ 서울특별시교육청 정보보안 기본지침(2022.5.) 제76조(휴대용 저장매체 보안)

업무시기

▸ 상시

주요내용

❑ **휴대용 저장매체**

- CD, 외장형 하드디스크, USB 등 정보를 저장할 수 있는 것으로 PC, 서버 등의 정보시스템과 분리할 수 있는 기억장치
- 비밀용/일반용으로 구분하여 관리하고, 수량 및 보관 상태를 정기적으로 점검하며 외부 반출·입 통제

구분	일반용	비밀용
보관자료	업무관련 일반자료(행정전자서명 인증서 등)만 보관	비밀등급별 각각 휴대용 저장매체를 마련하고 하나의 휴대용 저장매체에는 동일 등급의 자료만 보관
관리대장	휴대용 저장매체 관리대장(일반용) 작성	휴대용 저장매체 관리대장(비밀용) 작성
보관방법	개인서랍 및 캐비닛 등	이중 캐비닛 또는 금고

❑ **휴대용 저장매체 관리**

- 관리대장(일반용/비밀용)에 등록한 후 사용

휴대용 저장매체 관리대장(일반용)

<관리책임자 : ○○○>

연번	관리번호 (시리얼번호)	매체형태	등록일자	취급자	불용처리일자	불용처리방법 (재사용 용도)	비고

- 주기적(월 1회 이상)으로 보관상태 및 보안관리 실태 점검

휴대용 저장매체 점검대장

<관리책임자 : ○○○>

점검일시	현 보유수량				이상 유무	점검관		비고 (서명)
	Ⅱ급	Ⅲ급	대외비	일반		성명	서명	

- 외부로 가져가거나 내부로 가져올 때 작성하며 정보보안담당관 결재 필요

휴대용 저장매체(전산장비포함) 반출·입 대장

<관리책임자 : OOO>

장비명	관리번호 (시리얼번호)	담당자 (사용자)	용도	비공개 중요 자료 완전 삭제 확인 악성코드 감염 여부 확인	출입 일시 (입·출 구분)	확인

- 휴대용 저장매체 파기 등 불용처리, 비밀용을 일반용 또는 다른 등급의 비밀용으로 전환 시 완전삭제
- 불용처리 시 [휴대용 저장매체 불용처리 확인서]에 기재

휴대용 저장매체 불용처리 확인서

아래와 같이 휴대용 저장매체(종 점) 불용처리 및 휴대용 저장매체 (종 점) 재사용에 대해 확인을 요청함

연번	관리번호 (시리얼번호)	매체형태	사유	불용처리	재사용

확인일자 : 년 월 일
요 청 자 : 소속 · 직책 O급 성명 : (인)
확 인 자 : 정보보안담당관 O급 성명 : (인)

참고

▸ USB메모리 등 휴대용 저장매체 보안관리지침 별지1~6호 ☞ 표준서식(정보보안)에서 다운로드

10 정보화 용역사업 관리

관련 근거

- 서울특별시교육청 정보보안 기본지침(2022.5.) 제13조(제안요청서 기재사항)
- 서울특별시교육청 정보보안 기본지침(2022.5.) 제25~30조(계약 및 사업수행)
- 서울특별시교육청 정보보안 기본지침(2022.5.) 제49조(정보시스템 유지보수)

업무시기

- 사업추진시

주요내용

❑ 용역사업 보안관리

- 사업대상: 자체 홈페이지 유지보수 용역, PC 유지보수 등
- 계약서(또는 과업지시서, 입찰 공고)에 명시할 사항
  - 인원/장비/자료 등에 대한 보안조치 사항
  - 보안준수사항 위반 시 손해배상 책임 사항
  - 누출금지 대상정보 및 부정당업자의 제재조치 사항
  - 참여인원 임의 교체 금지
  - 개인정보 처리 위탁 시 표준개인정보처리위탁 계약서 작성

❑ 사업 진행시 주의사항

진행단계	주의 사항	비고
사업 착수 시	• 정보화 용역사업 보안 특약사항 및 표준개인정보처리위탁 계약서(또는 특약사항) 포함하여 계약 • 보안서약서 징구 ☞ 참여인력용 • 용역사업 인력에 대한 보안교육 실시	
사업 수행 시	• 업체에 자료(정보통신망도, IP현황, 개인정보 등) 제공 시 제공자료 **인계인수 관리대장** 작성 • 노트북, 휴대용 저장매체(USB 메모리 등) **반·출입 대장 작성** - 악성코드 감염여부, 누출금지 정보 무단 반출 여부 점검 • 유지보수 일시 및 담당자 인적사항, 출입통제 조치사항, 작업수행내용 등 기록	
사업 종료 시	• 보안확약서 징구 ☞ 대표자용 • 업체에 제공한 사업관련 제반자료 전량 회수 및 제공자료 인계인수 관리대장 기록 • 용역업체 보관자료 완전삭제 등의 보안조치	

참고

- 정보화 용역사업 보안특약 사항(예시)
- 표준개인정보처리위탁 계약서 및 특약사항(서식)
- 보안서약서(서식)
- 정보화사업 용역업체 보안교육 및 점검자료(예시)
- 자료 인수인계 대장(예시)
- 휴대용 저장매체(전산장비 포함) 반출 · 입 대장(서식)
- 보안확약서(서식)

정보화 용역사업 보안 특약사항

1. 사업자는 발주자의 보안정책을 위반하였을 경우 「사업자 보안위규 처리기준」에 따라 위규자 및 관리자를 행정조치하고 「보안 위약금 부과 기준」에 따라 보안 위약금을 발주기관에 납부한다.

2. 사업자는 사업 수행에 사용되는 문서, 인원, 장비 등에 대하여 물리적, 관리적, 기술적 보안대책 및 「누출금지 대상 정보」에 대한 보안 관리 계획을 사업수행계획서에 기재하여야 하며, 해당 정보 누출 시 「지방자치단체를 당사자로 하는 계약에 관한 법률」시행령 제92조에 따라 사업자를 부정당업체로 등록한다.

3. 사업 수행과정에서 취득한 자료와 정보에 관하여 사업수행 중은 물론 사업 완료 후에도 이를 외부에 유출해서는 안 되며, 사업완료 시 담당자의 입회하에 완전 폐기 또는 반납해야 한다.

4. 계약 시행일로부터 종료 후 30일이 경과하는 날까지의 기간 중에 발주기관, 발주기관의 상급기관 및 국가정보원장의 정기 또는 수시 보안점검(불시 점검 포함)을 수행할 수 있다.
   * 관련: 정보보안 기본지침 제26조제3항, 제28조의2제5호, 제50조제1항제5호

5. 사업자는 사업 최종 산출물에 대해 정보보안전문가 또는 전문 보안점검 도구를 활용하여 보안취약점을 점검, 도출된 취약점에 대한 개선을 완료하고 그 결과를 제출해야 한다.

[별표 1] 용역사업 보안 준수사항
[별표 2] 사업자 보안위규 처리기준
[별표 3] 보안 위약금 부과 기준
[별표 4] 누출금지 대상 정보

서약자	소속	직급	성명	(인)
확인자	소속	직급	성명	(인)

별표 1

용역사업 보안 준수사항

1. 참여인원에 대한 보안관리

가. 용역사업 참여인원별 개인 친필 서명이 들어간 **보안서약서 제출**(참여인력 교체 경우 포함)

나. 용역사업 **참여인원은 임의로 교체할 수 없으며** 부득이한 사유로 교체해야 하는 경우(퇴사, 국외여행 등) 발주자의 사전 승인 필요

다. 참여인원의 비밀유지의무 준수 등의 **보안교육 참여 및 자체 보안교육 실시**

2. 자료에 대한 보안관리

가. 계약서 등에 명시된 '기관 소유 정보통신망 구성도·IP주소 현황 등'을 제공 받을 시 **제공자료 인계인수 관리대장을 작성**(인계자·인수자 자필 서명)하고 무단 복사 및 외부 반출을 금지함

나. 사업 관련자료는 웹하드, P2P, 웹오피스, 클라우드 등 인터넷 자료공유 사이트 및 개인 메일함에 저장 금지

다. 사업자와 발주자 간 전자우편을 이용해 자료전송이 필요한 경우 SEN메일을 이용하며, 첨부자료는 암호화 후 수·발신

3. 사무실 및 장비에 대한 보안관리

가. 용역사업은 비인가자 출입통제 대책, CCTV, 잠금장치 등이 확보된 공간에서 수행

나. 용역사업 수행 공간에 대해서는 주요자료 방치 여부 등 보안점검을 수시·정기적으로 실시

다. 사업자의 노트북·휴대용 저장매체 사용이 불가피한 경우 발주자의 승인 후 사용

라. 반입 장비는 최신 백신프로그램으로 바이러스 및 악성코드 감염여부를 사전 점검 후 반입

마. 장비 반입·출시 발주자의 승인 후 반입 및 반출 (반출·입 대장 기재)

바. 노트북PC, 휴대용 저장매체 등 중요자료는 시건장치가 있는 보관함에 보관

사. 사업자의 노트북 및 보조기억매체 사용 종료 시 완전삭제 등 보안조치 확행

4. 산출물에 대한 보안관리

가. 사업 관련 **제반자료 전량 회수 및 제공자료 인계인수 관리대장 기록**

나. 복사본 등 사업 관련 자료를 일체 보유하고 있지 않다는 **업체 대표 명의의 보안 확약서 제출**

다. 사용 종료 시 사업자의 노트북·휴대용 저장매체 등 관련 장비 완전삭제

라. 사업자가 소프트웨어 산출물을 제3자에게 제공하고자 할 경우 제공하기 이전에 발주자의 승인을 받아야 함

5. 원격(온라인) 유지보수·개발에 대한 보안관리 (필요시)

가. 용역업체 작업장소에 대한 사전협의 및 비인가 출입통제 대책

나. 개발PC에 대한 목적 외 사용 금지, 보안프로그램 설치, 인터넷 접속 금지 등 보안점검 수행

다. 발주기관의 허가없이 정보통신망 또는 정보시스템 무단 접속 및 정보 수집 금지

별표 2

사업자 보안위규 처리기준

구 분	위 규 사 항	처 리 기 준
심 각	1. 비밀 및 대외비 급 정보 유출 및 유출시도 가. 정보시스템에 대한 구조, 데이터베이스 등의 정보 유출 나. 개인정보·신상정보 목록 유출 다. 비공개 항공사진·공간정보 등 비공개 정보 유출 2. 정보시스템에 대한 불법적 행위 가. 관련 시스템에 대한 해킹 및 해킹시도 나. 시스템 구축 결과물에 대한 외부 유출 다. 시스템 내 인위적인 악성코드 유포	• 사업참여 제한 (부정당업체 등록) • 위규자 및 직속 감독자 등 중징계 • 재발 방지를 위한 조치계획 제출 • 위규자 대상 특별 보안교육 실시
중 대	1. 비공개 정보 관리 소홀 가. 비공개 정보를 책상 위 등에 방치 나. 비공개 정보를 휴지통·폐지함 등에 유기 또는 이면지 활용 다. 개인정보·신상정보 목록을 책상 위 등에 방치 라. 기타 비공개 정보에 대한 관리소홀 2. 사무실·보호구역 보안관리 허술 가. 통제구역 출입문을 개방한 채 퇴근 등 나. 인가되지 않은 작업자의 내부 시스템 접근 다. 통제구역 내 장비·시설 등 무단 사진촬영 3. 전산정보 보호대책 부실 가. 업무망 인터넷망 혼용사용, 보안 USB 사용규정 위반 나. 웹하드·P2P 등 인터넷 자료공유사이트를 활용하여 용역사업 관련 자료 수발신 다. 개발·유지보수 시 원격작업 사용 라. 저장된 비공개 정보 패스워드 미부여 마. 인터넷망 연결 PC 하드디스크에 비공개 정보를 저장 바. 외부용 PC를 업무망에 무단 연결 사용 사. 보안관련 프로그램 강제 삭제 아. 사용자 계정관리 미흡 및 오남용(시스템 불법접근 시도 등)	• 위규자 및 직속 감독자 등 중징계 • 재발 방지를 위한 조치계획 제출 • 위규자 대상 특별 보안교육 실시

구분	위 규 사 항	처리기준
보 통	1. 기관 제공 중요정책·민감 자료 관리 소홀 가. 주요 현안 · 보고자료를 책상 위 등에 방치 나. 정책·현안자료를 휴지통·폐지함 등에 유기 또는 이면지 활용 다. 사무실 보안관리 부실 라. 캐비넷·서류함·책상 등을 개방한 채 퇴근 마. 출입키를 책상 위 등에 방치 3. 보호구역 관리 소홀 가. 통제·제한구역 출입문을 개방한 채 근무 나. 보호구역내 비인가자 출입허용 등 통제 미실시 4. 전산정보 보호대책 부실 가. 휴대용저장매체를 서랍·책상 위 등에 방치한 채 퇴근 나. 비인가 메신저 무단 사용 다. PC를 켜 놓거나 보조기억 매체(CD, USB 등)를 꽂아 놓고 퇴근 라. 부팅·화면보호 패스워드 미부여 또는 단순숫자 부여 마. PC 비밀번호를 모니터 옆 등 외부에 노출 바. 비인가 보조기억매체 무단 사용	• 위규자 및 직속 감독자 등 경징계 • 위규자 및 직속 감독자 사유서/경위서 징구 • 위규자 대상 특별보안 교육 실시
경 미	1. 업무 관련서류 관리 소홀 가. 진행 중인 업무자료를 책상 등에 방치, 퇴근 나. 복사기·인쇄기 위에 서류 방치 2. 근무자 근무상태 불량 가. 각종 보안장비 운용 미숙 나. 경보·보안장치 작동 불량 3. 전산정보 보호대책 부실 가. PC내 보안성이 검증되지 않은 프로그램 사용 나. 보안관련 소프트웨어의 주기적 점검 위반	• 위규자 서면·구두 경고 등 문책 • 위규자 사유서/경위서 징구

* 보안위규사항 및 처리기준은 기관별 실정에 맞게 조정

별표 3

보안 위약금 부과 기준

1. 위규 수준별로 A~D 등급으로 차등 부과

구분	위규 수준			
	A급	B급	C급	D급
위규	심각 1건	중대 1건	보통 2건 이상	경미 3건 이상
위약금 비중	부정당업자 등록	계약금액의 10%	계약금액의 5%	계약금액의 3%

※ 위규 수준은 [별표2]의 「사업자 보안위규 처리기준」 참고

2. 보안 위약금은 다른 요인에 의해 상쇄, 삭감이 되지 않도록 부과

※ 보안사고는 1회의 사고만으로도 그 파급력이 큰 것을 감안하여 타 항목과 별도 부과

3. 사업 종료 시 지출금액 조정을 통해 위약금 정산

별표 4

누출 금지 대상 정보

① 해당 기관의 정보시스템 내·외부 IP주소 현황
② 정보시스템 구성 현황 및 정보통신망 구성도
③ 개별사용자의 계정·비밀번호 등 정보시스템 접근권한 정보
④ 정보통신망 또는 정보시스템 취약점 분석·평가 결과물
⑤ 정보화사업 용역 결과물 및 관련 프로그램 소스코드(외부에 유출될 경우 국가안보 및 국익에 피해가 우려되는 중요 용역사업에 해당)
⑥ 암호자재 및 정보보호시스템 도입·운용 현황
⑦ 정보보호시스템 및 네트워크장비 설정 정보
⑧ 「공공기관의 정보공개에 관한 법률」 제9조제1항에 따라 비공개 대상 정보로 분류된 해당 기관의 내부문서
⑨ 「개인정보보호법」 제2조제1호에 따른 개인정보
⑩ 「보안업무규정」 제4조에 따른 비밀 및 「보안업무규정 시행규칙」 제16조제3항에 따른 대외비
⑪ 그 밖에 해당 기관의 장이 공개가 불가하다고 판단한 자료

표준 개인정보처리위탁 계약서

본 표준 개인정보처리위탁 계약서는 「개인정보 보호법」제26조제1항에 따라 위탁계약에 있어 개인정보 처리에 관하여 문서로 정하여야 하는 최소한의 사항을 표준적으로 제시한 것으로서, 위탁계약이나 위탁업무의 내용 등에 따라 세부적인 내용은 달라질 수 있습니다.

개인정보처리업무를 위탁하거나 위탁업무에 개인정보 처리가 포함된 경우에는 본 표준 개인정보처리위탁 계약서의 내용을 위탁계약서에 첨부하거나 반영하여 사용하실 수 있습니다.

OOO(이하 "위탁자"라 한다)과 △△△(이하 "수탁자"이라 한다)는 "위탁자"의 개인정보 처리업무를 "수탁자"에게 위탁함에 있어 다음과 같은 내용으로 본 업무 위탁계약을 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 및 고시, 「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시 제2023-6호) 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.
2.

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

계약 기간 : 20oo년 o월 o일 ~ 20oo년 o월 o일

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”은 「개인정보 보호법」제23조제2항 및 제24조제3항 및 제29조, 같은 법 시행령 제21조 및 제30조, 「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시 제2023-6호)에 따라 개인정보의 안전성 확보에 필요한 기술적·관리적 조치를 취하여야 한다.

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 제2023-6호)에 따라 즉시 파기하거나 “위탁자”에게 반납하여야 한다.

③ 제2항에 따라 “수탁자”가 개인정보를 파기한 경우 지체 없이 “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 접속기록
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 (__)회 “수탁자”를 교육할 수 있으며, “수탁자”는 이에 응하여야 한다.

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

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

제10조 (개인정보의 파기) “수탁자”는 제4조의 위탁업무 기간이 종료되면 특별한 사유가 없는 한 지체없이 개인정보를 파기하고, 이를 “위탁자”에게 파기 확인서(문서)를 제출하여 확인받아야 한다.

제11조 (손해배상) ① “수탁자” 또는 “수탁자”의 임직원 또는 기타 “수탁자”의 수탁자가 이 계약에 의하여 위탁 또는 재위탁 받은 업무를 수행함에 있어 이 계약에 따른 의무를 위반하거나 “수탁자” 또는 “수탁자”의 임직원 또는 기타 “수탁자”의 수탁자의 귀책사유로 인하여 이 계약이 해지되어 “위탁자” 또는 정보주체, 기타 제3자에게 손해가 발생한 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 : ○○시 ○○길 ○○	주 소 : ○○시 ○○로 ○○
기관(회사)명 :	기관(회사)명 :
성 명 : (인)	성 명 : (인)

예시 표준 개인정보처리위탁 특약사항

■ 조달청 입찰 등 계약서 징구가 어려운 경우 제안요청서 등 공식문서에 특약사항 추가 사용 가능

표준 개인정보처리위탁 특약사항

OOO(이하 “위탁자”라 한다)과 △△△(이하 “수탁자”이라 한다)는 “위탁자”의 개인정보 처리업무를 “수탁자”에게 위탁함에 있어 다음과 같은 내용으로 본 업무 위탁계약을 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 및 고시, 「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시 제2023-6호) 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.
2.

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

계약 기간 : 20oo년 o월 o일 ~ 20oo년 o월 o일

제5조 (재위탁 제한) ① “수탁자”는 “위탁자”의 사전 승낙을 얻은 경우를 제외하고 “위탁자”와의 계약상의 권리와 의무의 전부 또는 일부를 제3자에게 양도하거나 재위탁 할 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”은 「개인정보 보호법」제23조제2항 및 제24조 제3항 및 제29조, 같은 법 시행령 제21조 및 제30조, 「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시 제2023-6호)에 따라 개인정보의 안전성 확보에 필요한 기술적·관리적 조치를 취하여야 한다.

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 제2023-6호)에 따라 즉시 파기하거나 “위탁자”에게 반납하여야 한다.

③ 제2항에 따라 “수탁자”가 개인정보를 파기한 경우 지체 없이 “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 접속기록
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 (__)회 “수탁자”를 교육할 수 있으며, “수탁자”는 이에 응하여야 한다.

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

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

제10조 (개인정보의 파기) “수탁자”는 제4조의 위탁업무 기간이 종료되면 특별한 사유가 없는 한 지체없이 개인정보를 파기하고, 이를 “위탁자”에게 파기 확인서(문서)를 제출하여 확인받아야 한다.

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

서식 **보안서약서(사업시작시 참여인력 전원에게 징구)**

보안서약서

본인은 년 월 일부터 *OO회사(OO사업 수행)*으로 근무함에 있어 다음 사항을 준수할 것을 서약한다.

1. 본인은 비밀로 분류될 성질의 업무를 수행함에 있어 소관 업무가 국가안전보장과 관련된 기밀임을 인정한다.

2. 본인은 보안 관련 규정을 준수하며 재직 중은 물론 퇴직 후에도 직무상 알게 된 비밀을 누설하지 않는다.

3. 본인이 기밀을 누설하거나 유출하였을 때에는 관련 법령에 따라 처벌을 받을 것을 서약한다. 다만 「부패방지 및 국민권익위원회의 설치와 운영에 관한 법률」에 따른 부패행위 신고 및 「공익신고자 보호법」에 따른 공익신고 등을 위한 목적일 경우 비밀준수 의무를 위반하지 않은 것으로 본다.

서약자	소속	직급	생년월일	
		직위	성명	(인)
서약집행자	소속	직급		
		직위	성명	(인)

예시 정보화사업 용역업체 보안교육 및 점검 자료

<table>
<tr><th>번호</th><th colspan="2">용역업체 교육내용</th><th>내용
확인</th></tr>
<tr><td rowspan="6">1</td><td colspan="2">통제·제한 구역 내 휴대용 장비 및 저장매체(노트북, 태블릿PC, USB, MP3플레이어 등) 반입 금지</td><td>☐</td></tr>
<tr><td rowspan="5">반입
·
반출
시</td><td>반입 대장 기재(담당자 승인, 유·무선 네트워크 사용 제한: 외부 인터넷 사용 금지)</td><td>☐</td></tr>
<tr><td>카메라 렌즈, 외부입력 포트 보안스티커를 부착</td><td>☐</td></tr>
<tr><td>최신 백신 S/W 설치 및 악성코드 검사 완료</td><td>☐</td></tr>
<tr><td>OS 및 응용S/W를 최신 보안 업데이트 완료</td><td>☐</td></tr>
<tr><td>반출 대장 기재(비밀, 보안 및 개인정보 자료 포맷 완료)</td><td>☐</td></tr>
<tr><td rowspan="4">2</td><td rowspan="4">개발
보안</td><td>시스템 및 홈페이지 등 정보시스템의 소스코드는 비인가자의 소스 코드 열람 및 사용을 제한하도록 조치한다</td><td>☐</td></tr>
<tr><td>시스템 접속을 위한 단말은 지정된 PC 또는 노트북만 사용 가능하며 원격 작업을 할 수 없다.</td><td>☐</td></tr>
<tr><td>서버 또는 개발 소스코드에는 담당자가 인가한 모듈, 소스코드만 설치 및 적용 할 수 있다.</td><td>☐</td></tr>
<tr><td>보안에 취약하거나 특이 사항을 발견한 경우 즉시 담당자에게 알린다</td><td>☐</td></tr>
<tr><td>3</td><td colspan="2">
<table>
<tr><th>위 규 사 항</th><th>처 리 기 준</th></tr>
<tr><td>[심각]
1. 비밀 및 대외비 급 정보 유출 및 유출시도
가.정보시스템에 대한 구조, 데이터베이스 등의 정보 유출
나.개인정보·신상정보 목록 유출
다.비공개 항공사진·공간정보 등 비공개 정보 유출
2. 정보시스템에 대한 불법적 행위
가.관련 시스템에 대한 해킹 및 해킹시도
나.시스템 구축 결과물에 대한 외부 유출
다.시스템 내 인위적인 악성코드 유포</td><td>• 사업참여 제한
(부정당업체 등록)
• 위규자 및 직속 감독자
등 중징계
• 재발 방지를 위한
조치계획 제출
• 위규자 대상
특별보안교육 실시</td></tr>
<tr><td>[중대]
1. 비공개 정보 관리 소홀
가.비공개 정보를 책상 위 등에 방치
나.비공개 정보를 휴지통·폐지함 등에 유기 또는 이면지 활용
다.개인정보.신상정보 목록을 책상 위 등에 방치
라.기타 비공개 정보에 대한 관리소홀
2. 사무실 · 보호구역 보안관리 허술
가.통제구역 출입문을 개방한 채 퇴근 등
나.인가되지 않은 작업자의 내부 시스템 접근
다.통제구역 내 장비·시설 등 무단 사진촬영
3. 전산정보 보호대책 부실
가.업무망 인터넷망 혼용사용, 보안 USB 사용규정 위반
나.웹하드·P2P 등 인터넷 자료공유사이트를 활용하여 용역사업 관련 자료 수발신
다.개발·유지보수 시 원격작업 사용
라.저장된 비공개 정보 패스워드 미부여
마.인터넷망 연결 PC 하드디스크에 비공개 정보를 저장
바.외부용 PC를 업무망에 무단 연결 사용
사.보안관련 프로그램 강제 삭제
아.사용자 계정관리 미흡 및 오남용(시스템 불법접근 시도 등)</td><td>• 위규자 및 직속 감독자
등 중징계
• 재발 방지를 위한
조치계획 제출
• 위규자 대상
특별보안교육실시</td></tr>
<tr><td>[보통]
1. 기관 제공 중요정책·민감 자료 관리 소홀
가. 주요 현안·보고자료를 책상위 등에 방치
나. 정책·현안자료를 휴지통·폐지함 등에 유기 또는 이면지 활용
2. 사무실 보안관리 부실
가. 캐비넷·서류함·책상 등을 개방한 채 퇴근
나. 출입키를 책상위 등에 방치
3. 보호구역 관리 소홀
가. 통제·제한구역 출입문을 개방한 채 근무
나. 보호구역내 비인가자 출입허용 등 통제 미실시
4. 전산정보 보호대책 부실
가. 휴대용저장매체를 서랍·책상 위 등에 방치한 채 퇴근
나. 비인가 메신저 무단 사용
다. PC를 켜 놓거나 보조기억 매체(CD, USB 등)를 꽂아 놓고 퇴근
라. 부팅·화면보호 패스워드 미부여 또는 “1111” 등 단순숫자 부여
마. PC 비밀번호를 모니터옆 등 외부에 노출
바. 비인가 보조기억매체 무단 사용</td><td>• 위규자 및 직속 감독자
등 경징계
• 위규자 및 직속 감독자
사유서 / 경위서 징구
• 위규자 대상
특별보안교육 실시</td></tr>
</table>
</td><td>☐
☐
☐</td></tr>
</table>

번호	용역업체 교육내용		내용 확인
	[경미] 1. 업무 관련서류 관리 소홀 가. 진행중인 업무자료를 책상 등에 방치, 퇴근 나. 복사기·인쇄기 위에 서류 방치 2. 근무자 근무상태 불량 가. 각종 보안장비 운용 미숙 나. 경보·보안장치 작동 불량 3. 전산정보 보호대책 부실 가. PC내 보안성이 검증되지 않은 프로그램 사용 나. 보안관련 소프트웨어의 주기적 점검 위반	• 위규자 서면·구두 경고 등 문책 • 위규자 사유서 및 경위서 징구	□
	위의「보안위규 처리기준」위반 시 위규자 및 관리자 행정조치 숙지 완료		□
4	시스템 유지보수를 위해 제공받은 기관 정보통신망도, IP현황, 개인정보 등 인수인계대장에 작성된 누출금지 자료는 지정된 장소 이외에 별도 보관하지 않으며, 다른 누구에게도 제공하지 않는다. 〈누출금지정보〉 ① 해당 기관의 정보시스템 내·외부 IP주소 현황 ② 정보시스템 구성 현황 및 정보통신망 구성도 ③ 개별사용자의 계정·비밀번호 등 정보시스템 접근권한 정보 ④ 정보통신망 또는 정보시스템 취약점 분석·평가 결과물 ⑤ 정보화사업 용역 결과물 및 관련 프로그램 소스코드(외부에 유출될 경우 국가안보 및 국익에 피해가 우려되는 중요 용역사업에 해당) ⑥ 암호자재 및 정보보호시스템 도입·운용 현황 ⑦ 정보보호시스템 및 네트워크장비 설정 정보 ⑧「공공기관의 정보공개에 관한 법률」제9조제1항에 따라 비공개 대상 정보로 분류된 해당 기관의 내부문서 ⑨「개인정보보호법」제2조제1호에 따른 개인정보 ⑩「보안업무규정」제4조에 따른 비밀 및「보안업무규정 시행규칙」제16조제3항에 따른 대외비 ⑪ 그 밖에 해당 기관의 장이 공개가 불가하다고 판단한 자료		□

본인은 서울시교육청 정보화 사업과 관련하여 직·간접적으로 알게 된 모든 정보를 엄격히 보호하고 준수사항을 지키며 위반 시 사업자 부정당업자제재 조치 및 민·형사상 책임과 관계법규에 의한 조치가 따르게 됨을 충분히 인지하였음

년 월 일

소속 직위 성명 (인)

귀하

[누출금지정보 관련 법률 상세 내용]

아. '공공기관의 정보공개에 관한 법률' 제9조1항(비공개 대상정보)

1. 다른 법률 또는 법률에서 위임한 명령(국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙·대통령령 및 조례로 한정한다)에 따라 비밀이나 비공개 사항으로 규정된 정보
2. 국가안전보장·국방·통일·외교관계 등에 관한 사항으로서 공개될 경우 국가의 중대한 이익을 현저히 해칠 우려가 있다고 인정되는 정보
3. 공개될 경우 국민의 생명·신체 및 재산의 보호에 현저한 지장을 초래할 우려가 있다고 인정되는 정보
4. 진행 중인 재판에 관련된 정보와 범죄의 예방, 수사, 공소의 제기 및 유지, 형의 집행, 교정(矯正), 보안처분에 관한 사항으로서 공개될 경우 그 직무수행을 현저히 곤란하게 하거나 형사피고인의 공정한 재판을 받을 권리를 침해한다고 인정할 만한 상당한 이유가 있는 정보
5. 감사·감독·검사·시험·규제·입찰계약·기술개발·인사관리에 관한 사항이나 의사결정 과정 또는 내부검토 과정에 있는 사항 등으로서 공개될 경우 업무의 공정한 수행이나 연구·개발에 현저한 지장을 초래한다고 인정할 만한 상당한 이유가 있는 정보. 다만, 의사결정 과정 또는 내부검토 과정을 이유로 비공개할 경우에는 의사결정 과정 및 내부검토 과정이 종료되면 제10조에 따른 청구인에게 이를 통지하여야 한다.

자. '개인정보 보호법' 제2조(정의)

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 포함)

차. '보안업무규정' 제4조의 비밀, 동 시행규칙 제16조3항의 대외비

제4조(비밀의 구분) 비밀은 그 중요성과 가치의 정도에 따라 다음 각 호와 같이 구분한다.

1. Ⅰ급비밀: 누설될 경우 대한민국과 외교관계가 단절되고 전쟁을 일으키며, 국가의 방위계획·정보활동 및 국가방위에 반드시 필요한 과학과 기술의 개발을 위태롭게 하는 등의 우려가 있는 비밀
2. Ⅱ급비밀: 누설될 경우 국가안전보장에 막대한 지장을 끼칠 우려가 있는 비밀
3. Ⅲ급비밀: 누설될 경우 국가안전보장에 해를 끼칠 우려가 있는 비밀

자료 인계인수대장 *(예시)*

□ 업무(사업) 개요
- 업무(사업)명 :
- 업무(사업)기간 : 20 . . . ~ 20 . . .

□ 인계 기관명_부서명(담당자명) : 서울특별시교육청_OOO담당관(홍길동)

□ 인수 기관명(담당자명) : ㈜한국정보보안(나정보)

□ 인계인수 확인

연번	인계 자료명	인계일	회수일	확인(서명) *친필서명*		
				인계자	인수자	회수자
1	*정보통신망 구성도*	*2021. 3. 8.*	*2022. 2. 28.*	*홍길동*	*나정보*	*홍길동*
2	*IP현황*	*2021. 3. 8.*	*2022. 2. 28.*	*김유신*	*너보안*	*김유신*
3	.....					
4						
5						
.....						

서식 휴대용 저장매체(전산장비포함) 반출·입 대장

휴대용 저장매체(전산장비 포함) 반출·입 대장

<관리책임자 : 이순신(서명)>

장비명	관리번호 (시리얼번호)	사용자	용도	비공개 중요 자료 완전 삭제 확인 악성코드 감염 여부 확인	반출입 일시 (입·출 구분)	확인 *친필서명*
USB	총무-일반-01 (610-RUCW-61659)	홍길동	국회 제출	홍길동	2016.03.08.10:00(출)	김유신
				나보안	2016.03.08.18:00(입)	김유신
CD	총무-일반-03 (4589-KK-4585)	유관순	행자부 회의참석	유관순	2016.05.08.10:00(출)	김유신
				나보안	2016.05.08.18:00(입)	김유신
노트북PC	s111-001-113 (5004829800055)	유관순	세미나 발표	유관순	2017.12.1 13:00 (출)	김유신
				나보안	2017.12.1 19:00 (입)	김유신
USB	총무-일반-005 (610-RUFU-61747)	홍길자	재택근무	*홍길자*	2022.12.1 18:00(출)	김유신
				나보안	2022.12.2 10:00(입)	김유신

서식 **보안확약서(사업종료시)**

확 약 서 (대표자용)

본인은 (용역, 연구개발, 제작, 입찰, 유지보수, 그 밖의 업무) 사업 용역 업무와 관련한 장비, 서류, 중간·최종 산출물 등 모든 제반자료(개인정보 포함) 등에 대하여 다음과 같이 이행하였음을 확약합니다.

1. 용역사업(업무) 관련한 모든 제반자료 반환(인계인수대장 확인 완료)
2. 용역사업(업무) 관련한 저장매체 내 자료 삭제
3. 용역사업(업무) 관련한 사업산출물 복사본 등을 별도 보관하지 않음
4. 본인이 이 기밀(개인정보 포함)을 누설하거나 관계 규정을 위반한 때에는 관련 법령 및 계약에 따라 어떠한 처벌 및 불이익도 감수한다.

년 월 일

서약자 소속 직급
직위 성 명 인

서 약 소속 직급
집행자 직위 성 명 인

11 사이버침해사고 신고

관련 근거

- 서울특별시교육청 정보보안 기본지침(2022.5.) 제98조(보안관제센터 설치·운영)
- 서울특별시교육청 정보보안 기본지침(2022.5.) 제107조(사이버공격으로 인한 사고)

업무시기

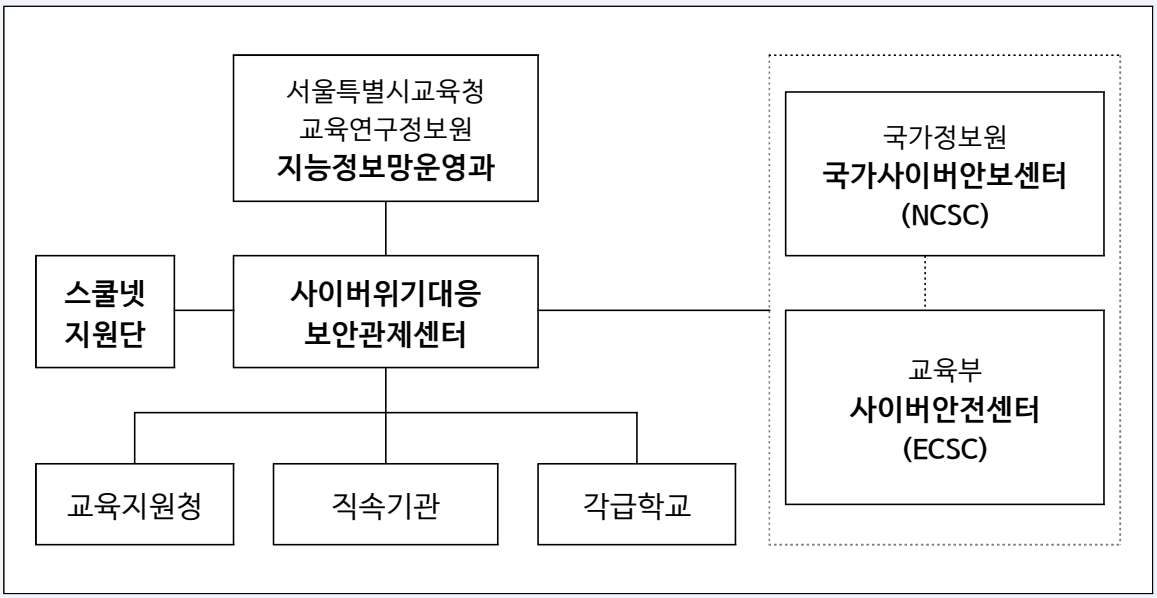
- 사안발생 시

주요내용

❑ 사이버위기란?

사이버공격으로 정보통신망을 통해 유통·저장되는 정보를 유출·변경·파괴함으로써 국가안보에 영향을 미치거나 사회·경제적 혼란을 발생시키거나 국가 정보통신시스템의 핵심기능이 훼손·정지되는 등 무력화되는 상황

❑ 서울시교육청 사이버위기 대응 업무 체계



❑ 사이버위기대응 보안관제센터 역할

- 본청(직속기관 포함) 및 11개 교육지원청(각급학교 포함)의 정보보호시스템 통합 관리
- 사이버 침해대응을 위한 실시간 보안관제 실시
- 로그 분석 및 사이버공격 대응, 정보보안 정책 관리
- 사이버위기 경보 발령 및 침해사고 전파 및 사고 대응

❑ **사이버 침해사고 발생 시 대응 절차**

- 기관(학교)에서 침해사고 자체 인지한 경우

1단계	2단계	3단계	4단계	5단계
사고인지 (발생기관·학교)	**초동대응 및 신고 (발생기관·학교)**	**사고조사 (보안관제센터)**	**피해복구**	**후속조치 (발생기관·학교)**
홈페이지 위·변조, 랜섬웨어 감염 등 침해사고 발생 확인	① 랜 케이블 분리 및 증거자료 백업 (포맷 금지) ② 기관 내 정보보안담당관에 신고 ③ 관할기관 신고	공격 유형별 사고조사(원인 및 공격근원지 추적)	우선순위, 복구범위 결정 후 피해복구 및 운영 정상화	사고 재발방지 대책 수립, 관할기관에 사고조치결과 통보

- 사이버보안관제센터(교육연구정보원 지능정보망운영과)에서 조치 요청 받은 경우

☞ 보안관제요원의 안내에 따라 초동 대응 및 사고 조사, 후속 조치 이행

※ 신고 및 조치 관련 자료는 보안관제센터 전용 e메일을 통해 송·수신(신고 시 안내)

- 침해사고 신고처

대상	신고처	신고방법
본청, 교육지원청, 직속기관, 학교(고/특/각종)	교육연구정보원 지능정보망운영과(사이버보안관제팀) ☎ 02-6973-9973	기관 정보보안담당자가 신고처에 신고 ① 인지 즉시 전화 신고 ② 보안관제센터 안내에 따라 '사고신고서' 제출 (전자우편 또는 공문)
학교(유/초/중)	관할 교육지원청 행정지원과(정보팀)	

참고

▸ 사이버침해사고 신고서(예시)

사이버침해사고 신고서

기 본 정 보			
기 관 명	00초등학교	부 서	OOO부
성 명	홍 길 동	직 위	OO부장
전자우편	hong@sen.go.kr		
연 락 처	전화: 02-555-5555 H.P: 010-555-5555 FAX: 02-555-5555		
사 고 내 용			
사고 일시	0000년 00월 00일 00시 00분	피해IP주소	10.123.xxx.1. ~ 255
피해시스템 용도	사, 아 * 뒷장의 '가. 시스템 분류' 기호 입력	운영체제	■ 윈도우 □ 유닉스 □ 네트워크장비 상세버전정보: Windows 10
사고 유형	D * 뒷장의 '나. 사고 유형' 기호 입력	피해범위	146 대 * 피해시스템이 여러대인 경우 피해숫자 기입
사고 내용	교내 PC실로부터 대량의 트래픽이 발생하고 있음		
조 치 내 용			
공격자 정보	수신된 전자우편의 발신지는 주로 seoul_ace@state.gov 임		
피해 현황	전쟁사진을 포함한 전자우편 수신 증가, 교내 네트워크 트래픽 급격히 증가, 3개의 교사용 PC 사용 불가		
긴급조치 실시사항	감염 PC 네트워크 차단		
관련보안제품 운영현황	OO 사용 중		
그 밖에 사고 관련 내용을 구체적으로 서술			
없음			
향후 대응 방안(재발 방지 대책)			
사고/조치 화면			
사고화면			
조치화면			

※ 관할 교육지원청 행정지원과(정보팀) 및 교육연구정보원 지능정보망운영과로 즉시 사고 신고하시기 바랍니다.

가. 시스템 분류 목록

기호	시스템 분류	설 명
가	웹서버	기관의 홈페이지 운영 및 웹서비스를 제공하는 서버
나	전자우편 서버	전자우편 송수신을 위해 운영하는 서버
다	DB/업무서버	홈페이지 및 업무지원을 위한 데이터베이스 서버
라	개발/임시서버	개발 및 운영 테스트를 위하여 사용하는 임시 서버
마	통신전송장비	라우터, 스위치 등 통신전송장비 일체
바	보안장비	방화벽, IDS, VPN 및 백신서버 등 정보보안제품 일체
사	개인/업무PC	기관내 사용자의 PC
아	교육/임시PC	교육장 또는 공용 작업을 위해 여러 명이 사용하는 PC
자	기타	위의 시스템 용도에 없는 경우 서술식으로 기술

나. 사고 유형 목록

기호	사고 유형	설 명
A	경유지 악용	타기관으로부터 해킹시도 항의를 받았거나, 시스템 점검 중 해킹 흔적 또는 해킹툴이 설치되어 타시스템에 접속한 기록이 발견되었을 경우
B	자료훼손 및 유출	내부 시스템의 자료가 변조가 되었거나, 대량의 데이터가 외부로 무단 송신된 흔적이 발견되었을 경우
C	악성코드 감염	기관내의 서버 PC에서 악성코드가 발견되었을 경우
D	홈페이지 접속 불가능	기관의 홈페이지 서버 또는 네트워크 이상으로 인해 홈페이지 접속이 불가능 할 경우
E	서비스거부공격 피해	불특정 다수의 IP로부터 접속 시도 또는 대량 트래픽이 일시에 유입될 경우
F	시스템 파괴	내부 시스템의 자료가 삭제되어 사용이 불가능한 경우
G	해킹메일	해킹메일 열람 및 해킹메일 내 악성파일 실행의 경우
H	기타	위의 사고유형에 포함되지 않을 경우 서술식으로 기술

부록

각급학교 정보보안 자율 진단표

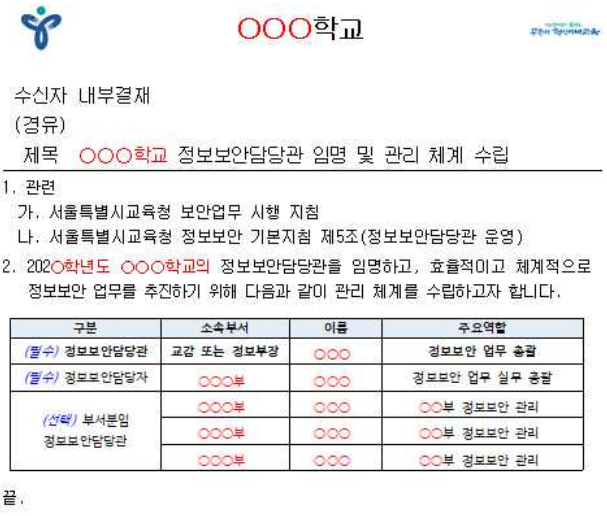
진단항목(클릭시 상세설명 연결)	진단내용	결과(양호/미흡)
❶ 정보보안담당관 지정 서울특별시교육청 정보보안 기본지침 제5조	▸ 지정 여부:	
❷ 정보보안 교육 실시 여부 서울특별시교육청 정보보안 기본지침 제9조	▸ 전직원 대상 교육 실시 여부: (연 1회 이상) ▸ 담당자 보안교육 이수 여부: (연 15시간 이상)	
❸ 사이버보안 진단의 날 운영 서울특별시교육청 보안업무규정 시행 지침 제11조 서울특별시교육청 정보보안 기본지침 제10조, 제72조제3항	▸ PC진단('내PC지키미') 조치 여부 (기준점수: 교사망 100점, 학생망 75점 이상) ▸ 개인정보파일 암호화 조치 여부	
❹ 정보시스템 관리 서울특별시교육청 정보보안 기본지침 제48조~제49조, 제69조, 제76조~제77조	▸ 정보시스템 관리대장 현행화 관리 여부: ▸ 반·출입 대장 기록 여부:	
❺ 정보통신망 현황 자료 관리 서울특별시교육청 정보보안 기본지침 제40조6항, 제69조, 제76조	▸ 구성도, IP대장 현행화 관리 여부:	
❻ 저장매체 불용처리 시 준수사항 이행 서울특별시교육청 정보보안 기본지침 제59조, 제88조	▸ 불용처리시 저장자료 삭제 확인:	
❼ 휴대용 저장매체 관리 서울특별시교육청 정보보안 기본지침 제76조	▸ 관리대장, 반출·입대장, 점검대장, 불용처리확인서 관리 유무:	
❽ 전산장비 설치 장소 보안구역 지정 및 관리 서울특별시교육청 보안업무 시행지침 제8조 서울특별시교육청 정보보안 기본지침 제84조~제85조	▸ 통제구역 표지 부착 및 이중 잠금장치 여부: ▸ 통제구역 출입자대장 작성 여부:	
❾ 디지털복합기 보안 관리 서울특별시교육청 정보보안 기본지침 제20조, 제88조	▸ 기본암호 변경 여부: ▸ 작업문서(복사, 스캔 등) 저장되지 않도록 설정 여부:	
❿ 정보화사업 추진 시 누출금지정보 명시 서울특별시교육청 정보보안 기본지침 제13조	▸ 용역계약서 또는 제안요청서 명시 여부	
⓫ 외부용역 정보화사업 관리 서울특별시교육청 정보보안 기본지침 제25조~제26조, 제49조	▸ 인수인계대장 작성 여부: ▸ 보안교육 실시 여부: ▸ 보안서약서(참여인력) 및 확약서(대표자) 보관 여부:	

각급학교 정보보안 자율 진단(상세설명)

진단항목	❶ 정보보안담당관 지정

진단방법

▸ **정보보안담당관 지정 여부::** *O/X*



○○○학교

수신자 내부결재
(경유)
제목 ○○○학교 정보보안담당관 임명 및 관리 체계 수립

1. 관련
 가. 서울특별시교육청 보안업무 시행 지침
 나. 서울특별시교육청 정보보안 기본지침 제5조(정보보안담당관 운영)
2. 202○학년도 ○○○학교의 정보보안담당관을 임명하고, 효율적이고 체계적으로 정보보안 업무를 추진하기 위해 다음과 같이 관리 체계를 수립하고자 합니다.

구분	소속부서	이름	주요역할
(필수) 정보보안담당관	교감 또는 정보부장	○○○	정보보안 업무 총괄
(필수) 정보보안담당자	○○○부	○○○	정보보안 업무 실무 총괄
(선택) 부서분임 정보보안담당관	○○○부	○○○	○○부 정보보안 관리
	○○○부	○○○	○○부 정보보안 관리
	○○○부	○○○	○○부 정보보안 관리

끝.

참고서류

▸ 업무분장 등 정보보안담당관 지정 문서 또는 업무분장표

관련규정

▸ **서울특별시교육청 정보보안 기본지침 제5조(정보보안담당관 운영)**

- 학교장이 정보보안 업무를 담당하는 부장 또는 교감 중 임명

진단항목	❷ 정보보안 교육 실시 여부

진단방법	참고서류
▸ **정보보안 교육 계획 수립 및 대상자별 교육 실시 여부:** *O/X* - 전 직원 대상 정보보안 교육 실시: 연 1회 이상 - 정보보안담당자 교육 이수(필수): 연간 15시간 이상 ※ 온라인교육 이수결과 현황관리로 자체교육 대체 가능(이수증 확인) ✤ 정보보안 교육 참고자료(온라인 교육센터) ※ 강좌명에 '정보보안', '개인정보보호' 포함된 경우 등 ① 서울시교육청교육연수원 https://www.seti.go.kr ② 교육부 정보보호교육센터 운영 교육 https://sec.keris.or.kr ③ 개인정보보호 종합포털(수탁자교육용) https://www.privacy.go.kr	▸ 정보보안 교육 실시 계획 (별도계획 수립 시) ▸ 교육실시 증빙자료: 교육관련 내부결재(학교장 결재), 교육자료, 출석부, 온라인 이수증 등

관련규정

▸ **서울특별시교육청 정보보안 기본지침 제9조(정보보안교육)**

- 교육계획을 수립하여 연1회 이상 모든 소속 공무원 등을 대상으로 교육 실시(온라인 교육 포함)
- 정보보안담당자는 연간 15시간 이상 정보보안 교육(「개인정보보호법」 제28조 제2항의 교육 등 포함)을 이수

진단항목	❸ 사이버보안 진단의 날 운영

진단방법

▸ **PC진단('내PC지키미') 및 기준점수 이행 여부:** *O/X*

(기준점수: 업무망(교사망) 100점, 학생망 75점 이상)

연번	점검 항목	점수	비고
1	악성코드 백신 설치 및 실행 점검	10	
2	악성코드 백신 최신 보안 패치 점검	10	
3	운영 체제, MS Office 최신 보안 패치 점검	20	
4	한글 프로그램 최신 보안 패치 점검	10	
5	로그온 패스워드 안전성 점검	10	교육망 제외 가능
6	로그온 패스워드 사용 기간 점검	10	〃
7	화면 보호기 설정 점검	5	〃
8	사용자 공유 폴더 설정 점검	10	
9	USB 자동 실행 설정 점검	5	
10	미사용 ActiveX 프로그램 점검	10	

▸ **개인정보파일 암호화 조치 여부:** *O/X*

참고서류

▸ EPP(PC보안통합시스템) 관리자 접속

-〉 보고서 -〉 보고서생성 -〉

① PC 보안 점검 정보 -〉 PC보안 점검 결과 현황

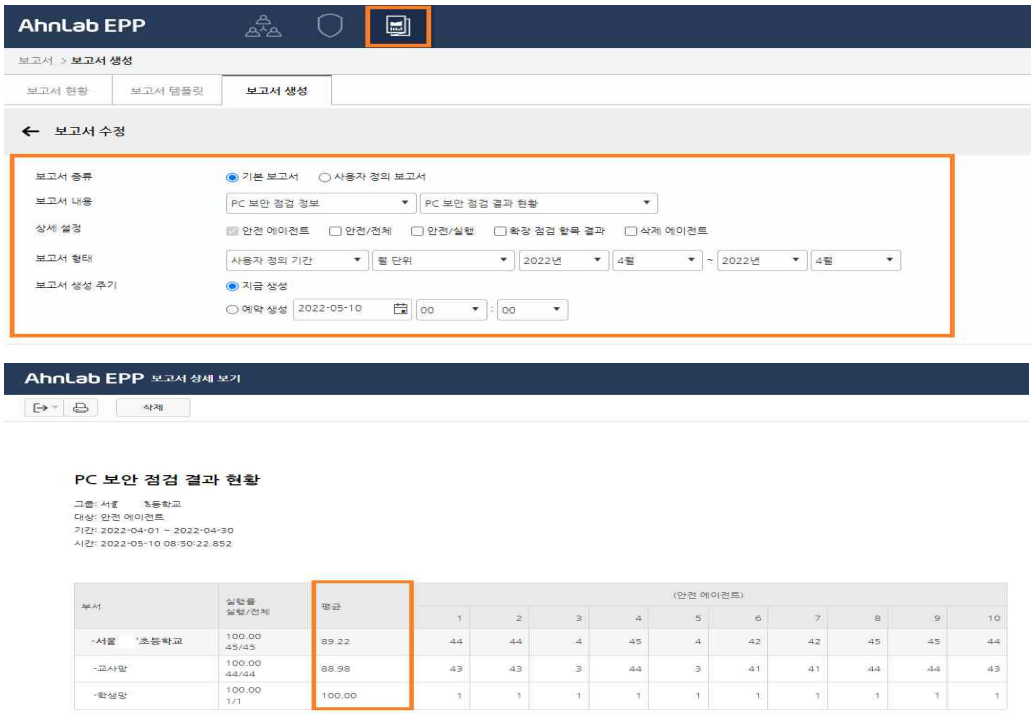
② 개인정보처리현황, 격리파일현황, 암호화파일현황, 예외처리파일현황, 미처리파일현황

(상세내용 EPP 매뉴얼 참조)

✤ '내PC지키미'진단결과 확인방법

- EPP 관리자 프로그램 접속: http://www.sen.go.kr/eclean 접속〉소속 교육지원청〉EPP 관리자페이지 바로가기 클릭
- 학교 계정, 비밀번호 재설정, 접속 PC IP변경 시 집선교육지원청 정보담당 문의

보고서 〉 보고서생성 〉 PC 보안 점검 정보 〉 PC보안 점검 결과 현황



관련규정

▸ **서울특별시교육청 보안업무규정 시행 지침 제11조(사이버보안 진단의 날 실시)**

▸ **서울특별시교육청 정보보안 기본지침 제10조(사이버보안진단의 날) , 제72조제3항**

진단항목	❹ 정보시스템 관리

진단방법

▸ **정보시스템 관리대장 현행화 관리 여부**: *O/X*

- 정보시스템 관리대장 작성 및 현행화 여부 점검 [지침 서식 제4호]

※ 정보시스템 관리대상: 서버, 네트워크 장비, 무선장비, PC, 노트북 등

▸ **정보시스템 반·출입 대장 기록 여부:** *O/X*

- 정보시스템 외부 반출·입 시 휴대용 저장매체(전산장비 포함) 반출·입 대장 작성 여부 확인 [지침 부록3 별지 제4호서식]

※ 외부 회의, 출장으로 노트북을 반출하는 경우 사전에 비공개 중요 자료는 완전 삭제하고 악성코드 감염여부 확인

✤ 서울특별시교육청 정보보안 기본지침 [서식 제4호]

(서식) 정보시스템 관리대장

연번	소속	취급자 성명	종류 (서버·PC 등)	제조사	모델명	관리번호	도입일자	관리자 확인(인)	비고

✤ 서울특별시교육청 정보보안 기본지침 부록3 [별지 제4호 서식]

휴대용 저장매체(전산장비포함) 반출·입 대장

〈관리책임자 : OOO〉

장비명	관리번호 (시리얼번호)	담당자 (사용자)	용도	비공개 중요 자료 완전 삭제 확인 / 악성코드 감염 여부 확인	출입 일시 (입·출 구분)	확인

참고서류

▸ 정보시스템 관리대장

- 서울특별시교육청 정보보안 기본지침 [서식 제4호] 양식

▸ 휴대용 저장매체(전산장비포함) 반출입·대장

▸ 서울틀별시교육청 정보보안 기본지침부록3 [별지 제4호 서식]

관련규정

▸ **서울특별시교육청 정보보안 기본지침 제48조(정보시스템 보안책임)~제49조(정보시스템 유지보수)**
▸ **서울특별시교육청 정보보안 기본지침 제69조(정보통신망 현황자료 관리)**
▸ **서울특별시교육청 정보보안 기본지침 제76조(휴대용 저장매체 보안)~제77조(비인가 기기 통제)**

- 정보시스템 관리책임자는 [서식 제4호]에 따른 정보시스템 관리대장을 수기 또는 전자적으로 작성·관리하여야 함
- 휴대용 저장매체 관리자는 휴대용 저장매체를 비밀용·일반용으로 구분·관리하고 수량 및 보관 상태를 정기적으로 점검하며 외부 반출·입을 통제하여야 함

진단항목	❺ 정보통신망 현황 자료 관리

진단방법	참고서류
▸ **정보통신망 구성현황(IP주소 할당현황 포함) 현행화 여부:** *O/X* - 학교 네트워크 구성도 및 IP대장 현행화 여부 확인 (※ 보안사고 발생 시 IP추적을 위해 구성도, PC이름, IP 등 정비 필요) - 정보통신망 구성현황 비공개 대상 정보로 지정·관리 여부 확인	▸ 학교 네트워크 구성도 ▸ 정보시스템 IP관리대장

관련규정

▸ **서울특별시교육청 정보보안 기본지침 제40조6항**
▸ **서울특별시교육청 정보보안 기본지침 제69조(정보통신망 현황자료 관리)**

- 각급기관의 장은 내부망과 기관 인터넷망의 IP주소 현황을 정보시스템 관리책임자를 통해 정기적으로 확인하고 갱신하여야 함
- 「공공기관의 정보공개에 관한 법률」제9조제1항에 따라 정보통신망 구성현황(IP주소 할당현황 포함) 및 정보시스템 운용현황은 비공개 대상 정보로 지정·관리

진단항목	❻ 저장매체 불용처리 시 준수사항 이행

진단방법

▸ **불용처리 시 저장자료 삭제 여부:** *O/X*

- 삭제대상: PC 하드디스크, HDD내장 복합기 등
- 저장매체 불용처리 외부업체 의뢰 시 정보보안담당관 입회하에 삭제 절차·방법 준수여부 등을 확인·감독하였는지 점검(내부결재, 삭제 시 사진 등 증적자료 등)
- 디지털·혁신미래교육과에서 추진하는 불용PC 수거로 처리 시 보안각서 및 삭제결과 확인

✤ 저장매체 불용처리 시 삭제방법

- 비밀·대외비를 저장한 저장매체는 소각·파쇄·용해 등의 방법으로 완전 파괴 필요

저장 자료 / 저장 매체	공개 자료	비공개 자료	대외비 자료	비밀 자료
자기테이프 플로피디스크	자체 판단	물리적 파괴	물리적 파괴	물리적 파괴
광디스크 (CD·DVD 등)	자체 판단	물리적 파괴	물리적 파괴	물리적 파괴
반도체메모리 (SSD·USB 등)	포맷 또는 삭제	물리적 파괴	물리적 파괴	물리적 파괴
하드디스크	포맷 또는 삭제	디가우징 또는 완전삭제 S/W	물리적 파괴	물리적 파괴

※ **물리적파괴:** 소각·파쇄·용해 등의 방법으로 완전파괴

※ **디가우징:** 강력한 자기장을 이용해 하드디스크에 저장된 데이터를 물리적으로 복구 불가능하게 삭제

참고서류

▸ 정보시스템 도입·임차 계약서 등

▸ 불용처리 시 관련서류(내부결재, 삭제 시 사진 등 증적자료 등)

관련규정

▸ **서울특별시교육청 정보보안 기본지침 제59조(저장매체 불용처리)**

▸ **서울특별시교육청 정보보안 기본지침 제88조(디지털복합기 보안)**

▸ **서울틀별시교육청 정보보안 기본지침 [부록4]「정보시스템 저장매체 불용처리지침」**

- 각급기관의 장은 정보시스템 또는 저장매체(하드디스크·반도체기반 저장장치(SSD) 등)를 외부수리·교체·반납·양여·폐기·불용 처리하고자 할 경우 정보시스템 및 저장매체에 저장된 자료가 외부에 유출되지 않도록 자료 삭제 등 보안조치를 실시하여야 함

진단항목	❼ 휴대용 저장매체 관리

진단방법

▸ **휴대용 저장매체 관련 대장 관리 유무:** *O/X*

☞「USB메모리 등 휴대용 저장매체 보안관리지침」별지 제1호~제6호 서식

- 휴대용 저장매체 관리대장 [별지 제1호~제2호 서식]
- 휴대용 저장매체 점검대장 [별지 제3호 서식]
- 휴대용 저장매체(전산장비 포함) 반출·입 대장 관리 [별지 제4호 서식]
- 휴대용 저장매체 불용처리 확인서 [별지 제6호 서식]

✤ 휴대용 저장매체 관리대장 [별지 제1호~제2호 서식]

휴대용 저장매체 관리대장(일반용)

<관리책임자 : ○○○>

연번	관리번호 (시리얼번호)	매체형태	등록일자	취급자	불용처리일자	불용처리방법 (재사용 용도)	비고

✤ 휴대용 저장매체 점검대장 [별지 제3호 서식]

휴대용 저장매체 점검대장

<관리책임자 : ○○○>

점검일시	현 보유수량				이상 유무	점검자		비고 (서명)
	Ⅱ급	Ⅲ급	대외비	일반		성명	서명	

✤ 휴대용 저장매체(전산장비 포함) 반출·입 대장 [별지 제4호 서식]

휴대용 저장매체(전산장비포함) 반출·입 대장

<관리책임자 : ○○○>

장비명	관리번호 (시리얼번호)	담당자 (사용자)	용도	비공개 중요 자료 완전 삭제 확인 / 악성코드 감염 여부 확인	출입 일시 (입·출 구분)	확인

✤ 휴대용 저장매체 불용처리 확인서 [별지 제6호 서식]

휴대용 저장매체 불용처리 확인서

아래와 같이 휴대용 저장매체(종 점) 불용처리 및 휴대용 저장매체 (종 점) 재사용에 대해 확인을 요청함

연번	관리번호 (시리얼번호)	매체형태	사유	불용처리	재사용

확인일자 : 년 월 일
요 청 자 : 소속 · 직책 ○급 성명 : (인)
확 인 자 : 정보보안담당관 ○급 성명 : (인)

참고서류

▸ 서울특별시교육청 정보보안 기본지침 [부록3]「USB메모리 등 휴대용 저장매체 보안관리지침」

- 휴대용 저장매체 관리대장
- 휴대용 저장매체 점검대장
- 휴대용 저장매체(전산장비 포함) 반출·입 대장 관리
- 휴대용 저장매체 불용처리 확인서

관련규정

▸ **서울특별시교육청 정보보안 기본지침 제76조(휴대용 저장매체 보안)**
▸ **서울특별시교육청 정보보안 기본지침 [부록3]「USB메모리 등 휴대용 저장매체 보안관리지침」**

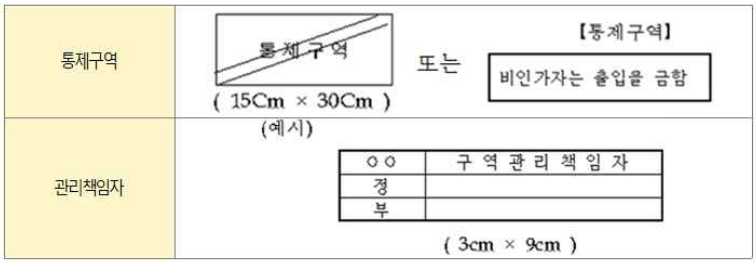
- 휴대용 저장매체 관리자는 휴대용 저장매체를 비밀용·일반용으로 구분·관리하고 수량 및 보관 상태를 정기적으로 점검하며 외부 반출·입을 통제하여야 함

진단항목 ❽ 전산장비 설치 장소 보안구역 지정 및 관리

진단방법

▸ **전산실 통제구역 표지 부착 및 이중 잠금장치 여부:** *O/X*

✤ 통제구역: 보안장비 설치구역, 전산실(주전산기 설치구역)



▸ **통제구역 출입통제 대장 작성 여부:** *O/X*

- 보안장비, 네트워크 장비 유지보수업체 정기점검 방문 시 등

☞ 통제구역인 전산실을 성적처리, 방송실 등과 공동사용 시 별도 출입통제 조치 필요

✤ 통제구역 출입통제 대장 관리 (교육부 보안업무규정 시행세칙 별지 제14호)

(서식) **통제구역 출입통제대장**

연월일	출입시간 퇴실시간	용무	출 입 자		입 회 자		비고 (서명)
			소속 (주소)	성명	직급	성명	

참고서류

▸ 통제구역 출입통제 대장 관리 (교육부 보안업무규정 시행세칙 별지 제14호)

관련규정

▸ **서울특별시교육청 보안업무 시행지침 제8조(정보보안감사 등)**
▸ **서울특별시교육청 정보보안 기본지침 제84조(정보통신시설 보호대책)~제85조(정보통신시설 출입관리)**

- 정보통신실 등 정보통신시설 및 장소는「보안업무규정」제34조에 따른 보호지역으로 지정·관리하여야 함

진단항목	❾ 디지털복합기 보안 관리

진단방법	참고서류
▸ **디지털복합기 기본암호 변경 여부:** *O/X* - 스캔파일 이메일 전송 설정 및 복합기 공유 폴더 설정 금지 ※ 기본암호 변경 방법은 유지보수 업체 및 제조사에 문의 ▸ **작업문서(복사, 스캔 등) 저장되지 않도록 설정 여부:** *O/X* ※ 설정방법은 유지보수 업체 및 제조사에 문의	

관련규정

▸ **서울특별시교육청 정보보안 기본지침 제20조(정보통신제품 도입), 제88조(디지털복합기 보안)**

- 복합기 내 저장매체가 있는 경우 자료 완전삭제 또는 디스크암호화 기능이 탑재된 기기 도입

진단항목	❿ 정보화사업 추진 시 누출금지정보 명시

진단방법	참고서류
▸ **정보화사업 용역계약서 또는 제안요청서에 누출금지정보 포함 여부:** *O/X* ✤ 사업대상 자체 홈페이지 유지보수 용역, 정보시스템 및 학내망 유지보수 등 ✤ 지침 제13조 제2항 누출금지정보 목록 1. 해당 기관의 정보시스템 내·외부 IP주소 현황 2. 정보시스템 구성 현황 및 정보통신망 구성도 3. 개별사용자의 계정·비밀번호 등 정보시스템 접근권한 정보 4. 정보통신망 또는 정보시스템 취약점 분석·평가 결과물 5. 정보화사업 용역 결과물 및 관련 프로그램 소스코드(외부에 유출될 경우 국가안보 및 국익에 피해가 우려되는 중요 용역사업에 해당) 6. 암호자재 및 정보보호시스템 도입·운용 현황 7. 정보보호시스템 및 네트워크장비 설정 정보 8. 「공공기관의 정보공개에 관한 법률」제9조제1항에 따라 비공개 대상 정보로 분류된 해당 기관의 내부문서 9. 「개인정보보호법」제2조제1호에 따른 개인정보 10. 「보안업무규정」제4조에 따른 비밀 및 「보안업무규정 시행규칙」 제16조제3항에 따른 대외비 11. 그 밖에 해당 기관의 장이 공개가 불가하다고 판단한 자료	▸ 정보화사업 제안요청서, 과업지시서 ▸ 정보화사업 용역계약서 ✤ 계약서(또는 과업지시서, 입찰공고)에 명시할 사항 - 인원·장비·자료 등에 대한 보안조치 사항 - 보안준수사항 위반 시 손해배상 책임 사항 - 누출금지 대상정보 및 부정당 업자의 제재조치 사항 - 참여인원 임의교체 금지 - 개인정보 처리 위탁 시 표준개인정보처리위탁 계약서 작성

관련규정

▸ **서울특별시교육청 정보보안 기본지침 제13조(제안요청서 기재사항)**

- 용역업체에 정보화사업을 발주하기 위하여 제안요청서를 작성할 경우 누출금지정보목록을 포함하여야 함

진단항목	⓫ 외부용역 정보화사업 관리

진단방법

▸ **외부용역 사업 수행 시 인수인계대장 작성 여부:** *O/X*

- 사업수행 시 업체에 자료(정보통신망도, IP현황, 개인정보 등) 제공 시 제공자료 인계인수 관리대장 작성
- 사업종료 시 업체에 제공한 자료 전량 회수 및 제공자료 인계인수 관리대장 기록

▸ **용역업체 보안교육 실시 여부:** *O/X*

- 사업수행 시 용역업체 보안교육 실시(업무 도움자료 관련 서식 활용)

▸ **보안서약서(참여인력) 및 확약서(대표자) 보관 여부:** *O/X*

- 사업착수 시 보안서약서 징구 ☞ 참여인력용
- 사업종료 시 보안확약서 징구 ☞ 대표자용

✤ 제공자료 인계인수 관리대장(예시)

제공자료 인계인수 관리대장 *(예시)*

□ 업무(사업) 개요
- 업무(사업)명 :
- 업무(사업)기간 : 20 . . . ~ 20 . . .

□ 인계 기관명_부서명(담당자명) : 서울특별시교육청_정보화담당관(홍길동)

□ 인수 기관명_부서명(담당자명) : ㈜한국정보보안(나정보)

□ 인계인수 확인

연번	인계 자료명	인계일	회수일	확인(서명) 친필서명		
				인계자	인수자	회수자
1	정보통신망 구성도	2019. 3. 8.	2020. 2. 28.	홍길동	나정보	홍길동
2	IP현황	2019. 3. 8.	2020. 2. 28.	김유신	너보안	김유신
3	·····					

참고서류

▸ 인수인계대장(예시 참조)
▸ 보안서약서(참여인력) [지침 서식제5호]
▸ 보안확약서(대표자) [지침 서식제6호]
▸ 보안교육 실시 증빙자료

관련규정

▸ **서울특별시교육청 정보보안 기본지침 제25조(계약 특수조건)~제26조(용역업체 보안), 제49조(정보시스템 유지보수)**

- 용역업체에 정보화사업 발주 시 보안준수사항 명시 및 이행여부 점검

정보보안 도움자료

서울특별시교육청
SEOUL METROPOLITAN OFFICE OF EDUCATION