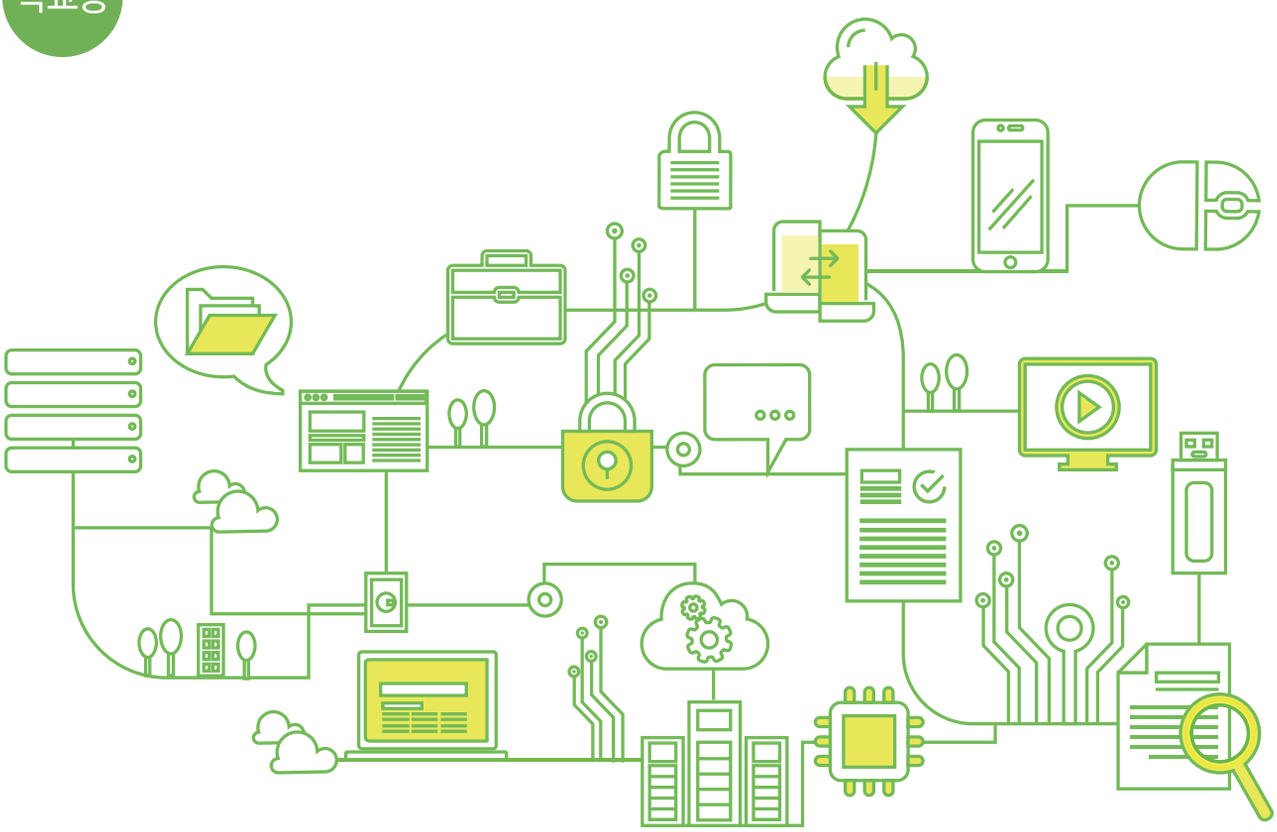
미래교육의 중심
새로운 경기교육
자율 균형 미래

경기도교육청 교육기관

정보보안 업무 매뉴얼

학교용



경기도교육청
GYEONGGIDO OFFICE OF EDUCATION

CONTENTS

제 1 장 정보보안 기본활동

1. 정보보안담당관 지정·운영 ····· 1
   참고 정보보안담당관 변경 지정 기안문(예시) ····· 2
2. 정보보안업무 추진계획 수립 ····· 3
   참고 정보보안업무 추진계획 수립·시행 기안문(예시) ····· 4
   참고 정보보호업무 추진계획(예시) ····· 5
3. 정보보안 감사 ····· 11
   참고 정보보안 감사 중점사항(예시) ····· 12
4. 정보보안 교육 ····· 13
   참고 정보보안 교육 실시 기안문(예시) ····· 14
   참고 정보보안 교육 실시 결과 보고 기안문(예시) ····· 15
5. 사이버보안진단의 날 지정·운영 ····· 16
   참고 사이버보안진단 실시 결과 보고 기안문(예시) ····· 17
6. 재난방지 대책 수립 ····· 19
   참고 재난방지 대책 수립 기안문(예시) ····· 20

제 2 장 정보보안 관리

1. 정보통신시설 보호대책 ····· 25
2. 정보통신시설 출입관리 ····· 27
   참고 보호구역 상시 출입인가자 기안문(예시) ····· 28
3. 개별사용자 단말기 보안관리 ····· 29
   참고 휴대용 저장매체 관리대장(일반용) ····· 32
   참고 휴대용 저장매체(전산장비 포함) 반출·입 대장 ····· 33
   참고 비업무 사이트 차단 및 접근 허용 절차 ····· 34
   참고 비업무 사이트 허용신청 기안문(예시) ····· 35
4. 홈페이지 게시자료 보안관리 ····· 37
   참고 학교홈페이지 운영 계획 수립 기안문(예시) ····· 38
5. 저장매체 불용처리 ····· 49
   참고 저장매체 삭제처리 확인서 ····· 51
   참고 저장매체 파기 계획 기안문(예시) ····· 52
   참고 저장매체 전용소자장비 이용 협조 요청 시행문(예시) ····· 53

6. 정보시스템 유지보수 및 용역사업 보안관리 ····· 55
참고 참여인원 보안서약서 ····· 58
참고 업체대표 보안서약서 ····· 59
참고 외부용역 업체직원 보안교육 ····· 60
참고 정보시스템 원격 접속 관리대장 ····· 61
참고 원격지 온라인 개발 서약서 ····· 62
참고 출입통제대장 ····· 63
참고 온라인 유지보수 서약서 ····· 64
참고 자료 인계인수 대장 ····· 65
참고 보안확약서(업체대표명의) ····· 66
7. 정보통신망 현황자료 관리 ····· 67
참고 정보시스템 관리대장 ····· 68
참고 정보통신망 세부 구성 현황(예시) ····· 69
8. 무선랜 보안 ····· 70
참고 무선인터넷 사용 시 주의 사항 ····· 71
9. 인터넷전화 보안 ····· 72
참고 학교 인터넷전화망 구성(예시) ····· 73
참고 인터넷전화망과 학내망이 혼용된 잘못된 사례 ····· 74
10. 영상정보처리기기 보안 ····· 75
11. 디지털 복합기 보안 ····· 76

제 3 장 안전성 확인

1. 보안성검토 ····· 77
참고 보안성 검토 요청 기안문(예시) ····· 80
참고 자체 보안성 검토 기안문(예시) ····· 81
참고 자체 보안대책(예시) ····· 82
참고 정보화사업 보안성 검토 체크리스트 ····· 88
2. 사이버침해사고 대응 ····· 94
참고 사이버침해사고 신고서(서식) ····· 96
참고 정보시스템(개인용 컴퓨터) 점검 매뉴얼 ····· 98

"학교 정보보안 연간 업무계획표"

연번 (페이지)	추진내용	업무시기	관련근거
1 (p.1)	정보보안담당관 운영 - 정보보안담당관 및 분임정보보안담당관 지정	정보보안 담당관 변경시	‣ 제5조(정보보안담당관 운영)
2 (p.3)	정보보안 활동계획(연간) - 정보보호업무 추진계획 수립(내부결재)	매년 3월~4월	‣ 제6조(연도 추진계획 수립)
3 (p.13)	정보보안 교육 - 정보보안 교육계획 수립 및 결과보고(내부결재)	학교 자체계획 (연1회 이상)	‣ 제9조(정보보안교육)
4 (p.16)	사이버보안진단의 날 운영 - 내PC지키미 프로그램 점검 및 취약점 조치 - 사이버보안진단의날 실시 일지 작성(내부결재)	매월 세 번째 수요일	‣ 제10조(사이버보안진단의 날)
5 (p.19)	재난방지 대책 - 정보통신망 재난방지대책 수립(내부결재)	시스템 도입 시	‣ 제89조(재난 방지대책)
6 (p.25)	정보통신시설 보안 - 정보통신실 및 전산관리실 보호구역 설정 - 보호구역 상시출입인가자 명부 관리 - 보호구역 출입통제대장 비치 및 기록유지	보호구역 설정 시 상시출입인가자 변경 시 상 시	‣ 제84조(정보통신시설 보호대책) ‣ 제85조(정보통신시설 출입관리)
7 (p.29)	개별사용자 단말기 보안관리 - PC등 단말기 항목별 보안대책 준수 - 접근단계별 비밀번호 설정	상 시 분기 1회	‣ 제71조(개별사용자 보안) ‣ 제72조(단말기 보안) ‣ 제74조(비밀번호 관리)
8 (p.37)	홈페이지 보안 - 학교홈페이지 관리·운영계획 수립(내부결재) - 학교홈페이지 게시판 담당자 지정(내부결재)	홈페이지 개편 시 게시판 담당자 변경 시	‣ 제68조(홈페이지 등 게시자료 보안)
9 (p.49)	저장매체 불용처리 - 정보시스템 불용처리 및 외부반출 시 보안조치 실시 - 저장매체(하드디스크) 완전삭제 계획 수립(내부결재)	저장매체 불용처리 및 외부반출 시	‣ 제59조(저장매체 불용처리)

연번 (페이지)	추진내용	업무시기	관련근거
10 (p.55)	정보시스템 유지보수 및 용역사업 보안관리 - 정보화사업 추진 시 자체 보안대책 (보안성검토) 실시 - 용역사업 참여 인력 보안관리	정보화사업 추진 시 유지보수 계약 시	‣ 제2장 정보화사업 보안 ‣ 제49조(정보시스템 유지보수)
11 (p.67)	정보통신망 현황자료 관리 - 정보통신망 세부 구성현황 비공개로 분류하여 관리	네트워크변경 또는 IP 변경 시	‣ 제69조 (정보통신망 현황자료 관리)
12 (p.70)	무선랜보안 - 교육목적 무선랜 구축 시 내부망과 분리	사안 발생시	‣ 제43조(무선랜 보안)
13 (p.72)	인터넷전화 보안 - 인터넷전화를 기관 내부망(업무망)을 제외하여 구축 권장	사안 발생시	‣ 제46조(인터넷전화 보안)
14 (p.75)	영상정보처리기기(CCTV 등) 보안 - CCTV에 대한 비인가자의 침입 통제 대책 강구 - 보안성검토 이행	사안 발생시	‣ 제86조(영상정보처리기기 보안)
15 (p.76)	디지털복합기 보안 - 자료 완전삭제 또는 암호화 기능 탑재된 복합기 도입 - 복합기 운영 보안대책 수립	도입 · 운영 시	‣ 제88조(디지털복합기 보안)
16 (p.77)	보안성 검토 - 보안성 검토 대상 정보화사업 계획단계 (사업공고전) - 보안성 검토의뢰 (자체보안심사위원회 생략)	사안 발생시	‣ 제14조~제19조
17 (p.95)	사이버침해 사고대응 - 학교별 통보 받은 후 5일 이내 조치결과 보고	사안 발생시	‣ 제103조(조치결과 통보)

제 1 장 정보보안 기본활동

1 정보보안담당관 지정·운영

관련근거

- 정보보안 기본지침 제5조(정보보안담당관 운영)

업무시기

- 정보보안담당관 및 분임정보보안담당관 변경 시

주요내용

- **효율적·체계적인 정보보안업무 수행을 총괄하는 정보보안담당관 지정·운영**
  - 정보보안담당관 : 정보보안업무를 담당하는 부서장
  - 분임정보보안담당관 : 학교장이 지정하며 미지정 시 부서의 장이 임명된 것으로 간주
    ※ 정보보호업무 추진계획 수립 또는 변경 시 정보보안담당관 및 분임정보보안담당관 지정 내용 포함

- **정보보안담당관 기본활동(요약)**
  - 정보보안 업무추진계획 수립·시행
  - 정보화사업 보안성 검토 및 보안적합성 검증 총괄
    ※ 검토시 상위기관과 협의 후 진행
  - 정보통신실, 정보통신망 현황자료 등에 관한 보안관리 총괄
  - 정보보안교육 총괄 및 '사이버보안진단의 날' 계획 수립·시행
  - 분임정보보안담당관 업무 감독
  - 그 밖에 정보보안과 관련한 사항

- **분임정보보안담당관 활동**
  - 정보보안담당관으로부터 위임받은 사항
  - 부서 내의 정보보안 업무와 관련한 사항

참고자료

- 정보보안담당관 변경 지정 기안문(예시)

참고자료 정보보안담당관 변경 지정 기안문(예시)

○ ○ 학 교

수신 내부결재
(경유)
제목 정보보안담당관 및 정보보안업무담당자 변경 지정

1. 관련: 경기도교육청 정보보안 기본지침 제5조(정보보안담당관 운영)

2. 효율적인 정보보안 업무추진을 위하여 정보보안담당관 및 분임정보보안담당관을 다음과 같이 변경 지정하고자 합니다.

가. 정보보안담당관 및 분임정보보안담당관 변경 지정

구분	직위	이름	비고
정보보안담당관	○○	○○○	정보보안 총괄
분임정보보안담당관	○○	○○○	부서 정보보안업무 담당
:	:	:	:
정보보안업무담당자	○○	○○○	업무담당자

나. 지정일: 20○○.○.○. (지정기간: ~ 정보보안 업무담당 해제 까지)
다. 정보보안담당관의 기본활동
1) 정보보안 업무추진계획 수립 · 시행
2) 정보화사업 보안성 검토 및 보안적합성 검증 총괄
※ 검토시 상위기관과 협의 후 진행
3) 정보통신실, 정보통신망 현황자료 등에 관한 보안관리 총괄
4) 정보보안교육 총괄 및 '사이버보안진단의 날' 계획 수립 · 시행
5) 분임정보보안담당관 업무 감독
6) 그 밖에 정보보안과 관련한 사항
라. 분임정보보안담당관의 기본활동
1) 정보보안담당관으로부터 위임받은 사항
2) 부서 내의 정보보안 업무와 관련한 사항
- 부서 사이버보안진단의 날 실시
- 부서 정보화사업 및 정보시스템 보안관리
- 소속 부서 개별사용자 단말기 보안 점검
- 기타 부서 내 정보보안 업무와 관련한 사항

2 정보보안업무 추진계획 수립

관련근거

- 정보보안 기본지침 제6조(연도 추진계획 수립)

업무시기

- 매년 3월 ~ 4월

주요내용

- **정보보안 및 개인정보보호 업무를 통합하여 정보보호 업무 추진계획 수립(내부결재)**

- **정보보호 업무 추진계획 수립시 포함되어야 할 사항**
  - 정보보안담당관 지정
  - 정보보안 업무 세부추진계획
  - 시스템 담당자 및 관리책임자 지정
  - 통제구역/제한구역 상시출입 인가자 지정
  - 시스템별 기술지원업체 비상연락망
  - 개인정보보호 업무 세부추진계획
  - 사이버침해대응 절차

참고자료

- 정보보호 업무 추진계획 수립 기안문(예시)

참고자료 정보보호업무 추진계획 수립·시행 기안문(예시)

기안문

○ ○ 학 교

수신 내부결재
(경유)
제목 20○○년도 정보보호업무 추진계획 수립·시행

1. 관련: 경기도교육청 정보보안 기본지침 제6조(연도 추진계획 수립)

2. 20○○년도 정보보호 업무 추진계획을 [붙임]과 같이 수립 · 시행하고자 합니다.

붙임 20○○년도 정보보호 업무 추진계획(안) 1부. 끝.

★담당자 부장 교감 교장

협조자

( ) 접수 ( )

우 00000 경기도 00시 00구 00로 00 (00동, 000) /
전화번호 031- /팩스번호 031- / / 비공개

참고자료 정보보호 업무 추진계획(예시)

붙임

○○학교 ○○년도 정보보호 업무 추진계획(예시)

(※학교실정에 맞게 수정하여 사용)

1. 목표

정보보안 및 개인정보보호 활동 전반에 대한 추진계획을 수립하여, 정보보호 활동을 강화함으로써 교육기관의 안전한 사이버 환경 조성

2. 기본방침

가. 정보시스템 관리 운영
나. 업무용PC 보안 강화
다. 정보통신시설 보안관리
라. 정보보안 및 개인정보보호 교육 실시
마. 정보보안 및 개인정보보호 사고 대응

3. 정보보안 활동

가. 정보보안담당관 지정

구분	직위	이름	비고
정보보안담당관	00	000	정보보안 총괄
분임정보보안담당관	00	000	부서 정보보안업무 담당
분임정보보안담당관	00	000	부서 정보보안업무 담당
정보보안담당자	00	000	업무담당자

나. 정보보안담당관의 기본활동

1) 정보보안 업무추진계획 수립 · 시행
2) 정보화사업 보안성 검토 및 보안적합성 검증 총괄
※ 검토시 상위기관과 협의 후 진행
3) 정보통신실, 정보통신망 현황자료 등에 관한 보안관리 총괄
4) 정보보안교육 총괄 및 '사이버보안진단의 날' 계획 수립 · 시행
5) 분임정보보안담당관 업무 감독
6) 그 밖에 정보보안과 관련한 사항

다. 정보보안 세부 활동

구분	세 부 추 진 계 획	비고
정보보호교육	가. 상반기 : oo년 o월 교직원 교육 (교육자료, 동영상교육, 온라인교육) 나. 하반기 : oo년 o월 교직원 교육 (교육자료, 동영상교육, 온라인교육) ※ 모든 공무원은 연1회 교육이수, 정보보안담당자는 연간15시간 교육 이수	
사이버보안진단의 날 운영	가. 대상 : 학교 내 모든PC(학생용PC 제외) 나. 진단방법 : ‘내PC지키미’를 실행하여 보안취약점 점검 및 제거 다. 결과보고 : 사이버보안진단의 날 실시 결과 보고 (사이버보안진단의 날 실시 일지)	[참고] 월별중점 사항 추진
PC등 보안관리	가. 관리자 및 사용자 지정 나. 숫자·문자·특수문자 등을 혼합하여 안전한 비밀번호 설정 - 주기적으로 변경 다. 화면보호기설정, 최신 백신S/W설치, 공유폴더 해제 라. 운영체제, 응용SW에 대한 최신 보안패치 유지 마. 수신된 전자우편 첨부파일을 다운로드할 경우 백신 소프트웨어로 악성코드 은닉여부 검사 바. 출처, 유통경로 및 제작자가 불분명한 응용프로그램의 사용 금지	
자료보안	가. 비공개 업무자료를 처리할 때에는 업무망 PC 및 서버에 작성 및 저장·보관 나. 비공개 업무자료를 전송해야 할 때는 공직자통합메일, 경기교육통합메신저(GOE)를 이용하여 전송 다. 소속 교직원들은 홈페이지에 비공개 업무자료가 무단 게시되지 않도록 주기적으로 점검 라. 정보통신망 구성현황(IP주소 할당현황 포함), 정보시스템 운용현황, 취약점 분석결과, 주요 정보화사업 추진현황은 비공개 대상 정보로 지정·관리	
외부용역업체 보안관리	가. 구비서류 - 용역 참여인원(대표자 포함) 보안서약서(사업 수행 시) - 용역 참여인원 보안교육(사업 수행 시) - 용역업체 대표자 명의 보안확약서(사업종료 시) - 온라인 유지보수 서약서(필요 시) 나. 유지보수 일시 및 담당자 인적사항, 출입통제 조치사항, 작업수행 내용 등 기록 유지 다. 유지보수와 관련한 노트북, USB등 전산장비 반출·입 시 악성코드 감염여부 및 자료 무단 반출여부 확인 등 보안조치를 실시하고 그 결과를 (분임)정보보안담당관에게 보고	
정보보안 사고대응	가. 사이버 공격에 대비한 초동 조치 - 사고 PC 인터넷회선 분리 - PC 종료 금지 및 보존 나. 사이버침해대응 절차에 따라 정보보안담당관 및 경기교육사이버안전센터에 신고	
정보시스템 저장매체 불용처리	가. 정보시스템(PC, 서버 등)을 교체, 폐기, 수리 등 기관 외부로 반출 시 저장매체에 보관된 자료의 삭제 나. 폐기, 고장 수리, 저장자료 복구 등 외부 의뢰 시 보안서약서 징구, 보안교육 등 보안조치를 강구하고 정보보안담당관의 통제를 받음 다. 불용처리, 외부 반출시 시스템 외부의 사용자 인식 표시물 (사용기관, 부서, 사용자 등)을 모두 제거	

구분	세 부 추 진 계 획	비고
무선랜 보안관리	가. 교육(수업) 목적으로 무선인터넷망 구축 시 반드시 업무망(교사망)과 분리 (논리/물리) 나. 무선인터넷망에서 업무자료를 저장·이용하는 컴퓨터(노트북) 사용 금지 다. 사용자 인증 비밀번호 설정	
디지털복합기 보안관리	가. 자료 완전삭제 또는 디스크 암호화 기능이 탑재된 복합기를 도입 나. 정기적으로 저장된 작업 내용(출력·스캔 등) 완전 삭제 다. 공유 저장소 사용 제한 및 접근 제어 라. 고정 IP주소 설정 및 불필요한 서비스 제거 마. 폐기·외부반출 시 저장자료 완전삭제 바. 유지보수 시 부서 분임정보보안담당관 입회·감독 하에 작업 실시 사. 교직원망과 학생망간 복합기를 공용으로 사용하지 않도록 조치	임대장비 포함
주요 정보통신 시설 관리	가. 정보통신시설 및 장소 통제구역 설정 - 통제구역 표찰 게시, 상시출입인가자 명부 비치 및 출입통제대장 기록 - 출입문에 이중 잠금장치 설치 나. 시스템 관리자 및 관리책임자 지정, 라벨 부착 다. 네트워크 구성도 및 IP 현황은 비공개자료로 관리 라. 홈페이지 등 공개서버 관리 - 내부망과 분리된 DMZ구간에 홈페이지 서버 설치(자체서버 구축 시) - 사용자 접근권한은 업무에 따라 차등 설정·관리 - 비공개 업무자료 무단 게시 금지, 개인정보 유출 등 수시 점검 - 관리자용 서비스 접속 시 특정 IP주소가 부여된 관리용 단말기 지정·운용 마. 시스템의 주기적 점검 - 비인가자에게 불필요한 서비스 허용 금지 - 시스템 접근자료(log) 1년 이상 보관 - 서버 설정 정보 및 저장자료에 대한 정기적 백업 실시	

라. 통제구역/제한구역 상시출입 인가자 지정

기준일:20○○.3.1.

연번	직위(급)	성 명	통제/제한구역	비고(담당업무)
1	교장	박○○	정보통신실	업무총괄
2	정보부장	김○○	정보통신실	정보보안담당관
3	교사	이○○	CCTV 통제실	분임정보보안담당관
4	교사	정○○	정보통신실	시스템관리책임자
5	행정실무사	최○○	정보통신실 CCTV 통제실	시스템관리자

※ 학교 교직원만 상시출입자로 지정함

마. 시스템 담당자 및 관리책임자 지정

시스템별 관리자 및 관리책임자

○○학교

연번	소속	취급자 성명	종류 (PC 등)	제조사	모델명	관리번호	도입일자	관리자 확인	비고
1	000	교사 000	정보보호 시스템	000	000	S-01	2022.5.19.	교사 000	스쿨넷 장비
2	000	교사 000	L2보안스위치	000	000	N-01	2022.5.19.	교사 000	스쿨넷 장비
3	000	행정 실무사 000	L2스위치	000	000	N-02	2022.5.19.	교사 000	스쿨넷 장비
4	000	주무관 000	UPS	· · ·			2016.12.19		학교 장비
	· · ·	· · ·	· · ·						

※ 학내망 유지보수장비 내역 작성 시 참고

바. 시스템별 기술지원업체 비상연락망

연번	시스템 및 장비명	기술지원협력 업체			비고
		소속	담당자	연락처	
1	스쿨넷장비				콜센터 전화번호
2	네트워크스위치				
3	PC 및 사무기기				
4	홈페이지관리				
· · ·	· · ·	· · ·			

4. 개인정보보호 활동

구분	세 부 추 진 계 획	비고
개인정보보호교육 실시	가. 개인정보취급자 교육(전직원) : oo년 o월 나. 신규채용, 전입자교육 : 사안 발생 시 다. 개인정보 처리 위탁 계약 체결 시 수탁사 교육 및 점검 실시	
개인정보 유·노출 예방활동	가. 업무용 PC 등에 보관된 개인정보파일을 검출하여 암호화 및 파기 등 보안조치(개인정보보호 솔루션(Privacy-i)을 이용) 나. 매월 '사이버보안진단의 날' 학교별 자체 홈페이지 게시글 및 첨부파일에 대한 개인정보 노출점검 실시	
개인정보파일 일제정비 및 개인정보처리방침 정비 실시	가. 행정안전부 개인정보보호종합지원시스템 (https://intra.privacy.go.kr)에 등록된 기관별 개인정보파일 현행화 나. 개인정보파일 전수조사를 통해 개인정보파일 등록 및 보유기간 경과된 개인정보파일의 파기 다. 개인정보파일 정비 결과를 홈페이지 내 개인정보처리방침에 반영	
개인정보 안전성 확보조치 준수사항 점검	가. 관리적 조치 - 내부관리계획 수립 및 개정 - 내부관리계획 이행실태 점검 나. 기술적 조치(개인정보처리시스템) - 접근권한 관리, 접근통제, 암호화, 접속기록 보관 및 점검, 백신 소프트웨어 설치, 관리용 단말기 안전조치 등 다. 물리적 안전조치 - 잠금장치가 있는 안전한 장소에 보관 - 정보통신실, 자료보관실 등은 출입통제 절차를 수립·운영	
개인정보 유출 시 조치 대응	가. 유출 시 - 정보주체에게 개인정보 유출사실 통지(5일 이내) 및 교육지원청을 경유하여 도교육청으로 보고 - 피해 최소화를 위한 긴급조치 수행 (접속경로 차단, 취약점 점검·보완, 삭제처리 등) - 유출원인 보완 및 재발방지 조치계획 수립·이행 - 개인정보취급자(전직원) 대상 사례 전파 및 재발방지 교육 - 그 밖에 개인정보의 유출 방지를 위해 필요하다고 판단되는 사항	

5. 사이버침해대응 절차

경기교육사이버안전센터(GECSC)		학교	
1. 사고 탐지	2. 사고 분석 및 초기대응	3. 초동조치 및 사고대응	4. 후속조치
◦ 침해사고 탐지 - 자체 탐지 (실시간 보안관제) - 사고 이관 (국정원, 교육부) ◦ 침해사고 신고접수 - 학교에서 사이버침해사고 특이징후 포착 시 신고 (☏031-240-6599)	◦ 사고 유형 분석 - DDoS 공격, 웹해킹, 웜·바이러스 등 ◦ 침해사고 통보 - 경미사안은 자체종결 - 침해 사고기관에 통보(각급학교는 교육지원청에 통보) ◦ 보안권고문 전파 - 공격자 IP, 피싱사이트 차단 등	◦ 초동조치 - 침해사고 시스템 (서버, 업무용PC 등) 네트워크 분리 ◦ 사고대응 - 백신 검사·치료, 포맷 등 ※사이버안전센터기술지원 (☏031-240-6599) - 웹방화벽 등 로그 분석 - 필요시 현장방문지원	◦ 조치완료 - 5일이내 처리 (주요침해사고는 2일이내 처리) - 침해사고 조치 결과 보고 (goeboan@korea.kr) ※ 사이버침해사고 조치보고서 제출 ※ 해킹 사고의 경우 재발방지 대책 수립

3 정보보안 감사

관련근거

- 정보보안 기본지침 제8조(정보보안 감사 등)

업무시기

- 지도감독기관의 보안감사 계획에 따름

주요내용

- **정보보안업무 전반에 걸쳐 정보보안 감사를 실시하며, 감사주기는 다음과 같다.**
  - (공립)단설유치원, (공·사립)초·중·고·특수학교 : 4년
- **정보보안 감사 중점사항은 감사시행일 이전 감사계획에 의거 해당 학교로 안내**
- **감사 대비 준비사항은 정보보안 감사 중점사항 참고**

참고자료

- 정보보안 감사 중점사항(예시)

참고자료 정보보안 감사 중점사항(예시)

1. 정보보안
   가. 정보보안담당관 및 정보보안담당자 지정 현황
   나. 연도별 정보보안 추진계획 수립 여부
   다. 연도별 정보보안 교육 실시 여부
   라. 재난방지 대책 수립 여부
   마. ‘사이버보안진단의 날’ 수행
      - 매월 사이버보안진단의 날 실시 및 일지 기록 여부
      - 모든 PC(학생용PC 제외)에 대해 실시 및 내PC지키미 수행 완료(점검항목: 안전) 여부
   바. 정보화사업 추진 내역
   사. 사이버 침해사고 발생/조치 현황

2. 개인정보보호
   가. 개인정보 보호책임자 지정 현황
   나. 영상정보처리기기(CCTV) 책임자 지정 현황
   다. 개인정보 파일 등록 현황
   라. 내부관리 계획 수립 및 이행점검
   마. 개인정보 처리방침 수립 및 홈페이지 공개(현행화) 여부
   바. 영상정보처리기기 운영 · 관리 방침 수립 및 홈페이지 공개(현행화) 여부
   사. 연도별 개인정보보호 교육 실시 여부
   아. 개인정보의 안전성 확보 조치

3. 홈페이지 운영
   가. 홈페이지 담당자 지정 현황
   나. 홈페이지 안전성 조치 여부(자체운영교)
   다. 홈페이지 운영지침 수립·시행 여부
   라. 게시판별 담당자 지정 및 게시글(자료실) 개인정보 노출 점검 주기적 실시

4 정보보안 교육

관련근거

- 정보보안 기본지침 제9조(정보보안교육)

업무시기

- 학교별 자체 계획에 의거(연 1회 이상)

주요내용

- **정보보안 교육계획을 수립하여 연1회 이상 소속 전 교직원을 대상으로 실시**
  - 전교직원은 연1회 이상 정보보안 교육을 이수하여야 함(온라인 교육 포함)
  - 교육실시에 대한 증빙자료 확보(교육계획, 실시결과(교육자료/등록부/사진) 내부결재)

- **정보보안담당자는 연간 15시간 이상 정보보안 교육을 이수하여야 함**
  - 개인정보보호 교육을 포함하여 15시간 이수
  - 교육부 정보보호교육센터(http://sec.keris.or.kr) 등 활용

참고자료

- 정보보안 교육 실시 계획 기안문(예시)
- 정보보안 교육 결과 보고 기안문(예시)

참고자료 **정보보안 교육 실시 기안문(예시)**

○ ○ 학 교

수신 내부결재
(경유)
제목 20○○년 정보보안 교육 실시

1. 관련
   가. 경기도교육청 정보보안 기본지침 제9조(정보보안교육)
   나. ○○교-0000(20○○.○.○.)호 『○○년도 정보보호업무 추진계획』

2. 정보보안에 대한 경각심 제고 및 보안의식 강화를 위해 20○○년 정보보안 교육을 아래와 같이 실시하고자 합니다.
   (※정보보호 업무 추진계획 중 정보보안 교육계획 수립 시 교육대상, 내용, 일정, 방법 등을 포함하여 수립한 경우 본 공문별도 기안 불필요)

   가. 교육일시: 20○○.○○.○○.(월) 00:00~00:00
   나. 교육장소: ○○○○
   다. 교육대상: 교직원 전체
   라. 교육내용(예시)
      - PC 보안, 전자우편 보안, 비업무 사이트 접속 금지, 사이버공격 대응 요령
      - 중요자료 파일 관리 요령
      - 내PC지키미 점검 및 조치 방법 안내
      - 기타 정보보안 중점사항
   마. 교육자료: 붙임

붙임 20○○년도 정보보안 교육자료 1부. 끝.

★담당자 부장 교감 교장

협조자

( ) 접수 ( )

우 00000 경기도 00시 00구 00로 00 (00동, 000) /
전화번호 031- /팩스번호 031- / / 비공개

참고자료 정보보안 교육 실시 결과 보고 기안문(예시)

○ ○ 학 교

수신 내부결재
(경유)
제목 20○○년 정보보안 교육결과 보고

1. 관련: ○○학교-○○○(20○○.○.○.)호

2. 20○○년 전 직원 대상 정보보안 교육결과를 아래와 같이 보고하고자 합니다.

가. 교육일시: 20○○.○○.○○.(월) 00:00~00:00
나. 교육장소: ○○○○
다. 참석자/대상자: 교직원 45/50명([붙임]등록부 및 사진 참조)
※출장:2명, 연가:3명
라. 교육내용
- PC 보안, 전자우편 보안, 비업무 사이트 접속 금지, 사이버공격 대응 요령
- 중요자료 파일 관리 요령
- 내PC지키미 점검 및 조치 방법 안내
- 기타 정보보안 중점사항
마. 기타
- 미참석자는 교육자료 배포 및 별도 교육실시

붙임 1. 정보보안 교육실시 결과(등록부 및 사진) 1부.
2. 정보보안 교육자료 1부. 끝.

★담당자 교감 교장

협조자

( ) 접수 ( )

우 00000 경기도 00시 00구 00로 00 (00동, 000) /
전화번호 031- /팩스번호 031- / / 비공개

5 사이버보안진단의 날 지정·운영

관련근거

- 정보보안 기본지침 제10조(사이버보안진단의 날)

업무시기

- 매월 세 번째 수요일에 실시

주요내용

- **매월 세 번째 수요일을 '사이버보안진단의 날'로 지정 운영함**

- **'사이버보안진단의 날 실시 일지'를 작성하여 실시 결과 보고(내부결재)**
  ※ 내PC지키미 프로그램을 이용하여 모든 PC 보안점검을 실시하고 모든 점검항목에 대한 점검결과가 "안전"이 되도록 취약점 제거(정보보안 감사 중점사항)

참고자료

- 사이버보안진단 실시 결과 보고 기안문(예시)

참고자료 사이버보안진단 실시 결과 보고 기안문(예시)

기안문

○ ○ 학 교

수신 내부결재
(경유)
제목 20○○년 ○월 사이버보안진단의 날 실시 결과

1. 관련: 경기도교육청 정보보안 기본지침 제10조(사이버보안진단의 날)

2. 본교 업무용 PC사용에 대한 보안진단 등 보안관리 실태를 종합적으로 점검하기 위해 실시한 "사이버보안진단의 날" 실시 결과를 아래와 같이 보고합니다.

가. 점 검 일: 20○○년 ○월 ○일
나. 점검대상: 교내 전체PC(학생용PC 제외) ○○대
다. 점검방법: "사이버보안진단의 날" 실시 일지에 따른 상세점검
라. 점검결과: 이상 없음(세부내역 붙임참조)
마. 특이사항
- 업무용PC ○대 OS보안업데이트 불가로 인하여 미조치(포맷예정)

붙임 20○○년 ○월 사이버보안진단의 날 실시 일지 1부. 끝.

★담당자 부장 교감 교장

협조자

( ) 접수 ( )

우 00000 경기도 00시 00구 00로 00 (00동, 000) /
전화번호 031- /팩스번호 031- / / 비공개

붙임

20○○년 ○월 “사이버보안진단의 날” 실시 일지(예시)

□ 실시일자 : 20○○년 ○월 ○일(수요일)

실 태 점 검 항 목		점 검 결 과(예시)
정보보안 및 개인정보	정보보안(개인정보보호) 교육 실시	- 실시여부: 실시 - 방법: 예)집합, 유인물 등
	홈페이지 게시판 개인정보 노출여부 점검	- 노출내용: - 노출건수 : 0건
	개인정보보호솔루션(Privacy-i) 시행 여부 점검	- 이상 없음
	개인정보파일 파기 사실 여부	- 파기여부: 없음 - 파기내용 :
	자체 보유중인 PC는 모두 몇 대입니까?	- 전체 PC : 50대
	내PC지키미 실행 완료(모든 점검항목 안전) PC는 몇 대입니까?	- 실행 PC : 50대
	PC 부팅(CMOS)/로그인 비밀번호 및 화면보호기 설정 여부	- 설정 PC : 50대
	공유폴더 삭제 여부 점검	- 이상 없음
정보 시스템	정보보호시스템 및 네트워크 장비 보안점검 - 원격차단, 관리자 IP·MAC 접근 등 관리	- 이상 없음
	정보시스템 용역 참여인원 보안점검 - 별도계정개설, 접근권한, 원격작업승인 등 관리	- 이상 없음
	정보시스템 보안 취약요소 점검 - 불필요한 포트제거, 불필요 계정삭제 등 관리	- 이상 없음
기타	내PC폰트 점검 여부	- 실행 PC : 50대 - 점검결과 : 이상 없음
	홈페이지 게시판 게시물 폰트 점검 여부(게시자 점검)	- 점검여부 : 이상 없음
중점 점검 사항	[예시] ○ 정보시스템 및 장비 현황 점검(관리대장) ※ 사이버보안진단의 날 월별중점 추진사항 참조 (*학교 (자체)정보보호추진* 계획에 따름)	- 이상 없음

※ 본 일지는 예시이므로, 학교 실정에 맞게 수정하여 사용

6 재난방지 대책 수립

관련근거

- 정보보안 기본지침 제89조(재난 방지대책)

업무시기

- 최초 재난방지 대책 수립 후 정보통신망 또는 정보시스템의 변경사항 발생 시 재수립

주요내용

- **인위적 또는 자연적인 원인으로 인한 정보통신 장애 발생에 대비하여 종합적인 재난방지 대책을 수립·시행함**

- **재난방지 대책 수립 시 포함되어야 할 내용**
  - 재난대응조직구성
  - 시스템별 책임자 및 담당자 지정
  - 재난별 시스템 조치 사항(시스템별 기동절차/유지보수 업체 연락처)
  - 기타 재난대비에 필요한 사항

참고자료

- 재난방지 대책 수립 기안문(예시)

참고자료 **재난방지 대책 수립 기안문(예시)**

기안문

○ ○ 학 교

수신 내부결재
(경유)
제목 재난 방지대책 수립(안)

1. 관련: 경기도교육청 정보보안 기본지침 제89조(재난 방지대책)

2. 인위적 또는 자연적인 원인으로 인한 정보통신망 장애 발생에 대비하여 [붙임]과 같이 종합적인 재난 방지대책(안)을 수립하고자 합니다.

붙임 재난 방지대책(안) 1부. 끝.

★담당자 부장 교감 교장

협조자

( ) 접수 ( )

우 00000 경기도 00시 00구 00로 00 (00동, 000) /
전화번호 031- /팩스번호 031- / / 비공개

붙임

정보통신망 재난방지대책(예시)

(※학교실정에 맞게 수정하여 사용)

Ⅰ 목적 및 근거

1. 추진목적

◦ 현재 우리학교에서 운영·관리하고 있는 정보통신망의 인위적 혹은 자연적인 원인으로 인한 장애 발생에 대비한 재난방지대책을 마련·시행함으로써,
- 장애 발생으로 인한 업무지연을 최소화 하고,
- 장애발생 및 자료의 손실 시 신속한 복구 체계를 확보하며,
- 정보의 위·변조에 대비하고자 함

2. 관련근거

◦『경기도교육청 보안업무 시행요령』(경기도교육청, 2000.00.)
◦『경기도교육청 정보보안 기본지침』(경기도교육청, 2000.00.)

Ⅱ 보호대상

◦ 네트워크 및 정보통신망 관련 장비
◦ PC 및 정보시스템 하드웨어 및 소프트웨어
◦ 주요 시스템 내의 자료 및 로그 자료(접근, 작업내역 포함) 등

Ⅲ 세부대책

1. 관리적 보호대책

가. 재난대응조직(보안관리 수행체계)

구 분	소속	직위(직급)	성명	임 무
정보보안담당관				재난대응반 업무 총괄
분임정보보안담당관				재난에 대한 정보 수집, 상황관리 및 조정
OO시스템 관리책임자				재난의 상황분석 및 시스템복구 총괄
OO시스템 관리자				담당 전산시스템 복구

※ 인사이동 등으로 인한 변경이 있을 경우에는 전임자가 편성된 반으로 자동 편성

1) 보고절차 : 시스템관리자→시스템관리책임자→정보보안담당관

2) 보고내용

- 재난발생 일시·장소
- 사고원인 및 피해 현황 등 개요
- 사고자 및 관계자의 인적사항
- 조치내용 등

나. 장비(시스템) 관리자 및 관리책임자 지정・운영

시스템별 관리자 및 관리책임자

○○학교

연번	소속	취급자 성명	종류 (PC 등)	제조사	모델명	관리번호	도입일자	관리자 확인	비고
1	OOO	교사 OOO	정보보호 시스템	OOO	OOO	S-01	2022.5.19.	교사 OOO	스쿨넷장비
2	OOO	교사 OOO	L2보안스위치	OOO	OOO	N-01	2022.5.19.	교사 OOO	스쿨넷장비
3	OOO	행정실무사 OOO	L2스위치	OOO	OOO	N-02	2022.5.19.	교사 OOO	스쿨넷장비
4	OOO	주무관 OOO	UPS	⋮			2016.12.19		학교 장비
	⋮	⋮	⋮						

다. 유지관리 체계

1) 신속한 복구를 위한 전문 기술지원(유지관리) 체계 구축

2) 유지보수 비상연락망

연번	시스템 및 장비명	기술지원협력 업체			비고
		소속	담당자	연락처	
1	스쿨넷장비				콜센터 전화번호
2	네트워크스위치				
3	PC 및 사무기기				
…	…	…			

2. 물리적 보호대책

가. 정보통신실 출입통제

1) 정보통신실 보호지역(**통제구역**) 지정・운영

2) 정보통신실 출입구 통제 단일화하고 이중 잠금장치 설치

3) 비인가자의 통제구역 출입 시 출입통제 대장 작성

나. 전력관리대책

- 정전에 대비한 비상전원 공급 : 무정전전원공급장치(UPS) 운영(권고)
- 대상장비 : 전화, 서버, 통신장비 등

다. 방화대책

- 소화기 설치・운영

라. 시설자료 관리대책

- 전화선, 전력선, 통신회선 등 설비도면을 최신으로 유지・관리

마. 물품 반출・입 관리대책

1) 정보통신실로 반출・입 되는 물품을 통제・허가하고 기록 유지

2) 카메라 장착 휴대폰 등을 이용한 **불법 촬영 금지**

3. 기술적 보호대책

가. 서버 보안대책 (※자체 운영 서버가 없는 경우 제외)

1) 서버 내 저장자료에 대하여 업무별・자료별 중요도에 따라 **개별사용자의 접근권한 차등 부여**

2) 개별사용자별 자료 접근범위를 서버에 등록하여 인가여부를 식별하도록 하고 인가된 범위 이외 **자료 접근통제**

3) 서버 운용에 필요한 서비스 포트 이외 불필요한 서비스 포트 제거, 관리자용 서비스와 개별사용자용 서비스 분리・운용

4) 관리자용 서비스 접속 시 특정 IP주소가 부여된 관리용 단말기 지정・운용

5) 서버 설정 정보 및 저장자료에 대한 정기적 백업 실시

6) 데이터베이스에 대하여는 개별사용자의 직접 접속 차단, **개인정보 등 중요정보 암호화** 등 데이터베이스별 보안조치 실시

7) 시스템별 **주기적인 보안패치 및 백신프로그램 업데이트 실시**

8) 시스템별 **숫자・문자・특수문자 등을 혼합하여 9자리 이상** 비밀번호 설정, **분기별 변경** 운영

9) 시스템 로그, 접근기록, 작업내역 등 **1년 이상** 기록・관리

10) 주요 시스템에 대한 백업 대책을 마련하여 정기적으로 백업 수행

나. 정보보호시스템・네트워크 보안대책

1) 외부 정보통신망에서의 원격 접속 금지

2) 최초 설치 시 기본계정은 삭제 또는 변경하고 관리를 위한 별도계정 생성・운영

3) 불필요한 서비스 포트와 개별사용자 계정은 차단 및 삭제

4) 시스템 보안 취약점 및 최신버전 업데이트 여부를 정기적으로 점검

5) 로그기록을 1년 이상 유지하고, 비인가자 접속여부를 정기적으로 점검

다. 사이버 침해사고 발생 시 대응절차

1) 피해시스템 네트워크 분리 후 경기교육사이버안전센터에 신고

2) 경기교육사이버센터와 연계하여 사고원인 및 공격근원지 파악

3) 백업자료 복원설치 등 피해복구, 운영 정상화

라. PC 보안

1) 교내 모든PC(학생용PC 제외)에 **“내PC지키미” 설치**

2) 매월 세번째 수요일 “사이버보안진단의 날”에 실행·점검하여 **안전 조치**

※ 기타 학교 전산망 및 시스템을 보호하기 위해 필요한 사항 작성

제2장 정보보안 관리

1 정보통신시설 보호대책

관련근거

- 정보보안 기본지침 제84조(정보통신시설 보호대책)

업무시기

- 정보통신시설 구축 또는 보호지역(통제구역, 제한구역) 관리책임자 변경 시

주요내용

- **정보통신실(전산기계실) 및 전산관리실은 보호구역으로 설정 관리**
  - 경기도교육청 보안업무시행요령 제59조(보호지역 지정)⑦항에 의거하면 전산기계실(주전산기 설치구역 및 자료보관실)은 보호구역의 중요도에 따른 분류에 따라 통제구역으로 지정되어야 함(※전산관리실은 제한구역으로 설정하며, 정보통신실과 전산관리실의 구분이 없을 경우 통제구역 설정)

- **보호지역 설정에 따른 표찰 게시**

(예시-1) 전산관리실	정보통신실(전산기계실)
 (세로 15㎝ × 가로 30㎝)	 (세로 15㎝ × 가로 30㎝)

(예시-2) 전산관리실	정보통신실(전산기계실)
관계직원외 출입을 금함 (세로 10㎝ × 가로 30㎝)	비인가자는 출입을 금함 (세로 10㎝ × 가로 30㎝)

- **보호지역 관리책임자는 동시설(정보통신실 및 전산관리실)을 관리하는 부서의 장 또는 부서의 장이 지정한 자**

(예시-3) 제한구역 및 통제구역 모두 표시

○○	구 역 관 리 책 임 자
정	
부	

(세로 3㎝ × 가로 9㎝)

- **보호지역 보호대책 수립 시 고려사항**

구 분	보 호 대 책	비 고
출입통제	◦ 정보통신시설의 출입이 허가되는 출입자 명부를 작성・비치 ◦ 방문자 등 외부 인력에 대한 신분확인 및 위해 물품 반입 점검 ◦ 담당자는 외부 인력과 동행하여 활동을 감시하고, 퇴실 시 불법적인 정보 및 정보시스템 반출을 검사 ◦ 통제구역 출입자 관리대장을 비치하고 출입 기록을 주기적으로 점검	
전력관리	◦ 전원공급 중단에 대비하여 무정전전원공급장치(UPS)를 설치하고 정기적으로 점검(권고) ◦ 갑작스런 전원공급 중단으로 인한 정보시스템 파손을 방지하기 위하여 자동 셧오프 기능을 설치 ◦ 비상출구 및 대피경로에 비상조명을 설치하여 전원 중단에 대비	
항온・습	◦ 항온・항습기 등을 설치하고 정기적으로 정비 및 점검(권고)	
물품 반출・입	◦ 정보보안담당관은 정보통신시설 내로 반입 또는 외부로 반출되는 물품을 통제・허가하고 기록을 유지 (반출・입자 성명 및 소속, 반출・입 시간, 물품, 사유 등)	
수해방지	◦ 마스터 잠금 밸브를 설치하여 수도관 파손 또는 기타 누수원으로 인해 발생하는 수해를 방지	
시설자료관리	◦ 네트워크회선, 전화선, 전력선, 통신회선 등의 설비도면을 최신으로 유지・관리	
기타	◦ 휴대용 저장매체를 보관할 수 있는 용기 비치 ◦ 상시 이용하는 출입문은 한 곳으로 정하고 이중 잠금장치 설치 ◦ 카메라 장착 휴대폰 등을 이용한 불법 촬영 방지 등	

2 정보통신시설 출입관리

관련근거

- 정보보안 기본지침 제85조(정보통신시설 출입관리)

업무시기

- 보호지역(통제구역, 제한구역) 관리책임자 변경 시

주요내용

- **상시출입인가자 명부**
  - 명단 변경 시 마다 내부결재 후 출입 통제 대장과 함께 비치 관리
  - 출입 통제 대장 맨 앞장에 철하여 운영(권고)

- **신원을 확인하고 보안교육 및 보안 검색 후 출입을 허용**

- **출입 통제 대장을 비치하여 상시출입인가자 외 인원에 대한 출입 기록 상시 유지**
  - 개발·유지관리요원 등의 업무처리 시 관리자 입회하에 처리
  - 개발·유지관리요원 등의 업무처리내용 기록 관리

출입 통제 대장

년월일	출입시간 및 퇴실시간	용 무	출입자		입회자		비고
			소속(주소)	성명	직급	성명	

※ 경기도교육청 보안업무시행요령 제60조(보호지역의 관리): 제한구역 및 통제구역에는 관계직원 및 출입이 인가 된 자 외에 출입을 통제하여야 하며 출입통제대장을 비치하고 기록 유지하여야 한다.

참고자료

- 보호구역 상시 출입인가자 기안문(예시)

참고자료 보호구역 상시 출입인가자 기안문(예시)

○ ○ 학 교

수신 내부결재
(경유)
제목 ○○학교 정보통신실(보호구역) 상시출입인가자 지정

1. 관련: 경기도교육청 정보보안 기본지침 제85조(정보통신시설 출입관리)

2. 우리 학교의 정보통신실(보호구역: 통제구역, 제한구역) 보안관리를 위하여 다음과 같이 상시출입인가자를 지정하여 운영하고자 합니다.

가. 기준일: 20○○.3.1.
나. 사 유: 인사발령에 따른 보호구역 상시출입인가자 변경
다. 상시출입인가자 명부

연번	직위(급)	성 명	통제/제한구역	비고(담당업무)
1	교장	박○○	정보통신실	업무총괄
2	정보부장	김○○	정보통신실	정보보안담당관
3	교사	이○○	CCTV 통제실	분임정보보안담당관
4	교사	정○○	정보통신실	시스템관리책임자
5	행정실무사	최○○	정보통신실 CCTV 통제실	시스템관리자

끝.

★담당자 부장 교감 교장

협조자

( ) 접수 ( )

우 00000 경기도 00시 00구 00로 00 (00동, 000) /
전화번호 031- /팩스번호 031- / / 비공개

3 개별사용자 단말기 보안관리

관련근거

- 정보보안 기본지침 제71조(개별사용자 보안)
- 정보보안 기본지침 제72조(단말기 보안)
- 정보보안 기본지침 제74조(비밀번호 관리)
- 정보보안 기본지침 제76조(휴대용 저장매체 보안)
- 정보보안 기본지침 제47조(인터넷 사용제한)

업무시기

- 상시

주요내용

- **개별 사용자는 본인이 PC 등 정보시스템을 사용하거나 정보통신망에 접속하는 행위와 관련하여 스스로 보안책임을 짐**

- **개별 사용자는 소속된 기관에서 지급 받은 PC·노트북·휴대폰·스마트패드 등 단말기 사용과 관련한 일체의 보안관리 책임을 짐**

  ※ 교육현장(유·초·중·고 등 각급학교의 교육 목적 정보통신 환경)에서는 단말기 보안과 관련한 사항을 학교장이 별도로 정할 수 있음(달리 정하지 않을 경우 경기도교육청 정보보안 기본지침을 준수 함)

- **휴대용 저장매체 관리자는 전산장비(노트북 등) 포함 외부 반출·입 통제 실시**
  - 휴대용 저장매체(전산장비 포함) 반출 · 입 대장 작성
  - 휴대용 저장매체(전산장비 포함)에 의한 보안사고 예방을 위해 보안교육 철저

- **단말기 보안대책**

연번	보안항목	항목별 보안대책
1	비밀번호 설정	◦ CMOS · 로그온 비밀번호의 정기적 변경 사용 ◦ 숫자, 문자, 특수문자 등을 혼합하여 비밀번호 부여규칙 적용하여 안전하게 설정
2	사용자계정 관리	◦ Guest 계정은 “사용안함”으로 설정 ※특히, 공용PC의 경우 Guest계정 사용 금지 ◦ 로그온 패스워드를 반드시 설정하고 주기적으로 변경
3	화면보호기 설정	◦ 단말기 작업을 일정 시간 이상 중단 시 비밀번호 등을 적용한 화면보호 조치 ◦ 화면 보호 해제 시 암호를 입력토록 설정
4	공유폴더	◦ 공유폴더 삭제

연번	보안항목	항목별 보안대책
5	백신 소프트웨어 설치	◦ 정품 백신 소프트웨어를 반드시 설치하고, 최신 보안 업데이트 상태로 운용 ◦ 바이러스 백신프로그램에서 제공하는 실시간 감시 기능 활성화 ※ 백신 SW내 랜섬웨어 관련 기능이 존재할 경우 해당 기능 활성화
6	중요자료, 개인정보 보호대책	◦ 보안을 요구하는 내용이나 민감 정보 등 개인정보를 포함하고 있는 파일은 반드시 비밀번호를 설정하여 저장 ◦ 중요자료는 주기적 백업
7	정품소프트웨어 사용 및 악성코드 방지	◦ 불법 소프트웨어 설치 및 사용 금지 ◦ 출처, 유통경로 및 제작자가 불분명한 응용프로그램 사용 금지 ◦ 보안이 취약한 웹사이트나 불법 파일공유 사이트 및 비인가 사이트 방문 금지 ◦ 웹브라우저를 통해 서명되지 않은 액티브-X 등이 다운로드·실행되지 않도록 보안 설정 ◦ PC 내부의 미사용(3개월) ActiveX 제거
8	해킹, 악성코드 보안대책	◦ 운영체제(OS), 응용프로그램에 대한 최신 보안패치 유지(자동업데이트 설정 권고) ◦ 출처(발송처), 첨부파일 등이 의심스러운 메일은 열람하지 않고 삭제 ◦ 인터넷을 통해 자료 획득 시 신뢰할 수 있는 인터넷사이트 활용 ◦ 자료(파일) 다운로드 시 최신 백신 소프트웨어로 검사 후 활용
9	랜섬웨어 감염이 의심되는 경우 행동요령	◦ 공유폴더, USB, 외장하드 등 외부 저장장치와의 연결 해제 ◦ 사용자가 감염피해 차단을 위해 PC 전원을 끌 경우 파일이 삭제될 수 있으므로 전원을 끄지 않도록 주의 (※인터넷회선만 분리하고 경기교육사이버안전센터에 신고) ◦ 해커에게 금전을 지불하거나 개인·기관의 개별적인 거래는 금지하고 각급기관 보안 담당부서에 신고, 체계적이고 전략적 대응방안 모색
10	기타	◦ 자동로그인 기능 사용 금지 ◦ 인터넷 파일공유, 상용메신저, P2P, 웹하드 등 업무상 불필요한 프로그램 설치 금지 ◦ 국가정보원장이 안전성을 확인하여 배포한 프로그램의 운용 및 보안권고문 이행

◦ **비밀번호 부여규칙**

- 비밀번호는 다음 각 호 사항을 반영하여 숫자와 문자, 특수문자 등의 조합·구성에 따라 10자리 또는 8자리 이상의 길이로 안전하게 설정하고 정기적으로 변경 사용하여야 함
- 최소10자리 이상: 영대문자, 영소문자, 숫자, 특수문자 중 2종류 이상 조합·구성
- 최소 8자리 이상: 영대문자, 영소문자, 숫자, 특수문자 중 3종류 이상으로 구성

※ 기술 발달에 따라 비밀번호의 최소 길이는 늘어날 수 있음

- 사용자계정(아이디)과 동일하지 않은 것
- 개인 신상 및 부서 명칭 등과 관계가 없는 것
- 일반 사전에 등록된 단어의 사용을 피할 것

- 동일한 단어 또는 숫자를 반복하여 사용하지 말 것
- 사용된 비밀번호는 재사용하지 말 것
- 동일한 비밀번호를 여러 사람이 공유하여 사용하지 말 것
- 응용프로그램 등을 이용한 자동 비밀번호 입력기능을 사용하지 말 것
- 비밀번호는 추측하거나 유추하기 어렵도록 설정: 잘 알려진 단어(love, happy 등), 키보드 상에서 나란히 있는 문자열(qwer 등)등을 사용하지 말 것
- 비밀번호 변경 시 동일한 비밀번호를 교대로 사용하지 말 것

- 공용 정보시스템(홈페이지 등) 관리자는 서버 등 정보시스템에 보관되는 비밀번호가 복호화 되지 않도록 일방향 암호화하여 저장하여야 함

용|어|설|명

- **랜섬웨어**: 몸값(Ransom)과 소프트웨어(Software)의 합성어다. 시스템을 잠그거나 데이터를 암호화해 사용할 수 없도록 만든 뒤, 이를 인질로 금전을 요구하는 악성코드 프로그램을 일컫는다.

- 인터넷사용 제한
  - 각급기관의 장은 국가비상사태 및 대형 재해 재난의 발생, 사이버공격 등으로부터 정보통신망과 정보시스템의 정상적인 운영을 보장하기 위하여 소속 공무원에 대한 인터넷 사용을 일부 제한할 수 있음
  - 각급기관의 장은 기관 인터넷망의 효율적인 운영 관리 및 악성코드 유입 차단을 위하여 게임·음란·도박 등 업무와 관련이 없는 인터넷 이용을 차단하여야 하며, 악성코드 유입 차단을 위하여 필요할 경우 상용 정보통신서비스의 접속을 제한할 수 있음

참고자료

- 휴대용 저장매체 관리대장(일반용)
- 휴대용 저장매체(전산장비 포함) 반출·입 대장
- 비업무 사이트 차단 및 접근 허용 절차
- 비업무 사이트 허용신청 기안문(예시)

참고자료 휴대용 저장매체 관리대장(일반용)

휴대용 저장매체 관리대장(일반용)

< 관리자 : 이순○ >

연번	관리번호 (S/N)	매체형태	등록일자	취급자	불용처리일자	불용처리방법 (재사용 용도)	비고
1	총무과-일반-01 (E-D900-04-3705B)	USB	10.10.20	5급 홍길○	11.10.20	물리적 파기	고장
2	총무과-일반-02 (NP00T512787J)	외장형 HDD	10.10.25	6급 김정○	11.10.27	포맷후 재사용 (시설과-일반-01)	
3	총무과-일반-03 (E-D900-04-3705B)	USB	10.11.1	5급 이수○	11.10.7	물리적 파기	고장
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							

참고자료 휴대용 저장매체(전산장비 포함) 반출·입 대장

휴대용 저장매체(전산장비 포함) 반출・입 대장

< 관리자 : 김유○ >

장비명	관리번호 (시리얼번호)	사용자	용도	출입 일시 (입・출 구분)	확인
노트북PC	교무노트북-01 (5004829800055)	홍길○	세미나 발표	2000.12.3 13:00 (출)	*김유○*
외장하드	교무외장하드-05 (610-RUFU-61747)	강감○	재택근무	2000.12.3 10:00(출)	*김유○*

참고자료 비업무용 사이트 차단 및 접근 허용 절차

1. 비업무 사이트 차단

① 대상 : 경기도교육청 전 기관에서 운영 중인 모든 PC

② 기본방침 : 모든 PC는 네트워크 방식을 기본으로 업무·교육과 무관한 사이트 접속 차단

2. 비업무 사이트 접근 허용 절차

① 학교 게임 대회, 교육목적 이용 등 계획단계에서 해당 사이트 접속 여부 확인

② 해당 지역 교육지원청 담당자와 협의 후 공문으로 신청서 제출

※ 당일 요청 시 처리 불가할 수도 있음

※ 해당 사이트 악성코드 감염이 확인된 경우 접속 허용 불가

참고자료 비업무 사이트 허용신청 기안문(예시)

기안문

○ ○ 학 교

수신 ○○교육지원청

(경유)

제목 비업무사이트 허용신청서 제출

1. 관련: 경기도교육청 정보보안 기본지침 제47조(인터넷 사용제한)
2. 정보보안사고 사전예방을 위한 개인용 비업무사이트의 사용금지 정책에 따라 학생-학부모-교사와의 교육관련 소통 교류 공유 목적으로 비업무사이트 접속 신청서를 붙임과 같이 제출합니다.

붙임 비업무사이트 접속허용 신청서 1부. 끝.

○○○학교장

★담당자 부장 교감 교장

협조자

( ) 접수 ( )

우 00000 경기도 00시 00구 00로 00 (00동, 000) /

전화번호 031- /팩스번호 031- / / 비공개

붙임

비업무 사이트 사용 신청서

신청 기관	학교명(부서)			
	담당자		연 락 처	
등 록 구 분	☑ 허용 (☑신규 / □변경 / □삭제)			
	□ 차단 (□신규 / □변경 / □삭제)			
신 청 일	20 . . .			

<신청자 유의사항>
1. 신청자가 책임을 지고 사이트(서비스) 접속 사유 및 용도로만 사용하고 업무자료 및 개인정보가 포함된 파일을 송·수신하여 개인정보유출 및 보안사고가 발생하지 않도록 할 것
2. 수업과 교육 목적으로만 허용(차단)을 신청함 (해당목적 외 신청 시 등록이 거부될 수 있음)

사유 및 용도	컴퓨터 IP	사이트(서비스)	사용기간	신청자 (직위/급)	신청자의 유의사항 확인여부 (O/X)
컴퓨터 활용수업	*10.xx.xx.87 ~ 100*	*www.webhard.co.kr*	*2021.12.1. ~ 2022.2.28.*	*홍길동 (교사)*	O
학부모 상담	*10.xx.xx.10*	*카카오톡*	*2022.12.1. ~ 12.9.*	*이순신 (교사)*	O

※ 사용기간 : 사이트를 사용할 기간 입력
- 신청한 사이트는 기간 만료시 자동 차단되며, 매년 3월 1일을 기준으로 일괄 삭제(초기화)됨

※ 본 양식은 기관별 운영에 따라 변경하여 사용 가능

4 홈페이지 게시자료 보안관리

관련근거

- 정보보안 기본지침 제68조(홈페이지 등 게시자료 보안)

업무시기

- 홈페이지 정보공개 보안지침 수립 : 홈페이지 개편 시 운영계획에 포함(필요시 개정 가능)
- 게시판 담당자 지정 : 게시판 담당자 변경 시, 신규 게시판 생성 시

주요내용

- **각급기관의 장은 비공개 업무자료가 홈페이지 또는 외부 웹사이트에 무단 게시되지 않도록 게시자료의 범위, 자료의 게시방법 등을 규정한 자체 홈페이지 운영 계획을 수립 · 시행하여야 함 (정보공개보안지침 포함)**
  - 홈페이지 서비스 제공자는 홈페이지의 효율적인 운영으로 기관 정보제공 서비스의 질을 향상시키고, 체계적인 관리로 이용자의 개인정보보호 및 보안 강화를 위하여 홈페이지 운영 계획을 수립하여 추진함
  - 운영계획 수립 시 홈페이지 정보공개 보안지침 내용 포함 권장

- 관리자 지정 및 임무(게시판별 담당자 포함)	- 자료 현행화 관리
- 게시판 권한 관리	- 게시판 자료 관리
- 메뉴 개설 및 폐지	- 홈페이지 링크(배너) 관리
- 팝업 관리	- 웹호스팅 및 서버관리
- 정보보안 및 개인정보 보호	- 저작권 보호

- **게시판담당자는 홈페이지에 업무자료를 게시하고자 할 경우 자료 내용을 사전 검토하여 비공개 업무자료가 게시되지 않도록 하여야 함**

- **(분임)정보보안담당관은 홈페이지에 비공개 업무자료가 무단 게시되었는지 여부를 정기적으로 점검하여야 함**

- **각급기관의 장은 홈페이지 또는 외부 웹사이트에 비공개 업무자료가 무단 게시된 사실을 알게 된 경우 즉시 삭제 또는 차단 등 보안조치를 취하여야 함**

참고자료

- 학교 홈페이지 운영 계획 수립 기안문(예시)

참고자료 학교 홈페이지 운영 계획 수립 기안문(예시)

기안문

○ ○ 학 교

수신 내부결재

(경유)

제목 ○○학교 홈페이지 운영 계획 수립

1. 관련
   가. 경기도교육청 정보보안 기본지침 제68조(홈페이지 등 게시자료 보안)
   나. 경기도교육청 학교 홈페이지 운영 가이드(2019.12.)

2. 우리학교 홈페이지 이용자에게 신뢰성 있는 정보와 질 높은 서비스를 제공하고, 홈페이지의 효율적인 운영을 위하여「00학교 홈페이지 운영계획(안)」을 [붙임]과 같이 수립하고자 합니다.

3. 주요내용
   가. 관리자, 게시판 및 메뉴별 담당자 및 임무 지정
   나. 서비스 및 콘텐츠 관리·운영 규칙
   다. 정보보호 및 저작권 보호에 관한 사항

붙임 1. 00학교 홈페이지 운영계획(안) 1부
2. 홈페이지 메뉴별 담당자 현황 1부. 끝.

★담당자 부장 교감 교장

협조자

( ) 접수 ( )

우 00000 경기도 00시 00구 00로 00 (00동, 000) /

전화번호 031- /팩스번호 031- / / 비공개

붙임 1

○○학교 홈페이지 운영 계획(예시)

(※학교실정에 맞게 수정하여 사용)

Ⅰ 개 요

1. 목 적

인터넷 이용자에게 질 높은 서비스를 제공하고, 홈페이지의 효율적인 운영을 위하여 필요한 사항을 규정함

2. 근 거

가. 『학교 홈페이지 운영 가이드』(경기도교육청)
나. 『경기도교육청 정보보안 기본지침』 및 『교육기관 정보보안 업무매뉴얼』(경기도교육청)
다. 개인정보 보호법
라. 저작권법

3. 추진방향

가. 홈페이지의 효율적 운영을 위하여 관리자 지정
나. 홈페이지에 게재된 정보가 최신의 상태로 유지될 수 있도록 관리
다. 홈페이지를 통하여 개인정보, 비공개 업무자료가 유출되지 않도록 점검 · 관리 강화
라. 홈페이지 게시 자료 및 콘텐츠에 대한 저작권 준수

4. 업무시기

가. 운영 계획 수립 : 학교 홈페이지 개편 시
나. 게시판(메뉴)별 담당자 지정 : 담당자 변경 시, 신규 게시판 생성 시(내부결재)

II 홈페이지 관리자 지정 및 임무

1. 홈페이지 관리자 지정

관리부서	관리책임자	관리담당자	게시판(메뉴)별 담당자
(예시) 교육정보부	교감	업무분장에 따른 담당자 [붙임 2] 참조	

※ 담당자 변경 시 후임자에게 인계하여 홈페이지 운영에 차질이 없도록 함

2. 임 무

가. 관리책임자

1) 홈페이지 총괄 운영 · 관리
2) 홈페이지 관리담당자 및 게시판(메뉴)별 담당자 지정

나. 관리담당자

1) 홈페이지 운영 계획 수립
2) 홈페이지 운영 및 시스템 유지 관리
3) 웹접근성과 웹취약점 점검 및 조치(연 1회)
4) 홈페이지 정보보안 및 개인정보 보호
5) 링크(배너) 및 팝업 정기적인 관리(분기 1회)

다. 게시판(메뉴)별 담당자

1) 게시 자료 선정 · 등록 및 현행화
2) 자료 점검 및 관리(“게시물 자료 삭제 또는 비공개 처리 기준”에 따른 조치)
3) 인사 이동시 후임자에게 인계

III 홈페이지 운영 및 관리

1. 홈페이지 운영

가. 자료 현행화 관리

1) 홈페이지 게재정보는 항상 최신의 상태를 유지
2) 오 · 탈자 등 오류 내용은 주기적으로 점검하여 발견 즉시 수정
3) 계획 및 정책의 변경 등에 따라 게시자료의 보완 · 갱신이 필요한 경우 즉시 현행화

나. 게시판 권한 관리

1) 게시판은 서비스별로 아래와 같이 구분하여 사용 권한을 설정 · 운영

구분		사용 권한			비고
서비스	메뉴명	쓰기	수정·삭제	읽기	
대국민 서비스	- 학교소개 - 공지사항 - 사전정보공개 :	교직원	게시자, 관리자	전체 사용자 (비회원 포함)	
	- 자유게시판 :	전체 사용자 (비회원 포함)			
교직원 서비스	- 교사마당 :	교직원	게시자, 관리자	교직원	
학생/학부모 서비스	- 학급홈페이지 - 학생/학부모마당 :	교직원, 학생/학부모	게시자, 관리자	교직원, 학생/학부모	
	- 학습정보 :	교직원			

※ 국민의 알권리 보장을 위해 비공개 사유가 없는 메뉴는 비회원에게도 공개될 수 있도록 읽기 권한 설정

다. 게시판 자료 관리

1) 홈페이지 게시판에는 비공개 대상정보(공공기관의 정보공개에 관한 법률 제9조) 게시 금지
2) 업무자료 게시자는 분임정보보안담당관에게 자료의 신뢰성, 보안성 등을 검토 받은 후 자료의 입력 및 수정
3) 게시판별 담당자는 게재되는 자료를 수시로 확인하며, 다음의 경우 홈페이지 관리책임자의 승인을 얻은 후 해당 게시물을 삭제 또는 비공개(블라인드) 처리

게시물 자료 삭제 또는 비공개 처리 기준
- 국가안전이나 보안에 위배되는 경우 - 정치적 목적이나 성향이 있는 경우 - 특정기관, 단체, 부서를 근거 없이 비난하는 경우 - 특정인을 비방하거나 명예훼손의 우려가 있는 경우 - 영리목적의 상업성 광고, 저작권을 침해할 수 있는 내용 - 개인정보, 비공개 공문서 및 민감자료가 포함된 경우 - 욕설, 음란물 등 불건전한 내용 - 실명을 원칙으로 하는 경우에 실명을 사용하지 않은 경우 - 동일인이라고 인정되는 자가 동일 또는 유사내용을 반복하여 게재하는 도배성 글 - 연습성, 오류, 장난성의 글 - 기타 해당 게시판의 취지와 부합하지 않을 경우 등

- 원본 내용 보존을 위해 비공개(블라인드) 처리를 원칙으로 하며,
- 완전 삭제가 필요한 경우에는 삭제 전 화면을 캡처하여 원본 내용을 보관하고, "홈페이지 게시물 삭제 기록대장[서식 제1호]"에 기록하여 1년 이상 관리
- 위 처리 기준을 게시물 작성자가 인지할 수 있도록 글쓰기 창에 안내

4) 게시판의 자료 게시 기간은 관련 법령 등에서 정해진 기간으로 하며, 정해진 기간이 없을 경우 3년 이하로 함
※ 자료 게시 기간의 연장이 필요한 경우에는 관리책임자에게 요청

라. 게시판 등 메뉴 개설/수정/삭제 - [서식 제3호] 참조

홈페이지 메뉴 운영 기본 원칙
o 홈페이지 메뉴구성은 관리책임자가 총괄 o 법령에 의해 공개 등이 의무화된 **정보 제공 메뉴 운영**함 ※ 경기도교육청 행정정보 공개 운영 규정 제5조(정보의 사전적 공개) 참조 o 학교의 조직구성, 담당업무(담임, 과목 등) 및 전화번호를 로그인 없이 공개함 ※ 전화번호: 교무실, 학년별 교무실, 행정실 등 실별 전화번호 (개인 휴대폰 제외, 교실 내선번호는 수업방해 예방차원에서 비공개) o 홈페이지의 각종 게시판 **이용자의 본인 확인**을 거치도록 운영함 ※ 본인확인 방법: 회원가입 및 비회원 글쓰기 시 휴대전화 또는 이메일 등 확인

1) 게시판 등 메뉴 개설/수정
- 홈페이지에 게시판 등 메뉴를 개설 및 수정하고자 하는 자는 홈페이지 관리담당자 및 담당 부장과 협의를 거친 후 관리담당자에게 요청

2) 게시판 등 메뉴 삭제
- 그 목적이 다하여 더 이상 운영의 필요가 없을 시에는 지체 없이 게시판 등 메뉴 삭제를 요청해야 함
- 홈페이지 관리책임자는 홈페이지에 개설된 메뉴가 일정기간 동안 정상적으로 운영되지 않을 경우 메뉴 담당자에게 보완을 요청하고, 요청 후 1개월 이내에 보완이 이루어지지 않을 경우 폐쇄 할 수 있음

마. 홈페이지 링크 관리

1) 공공기관 등에서 협조 요청 시 특별한 사유가 없는 한 협조하며, 데드링크(Dead Link, 이용이 불가능한 웹페이지)가 발생되지 않도록 정기적으로 점검, 링크주소 갱신 및 삭제처리(분기 1회)
2) 공공기관 등이 아닌 기타의 사이트로 연결될 때에는 정보제공에 대한 저작권과 책임을 명확히 하고 주의 사항을 표시함
3) 배너 설치가 필요할 경우 홈페이지 관리담당자에게 요청함

바. 팝업 관리

1) 팝업은 장애인 등의 접근성을 저해하지 않도록 팝업존으로 구성·운영하며,
별도의 팝업창이 필요한 경우 팝업의 수는 2개 이하로 운영함
2) 팝업 설치가 필요할 경우 홈페이지 관리담당자에게 요청하며, 팝업게재기간은 최대 4주로 함

사. 홈페이지 서버관리

1) ○○교육지원청(또는 교육정보기록원) 웹호스팅 운영 중임

2) 장애발생시 신속한 대처를 위하여 비상연락망 항시 업데이트 관리

- 홈페이지 유지관리 비상연락망 -

구 분	담당자명	전화번호	비 고
○○교육지원청	○○○	031-000-0000	웹호스팅 담당자
㈜ABC	○○○	031-000-0000	유지관리 담당자

2. 정보보호 및 저작권 보호

가. 정보보안 및 개인정보보호

1) 홈페이지 로그인 비밀번호는 문자, 숫자, 특수문자 등을 혼합하여 9자리 이상으로 정하고, 분기 1회 이상 주기적으로 변경 사용하여야 함

※「경기도교육청 정보보안 기본지침」제74조(비밀번호 관리) 참조

2) **홈페이지 이용자**는 개인정보, 비공개 공문서 및 민감 자료가 포함된 문서가 홈페이지에 공개되지 않도록 하며, 특히 주민등록번호는 등록할 수 없음

3) **게시판별 담당자**는 개인정보 유출에 따른 피해를 없애기 위해 매월1회 '사이버 보안진단의 날'에 홈페이지 개인정보 노출여부를 점검하여야 함

※ [서식 제2호] "홈페이지 개인정보 점검대장" 참조

4) 개인정보 유·노출 등 중요정보 공개의 문제발생 즉시 상위 관리자 또는 홈페이지 관리책임자에게 보고

5) **관리책임자**는 홈페이지에 중요정보가 공개된 것을 인지할 경우 이를 즉시 차단하는 등의 보안조치를 강구 시행하여야 함

6)「개인정보 보호법」에 따라 수립한 **「개인정보처리방침」**은 색상을 달리하여 다른 고지사항과 구분되도록 홈페이지 메인화면 하단에 게재하며, 방침을 변경하는 경우 변경 전·후 자료에 대한 이력관리를 함

7)「개인정보 보호법」에 따라 수립한 **「영상정보처리기기 운영·관리 방침」은** 홈페이지 메인화면 하단에 게재 함

나. 저작권 보호

1) 홈페이지 이용자는 홈페이지용 그림, 사진, 도안, 저작물 등의 정보를 등재할 때 저작권의 도용, 명예훼손 등의 문제가 발생하지 않도록 주의함

※「저작권법」참조

다. 웹 취약점 점검

1) 사이버침해사고 예방과 홈페이지 서비스의 안전성·신뢰성 확보를 위해 연1회 이상 웹 취약점을 점검 및 조치함

라. 홈페이지 보안사고 처리

1) 서비스 접속 장애 등 사고 발생 시 웹호스팅(서버) 운영 기관과 협조하여 처리

2) 사이버침해사고(해킹 등) 발생 시 피해시스템의 네트워크(랜 케이블) 분리 후 경기교육사이버안전센터에 신고(031-240-6599)하여 조치

3. 시스템 운영 관리(※홈페이지 서버 자체운영교만 해당)

가. 구성 및 변경관리

1) 시스템운영자는 응용시스템 구성도, 소프트웨어 구성도 등의 운영에 관련된 산출물 등 주요 구성요소들에 대한 관리를 주기적으로 수행함
2) 장애 혹은 사용자 요구로 인하여 웹사이트의 변경이 발생했을 시 변경이력 관리를 위하여 변경관리 대장 등을 활용하여 변경관리를 할 수 있도록 함

나. 성능 및 장애관리

1) 시스템운영자는 웹사이트를 통하여 제공하는 웹서비스의 안정적인 제공을 위하여 시스템의 성능 및 용량을 파악하여 사전대처 할 수 있도록 함(CPU 사용량, 디스크 용량 및 I/O, 응답속도 등)
2) 정상적인 서비스의 범주를 벗어난 모든 장애에 대하여 효율적으로 대처할 수 있도록 장애이력 관리를 하고 이를 통해 문제점을 파악하고 대응방안을 수립하는 것이 필요함
3) 장애발생시 신속한 대처를 위하여 장애유형별 대응 시나리오를 수립하고 비상연락망은 항시 업데이트 하여 관리될 수 있도록 함

다. 백업 및 보안관리

1) 시스템운영자는 비상시 긴급 복구를 위하여 필요한 백업목록 및 스케줄을 정의하고 주기적으로 백업을 실행하여야 함
2) 백업용량을 주기적으로 점검하여 정상적인 백업관리가 가능하도록 충분한 용량을 확보해야 함
3) 웹서버의 사이버 침해 및 관리 소홀로 인한 개인정보의 노출 등을 방지하기 위하여 보안강화에 대한 기술적 조치 및 보안에 대한 사항을 주기적으로 점검해야 함
4) 내부 관련자(교직원, 유지보수 요원, 시스템 개발요원)로 부터 내부정보 유출 및 해킹방지를 위한 관리적, 기술적 보안장치를 마련하고 상시 점검함
5) 웹서버의 보안 취약점으로 인한 보안사고의 근본적 예방을 위하여 정기적으로 웹서버 보안취약점을 점검하고 시정 조치함

붙임 2

홈페이지 메뉴별 담당자 지정현황(예시)

▣ 홈페이지 관리담당자:

메뉴구성			부서명	담당자명
1단계	2단계	3단계		
학교소개	인사말			
	학교연혁			
	학교상징			
	교육목표			
	교직원소개			
	학교현황			
	오시는 길			
알림마당	공지사항			
	가정통신문			
	행사일정			
	학교운영위원회	운영규정		
		구성현황		
		운영내용		
	급식정보	식단표		
	…			
행정정보 및 민원	학교재정공개	예·결산 현황		
		업무추진비집행내역		
		신용카드사용내역		
		상품권구매·사용내역		
		…		
	행정정보공개	정보공개제도안내		
		사전정보공표		
		비공개세부기준		
		정보공개자료실		
	민원사무안내			
	학교시설개방	…		
병설유치원	공지사항			

【서식 제1호】

홈페이지 게시물 삭제 기록대장

□ 대상 게시판명 :

연번	게시일 (삭제일)	게시자 (ID)	제 목	게시내용 및 삭제사유	확 인	
					담당자	책임자

※ 홈페이지 관리자가 홈페이지 게시자료 삭제에 대한 기록을 작성함(게시판별 작성)

【서식 제2호】

홈페이지 개인정보 점검대장

20 년 월 모니터링			점검일 : 20 . . .		
점검대상 메뉴(게시판)명			점검자	서명	점검결과
1단계	2단계	3단계			

※ 게시판별 담당자가 홈페이지내 개인정보 노출여부를 매월 1회 '사이버보안진단의 날'에 점검

【서식 제3호】

홈페이지 메뉴 (개설/수정/삭제) 요청서

요청사항	메뉴명	/대메뉴-하위메뉴순으로/
	메뉴위치	/대메뉴-하위메뉴순으로/
	개설목적 (관련근거)	/공문 또는 기타 자료/
	서비스 수요자 및 관리유형	/글쓰기 권한부여 등 요청사항/
	참고할 유사 사이트 메뉴	/URL/
	주요내용	/세부내용/

요청일		완료희망일	
부서명		요청자	
첨부파일명	/필요시 메뉴의 취지 및 내용을 포함하는 관련 파일 첨부/		
개인정보 보호대책	/게시판 담당자 지정 관리/		

5 저장매체 불용처리

관련근거

- 정보보안 기본지침 제59조(저장매체 불용처리)
  참 참고자료 : 정보시스템 저장매체 불용처리지침

업무시기

- 정보시스템(PC 등) 교체·반납·양여·폐기 및 불용처리 시
- 수리를 위해 기관 외부로 반출할 경우

주요내용

- **PC, 서버 등 정보시스템을 폐기·양여·교체·반납(이하 "불용처리")를 하거나 수리를 위하여 기관 외부로 반출할 경우 저장매체에 보관된 자료의 삭제 등 보안조치를 실시**

- **저장매체 불용처리 시 다음 분류 기준 이상으로 삭제**

저장 매체 \ 저장 자료	공개 자료	비공개 자료	대외비 자료	비밀 자료
광디스크 (CD · DVD 등)	자체 판단	물리적 파괴	물리적 파괴	물리적 파괴
반도체메모리 (SSD · USB 등)	포맷 또는 삭제	완전삭제 제품	물리적 파괴	물리적 파괴
하드디스크	포맷 또는 삭제	디가우징 또는 완전삭제 제품	물리적 파괴	물리적 파괴

- **정보보안담당관 확인사항**
  - 정보시스템 불용 처리 시 사전에 저장자료 삭제여부 확인
    ▶ 저장매체 삭제에 대한 내부결재([참고자료]저장매체 파쇄장비 이용신청 공문)
  - 저장자료 삭제를 외부업체에 의뢰할 경우 정보보안담당관이 입회하여 삭제 절차·방법 준수여부 등을 확인하고 감독

- **정보시스템 도입·반출·불용처리 시 보안 조치 방법**

구분	보안 조치 방법
도입 시	● 고장 수리 등 공급업체가 저장매체를 교환 · 반출해 갈 경우를 대비하여 저장자료 삭제방법 등 **저장매체 보안조치 방안을 계약서에 포함** ● 임차 만료 후 반납 시 해당 정보시스템의 저장자료 삭제 방법 등 저장매체 보안조치 방안을 임차 계약서에 포함
반출 시	● 저장매체의 고장수리 · 자료복구 등을 외부에 의뢰할 경우 용역 참여자의 보안서약서 집행 및 보안교육 등 필요한 보안조치를 강구하고 정보보안담당관의 통제를 받음 ※ 구비서류 - 보안서약서, 보안교육 ※ 보안서약서, 보안교육 서식은 2. 정보보안 관리 - ⑥정보시스템 유지보수 및 용역사업 보안관리 항목의 [참고자료] 참고
불용처리 시	● 불용처리나 외부로 반출 시에는 해당 정보시스템의 사용기관 · 부서 · 사용자 등을 인식할 수 있는 표시를 모두 제거 ● 저장매체 불용처리 기준 이상으로 삭제

- **저장매체 파기 절차**
  - 업체의뢰 시
    - 정보시스템 불용결정 → 파기(완전삭제) 계획 내부결재 → 업체의뢰 → 구비서류 준비(보안서약서, 보안교육, 저장매체 삭제처리확인서) → 업체 조치절차 확인감독
  - 저장자료 삭제 보유기관 의뢰시
    - 정보시스템 불용결정 → 파기(완전삭제) 계획 내부결재 → 파쇄장비 보유기관 협의 → 구비서류 준비(보유기관의 양식에 따름) → 파쇄장비 보유기관 방문파기

- **저장자료 전용 소자장비 이용 안내**
  - 소자장비 미보유기관은 소자장비 보유기관에 설치된 소자장비를 이용하여 완전삭제
  - 폐기할 저장매체를 지참하여 방문하고 데이터 삭제가 완료된 후 신청기관에서 자체 불용처리
  - 데이터가 소거된 저장매체는 재사용 불가능
  - 자세한 장비 이용 방법은 보유기관에 문의하거나 아래의 공문 참조
    - 정보시스템 저장매체 전용 소자장비 이용 안내
      [경기도교육정보기록원 사이버안전센터-284(2019.3.5.)]
    - 소자(파쇄)장비 보유기관 : 경기도교육정보기록원, 경기도교육청 북부청사, 교육지원청(광주하남, 안산, 의정부, 포천)

참고자료

- 저장매체 삭제처리 확인서
- 저장매체(하드디스크) 파기(완전삭제) 계획 기안문(예시)
- 저장매체(하드디스크) 전용소자장비 이용 협조 요청 시행문(예시)

참고자료 저장매체 삭제처리 확인서

정보시스템 저장매체 삭제처리 확인서

아래와 같이 정보시스템(　　종　　점) 불용처리에 따른 저장매체 삭제처리에 대해 확인을 요청함

연번	정보시스템	매체형태	사용자		삭제방법	관리책임자 (서명)
			직	성명		

확인일자 :　　년　　월　　일

요 청 자 :　소속・직책　　성명 :　　(인)
확 인 자 : 정보보안담당관　　성명 :　　(인)

※ 작성요령
- 정보시스템 : 개인용컴퓨터, 전산서버(서버는 용도 기재), 복사기, 팩스 등
- 매체형태 : 광디스크(CD, DVD), 하드디스크 등
- 삭제방법 : 완전파괴(소각·파쇄·용해), 전용 소자장비 이용, 완전포맷(횟수 기재)

참고자료 **저장매체 파기 계획 기안문(예시)**

○ ○ 학 교

수신 내부결재
(경유)
제목 저장매체(하드디스크) 파기(완전삭제) 계획

1. 관련: 경기도교육청 정보보안기본지침 제59조(저장매체 불용처리)

2. 정보시스템 불용 결정에 따라 다음과 같이 저장매체(하드디스크) 파기(완전삭제)를 수행하고자 합니다.

가. 정보시스템: 업무용PC
나. 사 유: 노후교체에 따른 불용
다. 대 상: 하드디스크 10개
라. 방 법: 00교육지원청 파쇄장비 이용
※ 일정 및 절차는 00교육지원청과 협의하여 결정. 끝.

★담당자 부장 교감 교장

협조자

( ) 접수 ( )

우 00000 경기도 00시 00구 00로 00 (00동, 000) /
전화번호 031- /팩스번호 031- / / 비공개

참고자료 저장매체 전용소자장비 이용 협조 요청 시행문(예시)

○ ○ 학 교

수신 경기도교육정보기록원장
(경유)
제목 저장매체 전용소자장비 이용 협조 요청

1. 관련
   가. 경기도교육청 정보보안 기본지침 제59조(저장매체 불용처리)
   나. 경기도교육정보기록원 사이버안전센터-284(2019.3.5.) 「저장매체(하드디스크)처리장비 이용 안내」
2. 정보시스템 불용처리와 관련하여 중요자료 유출에 따른 보안사고를 예방하고자 저장매체 소자장비 이용 신청서를 붙임과 같이 제출합니다.
   가. 삭제방법: 경기도교육청 북부청사 전용소자장비(디가우저) 이용
   나. 대상매체: 불용 처리된 정보시스템 저장매체(하드디스크 00개)
   다. 방문 희망 일정: 2000. 3. XX.

붙임 1. 저장매체 자료삭제 신청서 1부.
2. 불용저장매체 시리얼 번호(하드디스크 사진) 1부. 끝.

★담당자 부장 교감 교장

협조자

( ) 접수 ( )

우 00000 경기도 00시 00구 00로 00 (00동, 000) /
전화번호 031- /팩스번호 031- / / 비공개

【붙임1】

저장매체 자료삭제 신청서

담당자	관리자
담당자 서명	*정보보안담당관 서명*
서명월/일	*서명월/일*

작 성 일 : *20○○년 ○월 ○일*

연번	정보시스템	저장매체	Serial Number(S/N)	내용
1	*업무용 PC*	*하드디스크*	*E-D900-04-3705B*	*학생성적 등 중요 자료*

신 청 자		사이버안전센터 담당자	
성명	*방문자*	성명	
소속	*00초등학교*	소속	
직책	*교사*	직책	
연락처	*학교연락처*	연락처	
서명	*20 . . . (서명)*	서명	

1) 담당자 : 저장매체 자료삭제 요청기관 담당자의 서명
2) 관리자 : 저장매체 자료삭제 요청기관 관리자(정보보안담당관)의 서명
3) 작성일 : 저장매체 자료삭제 신청서 작성 일자
4) 정보시스템 : 업무용 PC, 학생용 PC, 전산서버(서버는 용도 기재) 등
5) 저장매체 : 하드 디스크 등
6) Serial Number(S/N) : 해당 저장매체의 Serial Number 기재
7) 내용 : 저장매체에 저장된 내용을 간단히 기재
8) 신청자 : 경기도교육정보기록원 사이버안전센터에 내방하여 사이버안전센터 담당자에게 삭제처리를 요청하는 자(※서명란에 방문일 기재)

6 정보시스템 유지보수 및 용역사업 보안관리

관련근거

- 정보보안 기본지침 제2장 제1절 사업계획
- 정보보안 기본지침 제2장 제4절 계약 및 사업수행
- 정보보안 기본지침 제3장 제2절 제49조(정보시스템 유지보수)
- 정보보안 기본지침 제3장 제2절 제50조(지정 단말기를 통한 온라인 유지보수)

업무시기

- 정보화 사업 추진 시
  - 정보통신제품, CCTV 및 제어시스템 도입
  - 정보시스템 개발(홈페이지 구축 등), 유지보수(학내망, 홈페이지 등) 용역

주요내용

- **정보화 사업 계획 시**
  - 자체 보안대책 수립 또는 보안성검토 실시(상세내용은 보안성검토 참고)
  - 제안요청서(과업지시서) 검토(제13조)

- **정보화관련 용역사업 계약 시 조치 사항**
  - 계약서에 보안 관련 특수조건 명시
    - 용역과정에서 취득한 보안약점의 누설 및 자료유출금지 등 보안준수사항과 위반 시 손해배상 책임(위약금 부과, 향후 입찰참여시 감점 등) 등 보안관련 특약조항 명시
    - 과업지시서 · 입찰공고 · 계약서에 누출금지 대상정보를 명시해야 하며 해당정보 누출 시 입찰 참가자격 제한을 위한 부정당업자로 등록
    - 누출금지 대상정보

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. 정보화 사업 용역 결과물 및 관련 프로그램 소스코드 (유출시 안보·국익에 피해가 우려되는 중요 용역사업에 해당)
6. 암호가 주 기능인 제품 및 정보보호시스템 도입·운용 현황
7. 정보보호시스템 및 네트워크장비 설정 정보
8. 「공공기관의 정보공개에 관한 법률」제9조 제1항에 따라 비공개 대상 정보로 분류된 해당 기관의 내부문서
9. 「개인정보보호법」제2조 제1호에 따른 개인정보
10. 「보안업무규정」제4조에 따른 비밀 및 동규정 시행규칙 제16조 제3항에 따른 대외비
11. 그 밖에 해당 기관의 장이 공개가 불가하다고 판단한 자료

정보화 사업 수행 시 정보보안 관련 검토사항

- 용역사업 참여 인력에 대한 보안관리
  - 용역사업 인력에 대해 보안서약서 집행, 보안교육 등을 포함한 용역사업 인가 절차를 마련하고 인가된 용역사업 참여 인력만 사업에 참여토록 함
  - 구비서류
    - ▶ [참고자료] 참여인원(업체대표) 보안서약서
    - ▶ [참고자료] 외부용역 업체직원 보안교육
    - ▶ [참고자료] 정보시스템 원격 접속 관리대장

- 원격지 개발보안(제28조 및 제28조의2)
  - 용역업체가 발주기관 이외 장소(이하 "원격지")에서 개발작업(유지보수 제외)을 수행하고자 요청할 경우 작업 장소에 대한 보안요구사항 등을 포함한 관리적·기술적 보안대책을 수립·시행하고 정보보안담당관의 승인을 받아야 함
  - 원격지에서의 온라인 개발은 해당 기관의 장이 필요하다고 판단하고, 용역업체가 보안대책에 서면으로 동의하는 경우에 한하여 허용할 수 있음.
    - ▶ 구비서류: [참고자료] 원격지 온라인 개발 서약서

용|어|설|명

- **원격지 개발:** 발주기관 이외 장소(이하 "원격지")에서의 개발작업 수행
  - * 발주기관 내 장소에서 개발작업을 수행하더라도 개발용 서버가 원격지(민간 클라우드 컴퓨팅서비스를 이용하는 등)에 위치할 경우는 원격지 개발로 간주함
- **온라인 개발:** 인터넷을 통해 발주기관 정보시스템에 온라인 접속한 상태의 개발

- 소프트웨어 산출물 제공(제29조)
  - 용역업체가 지식재산권을 행사하기 위하여 소프트웨어 산출물의 반출을 요청할 경우 누출금지정보에 해당하지 않으면 제공하여야 함
  - 산출물을 용역업체에 제공할 경우 업체의 노트북·휴대용 저장매체 등 관련 장비에 누출금지정보를 완전 삭제하여야 하며, 동 사항이 완전 삭제되었다는 대표자 명의의 **확약서를 받아야 함**

- 누출금지정보 유출시 조치(제30조)
  - 용역업체가 누출금지정보를 유출한 사실을 알게 된 경우 업체를 대상으로 계약 위반에 따른 조치를 취하여야 한다, 이 경우 즉시 정보보안담당관을 거쳐 소속 기관의 장에게 보고하여야 하고,
  - 그 사실을 상급기관의 장 및 국가정보원장에게 통보하여야 하며,
  - 해당 업체에 대한 입찰 참가자격 제한 등 관련조치를 취하여야 함

- 정보시스템 유지보수 시 추가 조치 사항
  - 정보시스템을 직접 또는 용역업체를 활용하여 유지 보수할 경우 콘솔(정보시스템과 직접 연결한 단말장치) 또는 지정된 단말기로부터의 접속만을 허용하여야 함.
    - ▶ 구비서류 : [참고자료] 출입통제대장
    - ▶ 구비서류 : 유지보수 점검표(점검표 서식은 업체와 상호 협의하여 결정)
  - 지정된 단말기를 통한 온라인 유지보수
    - ▶ 해당 기관의 장이 필요하다고 판단하고 용역업체가 제50조에 따른 보안대책에 서면으로 동의하는 경우에만 허용할 수 있으며 접속사실이 기록된 로그기록은 1년 이상 보관

▶ 보안 · 네트워크장비는 원격접속 금지(제42조)
▶ 구비서류 : [참고자료]온라인 유지보수 서약서

- 기관 업무수행에 현저한 저해가 예상되는 등의 불가피한 경우에는 인터넷망 정보시스템에 한하여 직접 접속을 허용하는 온라인 유지보수를 일시적으로 허용할 수 있음.

- 외부인력 제공 자료 보안대책
  - 외부 인력에게 용역에 필요한 최소한의 권한만 제공
  - 외부 인력의 정보시스템 접근기록 등 작업이력 점검
  - 외부 인력에게 제공되는 누출금지 대상자료(정보통신망, IP 현황, 선번장 등)는 무단 복사 · 반출 되지 않도록 관리 철저
    ▶ 구비서류 – [참고자료] 자료 인계인수대장
  - 용역사업 관련 자료의 자료 전송 시 첨부자료 암호화 후 수·발신

- **정보화관련 용역사업 종료 시 조치사항**
  - 용역업체로부터 용역 결과물을 전량 회수하고 비인가자에게 제공, 열람 금지
  - 사업 종료 시 외부업체의 노트북, 휴대용 저장매체 등을 통해 비공개 자료가 유출되는 것을 방지하기 위하여 복구가 불가능하도록 완전삭제
  - 용역사업 관련자료 회수 및 삭제조치 후 업체에게 복사본 등 용역사업관련 자료를 보유하고 있지 않다는 **업체대표 명의 보안확약서 징구**
    ▶ 구비서류 – [참고자료] 보안확약서(업체대표 명의)

참고자료

- 참여인원(업체대표) 보안서약서
- 외부용역 업체직원 보안교육
- 정보시스템 원격 접속 관리대장
- 원격지 온라인 개발 서약서
- 출입통제대장
- 온라인 유지보수 서약서
- 자료 인계인수대장
- 보안확약서(업체대표 명의)

참고자료 참여인원 보안서약서

[참여인원용]

보안서약서

본인은 년 월 일부로 _____와 관련한 업무(용역, 연구개발, 제작, 입찰, 그 밖의 업무)를 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약한다.

1. 본인은 관련 업무중 알게될 일체의 내용이 직무상 기밀사항임을 인정한다.
2. 본인은 이 기밀을 누설함이 국가안전보장 및 국가이익에 위해가 될 수 있음을 인식하여 업무수행 중 지득한 제반 기밀사항을 일체 누설하거나 공개하지 아니한다.
3. 본인은 사업주관 기관의 정보보안 기본지침을 준수한다.
4. 본인은 이 기밀을 누설하거나 관계규정을 위반한 때에는 관련 법령 및 계약에 따라 어떠한 처벌 및 불이익도 감수한다. 다만 「부패방지 및 국민권익위원회의 설치와 운영에 관한 법률」에 따른 부패행위 신고 및 「공익신고자 보호법」에 따른 공익 신고 등을 위한 목적일 경우 비밀준수 의무를 위반하지 않은 것으로 본다.

   가. 전자정부법 제35조(금지행위) 및 제76조(벌칙)

년 월 일

서약자	소속	직급		
(참여인원)		직위	성 명	인
서 약	소속	직급		
집행자		직위	성 명	인

참고자료 업체대표 보안서약서

[업체대표용]

보안서약서

본인은 년 월 일부로 _____와 관련한 업무(용역, 연구개발, 제작, 입찰, 그 밖의 업무)를 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약한다.

1. 본인은 관련 업무중 알게될 일체의 내용이 직무상 기밀사항임을 인정한다.
2. 본인은 이 기밀을 누설함이 국가안전보장 및 국가이익에 위해가 될 수 있음을 인식하여 업무수행 중 지득한 제반 기밀사항을 일체 누설하거나 공개하지 아니한다.
3. 본인은 사업주관 기관의 정보보안 기본지침을 준수한다.
4. 본인은 이 기밀을 누설하거나 관계규정을 위반한 때에는 관련 법령 및 계약에 따라 어떠한 처벌 및 불이익도 감수한다. 다만 「부패방지 및 국민권익위원회의 설치와 운영에 관한 법률」에 따른 부패행위 신고 및 「공익신고자 보호법」에 따른 공익 신고 등을 위한 목적일 경우 비밀 준수 의무를 위반하지 않은 것으로 본다.

   가. 전자정부법 제35조(금지행위) 및 제76조(벌칙)

년 월 일

서약자	소속	직급		
(업체대표)		직위	성 명	인
서 약	소속	직급		
집행자		직위	성 명	인

참고자료 외부용역 업체직원 보안교육

외부용역 업체 직원 보안교육

관련근거	경기도교육청 정보보안 기본지침 제26조(용역업체 보안)	
교육내용		교육 여부 (O,X)
◇ 유지보수 인력은 당해 기관의 사전 승인을 득하고, 보안서약서 제출		( )
◇ 통제구역 출입시 담당자와 동석해야 하고 임의 출입금지		( )
◇ 통제구역 출입시 화재위험이 있는 물품 소지 금지		( )
◇ 유지보수 업무 영역 외 타시스템 접근 금지		( )
◇ 정보시스템과 연결하여 자료 유출 가능성이 있는 USB, 스마트폰 등 휴대용 저장매체의 비인가 사용금지		( )
◇ 카메라 내장 휴대폰, 디지털 카메라 등 소지 및 촬영금지		( )
◇ 노트북 및 USB 등 정보시스템 사용 시 악성코드 등 감염여부 확인 및 자료 복사금지		( )
◇ 취급하는 비공개정보(정보통신망, IP, 비밀번호 등) 복사 및 유출 금지		( )
교육일시	2000 . . .	
피교육자	※ 본인은 상기 보안 교육사항을 성실히 준수한다. (소속) (성명) (서명)	
교 육 자	(소속) (성명) (서명)	

참고자료 정보시스템 원격 접속 관리대장

정보시스템 원격 접속 관리대장

원격접속 사용자			목적지 IP	접속 시간	접속사유	접속 후 조치사항	확인자(서명)	
소속	성명	원격 IP					보호시스템 관리자	정보보안 담당관

참고자료 원격지 온라인 개발 서약서

원격지 온라인 개발 서약서

본인은 년 월 일부로 (_____)와 관련한 개발 용역을 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 지정된 단말기에서만 접속 및 해당 단말기에 대한 접근인원 통제
2. 지정 단말기는 제3호에 따른 온라인 용역 통제시스템 접속 전용(專用)으로 운용하고 다른 목적의 인터넷 접속은 차단
3. 발주기관내 설치된 온라인 용역 통제시스템을 경유하여 개발에 필요한 정보시스템에 접속하는 등 소통구간 보호·통제
4. 접속사실이 기록된 로그기록을 1년 이상 보관
5. 계약 시행일로부터 종료 후 30일이 경과하는 날까지의 기간 중에 발주기관, 발주기관의 상급기관 및 국가정보원장의 정기 또는 수시 보안점검(불시 점검을 포함한다) 수검
6. 기타 국가정보원장이 배포한「국가·공공기관 용역업체 보안관리 가이드라인」에서 제시된 온라인 개발에 관련된 보안대책의 준수

년 월 일

서약자	소속	직급		
(참여인원)		직위	성 명	인
서 약	소속	직급		
집행자		직위	성 명	인

※ 온라인 개발이 필요하다고 판단하는 경우, 보안대책에 서면으로 동의하는 경우에 한하여 개발작업 허용 가능[정보보안 기본지침 제28조의2(원격지에서의 온라인 개발)]

참고자료 출입통제대장

출입통제대장

년월일	출입시간 및 퇴실시간	용 무	출입자		입회자		비고
			소속	성명 (연락처)	직급	성명	

참고자료 **온라인 유지보수 서약서**

서 약 서

본인은 년 월 일부로 (_____)와 관련한 유지관리 용역을 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 지정된 단말기에서만 접속 및 해당 단말기에 대한 접근인원 통제
2. 지정 단말기는 제3호에 따른 온라인 용역 통제시스템 접속 전용(專用)으로 운용하고 다른 목적의 인터넷 접속은 차단
3. 발주기관내 설치된 온라인 용역 통제시스템을 경유하여 개발에 필요한 정보시스템에 접속하는 등 소통구간 보호·통제
4. 접속사실이 기록된 로그기록을 1년 이상 보관
5. 계약 시행일로부터 종료 후 30일이 경과하는 날까지의 기간 중에 발주기관, 발주기관의 상급기관 및 국가정보원장의 정기 또는 수시 보안점검(불시 점검을 포함한다) 수검
6. 기타 국가정보원장이 배포한「국가·공공기관 용역업체 보안관리 가이드라인」에서 제시된 온라인 개발에 관련된 보안대책의 준수

년 월 일

서약자	소속	직급		
(참여인원)		직위	성 명	인
서 약	소속	직급		
집행자		직위	성 명	인

※ 온라인 유지보수가 필요하다고 판단하는 경우, 보안대책에 서면으로 동의하는 경우에 한하여 유지보수 허용 가능(보안·네트워크 장비는 제외)

참고자료 | 자료 인계인수 대장

자료 인계인수 대장

※ 대상자료 현황 및 인계인수 사항

일시	자료명	자료기준일	파일명 (자료유형)	암호화 여부 (O, X)	기록사항	자료 인계인수 목적	인계자	인수자
20xx.00.00 10:00~ 11:00	0000 대장	20xx. 00.00	열람	O	시스템명,IP,계정(ID및PW) (방화벽, IP관리시스템, ...)	유지관리 정기점검	서명	서명
20xx.9.1 14:30~ 16:00	0000 대장	20xx. 3.1	서면 제공	X	시스템명,IP,계정(ID및PW) (방화벽, IP관리시스템, ...)	유지관리 정기점검	홍xx	박xx
20xx.9.1 16:00	0000 대장	20xx. 3.1	서면 제공	X	시스템명,IP,계정(ID및PW) (방화벽, IP관리시스템, ...)	회수	박xx	홍xx

▣ 자료관리 준수사항

◦ 자료 인계인수 제공 목적이 완료되면 즉시 회수

▣ 동 서식은 학교의 실정 및 인계·인수사항에 따라 수정하여 사용 가능

참고자료 보안확약서(업체대표 명의)

보 안 확 약 서

본인은 귀 기관과 계약한 _____ 사업의 수행을 완료함에 있어, 다음 각 호의 보안사항에 대한 준수 책임이 있음을 서약하며 이에 확약서를 제출합니다.

1. 본 업체는 업체 및 사업 참여자가 사업수행 중 알게 된 모든 자료를 반납 및 파기하였으며, 알게 된 정보에 대한 유출을 금지하겠습니다.

2. 본 업체는 하도급업체에 대해 상기 항과 동일한 보안사항 준수 책임을 확인하고 보안확약서를 징구하였으며, 하도급업체가 위의 보안사항을 위반할 경우에 주사업자로서 이에 따른 법적 책임을 지겠습니다.

3. 본 업체는 상기 보안사항을 위반할 경우에 귀 기관의 사업에 참여 제한 또는 기타 관련 법규에 따른 책임과 손해배상을 감수하겠습니다.

년 월 일

서 약 자	업 체 명 :	
(업체 대표)	직 위 :	
	성 명 :	(서명)
서약집행자	소 속 :	
(담당공무원)	직 위 :	
	성 명 :	(서명)

7 정보통신망 현황자료 관리

관련근거

- 정보보안 기본지침 제69조(정보통신망 현황자료 관리)
- 정보보안 기본지침 제40조(내부망·인터넷망 분리)
  - 참 참고자료 : 국가·공공기관 망 분리 및 자료전송 보안 가이드라인, 학교전산망 구축·운영 계획

업무시기

- 상시

주요내용

- **아래 정보통신망 관련 현황·자료는 「공공기관의 정보공개에 관한 법률」제9조제1항에 따른 비공개 대상 정보로 지정 · 관리하여야 함**
  - 정보통신망 구성현황(IP주소 할당현황 포함)
  - 정보시스템 운용현황
  - 취약점 분석·평가 결과물
  - 주요 정보화사업 추진현황

※ 네트워크 구성도 및 선번장은 학교전산망 구축 시 구축업체로부터 제공되어 보유하여야 하나 현재 미보유하고 있는 학교는 유지보수 업체를 활용하여 관련 자료 정비 및 작성 권고

참고자료

- **정보시스템 관리대장**
- 정보통신망 세부 구성 현황(예시)

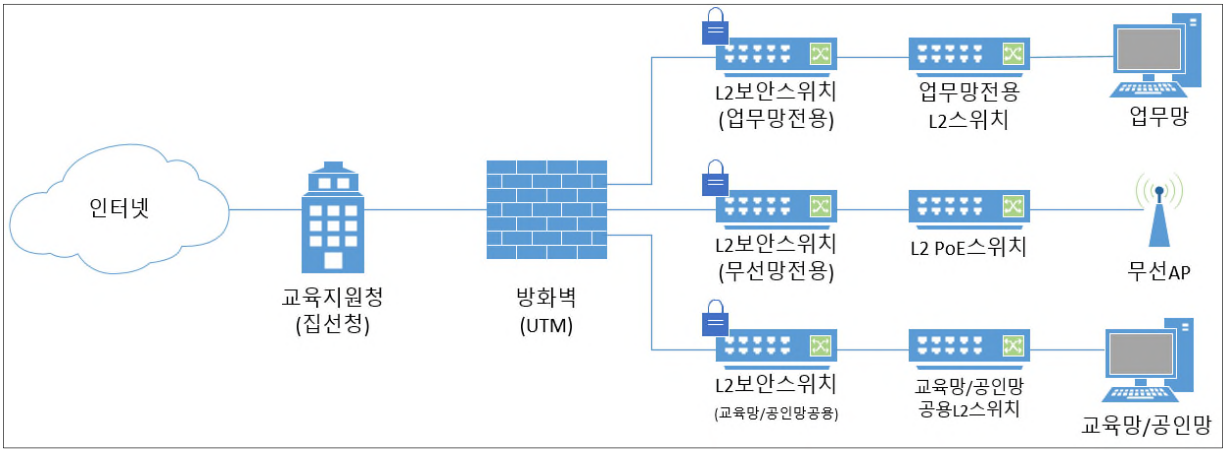
참고자료 정보시스템 관리대장

정보시스템 관리대장

연번	소속	취급자 성명	종류 (PC 등)	제조사	모델명	관리번호	도입일자	관리자 확인	비고
1	000	교사 000	정보보호 시스템	000	000	S-01	2022.5.19.	교사 000	스쿨넷 장비
2	000	교사 000	L2보안스위치	000	000	N-01	2022.5.19.	교사 000	스쿨넷 장비
3	000	행정실무사 000	L2스위치	000	000	N-02	2022.5.19.	교사 000	스쿨넷 장비
4	000	주무관 000	UPS	. . .			2016.12.19		학교 장비

참고자료 정보통신망 세부 구성 현황(예시)

학내망 네트워크 구성도 예시



용|어|설|명

- **업무망:** 교무실 등에서 교직원들이 업무용으로 사용하는 컴퓨터가 연결된 망
- **무선망:** 교육용 무선인터넷 서비스를 위한 무선AP를 설치하는 망
- **교육망:** 학생의 교육목적을 위하여 컴퓨터실, 스마트실, 과학실, 도서실 등에서 사용하는 인터넷망
- **공인망:** 각급학교에서 자체 서비스 중인 서버(홈페이지, 자체메신저, 시간표, 알리미 등)를 분리하여 운영하는 공인망

IP주소 세부 할당 현황

IP주소 세부 할당 현황

연번	장비명(모델명)	설치장소	*관리번호	취급자	IP Address	비고
1	방화벽	정보통신실		김○○	10.***.***.1	방화벽 GW
2	보안L2스위치	정보통신실		김○○	10.***.***.2	보안스위치
:	:	:	:	:	:	:
5	L2스위치	정보통신실		김○○	10.***.***.5	통신장비
6	L2스위치	정보통신실		김○○	10.***.***.6	
:	:	:	:	:	:	:
21	프린터_#1	교무실		이○○	10.***.***.21	사무기기
22	프린터_#2	교무실		박○○	10.***.***.22	사무기기
:	:	:	:	:	:	:
71	데스크탑_#1	교장실		최○○	10.***.***.71	업무용
72	노트북_#2	교무실		정○○	10.***.***.72	업무용
:	:	:	:	:	:	:
266	데스크탑_#1	컴퓨터실		강○○	10.###.###.11	학생용
267	데스크탑_#2	컴퓨터실		조○○	10.###.###.12	학생용
:	:	:	:	:	:	:

※ 관리번호는 정보보안 기본지침 [서식 제3호]정보시스템 관리대장의 관리번호와 일치시킬 것을 권고

8 무선랜 보안

관련근거

- 정보보안 기본지침 제43조(무선랜 보안)
  참 참고자료 : 국가 · 공공기관의 무선랜 구축 보안가이드라인, 학교전산망 구축·운영 계획

업무시기

- 사안발생시

주요내용

- **각급학교 교육용 무선인터넷 구축 원칙**
  - 각급학교의 경우 내부망(업무망)을 제외한 정보통신망에서 학생들의 교육목적으로 사용하고자 할 경우 학교장 책임하에 무선인터넷을 구축 · 운용 할 수 있음
  - 무선인터넷 구축 관련 세부사항은 학교전산망 구축·운영 계획 참조

    교육용 무선인터넷 사용 시 선행조건
    ▶ 교육(수업) 목적으로 무선인터넷망 구축 시 반드시 내부망(업무망)과 분리 (논리/물리) 되어야 함

    ※ 내부망(업무망)과 분리 : 학교 인터넷망 구간 최상단에서 단말까지, 혼용사용 불가
    ▶ 무선인터넷망에서 업무자료를 저장·이용하는 컴퓨터(노트북) 사용 금지

    교육용 단말기 보안관리
    ▶ 업무자료 저장금지
    ▶ 백신프로그램 설치 및 최신 업데이트
    ▶ OS 및 소프트웨어 최신 업데이트
    ▶ 단말기 비밀번호 설정 강화

참고자료

- 무선인터넷 사용 시 주의 사항

참고자료 무선인터넷 사용 시 주의 사항

무선인터넷 사용자

1. 모바일 전용 백신으로 주기적인 검사를 한다.
2. 비밀번호가 설정되지 않은 무선인터넷에는 접속을 자제한다.
3. 수상한 메시지 확인 시 클릭을 자제한다.
4. 제공자가 불명확한 무선인터넷은 이용하지 않는다.
5. 보안설정 없는 무선인터넷으로 민감한 서비스를 이용하지 않는다.
6. 무선인터넷에 자동 접속 기능을 사용하지 않는다.

스마트폰 정보보호 실천수칙

1. 공식 앱 마켓이 아닌 다른 출처(출처를 알 수 없는 앱)의 앱 설치 제한하기
2. 단문 문자(또는 SNS) 메시지에 포함된 URL 클릭하지 않기
3. 공인인증서는 USIM 등 안전한 저장장소에 보관하기
4. 스마트폰 운영체제와 모바일 백신을 항상 최신으로 업데이트하기
5. 스마트폰 보안 잠금(비밀번호 또는 화면 패턴)을 설정하여 이용하기
6. 루팅, 탈옥 등 스마트폰 구조를 임의로 변경하지 않기
7. 스마트폰 앱 설치시 과도한 권한을 요구하는 앱은 설치하지 않기
8. 스마트폰 WiFi 연결시 제공자 불분명한 공유기 이용하지 않기
9. 스마트폰에 중요정보 정리하기
   - 보안 소프트웨어 실행하여 PC, 스마트폰의 바이러스도 삭제
   - 주민등록증, 보안카드가 찍힌 사진 등은 보관하지 말고 삭제

9 인터넷전화 보안

관련근거

- 정보보안 기본지침 제46조(인터넷전화 보안)
  참 참고자료 : 국가·공공기관 인터넷전화 보안 가이드라인, 학교전산망 구축·운영 계획

업무시기

- 사안발생시

주요내용

- **각급 학교 인터넷전화 구축 보안**
  - 내부망(업무망)을 제외한 정보통신망에서 구축 권장
    ※ [상세예시] 학교 인터넷전화 물리적/논리적 망분리 참고
  - 인터넷전화 구축 관련 세부사항은 학교전산망 구축·운영 계획 참고
  - 민간인터넷전화 사업자망을 이용할 경우 해당 사업자로 하여금 서비스 제공 구간에 대한 보안대책을 수립하도록 안내

- **인터넷전화 망혼용 개선 방법**
  - 백본스위치 분리 : 학교전산망 스쿨넷 백본스위치에서 VLAN을 설정하여 논리적 분리
  - 워크그룹스위치 분리
    - 인터넷전화 전용 스위치가 없을 경우, 기존 워크그룹(백본/업무망) 스위치를 VLAN 설정하여 논리적으로 분리한 후 네트워크 케이블을 분리하여 포설
    - 인터넷전화 전용 스위치가 있을 경우 네트워크 케이블을 분리하여 포설
  - 학교정보화 현장지원시스템을 활용하여 현장지원컨설팅을 신청하여 망분리 여부 점검
    - 학교정보화 현장지원시스템(http://support.goeia.go.kr)

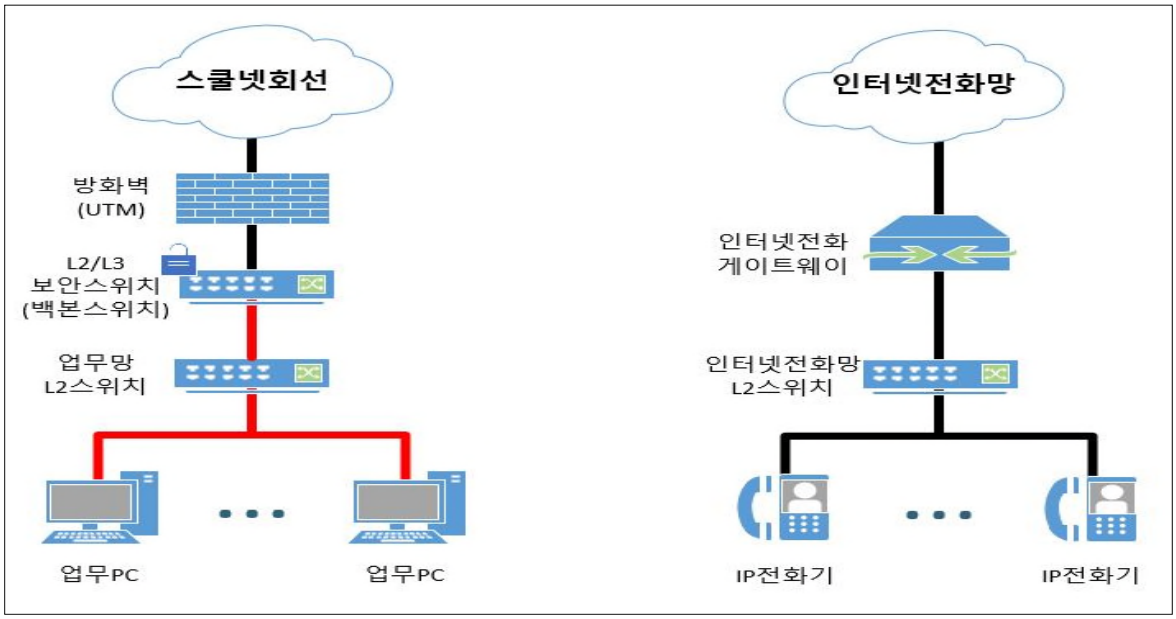
참고자료

- 학교 인터넷전화망 구성(예시)
- 인터넷전화망과 학내망이 혼용된 잘못된 사례(DHCP사용금지)

참고자료 학교 인터넷전화망 구성(예시)

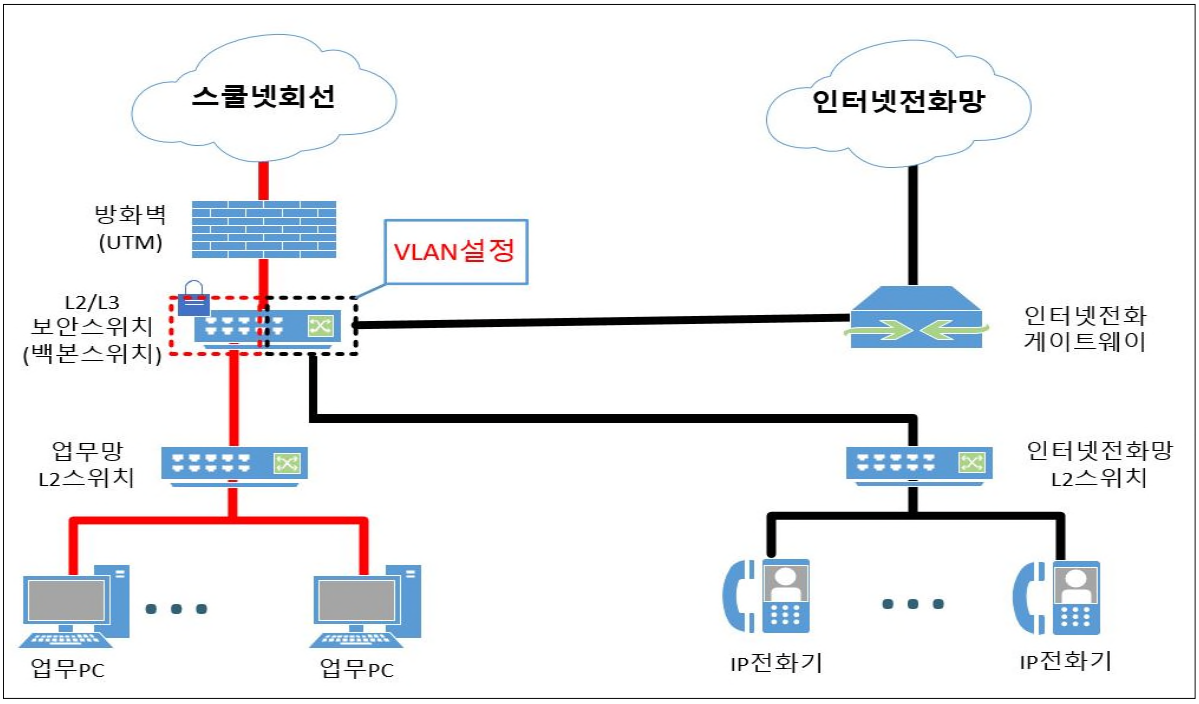
1. 물리적 망분리

스쿨넷 회선과 학내망 간섭을 주지 않기 위해 서로 독립적으로 인터넷전화망 구축



2. 논리적 망분리

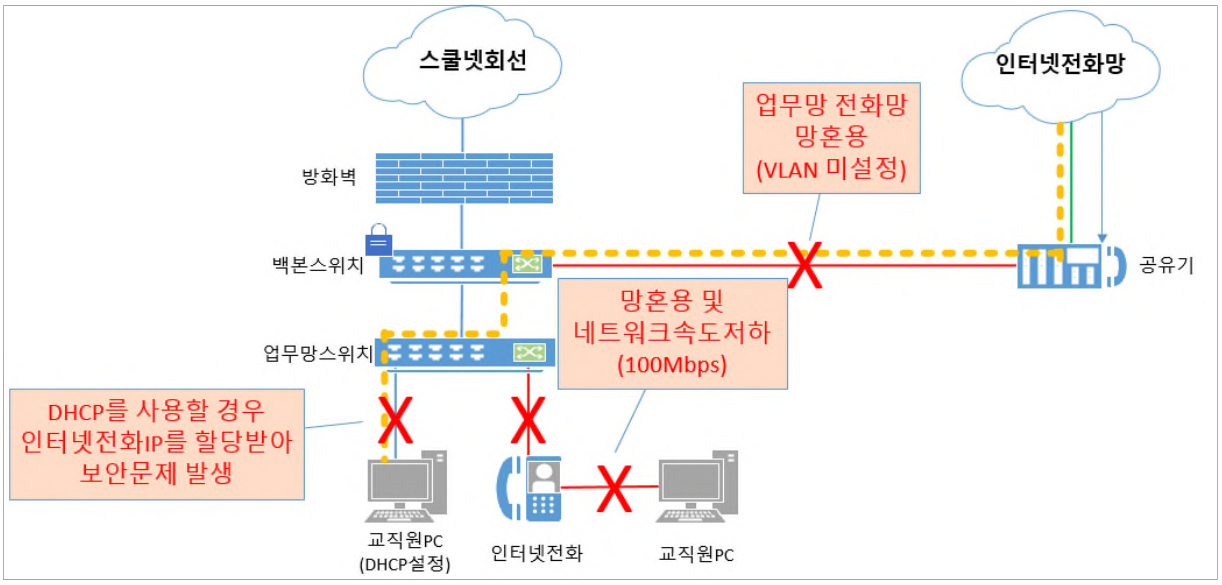
인터넷전화망 공유기에서 학내망 보안L2스위치 또는 L3스위치(백본)를 통해 논리적 망분리하여 IP 전화기로 연결하는 구조



용|어|설|명

- VLAN(Virtual Local Area Network)이란 물리적 스위치 한대를 논리적으로 나누어서 여러 개의 스위치처럼 만드는 기술로 한 대의 스위치를 업무망, 교육망, 무선망 등으로 나누어 사용하는 망구성 방법

참고자료 인터넷전화망과 학내망이 혼용된 잘못된 사례(DHCP사용금지)



- 인터넷전화용 상용인터넷(광랜 등)을 공유기에 연결하고, 공유기에서 학교 내부망의 백본스위치 또는 업무망 스위치(L2)로 연결·구성하여 인터넷전화망과 인터넷망이 혼용되는 잘못된 사례
- 공유기에서 인터넷전화기에 사용될 IP를 자동할당(DHCP 방식) 잘못된 사례
  교직원PC(업무망)에서 IP를 DHCP 방식으로 설정할 경우 공유기에서 인터넷전화용 IP를 할당받아 인터넷전화용 인터넷으로 통신함에 따라 보안 위협 발생 가능
  ※ 업무용 PC는 반드시 할당받은 업무망 고정 사설IP만 사용
- 인터넷전화기에 교직원PC를 연결하여 사용할 경우, 학교 전체 인터넷 속도 저하의 주된 원인이 됨

10 영상정보처리기기 보안

관련근거

- 정보보안 기본지침 제86조(영상정보처리기기 보안)

업무시기

- CCTV 등 영상정보처리기기 구축 · 운영 시

주요내용

- **CCTV 등 영상정보처리기기 구축 시 자체 보안성검토 이행**

- **각급 기관의 장은 영상정보처리기기에 대한 비인가자의 침입 통제대책을 강구해야 함**
  - 관리적 보안대책
    - 영상관제상황실은 보호구역으로 지정관리하고 출입통제장치(시건장치 등) 도입
    - 영상기록의 임의 열람 및 사적활용 방지대책을 마련하고 저장매체는 시건장치가 설치된 통제구역에 보관
    - 외부 경비서비스 이용시 제공업체에 대해 주기적인 보안점검을 실시하며 보안관리에 대한 보장 내역을 계약서에 명시
  - 기술적 보안대책
    - 영상정보처리기기 운용에 필요한 시스템(CCTV, IP카메라, 이동형 영상촬영장비, 중계서버, 관제서버, 관리용 PC 등의 기기 · 장비, 관련 전산망 등) 설치 시 업무망(교사망) 및 인터넷과 분리하여 별도 단독망 구성을 원칙으로 함
    - 부득이하게 인터넷망을 이용할 경우 전송내용을 암호화해야 함
    - 비인가자의 접근을 방지하기 위해 원격접근 서비스 차단설정, 관제용 서버IP만 접근 가능하도록 제한, 초기 패스워드 변경, 카메라IP 외부 공개 금지 등 보안조치
    - 관제시스템, 관리용PC는 최신 백신 설치, 비인가 USB메모리 사용금지 등 보안조치

- **사업부서가 CCTV 등 영상정보처리기기 구축 · 운영 시 정보보안담당자는 위 보안사항이 적용될 수 있도록 지원**

11 디지털 복합기 보안

관련근거

- 정보보안 기본지침 제88조(디지털복합기 보안)
  참 참고자료 : 정보시스템 저장매체 불용처리지침

업무시기

- 디지털복합기 도입(임대 포함) · 운영 시

주요내용

- **디지털복합기(디지털복사기 등도 포함, 이하 '복합기')를 설치 · 운용하고자 할 경우 복합기 내 저장매체가 있거나 장착이 가능한 경우 자료 완전삭제 또는 디스크 암호화 기능이 탑재된 복합기를 도입하여야 함**

  ※ (검증정책 2022-2호)에 따라 사전인증요건(CC인증 또는 보안기능확인서 등)과 무관하게 도입기관의 자체 판단에 의해 사전인증요건을 지정할 수 있음

  ※ 공급망 보안 강화 예방조치 : IT보안제품 도입시 우리나라를 비롯, 국제사회의 제재를 받는 국가(단체) 연루 여부 확인

  ▶ (검증정책 2022-2호) IT보안제품 보안적합성 검증체계 개편 통보(2022.10월)

- **복합기 운용 보안대책 수립 시 포함할 사항**
  - 암호화 저장 기능이 있는 경우 해당 기능사용
  - 정기적으로 저장된 작업 내용(출력 · 스캔 등) 완전 삭제
  - 공유 저장소(복합기 디스크) 사용 제한 및 접근 제어
  - 고정 IP주소 설정 및 불필요한 서비스 제거(USB출력, Wifi연결 등)

- **저장매체에 저장된 자료를 완전 삭제해야 하는 경우**
  - 복합기 사용연한이 경과하여 폐기 · 양여할 경우
  - 복합기 무상 보증기간 중 저장매체 또는 복합기 전체를 교체할 경우
  - 고장 수리를 위한 외부 반출 등의 사유로 해당 기관이 복합기의 저장매체를 통제 관리할 수 없는 장소로 이동할 경우
  - 그 밖에 저장자료의 삭제가 필요하다고 판단되는 경우

- **분임정보보안담당관 또는 정보보안담당관은 저장매체가 내장된 복합기 현황을 파악하여, 사고수리 이력 등을 기록 · 유지하고 복합기 유지관리 시 감독 철저**

- **복합기를 통해 업무망(교사망)과 학생망간 접점이 발생하지 않도록 공용으로 사용하지 않도록 조치**

제3장 안전성 확인

1 보안성 검토

관련근거

- 정보보안 기본지침 제14조 ~ 제19조

업무시기

- 정보화 사업 수행 계획 단계

주요내용

- **(검토시기) 정보화사업을 수행하고자 할 경우 추진하고자 하는 정보화사업과 관련한 보안대책의 적절성을 평가하기 위하여 사업 계획단계(사업 공고 전)에서 보안성 검토 이행**

- **(검토기관) 학교(자체), 경기도교육감, 국가정보원장**
  - 자체 보안성 검토 시, 소속 학교 정보보안담당관에게 의뢰
  - 상위기관(국가정보원장 또는 경기도교육감)에 보안성 검토 의뢰 시, 소속 학교 정보보안담당관 및 해당지역 교육지원청 정보보안담당관 사전검토 후 의뢰
    ※ 경기도교육청 정보보안 기본지침 제15조~제16조 참조

- **(보안성검토 대상 정보화사업)**

[학교(자체)]

- 영상회의시스템을 내부망 또는 기관 인터넷망과 분리하여 구축
- 영상정보처리기기를 인터넷과 분리하여 구축
- 백업시스템 구축
- 대민 콜센터시스템 구축
- 국가정보원 보안성검토 대상 정보화사업에 해당하지 아니하며, 예산 5억원 미만 또는 개인정보가 5만건 미만인 정보화사업
- 기타 해당기관의 장이 필요하다고 판단하는 정보통신망 또는 정보시스템 구축

[경기도교육감]

- 홈페이지 및 웹메일 등 웹기반 정보시스템 구축
- 인터넷전화시스템 구축(학교제외)
- 다른 기관의 정보통신망 또는 정보시스템과 연동하여 정보의 소통 또는 서비스를 제공하는 정보시스템 구축

- 상용 인터넷망(무선랜* 포함)의 구축
  ※ 상용 인터넷망에 중계기(AP)를 설치하여 공무원등의 개인 소유 이동통신단말기의 접속만을 허용하는 무선랜 또는 외부인 전용 무선랜
- 내부망에 구축하는 공무원등의 인사·복지시스템
- 주요정보통신기반시설 취약점 분석 · 평가, 정보보안컨설팅 등 용역사업
- 기존 분리된 내부망 · 기관 인터넷망간 자료전송시스템 구축 등 후속사업
- 대규모 백업 · 재해복구센터 구축

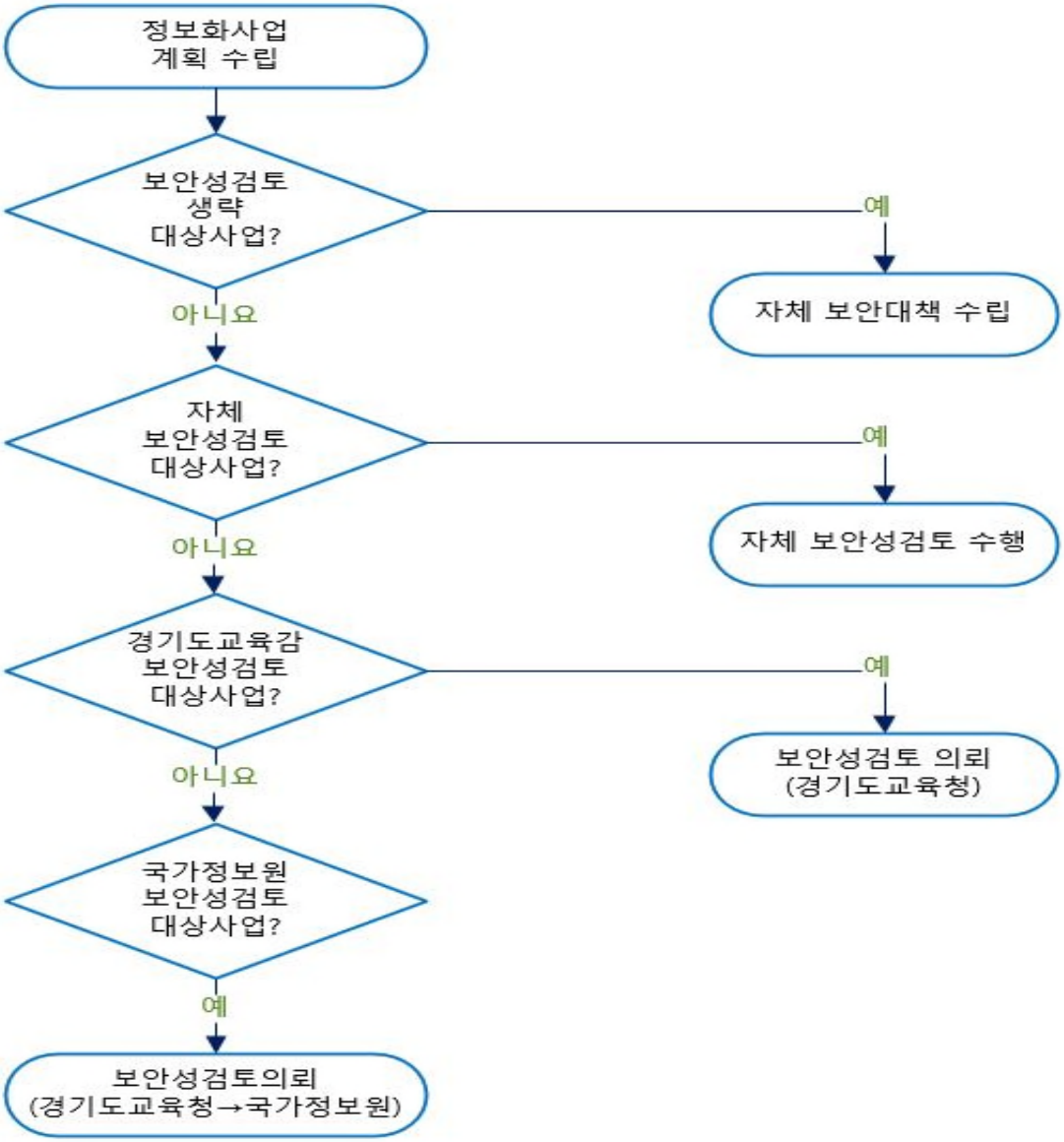
[국가정보원장]

- 100만명 이상의 개인에 대한「개인정보보호법」상 민감정보 또는 고유식별정보를 처리하는 정보시스템 구축
- 국가정보통신망 등 여러 기관이 공동으로 활용하기 위한 정보통신망 또는 정보시스템 구축
- 내부망 또는 폐쇄망을 인터넷 또는 다른 정보통신망과 연동하는 사업
- 내부망과 기관 인터넷망을 분리하는 사업
- 기관 인터넷망 등 소속 공무원등이 업무상 목적으로 이용하도록 하기 위한 인터넷망(무선랜* 포함) 및 이동통신망(HSDPA, WCDMA, LTE, 5G 등) 등 구축
  ※ 기관 인터넷망에 중계기(AP)를 설치하여 해당 기관의 장이 지급한 단말기의 접속만을 허용하는 업무용 무선랜
- 클라우드컴퓨팅서비스 제공자의 민간 클라우드컴퓨팅서비스를 이용하는 사업
- 첨단 정보통신기술을 활용하는 정보화사업으로서 국가정보원장이 해당기술에 대하여 안전성 확인이 필요하다고 지정하는 사업

- **(검토 생략) 다음의 정보화사업에 대하여는 보안성 검토 절차를 생략하고, 관련 지침 · 보안 가이드라인 등을 준수하는 등 자체 보안대책 수립 후, 시행**
  - 검토기관별 보안성검토 대상 정보화사업에 해당하지 않는 단순장비 · 물품 도입
  - 서버 · 스토리지 · 네트워크장비 등 장비 노후화로 인한 단순 장비 교체
  - 전화기 · 무전기 · CCTV 등 통신 · 영상기기의 노후화로 인한 단순 장비 교체
  - 기존 운용하던 정보보호시스템을 동일한 보안기능을 보유한 다른 정보보호 시스템으로 교체
  - PC · 프린터 및 상용 소프트웨어 등 단순 제품 교체
  - 「유아교육법」제2조의 유치원과 「초·중등교육법」제2조 각 호의 학교에 해당하는 인터넷전화시스템 구축
  - 교육현장에서 구축하는 무선랜, 클라우드 및 이동통신망 사업

- **보안성 검토 의뢰 시 제출 문서**
  - 사업계획서(사업목적 및 추진계획 포함)
  - 제안요청서
  - 정보통신망 구성도(필요시 IP주소체계 포함)
  - 자체 보안대책(관리적, 물리적, 기술적 보안대책 포함)

보안성 검토 절차



※ 각급학교 보안성 검토 절차 정보화사업 추진부서 → 기관 정보보안담당관→ 교육지원청 정보보안담당관(사전검토)→ 경기도교육청

참고자료

- 보안성 검토 요청 기안문(예시)
- 자체 보안성 검토 기안문(예시)
- 자체 보안대책(예시)
- 정보화사업 보안성 검토 체크리스트

참고자료 보안성 검토 요청 기안문(예시)

기안문

○ ○ 학 교

수신 ○○교육지원청
(경유)
제목 ○○시스템 도입(교체)에 따른 보안성 검토 요청

1. 관련 : 경기도교육청 정보보안 기본지침 제14~19조

2. ○○시스템 도입(교체)에 따른 보안성 검토를 [붙임]과 같이 요청하오니 보안성 검토 결과를 회신하여 주시기 바랍니다.

붙임 1. 사업계획서 1부.
2. 제안요청서 1부.
3. 정보통신망 구성도 1부.
4. 자체 보안대책 1부(예시 참조). 끝.

○ ○ 학교장

수신자

★담당자 부장 교감 교장

협조자

( ) 접수 ( )

우 00000 경기도 00시 00구 00로 00 (00동, 000) /
전화번호 031- /팩스번호 031- / / 비공개

참고자료 자체 보안성 검토 기안문(예시)

기안문

○ ○ 학교

수신 (내부결재)
(경유)
제목 ○○시스템 도입(교체)에 따른 자체 보안성 검토(보안대책 수립)

1. 관련 : 경기도교육청 정보보안 기본지침 제14~19조

2. ○○시스템 도입(교체)사업의 안정적 추진을 위하여 [붙임]과 같이 보안 적절성을 강구한 자체 보안대책을 수립하여 본 사업 추진에 만전을 기하고자 합니다.

붙임 1. 사업계획서 1부.
2. 제안요청서 1부.
3. 정보통신망 구성도 1부.
4. 자체 보안대책 1부(예시 참조). 끝.

★담당자 부장 교감 교장

협조자

( ) 접수 ( )

우 00000 경기도 00시 00구 00로 00 (00동, 000) /
전화번호 031- /팩스번호 031- / / 비공개

참고자료 자체 보안대책(예시)

자체보안대책

자 체 보 안 대 책 (예 시)

(※학교실정에 맞게 수정하여 사용)

※ [서식] 정보화사업 보안성 검토 체크리스트를 참조하여 학교에서 추진하고자 하는 정보화사업에 해당되는 부분 작성

Ⅰ 개 요

가. 사업명 :

나. 목적

-

다. 근거

- 정보보안 기본지침 제14조 ~ 제19조

라. 필요성

-

마. 보안대책 강구사항

- 보안관리체계(조직, 인원) 구축 등 관리적 보안대책
- 정보시스템 설치운용장소에 대한 보안관리 등 물리적 보안대책
- 각종 서버, 네트워크 등 정보통신시스템 요소별 기술적 보안대책
- 긴급사태 대비 및 재난복구계획
- 용역업체 작업장소에 대한 보안대책
- 온라인 개발 또는 온라인 유지보수가 필요하다고 판단할 경우, 원격지에서의 온라인 개발 또는 지정 단말기를 통한 온라인 유지보수에 따른 보안대책
- 누출금지정보 보안관리 방안

II 보안대책

1. 보안 기본방침

○ 모든 시스템은 정보통신실(통제구역)에 두어 내·외부로의 접근을 원칙적으로 차단

○ 추진하는 정보화사업에 대한 관리적, 물리적, 기술적으로 적정한 보안 대책 수립

○ 정보화사업 수행 시 참여인력, 각종 시스템보안 등의 정보보안 사고를 예방하기 위한 보안 대책 강구

○ 정보화사업 종료에 따른 시스템 운영 시, 주기적인 보안점검으로 보안정책 및 지침의 준수 여부 확인

2. 관리적 보안대책

○ 보안관리 수행체계

구 분	부서명	직위/직급	성명	비고
정보화사업 총괄책임자				
보안담당관				
정보보안담당관				
정보화사업 담당자				

○ 역할

- 정보화사업 총괄책임자 : 추진하는 부서의 장은 정보화사업에 대한 보안관리 책임을 지고 관리·감독 실시
- 정보화사업 담당자 : 추진하는 정보화사업을 담당하는 담당자는 해당 정보화사업에 대한 보안관리 수행
- 정보보안담당관/보안담당관 : 정보화사업과 관련한 보안대책의 적절성을 평가하고 정보화사업 수행 전반에 대하여 보안대책의 이행여부 점검 등

○ 업무수행에 지장을 초래하는 보안사고가 발생한 때에는 피해를 최소화하기 위한 조치를 즉시 취하고 다음과 같은 사항을 보고절차에 의하여 관계기관에 통보

- 일시 및 장소
- 사고원인, 피해현황 등 개요
- 사고자 및 관계자의 인적사항
- 조치내용 등

❍ 보안사고의 범위
- 비밀의 유출
- 주전산기(주요 서버 등)·대용량 전자기록(DB) 손괴
- 전자정보의 위조·변조·훼손 및 유출
- 정보통신망에 대한 해킹·악성코드의 유포
- 전산시스템 및 정보통신실 파괴
- 고의적인 중요 전산시스템 기능 장애 및 정지 등

❍ 작업 장소 보안 관리

1) 용역업체 작업장소에 대한 보안 대책
- 용역업체의 작업용 PC 등 단말기는 사업 수행과 관련 없는 정보통신망과 분리 구성
- 시스템 설치 및 홈페이지 구축 등 사업 수행 시 불가피할 경우 필요한 정보시스템에 한해 지정된 단말기로부터의 제한적 접근 허용
- 기타 용역사업 수행을 위해 필요한 경우 해당 정보보안담당관의 보안통제 하에 제한적 허용

2) 용역업체가 원격지 개발 작업 수행 요청할 경우, 용역업체 작업장소에 대한 보안요구사항 등을 포함한 관리적, 기술적 보안대책 징구
- 지정된 단말기에서만 접속 및 해당 단말기에 대한 접근인원 통제
- 원격지 개발을 위해 접속한 시스템에 대한 접속 로그 기록 관리
- 해당 시스템에 대한 정기 또는 수시 보안 점검 실시

3. 물리적 보안대책

1) 시스템 전산 자원을 보호하고 재해로부터 안전을 도모하기 위하여 보호구역 (제한구역, 통제구역)을 설정하고 외부 출입자 및 허가받지 아니한 자의 출입 통제에 관한 사항을 관리

2) 통제구역 지정 : ○○○학교 ○층 서버실(정보통신실)

3) 통제구역 운영
- 설치장소 출입문에 통제구역 표식 부착
- 별도의 출입통제장치(이중 시건장치, 카드식출입통제 등)를 마련하고 정상적으로 작동하는지 수시 점검

4) 통제구역 출입자 관리
- 통제구역 출입자명부 비치하여 모든 방문자 출입기록 유지
- 통제구역은 상시출입 인가자 이외 출입 통제
- 방문자에 대해서는 정보보안담당관이 신분 및 방문 목적을 확인하여 입실 여부를 허가해야 하며, 담당자는 통제구역 출입자 명부를 작성하여 기록 유지
- 유지관리 담당자는 보안준수 사항을 포함한 보안교육을 실시하고 보안서약서 징구
- 필요 시 출입자에 대한 카메라, 휴대폰 등 불법 촬영을 금지하고, 인화물질, 자석 등으로 인한 데이터의 손실을 사전에 예방

5) 정보통신실 보안대책
- 정전에 대비하여 별도의 무정전 전원공급시설을 설치・운영(권고)
- 온・습도를 적절히 유지할 수 있는 항온항습장치 설치・운영(권고)
- 화재에 대비하여 소화 설비 설치
- 배수가 잘되도록 배수 설비를 갖추고 누수경보기 설치
- 관리책임자 및 자료・장비별 취급자 지정 운영

4. 기술적 보안대책(※해당되는 정보화사업 작성)

1) 홈페이지 구축 보안 대책
- 웹서버 및 웹 어플리케이션 환경 설정 시 불필요한 서비스를 제거하고 보안설정 사전 확인
- '웹서버 보안취약점 대응 가이드'를 참고하여 취약점 제거
- 웹사이트 내 모든 유형의 웹페이지 콘텐츠에 대하여 개인정보 노출 점검 및 차단 기능 적용(개인정보 유・노출 상시 점검)
- 회원 및 관리자 접근 웹페이지 로그인 시 안전한 로그인을 위한 보안 적용
- 사용자 접근권한은 업무에 따라 차등 설정・관리
- DBMS에 개인정보 암호화 적용(민감 개인정보 취급불가 및 개인정보 암호화)
- 개인정보 입력 시 이용자가 개인정보를 입력 불가하도록 조치
- 관리자 기능은 내부망의 지정된 시스템에서만 접근 허용
- 웹 로그는 1년 이상 저장
- 홈페이지 서비스 전, 구축한 홈페이지에 대한 보안취약점 점검 및 보완 조치
- 학교 홈페이지 게시판 담당자에 대한 보안교육 실시

2) 네트워크 보안대책
- 신규 장비 및 관련 소프트웨어 도입・설치 시 기존 시스템의 변화로 인한 장애 등의 문제발생 소지에 대한 안전대책을 수립한 후 진행
- 물리적으로 안전한 장소(통제구역)에 장비를 설치하고, 비인가자의 무단출입 통제
- 원격접속은 원칙적으로 금지하고 장비 관리용 목적으로 내부망의 인가된 사용자 및 단말기만을 통하여 관리・운영
- IP주소의 체계적인 관리를 위해 사설주소체계(NAT) 적용
- 신규 네트워크장비 도입 시 제조사의 기본(default) 계정 삭제 또는 변경하고, 시스템 운영을 위한 관리자계정 별도 생성 및 비밀번호는 9자리(숫자, 문자, 특수문자 포함) 이상으로 설정
- 불필요한 서비스 포트 차단 및 사용자 계정 삭제
- 장비의 펌웨어 무결성 및 보안 취약점을 주기적으로 점검하여 최신 업데이트를 통한 최신 버전 유지
- 시스템관리자는 네트워크 장비의 접속기록을 1년 이상 유지하고, 비인가자의 접근 여부를 주기적으로 점검

3) ○○○장비(시스템) 보안대책
- 도입 장비(시스템)를 물리적으로 안전한 장소(통제구역)에 장비를 설치하고, 비인가자의 무단출입 통제

- ○○○장비(시스템)에 대한 인가되지 않은 접근을 차단하기 위하여 웹방화벽, 방화벽 등 보안시스템 설치·운영
- 정보시스템에 사용되는 IP주소를 체계적으로 관리하기 위해 사설주소체계(NAT) 를 적용하고 관리용 서비스와 사용자용 서비스를 분리하여 운영
- 내부망과 분리된 별도 네트워크 구간에 설치하고 서비스에 필요한 포트만 개방하여 운영
- 웹서버 등 외부에 공개하는 서버는 내부망과 분리된 영역(DMZ)에 설치하여 운영
- 도입 장비(시스템)의 제조사 기본 계정 및 비밀번호는 변경하여 사용하고 불필요한 서비스 제거 및 최신 보안 패치 등 보안관련 구성 설정 확인하여 보안 취약점 사전 제거
- ○○○서버 내 저장자료에 대해 업무별·자료별 중요도에 따라서 사용자의 접근 권한을 차등 부여
- ○○○서버의 관리용 서비스 접속 및 관리자 모드에 접근 가능한 단말기를 특정 IP와 MAC 주소를 부여하여 지정·운영
- 사용자의 직접적인 데이터베이스 접속을 차단하고 개인정보와 같은 중요 정보를 암호화하는 등 데이터베이스 보안 조치 실시
- 서버(장비) 운영체제 및 백신프로그램, 응용프로그램에 대한 필요한 보안패치를 주기적으로 점검하여 최신버전으로 설치
- 시스템 안정성 확보를 위하여 사용자 계정 관리 및 9자리(숫자, 특수문자, 영문자 모두 포함)이상의 비밀번호로 주기적 변경
- 외부 용역업체 등의 원격접속은 원칙적으로 차단하며, 필요한 경우에만 정보보안담당관의 승인을 받은 후 한시적으로 허용(해당 IP와 접속에 필요한 포트만 개방)
- 정보시스템의 안정적 운영을 위하여 ○○○장비(시스템)의 운영 시, 불필요한 포트 제거, FTP 제한, SNMP 서비스 제한, 불필요한 계정 삭제, 계정관리, 계정 인증 실패 등 정보시스템 보안취약 요소 정기적 점검 실시

4) CCTV 보안대책
- 카메라, 비디오서버, 관제서버, 소통망은 내부업무망 및 인터넷과 분리하여 별도 단독망으로 구성하여 설치
- 외부에 CCTV 설치 시 카메라, 중계서버는 비인가자의 임의 조작이 물리적으로 불가능하도록 위치하거나 시건장치 설치
- 인터넷 등을 이용하여 통제구역 이외 장소에서 모니터링 불가 조치
- 영상자료 유출과 영상기록의 임의열람 및 사적활용 방지대책 마련
- 영상자료 저장매체는 비인가자의 접근이 불가능하도록 시건장치가 설치된 통제구역에 보관

5. 용역업체 보안관리(※필수)

1) 정보화 용역사업 계약 시 보안대책
- 제안요청서 및 계약서에 누출금지 대상정보, 위반 시 손해 배상 책임(위약금 부과), 향후 입찰참여 감점 등 보안관련 특약조항 명시
- 용역사업 참여인원은 용역업체 임의로 교체할 수 없으며, 신상변동 사항 발생 시 즉시 보고 및 승인 절차 이행
- 업체 대표자 명의 및 수행 인력에 대한 보안서약서 징구

2) 정보화 용역사업 수행 시 보안대책
- 정보통신망 구성도, IP현황 등 용역업체에 제공한 중요 자료는 인계인수대장을 비치, 보안조치 후 인계·인수 실시하고 자료가 무단 복사 및 외부 반출되지 않도록 보안 철저

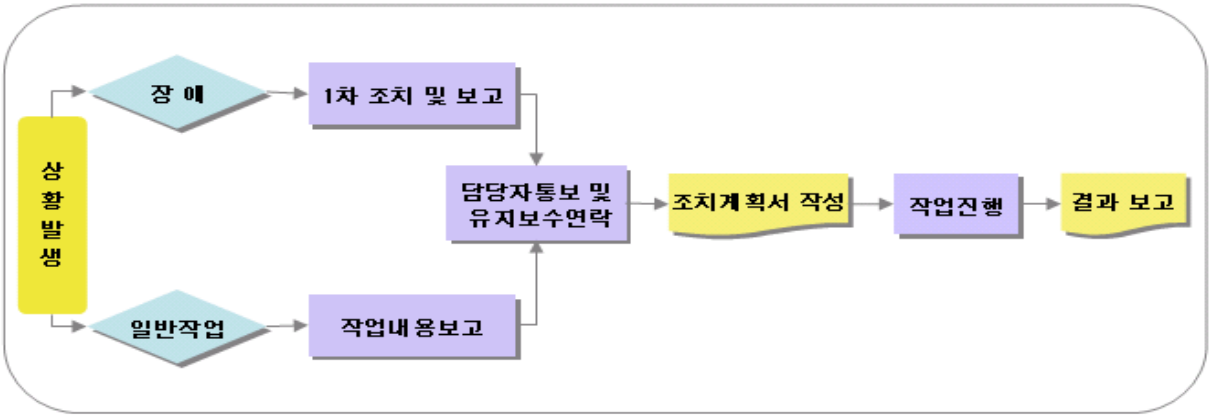
- 용역업체 인력이 사용하는 PC는 인터넷 연결을 금지하되, 사업 수행 상 연결이 필요한 경우에는 보안통제 하에 제한적 허용
- 용역업체의 노트북 등 관련 장비를 반출·반입시마다 악성코드 감염여부, 자료 무단방출 여부 확인

3) 정보화 용역사업 종료 시 보안대책

- 용역업체로부터 용역 결과물을 전량 회수 및 대표명의 자료 미보유 확약서 징구
- 사업 종료 시 외부업체의 노트북·휴대용 저장매체 등은 복구가 불가능하도록 완전 삭제하여 비공개 자료가 유출되는 것을 방지
- 용역업체로부터 전량 회수한 용역 결과물을 비인가자에게 제공·열람 금지

6. 전산자료 보안관리

1) 재난 발생 시 처리 절차



가) 비상연락 및 조치

- 재난 발생 시 장비별 담당자는 즉각적으로 관리책임자에 보고
- 경미한 장애는 장비별 담당자의 통제 하에 필요한 응급조치를 취하며, 상당한 수준의 장애일 경우 관리책임자의 통제를 받아 조치
- 장비별 담당자는 정확한 피해상황을 확인하고, 시스템 및 전산자료의 보안 등급이 높은 전산자원부터 복구하며, 복구 현황 및 결과를 관리책임자에게 보고

참고자료 정보화사업 보안성 검토 체크리스트

[서식]

정보화사업 보안성 검토 체크리스트

☐ 용역업체 보안

구분	점 검 내 용	반영 여부 (반영, 미반영, 향후 반영, 미적용 대상)
1	○ 정보화사업 제안요청서에 누출금지 대상정보 명시 - 용역업체 작업 장소에 대한 보안요구사항 - 누출금지 대상정보 명시 - 원격지에서 온라인 개발에 따른 보안사항	
2	○ 계약서에 참가 직원의 보안준수사항과 위반 시 손해배상 책임 등 보안관련 특약 조항 명시	
3	○ 용역사업 수행 관련 보안교육·점검 및 용역기간 중 참여인력 임의 교체 금지	
4	○ 정보통신망도·IP 현황 등 용역업체에 제공할 자료는 자료 인계인수대장을 비치, 보안조치 후 인계·인수하고 무단 복사 및 외부반출 금지	
5	○ 사업 종료 시 외부업체의 노트북·휴대용 저장매체 등을 통해 비공개 자료가 유출되는 것을 방지하기 위하여 복구가 불가능하도록 완전삭제	
6	○ 용역업체로부터 용역 결과물을 전량 회수하고 비인가자에게 제공·열람 금지	
7	○ 용역업체의 노트북 등 관련 장비를 반출·반입시마다 악성코드 감염여부, 자료 무단반출 여부 확인	
8	○ 외주 용역사업을 수행할 경우에는 외부인력에 대한 보안교육 및 외부유출 방지 등 보안조치 강구	
추가 보안 사항		

※ 용역업체 보안성 검토 사항은 모든 정보시스템 구축 및 용역 사업에 적용

☐ 소프트웨어 개발 보안

구분	점 검 내 용	반영 여부 (반영, 미반영, 향후 반영, 미적용 대상)
1	○ 독립된 개발시설 확보 및 비인가자의 접근 통제 여부	
2	○ 개발시스템과 운영시스템의 물리적 분리	
3	○ 소스코드 관리 및 소프트웨어 보안관리 대책	
4	○ 서버관리자는 개발 완료 후 시험하기 위해 사용된 도구(컴파일러 등) 삭제	
5	○ 외부인력 대상 신원확인, 보안서약서 징구, 보안교육 및 점검	
6	○ 외부인력의 보안준수 확인 및 위반 시 배상책임의 계약서 명시	
7	○ 외부인력의 정보시스템 접근권한 및 제공자료 보안대책	
8	○ 외부인력에 의한 장비 반입·반출 및 자료 무단반출에 대한 보안 대책	
9	○ 업무망과 인터넷 간 안전한 자료전송은 「국가·공공기관 업무망과 인터넷 간 안전한 자료전송 보안가이드라인」 적용	
10	○ 이벤트 로그는 1년 이상 저장	
11	○ 용역업체 보안성 검토 사항 반영 여부	
추가 보안 사항		

☐ 홈페이지 구축 보안

구분	점 검 내 용	반영 여부 (반영, 미반영, 향후 반영, 미적용 대상)
1	○ 웹서버 및 웹 어플리케이션 환경 설정 시 불필요한 서비스 제거 및 보안설정 사전 확인	
2	○ ‘웹서버 보안취약점 대응 가이드’를 참고, 취약점 제거	
3	○ 웹사이트 내 모든 유형의 웹페이지 컨텐츠에 대해 개인정보 노출 점검 및 차단 기능 적용	
4	○ 관리자 접근 웹페이지 로그인에 전자서명인증서 등 적용을 통해 보안 강화	
5	○ 사용자 접근권한은 업무에 따라 차등 설정 · 관리	
6	○ DBMS에 개인정보 암호화(주민등록번호, 핸드폰번호 등) 적용	
7	○ 개인정보 및 인증정보(로그인 등) 입력시 이용자 단말기에 개인정보 유출 방지 대책(보안서버, 키로깅, 전자서명인증, 화면캡쳐 방지 등) 마련	
8	○ 비인가자의 서버 저장자료 절치, 위·변조 및 분산서비스거부(DDoS) 공격 등에 대비하기 위하여 국가정보원장이 안전성을 검증한 침입차단· 탐지시스템 및 DDoS 대응시스템 설치하는 등 보안대책 강구	
9	○ 관리자 기능은 내부망의 지정된 시스템에서만 접근	
10	○ 외부에 공개될 목적으로 설치된 웹서버가 DMZ에 설치되어 있는 지 확인	
11	○ 민원서류발급시스템(이수증 등)의 경우 출력문서 위·변조 방지 등 보안대책 강구	
12	○ 웹 로그는 1년 이상 저장	
13	○ 소프트웨어 개발 보안 반영 여부	
14	○ 용역업체 보안성 검토 사항 반영 여부	
추가 보안 사항		

☐ 네트워크 보안

구분	점 검 내 용	반영 여부 (반영, 미반영, 향후 반영, 미적용 대상)
1	○ 원격접속은 원칙적으로 금지, 장비 관리용 목적으로 내부망의 인가된 사용자 및 단말기를 통해 관리·운영	
2	○ 물리적으로 안전한 장소에 설치, 비인가자 무단 접근 통제	
3	○ 신규 전산장비 도입 시 기본(default)계정을 삭제 또는 변경, 시스템 운영을 위한 관리자 계정 별도 생성	
4	○ 불필요한 서비스 포트 및 개별사용자 계정 차단·삭제	
5	○ 펌웨어 무결성 및 소프트웨어·서버 운영체제 취약점과 최신 업데이트 여부 주기적으로 확인, 최신 버전 유지	
6	○ 시스템관리자는 네트워크 장비의 접속기록을 1년 이상 유지, 비인가자의 접근 여부를 주기적으로 점검	
7	○ ‘IP주소’ 체계적 관리, 사설주소체계(NAT) 적용	
8	○ 보안기능이 있는 L2 스위치 이상 도입 시 국가사이버안전센터 검증필 제품 도입 (권장)	
9	○ 용역업체 보안성 검토 사항 반영 여부	
추가 보안 사항		

☐ 서버 보안

구분	점 검 내 용	반영 여부 (반영, 미반영, 향후 반영, 미적용 대상)
1	○ 서버 내 저장자료에 대해 업무별·자료별 중요도에 따라 사용자의 접근 권한 차등 부여	
2	○ 서버의 운영에 필요한 서비스 포트 외에 불필요한 서비스 포트 제거, 관리용 서비스와 사용자용 서비스를 분리·운영	
3	○ 서버의 관리용 서비스 접속시 특정 IP주소가 부여된 관리용 단말 지정 운영	
4	○ 사용자의 직접적인 데이터베이스 접속 차단, 개인정보와 같은 중요 정보를 암호화하는 등 데이터베이스 보안조치 실시	
5	○ 도입 시스템 환경 설정 시 보안취약점 사전제거 - 제조사 기본 계정 및 비밀번호는 변경하여 사용 - 서버 운영체제 및 응용프로그램에 대한 적시 보안패치 반영 - 불필요한 서비스 제거 및 보안관련 구성 설정 확인 등	
6	○ 서버 관리자는 외부인에게 공개할 목적으로 설치되는 웹서버 등 공개서버를 내부망과 분리된 영역(DMZ)에 설치 · 운영	
7	○ 업무망 관리자는 정보시스템에 사용되는 ‘IP주소’를 체계적으로 관리하여야 하며 사설주소체계(NAT) 적용	
8	○ 비안가자의 서버 저장자료 절취, 위 · 변조 등에 대비하기 위하여 국가정보원장이 안전성을 검증한 침입차단 · 탐지 시스템 및 DDoS 대응장비 설치 등 적용	
9	○ 서버 설정 정보 및 저장자료에 대한 정기적 백업 실시	
10	○ 용역업체 보안성 검토 사항 반영 여부	
추가 보안 사항		

☐ CCTV 보안

구분	점 검 내 용	반영 여부 (반영, 미반영, 향후 반영, 미적용 대상)
1	○ 영상정보처리기기를 설치.운영하고자 할 경우에는 내부업무망과 분리된 별도의 단독망으로 구성 운영	
2	○ 부득이한 사유로 인터넷을 활용할 경우 영상자료 유출을 방지하기 위하여 원격지카메라(비디오서버)↔관제서버 종단 간 VPN 설치 운영	
3	○ 원격지 감시 등의 사유로 단독망 구축 불가 시 전용회선 사용 여부	
4	○ 비인가자의 카메라(비디오서버) 접근을 방지하기 위하여 Telnet 등 원격접근 서비스 차단 설정, 접근 가능 IP제한(관제용서버 IP로 한정), 디폴트 패스워드 변경, 카메라 IP 외부 공개 금지 등 보안조치	
5	○ 외부에 CCTV 설치 시 카메라, 중계서버는 비인가자의 임의 조작이 물리적으로 불가능하도록 위치하거나 시건장치 설치	
6	○ 영상기록의 임의열람 및 사적활용 방지대책을 마련하고, 저장매체는 비인가자의 접근이 불가능하도록 시건장치가 설치된 통제구역에 보관	
7	○ CCTV 관련 서버 및 네트워크 장비, 서버·네트워크 부분 보안성 검토 사항 반영 여부	
8	○ 용역업체 보안성 검토 사항 반영 여부	
추가 보안 사항		

2 사이버침해사고 대응

관련근거

- 정보보안 기본지침 제102(초동 조치) 제103조(조치결과 통보), 제107조(사이버공격으로 인한 사고), 제109조(재발방지 조치)

업무시기

- 사이버침해사고 발생 및 탐지 시

주요내용

- **사이버침해사고 관련 주요 업무**

기관 구분	업 무
경기도교육청 (교육정보담당관)	◦ 경기도 교육(행정)기관의 피해현황 파악 및 복구활동 총지휘 ◦ 사이버침해사고 탐지 및 처리 ◦ 유관기관(국가정보원, 교육부 등)과 대응 공조
경기교육사이버안전센터 (경기도교육정보기록원)	◦ 보안관제센터 운영 ◦ 사이버침해사고 탐지 및 처리 ◦ 유관기관(국가사이버안보센터, 교육부 사이버안전센터)과 대응 공조
교육지원청	◦ 각급학교 사이버침해사고 관리 ◦ 해당기관 사이버공격으로 인하여 발생한 사고의 조사 및 복구
학교 및 직속기관	◦ 사이버침해사고 조치 ◦ 시스템별 담당자 지정 ◦ 해당기관 사이버공격으로 인하여 발생한 사고의 조사 및 복구

- **사이버침해사고 대응 절차**

1. 사고 탐지	2. 사고 분석 및 초기대응	3. 초동조치 및 사고대응	4. 후속조치
◦ 침해사고 탐지 - 자체 탐지 (실시간 보안관제) - 사고 이관 (국정원, 교육부) ◦ 침해사고 신고접수 - 각급기관에서 사이버침해사고 특이징후 포착 시 신고 (☏031-240-6599)	◦ 사고 유형 분석 - DDoS 공격, 웹해킹, 웜·바이러스 등 ◦ 침해사고 통보 - 경미사안은 자체종결 - 침해 사고기관에 통보 (각급학교는 교육지원청에 통보) ◦ 보안권고문 전파 - 공격자 IP, 피싱사이트 차단 등	◦ 초동조치 - (교육지원청) 공격자 IP, 피싱사이트 차단 등 - (침해사고기관) 침해사고 시스템 네트워크 분리 ◦ 사고대응 - 백신 검사 ·치료, 포맷 등 ※사이버안전센터 기술지원 (☏031-240-6599) - 웹방화벽 등 로그 분석 - 필요시 현장방문지원	◦ 조치완료 - 5일이내 처리 (주요침해사고는 2일이내 처리) - 침해사고 조치 결과 보고 (goeboan@korea..kr) ※ 사이버침해사고 조치보고서 제출 ※ 해킹 사고의 경우 재발방지 대책 수립
경기교육사이버안전센터(GECSC)		교육지원청/각급기관	각급기관

사이버침해사고 유형

침해 유형	내 용
침입시도	공격자가 접근 가능한 시스템 정보를 획득하기 위하여 시스템의 접속 및 탐색, 다양한 취약점 공격을 시도하는 행위
해킹메일	악의적인 메일을 유포하는 공격 행위 또는 해커가 교직원이 송수신한 메일을 무단 열람한 행위
악성코드 감염	악의적인 목적을 위해 작성된 실행 가능한 코드로 웜, 바이러스 등이 있으며 네트워크 트래픽 발생, 시스템 성능 저하, 파일삭제, 개인정보 탈취, 원격제어, 파일 암호화 등의 행위를 함
웹해킹	해커가 시스템 권한 및 이용자 정보를 탈취하여 악성코드를 유포하거나 홈페이지를 위변조하는 행위
경유지악용	공격자가 보안에 취약한 홈페이지 시스템을 경유지로 이용하여 악성코드 등을 유포하는 행위
서비스거부공격	동시에 특정 사이트를 공격하여 서비스를 하지 못하도록 하는 행위

랜섬웨어 피해 예방 5대 수칙

- 모든 소프트웨어는 최신 버전으로 업데이트하여 사용합니다.
- 백신 소프트웨어를 설치하고, 최신 버전으로 업데이트 합니다.
- 출처가 불명확한 이메일과 URL 링크는 실행하지 않습니다.
- 파일 공유 사이트 등에서 파일 다운로드 및 실행에 주의합니다.
- 중요 자료는 정기적으로 백업합니다.

피싱 예방

- 출처가 불분명한 이메일, 문자 메시지, 블로그 등에 포함된 URL에 접근하지 않기
- 개인정보(로그인), 금융정보(보안카드 등)에 대한 입력을 진행할 때 홈페이지 주소의 자물쇠 그림 또는 도메인 주소의 철자 확인하기
- 경품 이벤트 등 무분별한 인터넷 이벤트 참여를 통해 개인정보 입력하지 않기
- 안전한 비밀번호를 사용하고 주기적으로 변경하기
- 공유기 보안설정 강화하기

용|어|설|명

- **랜섬웨어(Ransomware)** : 몸값(Ransom)과 소프트웨어(Software)의 합성어. 시스템을 잠그거나 데이터를 암호화해 사용할 수 없도록 하고 금전을 요구하는 악성코드 프로그램을 말하며 신뢰할 수 없는 사이트, 스팸메일, 파일공유사이트, 네트워크망을 통해 유포됨
- **피싱(Phishing)** : 개인정보(Private data)와 낚시(Fishing)의 합성어. 전화·문자·메신저·가짜사이트 등 전기통신수단을 이용하여 피해자를 기만·공갈함으로써 이용자의 개인정보나 금융정보를 빼낸 후 금품을 갈취하는 사기 수법

참고자료

- 사이버침해사고 신고서(서식)
- 정보시스템(개인용 컴퓨터) 점검 매뉴얼

참고자료 사이버침해사고 신고서(서식)

서식 앞면

사이버침해사고 신고서

기 본 정 보			
기 관 명	00학교	부 서	정보부
성 명	홍 길 동	직 위	부장
전자우편	hong@sun.ac.kr		
연 락 처	전화: 031-555-5555 H.P:010-555-5555 Fax: 031-555-5555		
사 고 내 용			
사고 일시	년 월 일 시 분	피해IP주소	※ 00.00.00.00
피해시스템 용도	사, 아 * 뒷장의 '가.시스템 분류' 기호 입력	운영체제	■ 윈도우 □ 유닉스 □ 네트워크장비 □ 기타 상세버전정보: Windows 11
사고 유형	C * 뒷장의 '나.사고 유형' 기호 입력	피해범위	대 * 피해시스템이 여러대인 경우 피해숫자 기입
사고 내용	※ 홈페이지 위변조, DDoS 공격, 등		
조 치 내 용			
공격자 정보	※ 공격자 IP 현황(예: 0.0.0.0(중국))		
피해 현황	※ 정보유출, 홈페이지 위변조, 없음 등		
긴급조치 실시사항	※ 네트워크 차단, 백신 점검, 웹취약점 점검, 시스템 자체 점검 실행		
관련보안제품 운영현황	※ 00백신 사용		
그 밖에 사고 관련 내용을 구체적으로 서술			
※ 시간별 탐지화면, 캡쳐화면 등 기술			

※ 전화(031-240-6599), Fax(031-256-5469), 이메일(goeboan@korea.kr)로 사고신고 바랍니다.

서식 뒷면

가. 시스템 분류 목록

기호	시스템분류	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 운영테스트를 위하여 사용하는 임시 서버
마	통신전송장비	라우터, 스위치 등 통신전송장비 일체
바	보안장비	방화벽, IDS, VPN 및 백신서버 등 정보보안제품 일체
사	개인/업무PC	기관 내 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

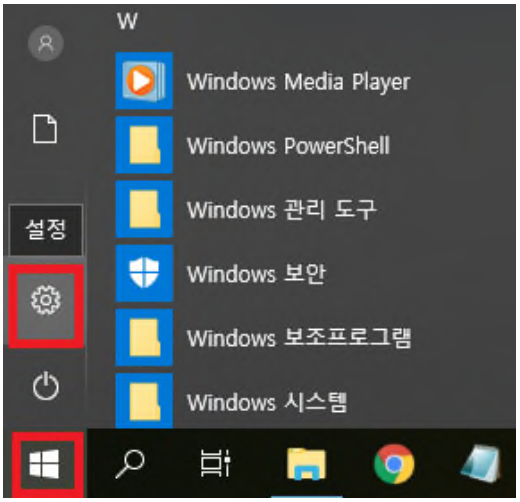
기호	사고 유형	설 명
A	경유지 악용	타기관으로부터 해킹시도 항의를 받았거나, 시스템 점검 중 해킹 흔적 또는 해킹 툴이 설치되어 타 시스템에 접속한 기록이 발견되었을 경우
B	자료훼손 및 유출	내부 시스템의 자료가 변조가 되었거나, 대량의 데이터가 외부로 무단 송신된 흔적이 발견되었을 경우
C	악성코드 감염	기관내의 서버 PC에서 악성코드가 발견되었을 경우
D	홈페이지 변조	기관의 홈페이지가 변조되었을 경우
E	홈페이지 접속 불가능	기관의 홈페이지 서버 또는 네크워크 이상으로 인해 홈페이지 접속이 불가능 할 경우
F	서비스거부공격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

참고자료 정보시스템(개인용 컴퓨터) 점검 매뉴얼

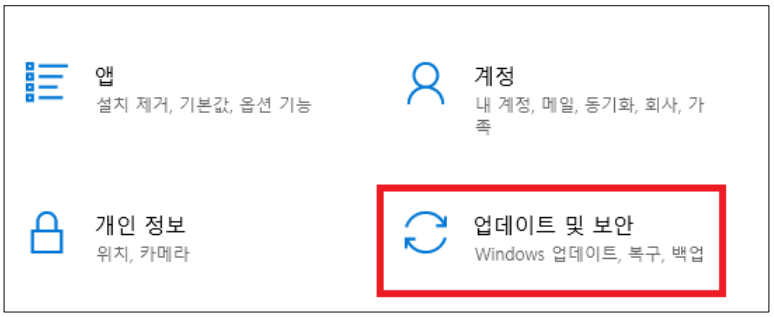
정보시스템(개인용 컴퓨터) 점검 매뉴얼

1. 운영체제 및 소프트웨어(ex.Windows 10) 최신 버전 업데이트

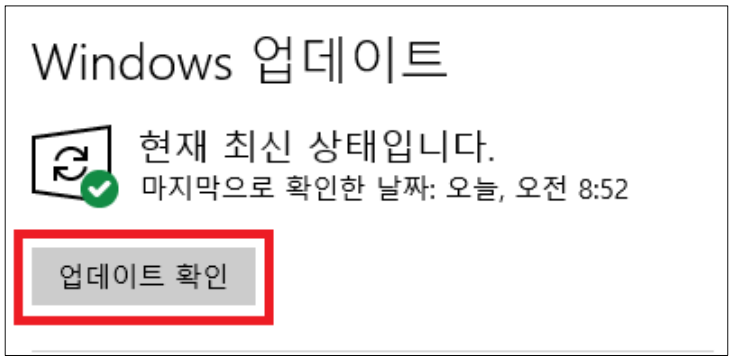
① 시작>설정 버튼



② 설정 > 업데이트 및 보안



③ 업데이트 확인



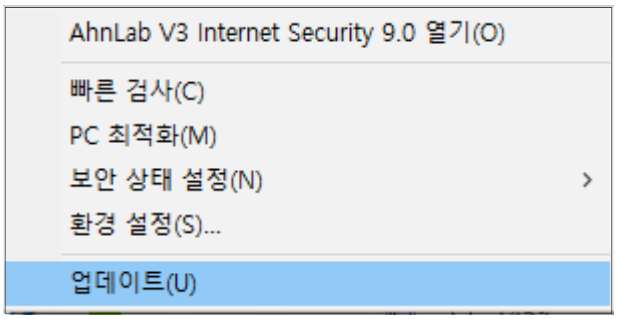
2. 백신 프로그램 설치 및 수행 여부 확인

- 백신. V3 Internet Security9.0 에이전트 설치 및 업데이트 확인

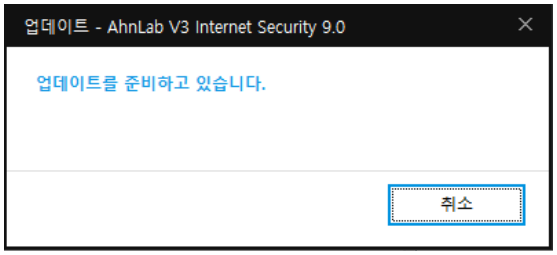
① 윈도우 작업표시줄 오른쪽 하단에 [숨겨진 아이콘 표시] 선택, 백신 소프트웨어 확인

② 만약, 설치되어 있지 않다면 초·중·고 모두 교육지원청에 설치 방법 문의하여 설치

③ 아이콘 마우스 우클릭 후, [업데이트]클릭

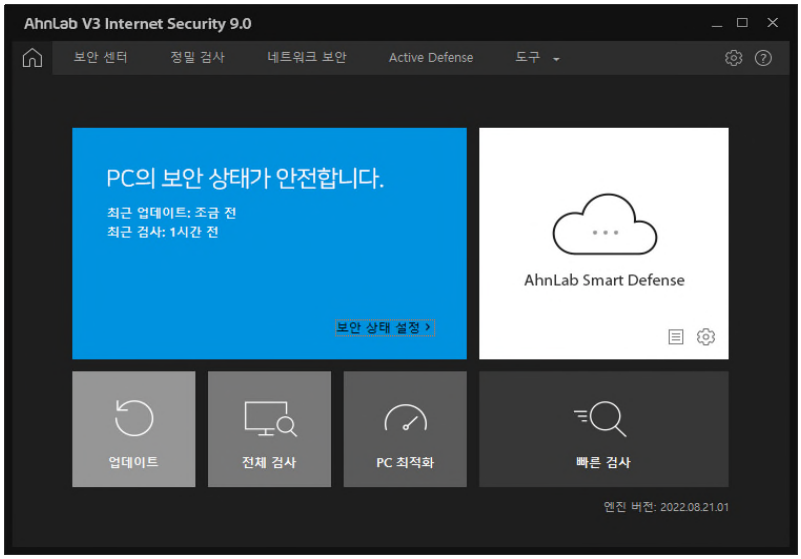


④ 자동으로 업데이트 확인 및 업데이트 실행



- PC 내 드라이브(디스크) 전체 검사 실시

① 메인화면 > 전체검사



3. P2P사이트 프로그램(Torrent 등) 삭제

① [시작] - [Windows 시스템] - [제어판] - [프로그램 제거] 선택 후 Torrent 등 각종 P2P사이트 접속 프로그램 삭제

4. 내PC지키미 수행

① 내PC지키미를 실행하여 모든 점검사항이 ‘안전’으로 나올 때까지 수행

GYEONGGIDO OFFICE OF EDUCATION

경기도교육청 교육기관

정보보안 업무 매뉴얼

경기도교육청

GYEONGGIDO OFFICE OF EDUCATION