보안업무 규정

제1장 총칙

제1조(목적) 이 규정은 보안업무규정(대통령령)에 의거 본교의 보안업무의 세부시행에 필요한 사항을 규정함을 목적으로 한다.

제2조(적용범위) 이 규정은 본교의 각 기관에 적용한다.

제3조(보안심사위원회) ① 본교 보안심사위원회의 위원은 다음과 같이 당연직위원으로 구성하며, 그 임기는 보직의 재임기간으로 한다.

1. 위원장 : 행정지원처장
2. 위원 : 기획조정처장, 교학지원처장
3. 간사 : 행정지원팀장

② 위원회는 다음 사항을 심의 결정한다.

1. 보안내규의 수립 및 그 개정에 관한 사항
2. 분야별 보안대책의 수립에 관한 사항
3. 신원특이자의 임용, 보직 등 인사관리에 관한 사항
4. 보안위반자 심사 및 처리에 관한 사항
5. 연간 보안업무 지침 수립과 그 이행상태의 확인처리에 관한 사항
6. 보안업무 심사분석 및 보안업무 수행상 조정과 협의를 요하는 사항
7. 기타 위원장 및 보안담당자가 필요하다고 인정하는 사항

제2장 인원보안

제4조(신원조사대상) 신원조사의 대상이 되는 자는 다음과 같다.

1. 교원임용예정자
2. 직원임용예정자
3. 비밀취급인가 예정자

제5조(임시직원의 관리) ① 잡급직원, 용원, 사환 등 임시직원에 대한 신원조사는 채용 전에 실시함을 원칙으로 한다. 다만, 시·읍·면장이 발행하는 신원보증서로 우선 처리하고 15일 이내에 요청할 수 있다.

② 임시직원에게 부득이한 사유로 행정보조, 문서수발 및 타자 등의 업무보조를 시키고자 할 때에는 다음 사항에 관하여 보안담당 책임자의 승인을 얻은 후 취업시켜야 한다.

1. 취업의 필요성
2. 보안감독 방안
3. 수행할 업무의 내용

③ 임시직원에게는 비밀취급인가를 할 수 없다.

④ 임시직원의 감독책임은 임용권자 및 소속과장 및 팀장과 당해 업무의 주무자가 진다.

제6조(신원조사의 요청) ① 신원조사 대상자에 대한 신원조사 요청은 교원은 교학지원처, 직원은 행정지원처에서 담당한다.

② 부교수 이상 교원은 교육부에 의뢰하고, 그 외 교원 및 사무직원은 해당기관에 요청한다.

제7조(신원대장 및 신원조사회보서 관리) ① 신원조사 결과는 신원대장[별지 제1호 서식]에 항시 기록유지하여야 하며, 비밀취급인가 및 주요 직책, 보직 등 제반 인사관리의 기본 자료로서 활용한다.

② 신원조사회보서는 접수와 동시에 신원대장에 그 내용을 기록한 후 개인의 인사기록 서류와 함께 관리하여야 한다.

③ 신원대장 및 신원조사회보서의 관리는 해당부처 과장 및 팀장이 관리한다.

제3장 문서보안

제1절 비밀의 수발 보관 및 관리

제8조(비밀문서의 수발) ① 비밀문서의 수발업무는 행정지원처 및 비밀취급인가자만이 하여야 한다.

② 비밀의 수발은 문서수발 계통을 경유하여 취급자가 직접 수발함을 원칙으로 한다.

③ 비밀을 수발할 때에는 반드시 이중 봉투를 사용하여야 한다.

④ 타 기관으로부터 접수된 비밀은 1시간(근무)내에 담당자에게 인계하고 수령인을 받아야 한다.

제9조(비밀의 보관 및 관리) 본교의 비밀은 행정지원처에서 통합 보관 · 관리한다.

제10조(비밀 보관 책임자) ① 본교의 비밀 보관 책임자는 다음과 같다.

1. 보관책임자(정) : 행정지원처장
2. 보관책임자(부) : 행정지원팀장

보관책임자	
정	
부	

② 보관책임자가 교체되었을 때에는 비밀인계인수서[별지 제2호 서식]에 인계·인수를 하여야 한다.

제11조(비밀관리 기록부의 관리) ① 본교의 비밀관리기록부[별지 제3호 서식]는 비밀 통합 보관·관리를 담당하는 행정지원처에서 작성 비치한다.

② 비밀관리기록부는 10년간 보존하여야 한다.

제12조(비밀의 발간 · 복제 · 복사의 통제) 비밀을 발간 또는 복제, 복사하고자 할 때 보안담당자는 다음 사항을 통제하여 통제인 날인 및 비밀문서 발간 · 복제 · 복사 업무일지[별지 제4호 서식]를 작성하여야 한다.

1. 발간되는 비밀문건의 분류기호 기재여부
2. 비밀의 표시 및 예고문의 기재여부
3. 비밀 열람 기록 전 첨부여부
4. 배부처의 적절성 검토
5. 기타 비밀문건으로서 갖추어야 할 사항

제13조(비밀의 열람) ① 비밀은 해당 등급의 비밀취급인가를 받은 자로서 그 비밀과 업무상 직접관계가 있는 자에 한하여 열람할 수 있다.

② 업무상 비밀을 열람하고자 하는 모든 자는 열람에 앞서 비밀열람기록전[별지 제5호 서식]에 관계 사항을 기재하고 서명 또는 날인 후 열람하여야 하며, 비밀문서를 결재할 때에도 또한 같다.

제14조(비밀문서의 지출) ① 비밀을 보관하고 있는 시설 밖으로 지출하여서는 아니 된다. 다만, 공무상 지출이 필요할 때에는 비밀지출승인신청서[별지 제6호 서식]를 제출하여 보안담당 책임자의 승인을 얻은 후 지출하여야 한다.

② 전항의 규정에 의하여 비밀을 지출할 때에는 지출자는 물론 보관책임자도 지출 후의 보안대책 및 사후 회수 등에 관하여 보안조치를 취하여야 한다.

③ 비밀을 지출 휴대하고 다닐 때에는 반드시 포장하거나 밀봉한 봉투에 의하여야 하며 안전에 대한 보안조치를 취하여야 한다.

제15조(비밀문서의 파기) ① 법령의 규정 및 비밀의 예고문에 의한 파기는 소각, 용해 또는 기타의 방법으로 원형을 완전히 소멸시켜야 한다.

② 비밀의 파기를 집행함에 있어서는 보안책임자 또는 보관책임자의 입회하에 처리담당자가 파기하여야 한다.

③ 전항의 규정에 의하여 파기가 끝나면 즉시 비밀관리기록부의 파기란에 파기집행자가 일시를 기입한 후 날인하고, 파기 확인자란에 입회자의 확인을 받아 파기사실을 증명토록 하여야 한다.

제2절 안전지출 및 파기

제16조(목적) 정규 또는 비정규전으로 인한 적의 내습이나 공습으로 인한 비상사태 시와 화재 등 재난으로부터 비밀문서 및 중요문서를 안전하게 지출하고, 파기하기 위한 절차를 규정한다.

제17조(지출, 파기, 시기 결정 등) ① 지출은 적의 공격, 화재, 천재지변 등의 사태로 비밀 및 중요문서를 보호하기 위하여 안전한 지역으로 이전이 필요할 때

② 파기는 비상사태 하에서 적에게 비밀과 중요문서가 피탈 될 우려가 있을 때

③ 시기결정은 일과시간에는 보안담당자가, 과외시간(일과 후 및 공휴일)에는 당직근무자가 총장의 승인을 얻어 결정한다.

제18조(편성) ① 총지휘 및 감독자는 다음과 같다.

1. 일과시간 중 : 보안담당자
2. 과외시간 : 당직근무자

② 일과시간 중에는 다음과 같이 편성하되, 중요문서는 각 단위 부서의 과장 및 팀장으로 한다.

1. 지출 및 파기책임자 : 보관책임자(정)
2. 경계책임자 : 보관책임자(부)

③ 과외시간(일과 후 및 공휴일)에는 다음과 같이 편성하되, 중요문서는 각 단위 부서의 과장 및 팀장 또는 담당관으로 한다.

1. 지출 및 파기책임자 : 당직근무자
2. 경계책임자 : 당직근무자, 경비요원
3. 상황이 급박할 때 이외에는 보관책임자(정) 또는 보관책임자(부)가 임무를 수행한다.

제19조(임무) ① 보안담당자의 임무는 다음과 같다.

1. 지출 및 파기시기를 총장에게 보고하여 승인을 받는다.
2. 지출 및 파기 지휘 감독 및 보호조치를 한다.
3. 필요할 때 자체훈련 및 감독을 한다.

② 지출 및 파기책임자의 임무는 다음과 같다.

1. 비밀지출 우선순위에 따라 지출 또는 파기임무를 수행한다.
2. 비밀지출함 또는 낭을 준비한다.

③ 경계책임자는 지출 및 파기할 때 신 보관소 또는 파기장소에 외부인의 출입 통제와 주위의 경계임무를 수행하여야 한다.

제20조(지출 및 파기절차) ① 일과시간 중

1. 지출 및 파기책임자는 비밀문서 보관함 열쇠 또는 다이얼을 열고 지출함 또는 배낭에 II급, III급, 대외비 문서 순으로 넣어 지출 장소로 이동한다.
2. 지출 및 파기책임자 부재 시는 보관책임자(부)가 위와 같이 시행하되 열쇠와 다이얼번호 불명 시는 당직실에 비상용으로 보관되어 있는 열쇠 및 다이알 번호봉투를 개봉하여 시행한다.
3. 중요문서는 지출 우선순위에 의거 간편한 포장을 하거나 상자 또는 낭에 넣어 지출한다.

② 과외시간(일과 후 및 공휴일)

1. 당직근무자가 시간적 여유가 있을 때는 보안담당자, 보관책임자(정·부)에게 긴급연락 조치하고 상황이 긴박할 때에는 당직실에 보관된 열쇠 및 다이얼번호 봉투를 개봉, 보관함을 열고 전항의 제1호와 같이 시행한다.
2. 중요문서는 소속과장 및 팀장 또는 담당관에게 긴급연락 조치하고 상황이 긴박할 때에는 당직실의 비상열쇠를 이용 위와 같이 시행한다.

3. 비밀 안전지출시 안전한 신 보관소까지의 수송은 승용차를 이용 지출한다.

제21조(최종확인 및 보고) ① 지출 및 파기책임자는 지출목록 및 파기내용을 확인하고 이를 총장에게 즉시 보고한다.

② 공휴일 및 일과시간 이후 당직근무자는 상황처리 후 총장에게 즉시 보고한다.

제4장 시설보안

제22조(보호구역설정) ① 제한구역 : 총장실, 학적부보관실, 통신기기실, 전자계산소, 변전실 등

제23조(보호구역의 관리) 보호구역 중 통제구역은 관계직원 및 출입이 인가된 자 외에는 출입을 통제하고 출입자 명부를 비치 기록 유지하여야 하며, 제한구역과 통제구역은 주서로 “제한구역”, “통제구역”의 표시를 하여 관리하되 각급 기관장실은 표시를 생략할 수 있다.

제24조(보호구역의 관리책임) 보호구역의 관리책임자는 다음과 같이 지정한다.

1. 총장실 : 행정지원팀장<개정 2019.01.23.>
2. 학적부 보관실 : 교무지원팀장
3. 통신기기실 및 전자계산소 : 행정지원팀장
4. 변전실 : 행정지원팀장<개정 2007.09.01>

제25조(비상사태대비) ① 일과 후 또는 공휴일에 발생되는 비상사태에 대비하기 위하여 비상연락망을 교원은 교학지원처에서, 직원은 행정지원처에서 작성 관리한다.

② 비상연락망은 당직실에 비치하고 변동사항은 수시 정리한다.

제5장 보안교육 및 보안점검

제26조(보안) ① 본교 보안관리와 보안업무의 향상을 위하여 보안담당자는 전교직원에게 년1회 이상 정기교육과 수시교육을 실시한다.

② 수시 교육 중 신규임용직원 및 전입자에 대하여는 임용 후 5일 이내에 보안담당자 또는 보관책임자(정) 책임 하에 보안교육을 실시한다.

제27조(보안점검) ① 팀 단위로 보안점검표를 사무실에 비치하여 매일 최종 퇴근자가 이상 유무를 확인한 후 퇴근하도록 한다.

② 소속 부서장 및 팀장은 보안점검의 이행을 생활화하도록 소속 직원에게 교육을 하고 보안 담당자는 이행상태를 수시 확인 점검하여야 한다.

제28조(보안진단) 정기 보안진단은 매월 제1주 금요일에 보안담당자 또는 보관책임자(정) 책임하에 보안업무 전반에 걸쳐 자체점검을 통한 보안진단을 실시한다.

제6장 정보보안 기본활동

제29조(기본목표) 컴퓨터와 네트워크의 기반에서 발생할 수 있는 모든 정보 보안상의 사고위험으로부터 내부의 정보자원을 보호하여 정보의 가용성, 비밀성, 완전성, 책임성을 유지할 수 있도록 관리한다.

제30조(책무) 학교의 장은 보유정보(전자정보를 포함한다. 이하 같다)와 정보통신망을 보호하기 위한 보안대책을 마련하여야 하며 정보보안에 대한 책임을 진다.

제31조(정보보안담당관 운영) ① 학교의 장은 효율적·체계적인 정보보안 업무를 수행하기 위하여 정보보안 전문지식을 보유한 인력을 확보하고 관련 전담조직을 구성 운영하여야 한다.

② 예원예술대학교 정보보안담당관은 전산실이 속한 부서장으로 한다.

③ 학교의 장이 정보보안담당관에 부여하는 기본활동은 다음 각 호와 같다.

1. 정보보안 정책 및 활동 세부계획 수립
2. 정보통신망 신·증설시 보안대책 수립

3. 정보통신실, 정보통신망 및 정보자료 등의 보안관리
4. 정보보안업무 지도·감독 및 교육
5. 정보보안 사고조사·복구 및 처리
6. 사이버위협정보 수집·분석 및 보안관제
7. 사이버공격 관련 경보 발령시 대응활동
8. 자체 정보보안관련 지침 등 제도 개선
9. 정보통신망 취약성 진단
10. 검증필 정보보호시스템의 운용·보안관리
11. 정보보안 예산 및 전문인력 확보
12. 정보보안 사고조사 결과 처리
13. 정보보안 교육 및 정보협력
14. 도청 위해 요소 측정·제거
15. 주요 정보통신 기반시설 보호활동
16. 정보통신망 보안대책의 수립·시행
17. '사이버보안진단의 날' 계획 수립·시행
18. 기타 정보보안 관련 업무

제32조(활동계획 수립 및 심사분석) ① 학교의 장은 당해 기관의 정보보안업무 세부추진계획(「교육과학기술부 사이버안전센터운영규정」제8조에 따른 사이버안전대책을 포함한다)을 수립·시행하고 그 추진결과를 심사분석·평가하여야 한다.

제33조(정보보보 수준진단) 학교의 장은「전자정부법」제56조 및 同法 시행령 제69조·제70조,「공공기록물 관리에 관한 법률 시행령」제5조 등의 규정에 의한 보안대책의 수립·시행 등을 교육과학기술부장관이 매년 정하는 진단 대상·기준, 진단항목 및 기간에 따라 자체 진단하고 그 결과를 교육과학기술부장관에게 통보하여야 한다.

제34조(정보보안감사) ① 학교의 장은 연1회 이상 정보보안감사를 실시하여야 한다.

② 정보보안감사는 제32조에 따른 정보보안업무 세부추진계획에 따라 실시한다.

제35조(정보보안 지도방문) 정보보안담당관은 정보통신시스템 운용관리에 따른 보안취약성 개선을 위하여 정보보안 지도방문을 실시하여야 한다.

제36조(모의훈련) ① 학교의 장은 자체 정보통신망을 대상으로 매년 정기 또는 수시 사이버위기 대응 모의훈련을 실시하여야 한다.

제37조(정보보안 교육) ① 학교의 장은 자체 정보보안 교육계획을 수립하여 연 1회 이상 전 직원을 대상으로 관련 교육을 실시하여야 한다.

② 학교의 장은 정보보안 관련 전문기관 교육 및 기술 세미나 참석을 장려하는 등 정보보안 담당자의 업무 전문성을 제고하기 위하여 노력하여야 한다.

제38조(사이버보안 진단의 날) ① 학교의 장은 당해 기관 실정에 맞게 매월 세 번째 수요일을 '사이버보안진단의 날'로 지정·운영하여야 한다.

② 정보보안담당관은 '사이버보안진단의 날'에 소관 정보보안업무 전반에 대하여 체계적이고 종합적인 보안진단을 실시하여야 한다.

제39조(정보보안사고 조사) ① 학교의 장은 [별표 제1호]의 정보보안사고가 발생한 때에는 즉시 피해확산 방지를 위한 조치를 취하고 다음 각 호의 사항을 교육과학기술부장관에게 통보하여야 한다. 이 경우, 사고원인 규명 시까지 피해 시스템에 대한 증거를 보전하고 임의로 관련 자료를 삭제하거나 포맷하여서는 아니 된다.

1. 일시 및 장소
2. 사고 원인, 피해현황 등 개요

3. 사고자 및 관계자의 인적사항
4. 조치내용 등

② 교육과학기술부장관은 보안사고 조사결과를 해당기관의 장에게 통보하고 동일유형의 사고가 발생하지 않도록 제반 보안조치를 해당기관에 권고할 수 있다.

③ 교육과학기술부장관은 제2항에도 불구하고, 필요하다고 인정할 경우 해당기관의 장에게 사고조사에 관한 권한의 일부를 위임할 수 있다. 다만, 권한을 위임받은 기관의 장은 교육과학기술부장관에게 조사결과를 통보해야 한다.

④ 교육과학기술부장관은 사고조사 결과 피해가 심각하다고 판단되는 경우 해당기관의 장과 협의하여 사고대책본부를 구성·운영할 수 있다.

⑤ 학교의 장은 규정에 의한 관련자 징계, 재발방지를 위한 보안대책의 수립·시행 등 사고조사 결과에 따라 필요한 조치를 이행하고 결과를 교육과학기술부장관에게 제출하여야 한다.

제40조(재난방지) ① 학교의 장은 인위적 또는 자연적인 원인으로 인한 정보통신망의 장애 발생에 대비하여 정보시스템 이원화, 백업관리, 복구 등 종합적인 재난방지 대책을 수립·시행하여야 한다.

② 학교의 장은 재난방지대책을 정기적으로 시험하고 검토해야 하며 업무 연속성에 대한 영향평가를 실시하여야 한다.

③ 학교의 장은 정보시스템 장애에 대비한 백업시설을 확보하고 정기적으로 백업을 수행하여야 한다.

④ 학교의 장은 제3항에 의거 백업시설을 설치할 경우에는 정보통신실과 물리적으로 일정거리 이상 위치한 안전한 장소에 설치하여야 하며 전력공급원 분리 등 정보시스템의 가용성을 최대화 할 수 있도록 하여야 한다.

제41조(표준적용) 학교의 장은 정보보안 대책을 강구하는 경우 정보보안에 필요한 기술의 호환성 유지 및 안전성 확보를 위하여 국가정보원장이 제정한 「국가표준기본법」의 표준을 우선 적용하여야 한다.

제42조(정보협력) 학교의 장은 정보보안 업무의 발전을 도모하고 상호 교류협력을 증진하기 위하여 협의기구를 구성·운영할 수 있다.

제7장 정보통신보안 관리

제43조(인적 보안) ① 학교의 장은 소관 정보통신망(정보시스템 포함) 사용과 관련하여 사용자의 직위·임무별 정보통신망 접근 자격부여 심사 등 인적보안에 관한 절차 및 방법을 마련하여야 한다.

② 학교의 장은 정보통신망을 통하여 비밀 등 중요정보를 취급하는 사용자에 대해서는 비밀취급인가, 보안서약서 징구 등의 보안조치를 하여야 한다.

③ 학교의 장은 사용자가 보직변경, 퇴직 등 인사이동이 있을 경우 관련 정보시스템 접근권한을 조정하여야 한다.

④ 학교의 장은 외부 인력을 활용하여 정보시스템의 개발, 운용, 정비 등을 수행할 경우에는 해당 인력의 고의 또는 실수로 인한 정보유출이나 파괴를 방지하기 위하여 보안조치를 수행하여야 한다.

제44조(정보시스템 보안) ① 학교의 장은 당해 기관에 필요한 일체의 정보시스템(PC·서버·네트워크장비 등 포함)을 도입·사용할 경우, 사용자·시스템관리자 및 관리책임자를 지정 운용하여야 한다.

② 사용자는 개인PC 등 소관 정보시스템을 사용하거나 본인 계정으로 정보통신망에 접속하는 것과 관련한 보안책임을 가진다.

③ 시스템관리자는 서버·네트워크 장비 등 부서 공통으로 사용하는 정보시스템의 운용과 관련한 보안책임을 가진다.

④ 제1항 내지 제3항과 관련하여 정보시스템을 실제 운용하는 부서의 과장 또는 팀장이 정보시스템 '관리책임자'가 되며, 관리책임자는 정보시스템 관리대장[별지 제9호 서식]을 수기 또는 전자적으로 운용 관리하여야 한다.

⑤ 관리책임자는 해당 부서의 정보시스템 관리대장에 정보시스템의 변경 최종 현황을 유지 및 관리하

여야 한다.

⑥ 정보보안담당관은 제1항 내지 제5항에 명시된 정보시스템 운용과 관련한 보안취약점을 발견하거나 보안대책 강구가 필요하다고 판단할 경우, 사용자·시스템관리자 및 관리책임자에게 시정을 요구할 수 있다.

제45조(정보통신시설 보안) ① 학교의 장은 다음 각 호의 중요 정보통신시설 및 장소를「보안업무규정」제40조에 따른 보호구역으로 설정 관리하여야 한다.

1. 암호실·통신실
2. 정보통신실
3. 국가용 보안시스템 개발·설치 장소
4. 경호통신, 국가비상통신 등 중요통신망의 교환국, 회선집중국 또는 중계국
5. 보안관제센터, 백업센터 및 중요한 정보통신시설을 집중 제어하는 국소
6. 그 밖에 보안관리가 필요하다고 인정되는 정보시스템 설치 장소

② 학교의 장은 제1항에서 지정된 보호구역에 대한 보안대책을 강구할 경우 다음 각 호 사항을 참고하여야 한다.

1. 방재대책 및 외부로부터의 위해(危害) 방지대책
2. 상시 이용하는 출입문은 한 곳으로 정하고 이중 잠금장치 설치
3. 출입자 인증·식별 등을 위한 출입문 보안장치 설치 및 주야간 감시대책
4. 휴대용 저장매체를 보관할 수 있는 용기 비치
5. 정보시스템 안전지출 및 긴급파기 계획 수립
6. 관리책임자 및 자료·장비별 취급자 지정 운용
7. 정전에 대비한 비상전원 공급, 시스템의 안정적 중단 등 전력관리 대책
8. 비상조명 장치 등 비상탈출 대책
9. 전자파 누설 방지 대책
10. 카메라 장착 휴대폰 등을 이용한 불법 촬영 방지 대책 등

③ 정부통합전산센터 등 타 기관의 정보통신망을 통합 운영하는 기관의 장은 해당 기관의 보안요구사항을 반영하여 보안대책을 수립하고 이를 교육과학기술부장관과 협의하여야 한다.

제46조(PC 등 단말기 보안관리) ① 단말기 사용자는 PC·노트북·PDA 등 단말기(이하 PC 등) 사용과 관련한 일체의 보안관리 책임을 가진다.

② 정보보안담당관은 비인가자가 PC 등을 무단으로 조작하여 전산자료를 절취, 위·변조 및 훼손시키지 못하도록 다음 각 호의 보안대책을 단말기 사용자에게 지원하며, 사용자는 이를 준수하여야 한다.

1. 장비(CMOS 비밀번호)·자료(중요문서자료 암호화 비밀번호)·사용자(로그온 비밀번호)별 비밀번호를 주기적으로 변경 사용하고 지문인식 등 생체인식 기술 적용 권고
2. 10분 이상 PC 작업 중단 시 비밀번호가 적용된 화면보호 조치
3. PC용 최신백신 운용·점검, 침입차단·탐지시스템 등을 운용하고 운영체제(OS) 및 응용프로그램(한컴 오피스, MS Office, Acrobat 등)의 최신 보안패치 유지
4. 업무상 불필요한 응용프로그램 설치 금지 및 공유 폴더의 삭제
5. 그 밖에 국가정보원장이 안전성을 확인하여 배포 승인한 프로그램의 운용 및 보안권고문

③ 사용자는 PC 등 단말기를 교체·반납·폐기하거나 고장으로 외부에 수리를 의뢰하고자 할 경우에는 관리책임자와 협의하여 하드디스크에 수록된 자료가 유출, 훼손되지 않도록 보안조치 하여야 한다.

④ 관리책임자는 사용자가 PC 등을 기관 외부로 반출하거나 내부로 반입할 경우에 최신 백신 등을 활용하여 해킹프로그램 및 웜·바이러스 감염여부를 점검하여야 한다.

⑤ 개인소유의 PC 등 단말기를 무단 반입하여 사용하여서는 아니 된다. 다만, 부득이한 경우에는 관리책임자의 승인을 받아 사용할 수 있다.

제47조(인터넷PC 보안관리) ① 정보보안담당관은 인터넷과 연결된 PC(이하 인터넷PC)를 비인가자가 무단으로 조작하여 전산자료를 절취, 위·변조 및 훼손시키지 못하도록 다음 각 호의 보안대책을 사용자에게 지원하며, 사용자는 이를 준수하여야 한다.

1. 메신저·P2P·웹하드 등 업무에 무관하거나 불필요한 Active-X 등 보안에 취약한 프로그램과 비인가 프로그램·장치의 설치 금지
2. 특별한 사유가 없는 한 문서프로그램은 읽기 전용으로 운용(단, 업무망과 인터넷망이 분리된 경우)
3. 음란·도박·증권 등 업무와 무관한 사이트 접근차단 조치

② 사용자는 인터넷PC에서 무단으로 업무자료의 작성·저장 및 소통을 금지하고 최신백신을 활용하여 주기적으로 점검하여야 한다.(단, 업무망과 인터넷망이 분리된 경우)

③ 그 밖에 인터넷 PC의 보안관리에 관련한 사항에 대해서는 제39조(PC 등 단말기 보안대책)를 따른다.

제48조(서버 보안관리) ① 서버 관리자는 서버를 도입·운용할 경우, 정보보안담당관과 협의하여 해킹에 의한 자료 절취, 위·변조 등에 대비한 보안대책을 수립·시행하여야 한다.

② 서버 관리자는 서버 내 저장자료에 대해 업무별·자료별 중요도에 따라 사용자의 접근권한을 차등 부여하여야 한다.

③ 서버 관리자는 사용자별 자료의 접근범위를 서버에 등록하여 인가여부를 식별토록 하고 인가된 범위 이외의 자료접근을 통제하여야 한다.

④ 서버 관리자는 서버의 운용에 필요한 서비스 포트 외에 불필요한 서비스 포트를 제거하며 관리용 서비스와 사용자용 서비스를 분리 운용하여야 한다.

⑤ 서버 관리자는 서버의 관리용서비스 접속시 특정 IP와 MAC 주소가 부여된 관리용 단말을 지정 운용하여야 한다.

⑥ 서버 관리자는 서버 설정 정보 및 서버에 저장된 자료에 대해서는 정기적으로 백업을 실시하여 복구 및 침해행위에 대비하여야 한다.

⑦ 서버관리자는 데이터베이스에 대하여 사용자의 직접적인 접속을 차단하고 개인정보 등 중요정보를 암호화하는 등 데이터베이스별 보안조치를 실시하여야 한다.

⑧ 정보보안담당관은 제1항 내지 제7항에서 수립한 보안대책의 적절성을 수시 확인하되, 연1회 이상 보안도구를 이용하여 서버 설정 정보 및 저장자료의 절취, 위·변조 가능성 등 보안취약점을 점검하여야 한다.

제49조(웹서버 등 공개서버 보안관리) ① 서버 관리자는 외부인에게 공개할 목적으로 설치되는 웹서버 등 공개서버를 내부망과 분리된 영역(DMZ)에 설치·운용하여야 한다.

② 서버 관리자는 비인가자에 의한 서버 저장자료의 절취, 위·변조 및 분산서비스거부(DDoS) 공격 등에 대비하기 위하여 국가정보원장이 안전성을 검증한 침입차단·탐지시스템 및 DDoS 대응시스템을 설치하는 등 보안대책을 강구하여야 한다.

③ 서버 관리자는 공개서버에 대한 무단 접속 등을 방지하기 위해 서버에 접근할 수 있는 사용자계정을 제한하며 불필요한 계정들은 삭제하여야 한다.

④ 서버 관리자는 공개서버의 서비스에 필요한 프로그램을 개발하고 시험하기 위해 사용된 도구(컴파일러 등)는 개발 완료 후 삭제를 원칙으로 한다.

⑤ 공개서버의 보안관리에 관련한 그 밖에 사항에 대해서는 제34조(서버 보안관리)에 따른다.

제50조(홈페이지 게시자료 보안관리) ① 학교의 장은 개인정보를 포함한 중요 업무자료가 홈페이지에 무단 게시되지 않도록 홈페이지 게시자료의 범위·방법 등을 명시한 자체 홈페이지 정보공개 보안지침을 수립 시행하여야 한다.

② 사용자는 개인정보, 비공개 공문서 및 민감 자료가 포함된 문서를 홈페이지에 공개하여서는 아니된다.

③ 홈페이지에 정보를 게시하고자 하는 부서의 관리책임자는 비밀 등 비공개 자료가 게시되지 않도록

하여야 한다.

④ 사용자는 블로그·카페·게시판·개인 홈페이지 또는 소셜네트워크 서비스 등 인터넷에 업무관련 자료를 무단 게재하여서는 아니 된다.

⑤ 정보보안담당관은 소속기관의 홈페이지 등에 비공개 내용이 게시되었는지 여부를 주기적으로 확인하고 개인정보를 포함한 중요정보가 홈페이지에 공개되지 않도록 보안교육을 주기적으로 실시하여야 한다.

⑥ 학교의 장은 홈페이지에 중요정보가 공개된 것을 인지할 경우 이를 즉시 차단하는 등의 보안조치를 강구 시행하여야 한다.

제51조(사용자계정 관리) ① 시스템관리자는 사용자에게 정보시스템 접속에 필요한 사용자계정(ID) 부여 시 비인가자 도용 및 정보통신시스템 불법 접속에 대비하여 다음 각 호의 사항을 반영하여야 한다.

1. 사용자별 또는 그룹별로 접근권한 부여
2. 외부인에게 계정 부여는 불허하되 업무상 불가피 시 학교장의 책임 하에 필요업무에 한해 특정기간 동안 접속토록 하는 등 보안조치 강구 후 허용
3. 비밀번호 등 사용자 식별 및 인증 수단이 없는 사용자계정 사용 금지

② 시스템관리자는 사용자가 5회 이상에 걸쳐 로그인 실패 시 정보시스템 접속을 중단시키도록 시스템을 설정하고 비인가자의 침입 여부를 확인 점검하여야 한다.

③ 시스템관리자는 교·직원의 퇴직 또는 보직변경 발생 시 사용하지 않는 사용자계정을 신속히 삭제하고, 특별한 사안이 없는 한 유지보수 등을 위한 외부업체 직원에게 관리자계정 제공을 금지하여야 한다.

④ 정보보안담당관은 사용자계정의 부여 및 관리가 적절한 지 연2회 이상 점검하여 관련 결과를 시스템 관리자에게 통보하여야 한다.

제52조(비밀번호 관리) ① 사용자는 비밀번호 설정 사용 시 정보시스템의 무단사용 방지를 위하여 다음과 같이 구분하여야 한다.

1. 비인가자의 정보통신시스템 접근방지를 위한 장비 접근용 비밀번호(1차)
2. 정보시스템 사용자가 서버 등 정보통신망에 접속 인가된 인원인지 여부를 확인하는 사용자인증 비밀번호(2차)
3. 문서에 대한 열람·수정 및 출력 등 사용권한을 제한할 수 있는 자료별 비밀번호(3차)

② 비밀이나 중요자료에는 자료별 비밀번호를 반드시 부여하되, 공개 또는 열람 자료에 대해서는 부여하지 아니할 수 있다.

③ 비밀번호는 다음 각 호 사항을 반영하여 숫자와 문자, 특수문자 등을 혼합하여 8자리 이상으로 정하고, 분기1회 이상 주기적으로 변경 사용하여야 한다.

1. 사용자계정(ID)과 동일하지 않은 것
2. 개인 신상 및 부서명칭 등과 관계가 없는 것
3. 일반 사전에 등록된 단어는 사용을 피할 것
4. 동일단어 또는 숫자를 반복하여 사용하지 말 것
5. 사용된 비밀번호는 재사용하지 말 것
6. 동일 비밀번호를 여러 사람이 공유하여 사용하지 말 것
7. 응용프로그램 등을 이용한 자동 비밀번호 입력기능 사용 금지

④ 서버에 등록된 비밀번호는 암호화하여 저장하여야 한다.

제53조(악성코드 방지대책) ① 학교의 장은 웜·바이러스, 해킹프로그램, 스파이웨어 등 악성코드 감염을 방지하기 위하여 다음 각 호와 같은 대책을 수립·시행하여야 한다.

1. 사용자는 개인PC에서 작성하는 문서·데이터베이스 작성기 등 응용프로그램을 보안패치하고 백신은 최신상태로 업데이트·상시 감시상태로 설정 및 주기적인 점검을 실시하여야 한다.
2. 사용자는 출처, 유통경로 및 제작자가 명확하지 않은 응용프로그램 사용을 금지하고 인터넷 등

상용망으로 자료 입수 시 신뢰할 수 있는 인터넷사이트를 활용하되 최신 백신으로 진단 후 사용하여야 한다.

3. 사용자는 인터넷 파일공유 프로그램과 메신저·대화방 프로그램 등 업무상 불필요한 프로그램을 사용 금지하고 시스템관리자는 인터넷 연동구간의 침입차단시스템 등에서 관련 사이트 접속을 차단하도록 보안설정 하여야 한다.

4. 사용자는 웹브라우저를 통해 서명되지 않은(Unsigned) Active-X 등이 PC내에 불법 다운로드 되고 실행되지 않도록 보안 설정하여야 한다.

5. 제1호부터 제4호까지의 보안대책과 관련하여 시스템관리자는 정보보안담당관과 협조하여 사용자가 적용할 수 있는 보안기술을 지원하여야 한다.

② 시스템관리자 또는 PC 등의 사용자는 시스템에 악성코드가 설치되거나 감염된 사실을 발견하였을 경우에 다음 각 호의 조치를 하여야 한다.

1. 악성코드 감염원인 규명 등을 위하여 파일 임의삭제 등 감염 시스템 사용을 중지하고 전산망과의 접속을 분리한다.

2. 악성코드의 감염확산 방지를 위하여 정보보안담당관에게 관련 사실을 즉시 통보한다.

③ 제2항의 조치가 완료된 후 정보보안사고 조사권한이 해당기관의 장(정보보안담당관)에게 위임되었을 경우, 정보보안담당관은 감염 PC 등에 대하여 다음 각 호의 조치를 하여야 한다.

1. 최신 백신 등 악성코드 제거 프로그램을 이용하여 악성코드를 삭제한다.

2. 감염이 심각할 경우 포맷 프로그램을 사용하여 하드디스크를 포맷한다.

3. 악성코드 감염의 확산 및 재발을 방지하기 위하여 원인을 분석하고 예방조치를 수행한다.

④ 학교의 장은 악성코드가 신종이거나 감염피해가 심각하다고 판단할 경우에는 관련사항을 교육과학기술부장관에게 신속히 통보하여야 한다.

⑤ 학교의 장은 교육과학기술부장관이 해당 기관에 악성코드 감염사실을 확인하여 조치를 권고할 경우, 즉시 이행하여야 한다.

제54조(전자우편 등 보안관리) ① 시스템관리자는 웜·바이러스 등 악성코드로부터 사용자 PC 등 전자우편 시스템 일체를 보호하기 위하여 국가정보원장이 안전성을 확인한 백신, 바이러스 월, 해킹메일 차단시스템을 구축하는 등 보안대책을 강구하여야 한다.(단, 사립학교는 이를 준용할 수 있음)

② 사용자는 상용 전자우편을 이용한 업무자료 송·수신을 금지하며 기관 전자우편으로 송·수신한 업무자료는 열람 등 활용 후 메일함에서 즉시 삭제하여야 한다.

③ 사용자는 메일에 포함된 첨부파일이 자동 실행되지 않도록 설정하고 첨부파일 다운로드 시 반드시 최신백신으로 악성코드 은닉여부를 검사하여야 한다.

④ 사용자는 출처가 불분명하거나 의심되는 제목의 전자우편은 열람을 금지하고 해킹메일로 의심되는 메일 수신시에는 즉시 정보보안담당자를 경유하여 교육과학기술부 사이버안전센터에 신고하여야 한다.(신고메일 : cert@ecsc.go.kr, sntsec@kisti.re.kr)

제55조(정보통신망 현황·자료 관리) ① 정보보안담당관은 다음 각 호에 해당하는 정보통신망 관련 현황·자료 관리에 유의하여야 한다.

1. 정보시스템 운용현황

2. 정보통신망 구성현황

3. IP 할당현황

4. 주요 정보화사업 추진현황

② 정보보안담당관은 다음 각 호의 자료를 대외비로 분류하여 관리하여야 한다. 다만, 국가안보와 직결되는 중요한 정보통신망 관련 세부자료는 해당 등급의 비밀로 분류 관리하여야 한다.

1. 정보통신망 세부 구성현황(IP 세부 할당현황 포함)

2. 국가용 보안시스템 운용 현황

3. 보안취약점 분석·평가 결과물
4. 정보시스템 관리대장[별지 제9호 서식]
5. 기타 보호할 필요가 있는 정보통신망 관련 자료

③ 정보통신망에 비밀번호를 저장하고자 할 경우에는 암호화하여 보관하여야 하고, 서버 등 주요 정보시스템의 비밀번호를 종합기록 관리하고자 할 경우에는 정보시스템 관리대장[별지 제9호 서식]에 등재하여 관리하여야 한다.

제56조(네트워크장비 보안관리) ① 시스템관리자는 라우터, 스위치 등 네트워크 장비 운용과 관련하여 다음 각 호의 보안조치를 강구해야 한다.

1. 네트워크 장비에 대한 원격접속은 원칙적으로 금지하되, 불가피할 경우 장비 관리용 목적으로 내부 특정 IP・MAC 주소에서의 접속은 허용
2. 물리적으로 안전한 장소에 설치하여 비인가자의 무단접근 통제
3. 최초 설치 시 보안취약점을 점검하여 제거하고 주기적으로 보안패치 실시
4. 불필요한 서비스 포트 제거

② 시스템관리자는 라우터 등 중요 네트워크장비의 접속기록을 6개월 이상 유지하여야 하고 비인가자에 의한 침투 여부를 주기적으로 점검하여 정보보안담당관에게 관련결과를 제출하여야 한다.

제57조(업무망 보안관리) ① 학교의 장은 업무자료를 소통하기 위한 전산망 구축 시 인터넷과 분리하도록 망을 설계하여야 한다. 이 경우 다음 각 호의 보안대책을 강구하여 사업 계획단계(사업 공고 전)에서 국가정보원장에게 보안성 검토를 의뢰하여야 한다.

1. 비인가자의 업무망·인터넷 침입 차단대책(침입차단·탐지시스템 등)
2. 비인가 장비의 업무망 접속 차단대책(네트워크 관리시스템 등)
3. 업무PC의 인터넷 접속 차단대책

② 학교의 장은 제1항에도 불구하고, 부득이 한 경우 적정 보안대책을 강구한 후 망 분리하지 아니할 수 있다.

③ 업무망 관리자는 정보시스템에 사용되는 'IP주소'를 체계적으로 관리하여야 하며, 업무망을 보호하기 위하여 사설주소체계(NAT)를 적용하여야 한다. 또한, IP주소별로 정보시스템 접속을 통제하여 비인가 정보통신기기나 PC 등을 이용한 업무망 내 정보시스템 접속을 차단하여야 한다.

④ 학교의 장은 업무망을 여타 기관의 망 및 인터넷과 연결 사용하고자 할 경우에는 보안관리 책임한계를 설정하고 망 연동에 따른 보안대책을 마련하여 자체 보안심사위원회 심의 후 국가정보원장에게 보안성검토를 의뢰하여야 한다.

⑤ 업무망 관리자는 제4항과 관련하여 비인가자의 업무망 무단침입을 방지하기 위하여 안전성이 검증된 침입차단・탐지시스템을 설치하고 중계서버를 운용하는 등 관련 보안대책을 강구하여야 한다.

⑥ 업무망 관리자는 업무망을 인터넷과 연동 시 효율적인 보안관리를 위하여 연결지점을 최소화 운용하여야 한다.

⑦ 정보보안담당관은 업무망의 외부망 연결에 따른 보안취약성 해소를 위하여 보안도구를 이용하여 수시 점검하여야 한다.

제58조(정보시스템 개발보안) ① 시스템 개발사업 담당자는 정보시스템을 자체적으로 개발하고자 하는 경우에는 다음 각 호의 사항을 고려하여 보안대책을 수립하고 정보보안담당관의 승인을 득하여야 한다.

1. 독립된 개발시설을 확보하고 비인가자의 접근 통제
2. 개발시스템과 운영시스템의 물리적 분리
3. 소스코드 관리 및 소프트웨어 보안관리

② 시스템 개발사업 담당자는 외부용역 업체와 계약하여 정보시스템을 개발하고자 하는 경우에는 다음 각 호의 사항을 고려하여 보안대책을 수립하고 정보보안담당관의 승인을 득하여야 한다.

1. 외부인력 대상 신원확인, 보안서약서 징구, 보안교육 및 점검

2. 외부인력의 보안준수 사항 확인 및 위반 시 배상책임의 계약서 명시
3. 외부인력의 정보시스템 접근권한 및 제공자료 보안대책
4. 외부인력에 의한 장비 반입·반출 및 자료 무단반출 여부 확인
5. 제1항의 제1호부터 제3호까지의 사항

③ 정보보안담당관은 제1항 및 제2항과 관련하여 보안대책의 적절성을 수시로 점검하고 정보시스템 개발을 완료한 경우에는 정보보안 요구사항을 충족하는지 검토하여야 한다.

제59조(정보시스템 유지보수) ① 학교의 장은 정보시스템 유지보수와 관련한 절차, 주기, 문서화 등에 관한 사항을 자체 규정에 포함하여야 한다. 유지보수 절차 및 문서화 수립 시 고려사항은 아래의 각 호와 같다.

1. 유지보수 인력에 대해 보안서약서 집행, 보안교육 등을 포함한 유지보수 인가 절차를 마련하고 인가된 유지보수 인력만 유지보수에 참여한다.
2. 결함이 의심되거나 발생한 결함, 예방 및 유지보수에 대한 기록을 보관한다.
3. 유지보수를 위해 원래 설치장소 외 다른 장소로 정보시스템을 이동할 경우, 통제수단을 강구한다.
4. 정보시스템의 유지보수 시에는 일시, 담당자 인적사항, 출입 통제조치, 정비내용 등을 기록·유지하여야 한다.

② 시스템관리자는 자체 유지보수 절차에 따라 정기적으로 정보시스템 정비를 실시하고 관련 기록을 보관하여야 한다.

③ 시스템관리자는 정보시스템의 변경이 발생할 경우, 정보보안담당관과 협조하여 정보시스템의 설계·코딩·테스트·구현과정에서의 보안대책을 강구하며 정보보안담당관은 관련 적절성을 주기적으로 확인하여야 한다.

④ 정보보안담당관은 시스템관리자 등이 유지보수와 관련된 장비·도구 등을 반출입할 경우, 악성코드 감염여부, 자료 무단반출 여부를 확인하는 등 보안조치 하여야 한다.

⑤ 시스템관리자는 외부에서 원격으로 정보시스템을 유지보수 하는 것을 원칙적으로 금지하여야 하며 부득이한 경우에는 정보보안담당관과 협의하여 자체 보안대책을 강구한 후 한시적으로 허용할 수 있다.

제60조(휴대용 저장매체 보안대책) ① 휴대용 저장매체 관리책임자는 휴대용 저장매체를 사용하여 업무자료를 보관할 필요가 있을 때에는 위변조, 훼손, 분실 등에 대비한 보안대책을 강구하여 정보보안담당관의 승인을 받아야 한다.

② 휴대용 저장매체 관리책임자는 휴대용 저장매체를 비밀용, 일반용으로 구분하고 주기적으로 수량 및 보관 상태를 점검하며 반출·입을 통제하여야 한다.

③ 휴대용 저장매체 관리책임자는 USB 관리시스템을 도입할 경우 국가정보원장이 안정성을 확인한 제품을 도입하여야 한다.

④ 휴대용 저장매체 관리책임자는 사용자가 USB 메모리를 PC 등에 연결 시 자동 실행되지 않도록 하고 최신 백신으로 악성코드 감염여부를 자동 검사하도록 보안 설정한다.

⑤ 비밀자료가 저장된 휴대용 저장매체는 매체별로 비밀등급 및 관리번호를 부여하고 비밀관리기록부에 등재 관리하여야 한다. 이 경우에는 매체 전면에 비밀등급 및 관리번호가 표시되도록 하여야 한다. 다만, 휴대용 저장매체가 국가용 보안시스템에 해당될 경우에는 해당 보안시스템의 운용·관리체계에 따라 관리하여야 한다.

⑥ 휴대용 저장매체를 파기 등 불용처리 하거나 비밀용을 일반용 또는 다른 등급의 비밀용으로 전환하여 사용할 경우 저장되어 있는 정보의 복구가 불가능하도록 완전삭제 프로그램을 사용하여야 한다.

⑦ 정보보안담당관은 사용자의 휴대용 저장매체 무단 반출 및 미등록 휴대용 저장매체 사용 여부 등 보안관리 실태를 주기적으로 점검하여야 한다.

제61조(전자정보 저장매체 불용처리) ① 사용자 및 시스템관리자는 하드디스크 등 전자정보 저장매체를 불용처리(교체·반납·양여·폐기 등) 하고자 할 경우에는 정보보안담당관의 승인 하에 저장매체에

수록된 자료가 유출되지 않도록 보안조치 하여야 한다.

② 자료의 삭제는 해당 정보가 복구될 수 없도록 해당 기관 실정에 맞게 저장매체별, 자료별 차별화된 삭제방법을 적용하여야 한다.

③ 해당 기관 내에서 정보시스템의 사용자가 변경된 경우, 비밀처리용 정보시스템은 완전포맷 3회 이상, 그 외의 정보시스템은 완전포맷 1회 이상으로 저장자료를 삭제하여야 한다.

제62조(접근기록 관리) ① 시스템관리자는 정보시스템의 효율적인 통제·관리, 사고 발생 시 추적 등을 위하여 사용자의 정보시스템 접근기록을 유지 관리하여야 한다.

② 제1항의 접근기록에는 다음 각 호의 내용이 포함되어야 한다.

1. 접속자, 정보시스템·응용프로그램 등 접속 대상
2. 로그 온·오프, 파일 열람·출력 등 작업 종류, 작업 시간
3. 접속 성공·실패 등 작업 결과
4. 전자우편 사용 등 외부발송 정보 등

③ 시스템관리자는 접근기록을 분석한 결과, 비인가자의 접속 시도, 정보 위변조 및 무단 삭제 등의 의심스러운 활동이나 위반 혐의가 발생한 사실을 발견한 경우 정보보안담당관에게 즉시 보고하여야 한다.

④ 접근기록은 정보보안사고 발생 시 확인 등을 위하여 최소 6개월 이상 보관하여야 하며 접근기록 위·변조 및 외부유출 방지 대책을 강구하여야 한다.

제63조(전자정보 저장매체 불용처리) ① 사용자 및 시스템관리자는 하드디스크 등 전자정보 저장매체를 불용처리(교체·반납·양여·폐기 등) 하고자 할 경우에는 정보보안담당관의 승인 하에 저장매체에 수록된 자료가 유출되지 않도록 보안조치 하여야 한다.

② 자료의 삭제는 해당 정보가 복구될 수 없도록 해당 기관 실정에 맞게 저장매체별, 자료별 차별화된 삭제방법을 적용하여야 한다.

③ 해당 기관 내에서 정보시스템의 사용자가 변경된 경우, 비밀처리용 정보시스템은 완전포맷 3회 이상, 그 외의 정보시스템은 완전포맷 1회 이상으로 저장자료를 삭제하여야 한다.

제64조(무선랜 보안관리) ① 학교의 장은 무선랜(와이파이 등)을 사용하여 업무자료를 소통하고자 할 경우 자체 보안대책을 수립하여 관련 사업 계획단계(사업 공고 전)에서 국가정보원장에게 보안성 검토를 의뢰하여야 한다.

② 시스템관리자는 제1항의 보안대책 수립 시, 다음 각 호의 사항을 포함하여야 한다.

1. 네트워크 이름(SSID, Service Set Identifier) 브로드캐스팅 중지
2. 추측이 어려운 복잡한 SSID 사용
3. WPA2 이상(256비트 이상)의 암호체계를 사용하여 소통자료 암호화(국가정보원장이 승인한 암호논리 사용)
4. MAC 주소 및 IP 필터링 설정, DHCP 사용금지
5. RADIUS(Remote Authentication Dial-In User Service) 인증 사용
6. 그 밖에 무선단말기·중계기(AP) 등 무선랜 구성요소별 분실·탈취·훼손·오용 등에 대비한 관리적·물리적 보안대책

③ 정보보안담당관은 제1항 및 제2항과 관련한 보안대책의 적절성을 수시로 점검하고 보완하여야 한다.

제65조(국제회의 보안관리) ① 학교의 장은 국제협상 등 중요 국제회의를 위하여 노트북, PC 등의 정보시스템을 해외 현지에서 사용하고자 하는 경우 회의정보가 유출되지 않도록 다음 각 호의 보안대책을 수립·시행하여야 한다.

1. 정보시스템 설치장소에 대한 물리적 접근통제 대책
2. 정보시스템 접근통제 및 분실방지 등 보안관리 대책
3. 암호화 등 정보시스템 저장정보 보안대책

4. 전화·팩스 등 통신시설에 대한 도청방지 대책
5. 그 밖에 회의정보 보호를 위하여 필요하다고 인정되는 대책

② 학교의 장은 제1항의 보안대책을 수립한 경우 적절성을 확인하이 위하여 사전에 국가정보원장에게 보안성 검토를 의뢰할 수 있다.

③ 국제회의 참가자는 회의 대상국이 제공한 정보시스템을 이용하여 중요 회의 정보를 작성하거나 저장 또는 송·수신하여서는 아니 된다. 다만 불가피한 경우에는 보안대책을 수립한 후 그러하지 아니할 수 있다.

④ 국제회의 참가자는 회의 대상국이 제공한 USB메모리 등 휴대용 저장매체를 사용하여서는 아니 된다. 다만, 불가피할 경우에는 최신 백신으로 악성코드 감염여부를 확인하는 등 보안조치 후 사용토록 하여야 한다.

제66(무선인터넷 보안관리) ① 학교의 장은 무선인터넷(WiBro, HSDPA 등) 시스템을 구축하여 업무자료를 소통하고자 할 경우 자체 보안대책을 수립하여 관련 사업 계획단계(사업 공고 전)에서 국가정보원장에게 보안성 검토를 의뢰하여야 한다.

② 시스템관리자는 청사 전역에 무선인터넷 사용을 제한하고 민원실 등 특별히 무선인터넷 사용이 필요한 구역에 한해 기관장 책임 하에 운용한다.

③ 시스템관리자는 업무용PC에서 무선인터넷 접속장치(USB형 등)가 작동되지 않도록 관련 프로그램 설치 금지 등 기술적 보안대책을 강구하여야 한다.

④ 정보보안담당관은 개인 휴대폰을 제외한 무선인터넷 단말기의 사무실 무단 반입·사용을 금지하는 한편 제1항부터 제3항까지와 관련한 보안대책의 적절성을 수시로 점검하고 보완하여야 한다.

제67조(인터넷전화 보안관리) ① 학교의 장은 인터넷전화 시스템을 구축하거나 민간 인터넷전화 사업자망(070)을 사용하고자 할 경우에는 사업 계획단계에서 자체 보안대책을 수립 시행하여야 한다.

② 시스템관리자는 제1항의 보안대책 수립 시, 다음 각 호의 사항을 포함하여야 한다.

1. 인터넷전화기에 대한 장치 인증 및 사용자 인증
2. 제어신호 및 통화내용의 암호화
3. 인터넷전화망(음성 네트워크)과 일반 전산망(데이터 네트워크)의 분리
4. 인터넷전화 전용 방화벽 등 정보보호시스템
5. 백업체제 구축

③ 시스템관리자는 인터넷전화 시스템 구축을 위해 민간 사업자망을 이용할 경우, 해당 사업자로 하여금 서비스 제공 구간에 대한 보안대책을 강구하도록 하여야 한다.

④ 제1항부터 제3항까지와 관련하여 인터넷전화를 실제 운영하는 부서의 장이 '관리책임자'가 된다.

제68조(CCTV운용 보안관리) ① 학교의 장은 CCTV운용에 필요한 카메라, 중계·관제서버, 관리용PC 등 관련 시스템을 비인가자의 임의 조작이 물리적으로 불가능하도록 설치하여야 한다.

② CCTV 상황실은 보호구역으로 지정 관리하고 출입통제장치를 도입하여야 한다.

③ 시스템관리자는 CCTV 카메라, 비디오서버, 관제서버 및 관련 전산망 설치 시 업무망 및 인터넷과 분리 운영하는 것을 원칙으로 한다. 다만, 부득이하게 인터넷망을 이용할 경우에는 전송내용을 암호화하여야 한다.

④ CCTV 시스템 일체는 사용자계정·비밀번호 등 시스템 인증대책을 강구하고 허용된 특정 IP에서만 접속 허용하는 등 비인가자의 침입 통제대책을 강구하여야 한다.

⑤ 제1항부터 제4항까지와 관련하여 CCTV를 실제 운영하는 부서의 장이 '관리책임자'가 된다.

⑥ 정보보안담당관은 제1항부터 제4항까지와 관련하여 보안대책의 적절성을 수시로 점검하고 보완하여야 한다.

제69조(디지털복사기 보안관리) ① 학교의 장은 디지털복사기(이하 '복사기'라 한다)를 도입하고자 할 경우 복사기內 저장매체에 보관된 자료유출 방지를 위해 자료의 완전삭제 기능이 탑재된 제품을 도입

하여야 한다.

② 시스템관리자는 다음 각 호의 경우에 복사기 저장매체의 저장자료를 완전삭제 하여야 한다.

1. 복사기의 사용연한이 경과하여 폐기·양여할 경우
2. 복사기의 무상 보증기간 중 저장매체 또는 복사기 전체를 교체할 경우
3. 고장수리를 위한 외부반출 등 당해 기관이 복사기의 저장매체를 보안통제 할 수 없는 환경으로 이동할 경우
4. 기타, 당해 기관에서 저장자료 삭제가 필요하다고 판단하는 경우

③ 시스템관리자는 복사기의 소모품 등을 교체하기 위한 유지보수 시 정보보안담당자 입회·감독 하에 작업을 실시하여 저장매체 무단 교체 등을 예방하여야 한다.

④ 정보보안담당관은 해 기관의 저장매체 내장 복사기 현황을 파악하고 복사기의 유지보수 및 불용처리 시 저장매체에 대한 보안조치를 수행하여야 한다.

제70조(첨단 정보통신기기 보안관리) ① 학교의 장은 개인휴대단말기(PDA)·스마트폰, 전자제어장비 등 첨단 정보통신기기를 활용하여 업무자료 등 중요정보를 소통·관리하고자 할 경우에는 자체 보안대책을 수립하여 관련 사업 계획단계(사업 공고 전)에서 국가정보원장에서 보안성 검토를 의뢰하여야 한다.

② 시스템관리자는 제1항의 보안대책 수립 시, 다음 각 호의 사항을 포함하여야 한다.

1. 첨단 정보통신기기에 대한 장치 인증 및 사용자 인증
2. 제어신호, 통화내용 등 데이터의 암호화
3. 업무자료의 무단 저장 금지 및 업무용·인터넷 PC에 무단 연동 금지
4. 시스템의 분실·훼손·탈취 등에 대비한 관리적·물리적·기술적 보안대책

③ 정보보안담당관은 개인이 소지한 첨단 정보통신기기가 업무와 무관하더라도 업무자료 유출에 직·간접 악용될 소지가 있다고 판단될 경우, 반·출입 통제 등 관련 대책을 강구할 수 있다.

④ 정보보안담당관은 제2항과 관련한 대책 수립·시행을 위해 국가정보원장에게 해당 첨단 정보통신기기 도입에 따른 보안취약점과 대책 등 기술지원을 요청할 수 있다.

제71조(용역사업 보안관리) ① 학교의 장은 정보화·정보보호사업 및 보안컨설팅 수행 등을 외부용역으로 추진할 경우 사업 책임자로 하여금 다음 각 호의 사항을 포함한 보안대책을 수립·시행하여야 한다.

1. 용역사업 계약 시 계약서에 참가직원의 보안준수 사항과 위반 시 손해배상 책임 등 명시
2. 용역사업 수행 관련 보안교육·점검 및 용역기간 중 참여인력 임의교체 금지
3. 정보통신망도·IP현황 등 용역업체에 제공할 자료는 자료 인계인수대장을 비치, 보안조치 후 인계·인수하고 무단 복사 및 외부반출 금지
4. 사업 종료 시 외부업체의 노트북·휴대용 저장매체 등을 통해 비공개 자료가 유출되는 것을 방지하기 위해 복구가 불가능하도록 완전삭제
5. 용역업체로부터 용역 결과물을 전량 회수하고 비인가자에게 제공·열람 금지
6. 용역업체의 노트북 등 관련 장비를 반입·반출시마다 악성코드 감염여부, 자료 무단반출 여부를 확인
7. 그 밖에 각급기관의 장이 보안관리가 필요하다고 판단하는 사항이나 국가정보원장이 보안조치를 권고하는 사항

② 학교의 장은「국가계약법」시행령 제76조 제1항 제18호에 따라 용역사업 추진 시 과업지시서·입찰공고·계약서에 다음 각 호의 누출금지 대상정보를 명시해야 하며 해당정보 누출 시 입찰 참가자격 제한을 위한 부정당업자로 등록하여야 한다.

1. 기관 소유 정보시스템의 내·외부 IP주소 현황
2. 세부 정보시스템 구성 현황 및 정보통신망 구성도
3. 사용자계정·비밀번호 등 정보시스템 접근권한 정보
4. 정보통신망 취약점 분석·평가 결과물

5. 정보화 용역사업 결과물 및 관련 프로그램 소스코드(유출시 안보·국익에 피해가 우려되는 중요 용역사업에 해당)
6. 국가용 보안시스템 및 정보보호시스템 도입 현황
7. 침입차단시스템·방지시스템(IPS) 등 정보보호제품 및 라우터·스위치 등 네트워크 장비 설정 정보
8.「공공기관의 정보공개에 관한 법률」제9조 제1항에 따라 비공개 대상 정보로 분류된 기관의 내부문서
9.「공공기관의 개인정보보호에 관한 법률」제2조 제2호의 개인정보
10. 기타 각급기관의 장이 공개가 불가하다고 판단한 자료

③ 학교의 장은 비밀관련 용역사업을 수행할 경우, 외부인원에 대한 신원조사·비밀취급인가, 보안교육 등 보안조치를 수행하여야 한다.

④ 정보보안담당관은 제1항 내지 제3항에서 규정한 보안대책의 시행과 관련한 이행실태를 주기적으로 점검하고 미비점 발견 시 사업 책임자로 하여금 보완토록 조치하여야 한다.

제72조(정보시스템 위탁운영 보안관리) ① 학교의 장은 소관 정보시스템에 대한 외부업체의 위탁 운영을 최소화하되, 위탁 운영과 관련한 관리적·물리적·기술적 보안대책을 수립하여 시행하여야 한다.

② 정보시스템의 위탁 운영은 여타 기관 또는 업체 직원이 당해 기관에 상주하여 수행하는 것을 원칙으로 한다. 다만, 당해 기관에 위탁업무 수행 직원의 상주가 불가한 타당한 사유가 있을 경우, 그러하지 아니할 수 있다.

③ 정보시스템의 위탁운영과 관련하여 동 조문에 명시되지 않은 사항에 대해서는 제71조(용역사업 보안관리) 등을 참조한다.

제73조(원격근무 보안관리) ① 학교의 장은 재택·파견·이동근무 등 원격 근무를 지원하기 위한 정보시스템을 도입·운영할 경우 기술적·관리적·물리적 보안대책을 수립하고 교육과학기술부장관을 경유하여 국가정보원장의 보안성 검토를 거쳐 시행하여야 한다.

② 학교의 장은 원격근무 가능 업무 및 공개·비공개 업무 선정기준을 수립하되 대외비 이상 비밀자료를 취급하는 업무는 원격근무 대상에서 원칙적으로 제외하되 반드시 수행해야 하는 경우 교육과학기술부장관과 협의하여 수행여부를 결정한다.

③ 학교의 장은 모든 원격근무자에게 보안서약서를 징구하고 원격근무자의 업무변경·인사이동·퇴직 등 상황 발생 시 정보시스템 접근권한 재설정 등 관련 절차를 수립하여야 한다.

④ 학교의 장은 원격근무자가 원격근무 시 해킹에 의한 업무자료 유출을 방지하기 위하여 원격근무용 PC내 업무자료 저장금지, 화면복사 금지 등 보안조치를 수행하여야 한다.

⑤ 원격근무자는 정보시스템 고장 시 정보유출 방지 등 보안대책을 강구한 후 정보보안담당관과 협의하여 정비·반납 등 조치를 취하여야 한다.

⑥ 비공개 원격업무인 경우에는 국가용 보안시스템을 사용하여 소통자료를 암호화하고 행정전자서명 체계를 이용하여 인증하며 인증강화를 위해 일회용 비밀번호· 생체인증 등 보안기술을 사용하여야 한다.

⑦ 정보보안담당관은 주기적인 보안점검을 실시하여 원격근무 보안대책의 이행 여부를 확인하여야 한다.

제74조(국가비상사태시 보호관리) ① 학교의 장은 전시·사변 또는 이에 준하는 국가비상사태 발생 시에 비밀 및 중요 정보시스템의 효율적인 보호 관리를 위한 대책을 강구하여야 한다.

② 제1항의 비밀 및 중요 정보시스템에는 다음 각 호의 사항을 포함한다.

1. 국가비상사태 발생 시 후송하여 계속 보관해야 할 비밀(A급 비밀)
2. 암호장비, 음어자재, 비밀관리시스템 등 국가용 보안시스템
3. 비밀이 저장된 CD·외장형 하드디스크·USB메모리 등 휴대용 저장매체
4. 각급기관의 장이 보관이 필요하다고 결정한 중요자료 및 중요 정보시스템 등

③ 학교의 장은 제1항의 보호관리 대책 수립시 충무사태 단계별 비밀 및 중요 정보시스템의 소산·이동·파기 절차·방법 등 조치방안 일체를 포함하여야 한다.

④ 학교의 장은 비상사태에 따른 소관 업무지역 이동시 비밀을 정보통신망을 통하여 유통·관리하고자 할 경우에는 국가지도통신망 등 국가정보원장이 안전성을 확인한 보안조치를 하여야 한다.

제75조(보안관제센터 구축) ① 학교의 장은 소관 정보통신망에 대한 사이버공격 정보를 수집·분석·대응할 수 있는 보안관제센터를 설치하여야 한다. 다만 국가·공공기관이 운영하는 보안관제센터에 관련 업무를 위탁할 수 있다.

② 보안관제센터를 운영할 경우 학교의 장은 보안관제 업무를 하루 24시간 중단 없이 수행하여야 하며 보안관제센터 운영에 필요한 전담직원을 배치하여야 한다.

③ 학교의 장은 사이버공격 정보를 수집할 경우, 피해 유무를 파악하고 공격 IP차단, 로그자료 보존 등 초동조치를 신속하게 취하여야 한다. 이 경우, 사고원인 규명 시까지 피해시스템에 대한 증거를 보전하고 임의로 관련 자료를 삭제하거나 포맷하여서는 아니 된다.

④ 학교의 장은 초동조치가 끝난 경우에 국가사이버안전센터장과 협의하여 보안대책을 수립·시행하여야 한다.

⑤ 학교의 장은 사이버공격 정보의 신속한 수집 및 전파를 위하여 국가사이버안전센터 등과 비상연락체계를 구축하여야 한다.

제76조(정보공유) ① 학교의 장은 관계법규에 위배되지 않는 범위 내에서 수집·탐지한 사이버공격 정보를 교육과학기술부 사이버안전센터장 및 관계기관의 장에게 제공하여야 한다.

② 보안관제센터를 운영할 경우 학교장은 [별지 제22호 서식]에 따라 보안관제센터의 운영현황을 작성하여 교육과학기술부 사이버안전센터장에 통보하여야 한다. 다만, 기 제출한 경우에는 변동사항에 한하여 통보한다.

③ 보안관제센터를 운영하는 기관의 장은 보안관제시 수집된 사이버공격 정보가 여타 보안관제센터의 소관 업무와 연관될 경우에 해당 보안관제센터의 장에게 [별지 제21호 서식]에 따라 신속히 이관하여야 한다.

④ 국가정보원장은 제1항 내지 제3항의 규정에 따른 사이버공격 정보를 전자적으로 공유하기 위해 보안대책이 강구된 통합보안관제정보공유시스템을 구축·운영할 수 있으며, 학교의 장은 특별한 사정이 없는 한 동 시스템을 활용하여야 한다.

제77조(정보보호시스템의 도입 등) ① 학교의 장은 국가용 보안시스템을 제외한 정보보호시스템을 도입할 경우, [별표 제2호]의 도입요건을 충족시키는 제품을 도입하여야 한다. 다만, [별표 제2호] 이외 기타 유형의 정보보호시스템을 도입하거나 긴급한 사유 등으로 [별표 제2호]의 도입요건을 만족하지 못하는 제품을 도입해야 할 경우에는 국가정보원장과 도입 가능 여부를 사전 협의하여야 한다.

② 제1항의 제품에 중요자료 저장·소통을 위한 암호기능이 포함될 경우 아래와 같은 알고리즘 및 보호함수가 포함된 검증필 암호모듈을 탑재하여야 하며 구체적인 사항은 국가정보원장이 별도 지침으로 정한다.

1.「암호검증기준」(KS X ISO/IEC 19790)에서 제시하는 보호함수

2. 그 밖에 국가정보원장이 사용을 허용한 암호 알고리즘

제78조(보안적합성 검증대상 및 신청) ① 학교의 장은 제73조에 의해 정보보호시스템 도입할 경우에는 도입계약 체결 후 15일 이내에 국가정보원장에게 보안적합성 검증을 신청하여야 한다. 다만, 자체 개발하거나 외부업체 등을 통해 개발한 시스템은 검수 전 15일 이내에 신청하여야 한다.

② 보안적합성 검증대상 시스템은 다음 각 호와 같다.

1. 국제공통평가기준(CC)에 따라 인증을 받은 제품이나 국가정보원장이 그와 동등한 효력이 있다고 인정한 제품

2. 각급기관의 장이 자체 개발하거나 외부업체 등에 의뢰하여 개발한 제품

③ 제1항 및 제2항에도 불구하고, 다음 각 호의 시스템을 도입할 경우에는 검증을 생략한다.

1.「국내용 정보보호제품 평가인증 수행지침」(2010.4, 국정원)에 따라 IT인증사무국으로부터 국내용으로 CC인증을 받은 제품

2. 국가정보원장이 사용 승인한 국가용 암호제품

3. 국가정보원장의 별도지정제품(저장자료완전삭제 제품을 포함한다)

4. 디지털복합기(복사기, 프린터, 스캐너, 팩스 등) 하드디스크 소거용 제품으로서 국제공통평가기준(CC) EAL2 등급 이상을 받은 제품

5. 기타 국가정보원장이 보안적합성 검증이 불요하다고 인정한 제품

제79조(제출문서) ① 보안적합성 검증 신청에 필요한 제출문서는 다음과 같다.

1. 국제공통평가기준(CC)에 따라 인증을 받은 제품이나 국가정보원장이 그와 동등한 효력이 있다고 인정한 제품

가. [별지 제20호 서식]의 정보보호시스템 자체 점검결과 1부

나. [별지 제21호 서식]의 보안적합성 검증 신청서 1부

다. 기술제안요청서 사본 1부

2. 자체 개발하거나 외부업체 등에 의뢰하여 개발한 시스템

가. [별지 제20호 서식]의 정보보호시스템 자체 점검결과 1부

나. [별지 제21호 서식]의 보안적합성 검증 신청서 1부

다. 기술제안요청서 사본 1부

라. 상세설계서 1부

마. 개발완료 보고서 1부

바. 제품사용설명서 1부

② 국가정보원장은 제1항의 제출문서 이외에 보안적합성 검증에 필요하다고 판단될 경우 추가 자료를 요청할 수 있으며 이 경우, 요청받은 기관의 장은 특별한 사유가 없는 한 15일 이내에 추가 자료를 제출하여야 한다.

제80조(검증시험 및 결과조치) ① 국가정보원장은 각급기관으로부터 제출받은 문서에 대하여 타당성 및 적절성을 검토하고 시스템의 보안기능 정상동작 여부 등 안전성을 시험한다.

② 국가정보원장은 제1항의 시험과 관련하여 국가정보보안기술 연구개발을 수행하는 정부출연 연구기관의 장 등에게 안전성 시험을 의뢰할 수 있다.

③ 각급기관의 장은 국가정보원장이 시스템 개발업체의 개발환경에 대한 보안관리 실태점검을 요청할 경우 특별한 사유가 없는 한 협조하여야 한다.

④ 국가정보원장은 보안적합성 검증결과 취약점이 발견될 경우에는 이를 해당 기관에 통보한다.

⑤ 각급기관의 장은 제4항과 관련한 취약점을 통보받았을 때에는 30일 이내에 보완대책을 수립하여 조치하고 그 결과를 국가정보원장에게 통보하여야 한다.

제8장 개인정보 처리 기준

제1절 개인정보의 처리

제81조(개인정보의 수집) ① 개인정보의 “수집”이란 정보주체로부터 직접 이름, 주소, 전화번호 등의 정보를 제공받는 것뿐만 아니라 정보주체에 관한 모든 형태의 개인정보를 취득하는 것을 말한다.

② 개인정보처리자는 다음 각 호의 경우에 개인정보를 수집할 수 있으며, 그 수집 목적의 범위에서 이용할 수 있다.

1. 정보주체로부터 사전에 동의를 받은 경우

2. 법률에서 개인정보를 수집·이용할 수 있음을 구체적으로 명시하거나 허용하고 있는 경우

3. 법령에서 개인정보처리자에게 구체적인 의무를 부과하고 있고, 개인정보처리자가 개인정보를 수집·이용하지 않고는 법령에서 부과하는 구체적인 의무를 이행하는 것이 불가능하거나 현저히 곤란한 경우

4. 본교에서 개인정보를 수집·이용하지 않고는 법령 등에서 정한 소관업무를 수행하는 것이 불가능하거나 현저히 곤란한 경우

5. 개인정보를 수집·이용하지 않고는 정보주체와 계약을 체결하고, 체결된 계약의 내용에 따른 의무를 이행하는 것이 불가능하거나 현저히 곤란한 경우

6. 정보주체 또는 제3자(정보주체를 제외한 그 밖의 모든 자를 말한다.)의 생명, 신체, 재산에 대한 피해를 방지해야 할 급박한 상황이어서 개인정보를 수집·이용해야 할 필요성이 명백히 인정됨에도 불구하고 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 연락을 취할 수 없는 상황이어서 사전에 동의를 받을 수 없는 경우

7. 개인정보처리자가 법령 또는 정보주체와의 계약에 따른 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 개인정보의 수집·이용에 관한 동의 여부 및 동의 범위 등을 선택하고 결정할 권리보다 우선하는 경우. 다만, 이 경우 개인정보의 수집·이용은 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 범위로 한정된다.

③ 개인정보처리자가 정보주체로부터 직접 명함 또는 그와 유사한 매체(이하 “명함 등”이라 함)를 제공받음으로써 개인정보를 수집하는 경우, 정보주체가 동의의사를 명확히 표시하거나 그렇지 않은 경우 명함 등을 제공하는 정황 등에 비추어 사회통념상 동의 의사가 있었다고 인정되는 범위 내에서만 이용할 수 있다.

④ 개인정보처리자가 인터넷 홈페이지 등 공개된 매체 또는 장소(이하 "인터넷 홈페이지등"이라 함)에서 개인정보를 수집하는 경우, 해당 개인정보는 본인의 개인정보를 인터넷 홈페이지등에 게시하거나 게시하도록 허용한 정보주체의 동의 의사가 명확히 표시되거나 인터넷 홈페이지등의 표시 내용에 비추어 사회통념상 동의 의사가 있었다고 인정되는 범위 내에서만 이용할 수 있다.

⑤ 개인정보처리자는 계약 등의 상대방인 정보주체가 대리인을 통하여 법률행위 또는 의사표시를 하는 경우 대리인의 대리권 확인을 위한 목적으로만 대리인으로부터 또는 의사표시를 하는 경우 대리인의 개인정보를 수집·이용할 수 있다.

⑥ 근로자와 사용자가 근로계약을 체결하는 경우 「근로기준법」 제2조제5호의 임금지급, 교육, 증명서 발급, 근로자 복지제공을 위하여 근로자의 동의 없이 개인정보를 수집·이용할 수 있다.

제82조(정보주체의 사전 동의를 받을 수 없는 경우) 개인정보처리자가 법 제15조제1항제5호 및 제18조제2항제3호에 따라 정보주체의 사전 동의 없이 개인정보를 수집, 이용 또는 제공한 경우, 당해 사유가 해소된 때에는 개인정보의 처리를 즉시 중단하여야 하며, 정보주체에게 사전 동의 없이 개인정보를 수집 또는 이용한 사실, 그 사유와 이용내역을 알려야 한다.

제83조(개인정보의 제공) ① 개인정보의 “제공”이란 개인정보의 저장매체 또는 개인정보가 담긴 출력물이나 책자 등의 물리적 이전, 네트워크를 통한 개인정보의 전송, 개인정보에 대한 제3자의 접근권한 부여, 개인정보처리자와 제3자의 개인정보 공유 등 개인정보의 이전과 공동으로 이용할 수 있는 상태를 초래하는 모든 행위를 말한다.

② 법 제17조의 “제3자”란 정보주체와 정보주체 또는 그의 법정대리인으로부터 개인정보를 실질적·직접적으로 수집·보유한 개인정보처리자를 제외한 모든 자를 의미하며, 법 제26조제2항에 따른 수탁자는 제외한다.

③ 개인정보처리자가 법 제17조제2항제1호에 따라 정보주체에게 개인정보를 제공받는 자를 알리는 경우에는 그 성명(법인 또는 단체인 경우에는 그 명칭)과 연락처를 함께 알려야 한다.

제84조(개인정보의 목적 외 이용 등) ① 법 제18조의 “제3자”란 정보주체와 정보주체 또는 그의 법정대리인으로부터 개인정보를 실질적·직접적으로 수집·보유한 개인정보처리자를 제외한 모든 자를 의미하

며, 법 제26조제2항에 따른 수탁자는 제외한다.

② 개인정보처리자가 법 제18조제2항에 따라 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우에는 제공과 동시에 또는 필요한 경우 제공한 이후에 개인정보를 제공받는 자에게 이용 목적, 이용 방법, 이용 기간, 이용 형태 등을 제한하거나, 개인정보의 안전성 확보를 위하여 필요한 구체적인 조치를 마련하도록 문서(전자문서를 포함한다. 이하 같다)로 요청하여야 한다. 이 경우 요청을 받은 자는 그에 따른 조치를 취하고 그 사실을 개인정보를 제공한 개인정보처리자에게 문서로 알려야 한다.

③ 법 제18조제2항에 따라 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우에는 개인정보를 제공하는 자와 개인정보를 제공받는 자는 개인정보의 안전성에 관한 책임관계를 명확히 하여야 한다.

④ 개인정보처리자가 법 제18조제3항제1호에 따라 정보주체에게 개인정보를 제공받는 자를 알리는 경우에는 그 성명(법인 또는 단체인 경우에는 그 명칭)과 연락처를 함께 알려야 한다.

⑤ 개인정보처리자가 법 제18조제2항제4호에 따라 개인정보를 제3자에게 제공하는 경우에는 다른 정보와 결합하여서도 특정 개인을 알아볼 수 없는 형태로 제공하여야 한다.

제85조(개인정보 수집 출처 등 고지) ① 개인정보처리자가 정보주체 이외로부터 수집한 개인정보를 처리하는 때에는 정당한 사유가 없는 한 정보주체의 요구가 있은 날로부터 3일 이내에 법 제20조제1항 각 호의 모든 사항을 정보주체에게 알려야 한다.

② 법 제20조제2항 각 호에 근거하여 제1항에 따른 정보주체의 요구를 거부하는 경우에는 정당한 사유가 없는 한 정보주체의 요구가 있은 날로부터 3일 이내에 그 거부의 근거와 사유를 정보주체에게 알려야 한다.

제86조(개인정보의 파기방법 및 절차) ① 개인정보처리자는 개인정보의 보유기간이 경과된 경우에는 정당한 사유가 없는 한 보유기간의 종료일로부터 5일 이내에, 개인정보의 처리 목적 달성, 해당 서비스의 폐지, 사업의 종료 등 그 개인정보가 불필요하게 되었을 때에는 정당한 사유가 없는 한 개인정보의 처리가 불필요한 것으로 인정되는 날로부터 5일 이내에 그 개인정보를 파기하여야 한다.

② 시행령 제16조제2호의 '복원이 불가능한 방법'이란 사회통념상 현재의 기술수준에서 적절한 비용이 소요되는 방법을 말한다.

③ 개인정보처리자는 개인정보의 파기에 관한 사항을 기록·관리하여야 한다.

④ 개인정보파기의 시행 및 확인은 개인정보 보호책임자의 책임하에 수행된다.

⑤ 개인정보 보호책임자는 개인정보 파기 시행 후 파기 결과를 확인하여야 한다.

⑥ 개인정보처리자 중 공공기관의 개인정보파일 파기에 관하여는 제62조 및 제63조를 적용한다.

제87조(법령에 따른 개인정보의 보존) 개인정보처리자가 법 제21조제1항 단서에 따라 개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 법령에 따라 해당 개인정보 또는 개인정보파일을 보존한다는 점을 분명히 표시하여야 한다.

제88조(동의를 받는 방법) ① 개인정보처리자는 법 제15조제1항제1호에 따라 개인정보의 수집과 이용을 위하여 정보주체의 동의를 받고자 하는 경우에는 기본적인 재화 또는 서비스의 제공을 위하여 반드시 필요한 최소한의 개인정보와 부가적인 재화 또는 서비스의 제공을 위하여 필요한 최소한의 개인정보를 구분하여 정보주체에게 알리고 동의를 받아야 한다.

② 개인정보처리자가 법 제15조제1항제1호, 법 제17조제1항제1호, 법 제23조제1호 및 법 제24조제1항제1호에 따라 개인정보를 처리하기 위하여 정보주체의 동의를 얻고자 하는 경우에는 정보주체의 동의가 필요한 경우와 필요하지 않은 경우를 구분하고, 후자의 경우에는 정보주체의 동의 없이 개인정보를 처리할 수 있다는 점과 그 사유를 알려야 한다.

③ 개인정보처리자는 법 제18조제2항제1호에 따라 정보주체로부터 별도의 동의를 받고자 하는 경우에는 정보주체가 다른 개인정보처리의 목적과 별도로 동의여부를 표시할 수 있도록 조치를 취하고 동의를 받아야 한다.

④ 개인정보처리자가 시행령 제17조제1항제2호의 규정에 따라 전화에 의한 동의와 관련하여 통화내

용을 녹취할 때에는 녹취사실을 정보주체에게 알려야 한다.

⑤ 개인정보처리자가 친목단체를 운영하기 위하여 다음 각 호의 어느 하나에 해당하는 개인정보를 수집하는 경우에는 제1항에 의한 의무를 부담하지 아니한다.

1. 친목단체의 가입을 위한 성명, 연락처 및 친목단체의 회칙으로 정한 공통의 관심사나 목표와 관련된 인적 사항
2. 친목단체의 회비 등 친목유지를 위해 필요한 비용의 납부현황에 관한 사항
3. 친목단체의 활동에 대한 구성원의 참석여부 및 활동내용에 관한 사항
4. 기타 친목단체의 구성원 상호간의 친교와 화합을 위해 구성원이 다른 구성원에게 알리기를 원하는 생일, 취향 및 가족의 애경사 등에 관한 사항

제89조(법정대리인의 동의) ① 시행령 제17조제2항에 따라 개인정보처리자가 법정대리인의 성명·연락처를 수집할 때에는 해당 아동에게 자신의 신분과 연락처, 법정대리인의 성명과 연락처를 수집하고자 하는 이유를 알려야 한다.

② 시행령 제17조제1항 각 호의 동의를 얻는 방법은 법 제22조제5항에 따라 법정대리인으로부터 동의를 얻는 경우에도 적용된다.

③ 개인정보처리자는 법 제22조제5항에 따라 수집한 법정대리인의 개인정보를 법정대리인의 동의를 얻기 위한 목적으로만 이용하여야 하며, 법정대리인의 동의 거부가 있거나 법정대리인의 동의 의사가 확인되지 않는 경우 수집일로부터 5일 이내에 파기해야 한다.

제90조(민감정보 처리) ① 개인정보처리자가 법 제23조제1호에 따라 민감정보의 처리를 위하여 정보주체에게 동의를 받고자 하는 경우에는 다른 개인정보와 민감정보를 구분하여 민감정보에 대하여는 정보주체가 별도로 동의할 수 있도록 조치를 취하여야 한다.

② 개인정보처리자는 제1항에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.

1. 민감정보의 수집·이용 목적
2. 수집하려는 민감정보의 항목
3. 민감정보의 보유 및 이용 기간
4. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

제91조(고유식별정보 처리에 대한 동의) ① 개인정보처리자가 법 제24조제1항제1호에 따라 고유식별정보의 처리를 위하여 정보주체에게 동의를 받고자 하는 경우에는 다른 개인정보와 고유식별정보를 구분하여 고유식별정보에 대하여는 정보주체가 별도로 동의할 수 있도록 조치를 취하여야 한다.

② 개인정보처리자는 제1항에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.

1. 고유식별정보의 수집·이용 목적
2. 수집하려는 고유식별정보의 항목
3. 고유식별정보의 보유 및 이용 기간
4. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

제92조(주민등록번호 이외의 회원가입 방법 제공) ① 시행령 제20조제1항제2호의 “홈페이지를 이용한 정보주체의 수”는 홈페이지의 방문자 수를 말한다.

② 개인정보처리자가 시행령 제20조제1항에 따라 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법(이하 “대체수단”이라 한다)을 제공해야 하는 경우, 정보주체는 주민등록번호가 아닌 대체수단을 사용하여서도 회원으로 가입할 수 있다는 점을 회원가입절차를 위한 화면을 통하여 명시적으로 알리고 회원가입을 받아야 한다. 이 경우 주민등록번호를 이용한 회원가입 방법과 대체수단을 이용한 회원가입 방법을 하나의 화면을 통하여 제공하여야 한다.

제93조(개인정보취급자에 대한 감독) ① 개인정보처리자는 개인정보취급자를 업무상 필요한 한도 내에

서 최소한으로 두어야 하며, 개인정보취급자의 개인정보 처리범위를 업무상 필요한 한도 내에서 최소한으로 제한하여야 한다.

② 개인정보처리자는 개인정보 처리시스템에 대한 접근권한을 업무의 성격에 따라 당해 업무수행에 필요한 최소한의 범위로 업무담당자에게 차등 부여하고 접근권한을 관리하기 위한 조치를 취해야 한다.

③ 개인정보처리자는 개인정보취급자로 하여금 보안서약서를 제출하도록 하는 등 적절한 관리·감독을 해야 하며, 인사이동 등에 따라 개인정보취급자의 업무가 변경되는 경우에는 개인정보에 대한 접근권한을 변경 또는 말소해야 한다.

제2절 개인정보 처리의 위탁

제94조(수탁자의 선정 시 고려사항) ① 개인정보의 처리 업무를 위탁하는 개인정보처리자(이하 "위탁자"라 한다)가 개인정보 처리 업무를 위탁받아 처리하는 자(이하 "수탁자"라 한다)를 선정할 때에는 인력과 물적 시설, 재정 부담능력, 기술 보유의 정도, 책임능력 등을 종합적으로 고려하여야 한다.

② 개인정보처리자가 개인정보의 처리 업무를 위탁하는 때에는 수탁자의 처리 업무의 지연, 처리 업무와 관련 없는 불필요한 개인정보의 요구, 처리기준의 불공정 등의 문제점을 종합적으로 검토하여 이를 방지하기 위하여 필요한 조치를 마련하여야 한다.

제95조(개인정보 보호 조치의무) 수탁자는 위탁받은 개인정보를 보호하기 위하여 「개인정보의 안전성 확보조치 기준 고시」에 따른 관리적·기술적·물리적 조치를 한다.

제96조(정보주체와 재위탁의 관계) ① 정보주체는 수탁자로부터 개인정보 처리 업무를 재위탁 받아 처리하는 자(이하 "재수탁자"라 한다)가 재위탁 받은 개인정보 처리 업무를 수행하면서 발생하는 손해에 대한 배상을 청구할 수 있다.

② 개인정보 처리 업무의 재위탁에 대해서는 법 제26조를 준용한다.

제3절 개인정보 보호책임자

제97조(개인정보 보호책임자의 지정) ① 예원예술대학교의 개인정보 보호책임자는 보안업무를 담당하고 있는 행정지원처장으로 한다.

제98조(개인정보 보호책임자의 공개) ① 개인정보처리자가 개인정보 보호책임자를 지정하거나 변경하는 경우 개인정보 보호책임자의 지정 및 변경 사실, 성명과 부서의 명칭, 전화번호 등 연락처를 공개하여야 한다.

② 개인정보처리자는 개인정보 보호책임자를 공개하는 경우 개인정보 보호와 관련한 고충처리 및 상담을 실제로 처리할 수 있는 연락처를 공개하여야 한다. 다만, 개인정보 보호책임자와 개인정보 보호업무를 처리하는 담당자의 성명, 부서의 명칭, 전화번호 등 연락처를 함께 기재할 수 있다.

제99조(개인정보 보호책임자의 교육) 개인정보보호법 시행령 제32조제3항에 따라 행정안전부장관이 개설 운영할 수 있는 개인정보 보호책임자에 대한 교육의 내용은 다음 각 호와 같다.

1. 개인정보 보호 관련 법령 및 제도의 내용
2. 법 제31조제2항 및 시행령 제32조제1항 각 호의 업무수행에 필요한 사항
3. 그 밖에 개인정보처리자의 개인정보 처리를 위하여 필요한 사항

제100조(교육계획의 수립 및 시행) ① 학교의 장은 매년 초 당해연도 개인정보 보호책임자 교육계획을 수립하여 시행한다.

② 학교의 장은 제1항의 교육계획에 따라 사단법인 한국개인정보보호협의회 등의 단체에 개인정보 보호책임자 교육을 실시하게 할 수 있다.

③ 학교의 장은 개인정보 보호책임자가 지리적·경제적 여건에 구애받지 않고 편리하게 교육을 받은 수 있는 여건 조성을 위해 노력하여야 한다.

제4절 개인정보 유출 통지

제101조(개인정보의 유출) 개인정보의 유출이라 함은 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고, 정보주체의 개인정보에 대하여 개인정보처리자가 통제를 상실하거나 또는 권한 없는 자의 접근을 허용한 것으로서, 다음 각 호의 어느 하나에 해당하는 경우를 말한다.

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

제102조(통지시기 및 항목) ① 개인정보처리자는 실제로 유출 사고가 발생한 것으로 확인된 때에는 정당한 사유가 없는 한 5일 이내에 해당 정보주체에게 다음 각 호의 사항을 알려야 한다.

1. 유출된 개인정보의 항목
2. 유출된 시점과 그 경위
3. 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
4. 개인정보처리자의 대응조치 및 피해구제절차
5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

② 개인정보처리자는 제1항제2호의 경우 개인정보 유출 사고가 최초 발생한 시점과 알게 된 시점 사이에 시간적 차이가 있는 경우에는 이에 대한 과실유무를 입증하여야 한다.

③ 개인정보처리자는 제1항 각 호의 조치를 취한 이후에는 정보주체에게 다음 각 호의 사실만을 일차적으로 알리고, 추후 확인되는 즉시 알릴 수 있다.

1. 정보주체에게 유출이 발생한 사실
2. 제102조제1항의 통지항목 중 확인된 사항

제103조(통지방법) ① 개인정보처리자는 정보주체에게 제27조제1항 각호의 사항을 통지할 때에는 서면, 전자우편, 모사전송, 전화, 휴대전화 문자전송 또는 이와 유사한 방법을 통하여 지체 없이 정보주체에게 알려야 한다.

② 개인정보처리자는 제1항의 통지방법과 동시에, 홈페이지 등을 통하여 제102조제1항 각호의 사항을 공개할 수 있다.

제104조(개인정보 유출신고) ① 개인정보처리자는 1만명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 정보주체에 대한 통지 및 조치결과를 5일 이내에 행정안전부장관 또는 시행령 제39조제2항 각호의 전문기관 중 어느 하나에 신고하여야 한다.

② 제1항에 따른 신고는 [별지 제1호 서식]에 따른 개인정보 유출신고서를 통하여 하여야 한다.

③ 개인정보처리자는 전자우편, 팩스 또는 인터넷 사이트를 통하여 유출신고를 할 시간적 여유가 없거나 그밖에 특별한 사정이 있는 때에는 먼저 전화를 통하여 제27조제1항의 사항을 신고한 후, [별지 제1호 서식]에 따른 개인정보 유출신고서를 제출할 수 있다.

④ 개인정보처리자는 1만명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 제102조제1항에 따른 통지와 함께 인터넷 홈페이지에 정보주체가 알아보기 쉽도록 제102조제1항 각호의 사항을 7일 이상 게재하여야 한다.

제5절 정보주체의 권리 보장

제105조(개인정보 열람 연기 사유의 소멸) 개인정보처리자가 법 제35조제3항 후문에 따라 개인정보의

열람을 연기한 후 그 사유가 소멸한 경우에는 정당한 사유가 없는 한 사유가 소멸한 날로부터 10일 이내에 열람하도록 하여야 한다.

② 정보주체로부터 시행령 제41조제1항제4호의 규정에 따른 개인정보의 제3자 제공현황의 열람청구를 받은 개인정보처리자는, 국가안보에 긴요한 사안으로 법 제35조제4항제3호마목의 규정에 따른 업무를 수행하는데 중대한 지장을 초래하는 경우, 제3자에게 열람청구의 허용 또는 제한, 거부와 관련한 의견을 조회하여 결정할 수 있다.

제106조(개인정보의 정정·삭제) ① 개인정보처리자가 법 제36조제1항에 따른 개인정보의 정정·삭제 요구를 받았을 때에는 정당한 사유가 없는 한 요구를 받은 날로부터 10일 이내에 그 개인정보를 조사하여 정보주체의 요구에 따라 정정·삭제 등 필요한 조치를 한 후 그 결과를 정보주체에게 알려야 한다.

② 정보주체의 정정·삭제 요구가 법 제36조제1항 단서에 해당하는 경우에는 정당한 사유가 없는 한 요구를 받은 날로부터 10일 이내에 삭제를 요구할 수 없는 근거법령의 내용을 정보주체에게 알려야 한다.

제107조(개인정보의 처리정지) ① 개인정보처리자가 정보주체로부터 법 제37조제1항에 따라 개인정보처리를 정지하도록 요구받은 때에는 법 제37조제2항단서에 해당하지 않고 다른 정당한 사유가 없는 한 요구를 받은 날로부터 10일 이내에 개인정보의 처리의 일부 또는 전부를 정지하여야 한다.

② 개인정보처리자는 정보주체의 요구에 따라 처리가 정지된 개인정보에 대하여는 정당한 사유가 없는 한 처리정지의 요구를 받은 날로부터 10일 이내에 해당 개인정보의 파기 등 정보주체의 요구에 상응하는 조치를 취하고 그 결과를 정보주체에게 알려야 한다.

제108조(권리행사의 방법 및 절차) 개인정보처리자는 개인정보를 수집하는 방법과 동일하거나 보다 쉽게 정보주체가 열람요구 등 권리를 행사할 수 있도록 간편한 방법을 제공하여야 하며, 개인정보의 수집시에 요구되지 않았던 증빙서류 등을 요구하거나 추가적인 절차를 요구할 수 없다. 이는 시행령 제46조에 따라 본인 또는 정당한 대리인임을 확인하고자 하는 경우와 수수료와 우송료의 정산에도 마찬가지로 적용된다.

제6절 개인정보 처리방침 작성

제109조(개인정보 처리방침의 공개) ① 개인정보처리자가 법 제30조제2항에 따라 개인정보 처리방침을 수립하거나 변경하는 경우에는 인터넷 홈페이지를 통해 지속적으로 개제하여야 하며 이 경우 “개인정보 처리방침”이라는 명칭을 사용하되, 글자 크기, 색상 등을 활용하여 다른 고지사항과 구분함으로써 정보주체가 쉽게 확인할 수 있도록 하여야 한다.

② 개인정보처리자가 인터넷 홈페이지를 운영하지 않는 경우 또는 인터넷 홈페이지 관리상의 하자가 있는 경우에는 시행령 제31조제3항 각 호의 어느 하나 이상의 방법으로 개인정보 처리방침을 공개하여야 한다. 이 경우에도 “개인정보 처리방침”이라는 명칭을 사용하되, 글자 크기, 색상 등을 활용하여 다른 고지사항과 구분함으로써 정보주체가 쉽게 확인할 수 있도록 하여야 한다.

③ 개인정보처리자가 시행령 제31조제3항제3호의 방법으로 개인정보 처리방침을 공개하는 경우에는 간행물·소식지·홍보지·청구서 등이 발행될 때마다 계속하여 게재하여야 한다.

④ 친목단체는 법 제58조제3항에 따라 개인정보 처리방침을 수립·공개하지 아니할 수 있다.

제110조(개인정보 처리방침의 변경) 개인정보처리자가 개인정보 처리방침을 변경하는 경우에는 변경 및 시행의 시기, 변경된 내용을 지속적으로 공개하여야 하며, 변경된 내용은 정보주체가 쉽게 확인할 수 있도록 변경 전·후를 비교하여 공개하여야 한다.

제111조(개인정보 처리방침의 작성기준 등) ① 개인정보처리자가 개인정보 처리방침을 작성하는 때에는 법 제30조제1항제1호부터 제5호 및 시행령 제31조제1항 각 호의 사항을 명시적으로 구분하되, 알기 쉬운 용어로 구체적이고 명확하게 표현하여야 한다.

② 개인정보처리자는 개인정보의 처리 목적에 필요한 최소한의 개인정보라는 점을 밝혀야 한다.

③ 개인정보처리자가 목적에 필요한 최소한의 개인정보 이외에 개인별 맞춤서비스 등을 위하여 처리하는 개인정보의 항목이 있는 경우에는 양자를 구별하여 표시하여야 한다.

제112조(필수적 기재사항) 개인정보처리자가 개인정보처리방침을 작성할 때에는 법 제30조제1항에 따라 다음 각 호의 사항을 모두 포함하여야 한다.

1. 개인정보의 처리 목적
2. 개인정보의 처리 및 보유 기간
3. 개인정보의 제3자 제공에 관한 사항(해당되는 경우에만 정한다)
4. 개인정보처리의 위탁에 관한 사항(해당되는 경우에만 정한다)
5. 정보주체의 권리·의무 및 그 행사방법에 관한 사항
6. 처리하는 개인정보의 항목
7. 개인정보의 파기에 관한 사항
8. 개인정보 보호책임자에 관한 사항
9. 개인정보 처리방침의 변경에 관한 사항
10. 시행령 제30조제1항에 따른 개인정보의 안전성 확보조치에 관한 사항

제113조(임의적 기재사항) 개인정보처리자는 제112조의 필수적 기재사항 이외에도 다음 각 호의 사항을 개인정보 처리방침에 포함할 수 있다.

1. 정보주체의 권익침해에 대한 구제방법
2. 개인정보의 열람청구를 접수·처리하는 부서

제9장 영상정보처리기기 설치·운영

제1절 영상정보처리기기의 설치

제114조(적용범위) 이 장은 영상정보처리기기 운영자가 공개된 장소에 설치·운영하는 영상정보처리기기와 이 기기를 통하여 처리되는 개인영상정보를 대상으로 한다.

제115조(영상정보처리기기 운영·관리 방침) ① 영상정보처리기기 운영·관리 방침을 수립하거나 변경하는 경우에는 정보주체가 쉽게 확인할 수 있도록 공개하여야 한다.

② 영상정보처리기기 운영·관리 방침을 마련한 경우에는 법 제30조에 따른 개인정보 처리방침을 정하지 아니하거나, 영상정보처리기기 설치·운영에 관한 사항을 법 제30조에 따른 개인정보 처리방침에 포함하여 정할 수 있다.

제116조(관리책임자의 지정) ①영상정보처리기기운영자는 개인영상정보의 처리에 관한 업무를 총괄해서 책임질 개인영상정보 보호책임자를 지정하여야 한다.

② 제1항의 관리책임자는 법 제31조 제2항에 따른 개인정보 보호책임자의 업무에 준하여 다음 각 호의 업무를 수행한다.

1. 개인영상정보 보호 계획의 수립 및 시행
2. 개인영상정보 처리 실태 및 관행의 정기적인 조사 및 개선
3. 개인영상정보 처리와 관련한 불만의 처리 및 피해구제
4. 개인영상정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
5. 개인영상정보 보호 교육 계획 수립 및 시행
6. 개인영상정보 파일의 보호 및 파기에 대한 관리·감독
7. 그 밖에 개인영상정보의 보호를 위하여 필요한 업무

③ 법 제31조에 따른 개인정보 보호책임자가 지정되어 있는 경우에는 그 개인정보 보호책임자가 개인영상정보 보호책임자의 업무를 수행할 수 있다.

제117조(사전의견 수렴) 영상정보처리기기의 설치 목적 변경에 따른 추가 설치 등의 경우에도 시행령

제23조제1항에 따라 관계 전문가 및 이해관계인의 의견을 수렴하여야 한다.

제118조(안내판의 설치) ①영상정보처리기기 운영자는 정보주체가 영상정보처리기기가 설치·운영 중임을 쉽게 알아볼 수 있도록 법 제25조제4항 본문에 따라 다음 각 호의 사항을 기재한 안내판 설치 등 필요한 조치를 하여야 한다.

1. 설치목적 및 장소
2. 촬영범위 및 시간
3. 관리책임자의 성명 또는 직책 및 연락처
4. 영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우, 수탁자의 명칭 및 연락처

② 제1항에 따른 안내판은 촬영범위 내에서 정보주체가 알아보기 쉬운 장소에 누구라도 용이하게 판독할 수 있게 설치되어야 하며, 이 범위 내에서 영상정보처리기기 운영자가 안내판의 크기, 설치위치 등을 자율적으로 정할 수 있다.

③ 공공기관의 장이 기관 내 또는 기관 간에 영상정보처리기기의 효율적 관리 및 정보 연계 등을 위해 용도별·지역별 영상정보처리기기를 물리적·관리적으로 통합하여 설치·운영(이하 '통합관리'라 한다)하는 경우에는 설치목적 등 통합관리에 관한 내용을 정보주체가 쉽게 알아볼 수 있도록 제118조제1항에 따른 안내판에 기재하여야 한다.

제2절 개인영상정보의 처리

제119조(개인영상정보 이용·제3자 제공 등 제한 등) ① 영상정보처리기기운영자는 다음 각 호의 경우를 제외하고는 개인영상정보를 수집 목적 이외로 이용하거나 제3자에게 제공하여서는 아니된다. 다만 제5호부터 제9호까지의 경우는 공공기관의 경우로 한정한다.

1. 정보주체에게 동의를 얻은 경우
2. 다른 법률에 특별한 규정이 있는 경우
3. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
4. 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인영상정보를 제공하는 경우
5. 개인영상정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우
6. 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우
7. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우
8. 법원의 재판업무 수행을 위하여 필요한 경우
9. 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우

제120조(보관 및 파기) ① 영상정보처리기기 운영자는 수집한 개인영상정보를 영상정보처리기기 운영·관리 방침에 명시한 보관 기간이 만료한 때에는 지체없이 파기하여야 한다. 다만, 다른 법령에 특별한 규정이 있는 경우에는 그러하지 아니하다.

② 영상정보처리기기 운영자가 그 사정에 따라 보유 목적의 달성을 위한 최소한의 기간을 산정하기 곤란한 때에는 보관 기간을 개인영상정보 수집 후 30일 이내로 한다.

③ 개인영상정보의 파기 방법은 다음 각 호의 어느 하나와 같다.

1. 개인영상정보가 기록된 출력물(사진 등) 등은 파쇄 또는 소각
2. 전자기적(電磁氣的) 파일 형태의 개인영상정보는 복원이 불가능한 기술적 방법으로 영구 삭제

제121조(이용·제3자 제공·파기의 기록 및 관리) ① 영상정보처리기기 운영자는 개인영상정보를 수집 목

적 이외로 이용하거나 제3자에게 제공하는 경우에는 다음 각 호의 사항을 기록하고 이를 관리하여야 한다.

1. 개인영상정보 파일의 명칭
2. 이용하거나 제공받은 자(공공기관 또는 개인)의 명칭
3. 이용 또는 제공의 목적
4. 법령상 이용 또는 제공근거가 있는 경우 그 근거
5. 이용 또는 제공의 기간이 정하여져 있는 경우에는 그 기간
6. 이용 또는 제공의 형태

② 영상정보처리기기 운영자가 개인영상정보를 파기하는 경우에는 다음 사항을 기록하고 관리하여야 한다.

1. 파기하는 개인영상정보 파일의 명칭
2. 개인영상정보 파기일시 (사전에 파기 시기 등을 정한 자동 삭제의 경우에는 파기 주기 및 자동 삭제 여부에 대한 확인 시기)
3. 개인영상정보 파기 담당자

제122조(영상정보처리기기 설치 및 관리 등의 위탁) ① 영상정보처리기기운영자가 시행령 제26조제1항에 따라 영상정보처리기기의 설치·운영에 관한 사무를 제3자에게 위탁하는 경우에는 그 내용을 정보주체가 언제든지 쉽게 확인할 수 있도록 시행령 제24조에 따른 안내판 및 시행령 제27조에 따른 영상정보처리기기 운영·관리 방침에 수탁자의 명칭 등을 공개하여야 한다.

② 영상정보처리기기운영자가 시행령 제26조제1항에 따라 영상정보처리기기의 설치·운영에 관한 사무를 제3자에게 위탁할 경우에는 그 사무를 위탁받은 자가 개인영상정보를 안전하게 처리하고 있는지를 관리·감독하여야 한다.

제3절 개인영상정보의 열람등 요구

제123조(정보주체의 열람등 요구) ① 정보주체는 영상정보처리기기 운영자가 처리하는 개인영상정보에 대하여 열람 또는 존재확인(이하 “열람등”이라 한다)을 해당 영상정보처리기기 운영자에게 요구할 수 있다. 이 경우 정보주체가 열람등을 요구할 수 있는 개인영상정보는 정보주체 자신이 촬영된 개인영상정보 및 명백히 정보주체의 급박한 생명, 신체, 재산의 이익을 위하여 필요한 개인영상정보에 한한다.

② 영상정보처리기기 운영자가 공공기관인 경우에는 해당 기관의 장에게 [별지 제25호 서식] 에 따른 개인영상정보 열람·존재확인 청구서(전자문서를 포함한다)로 하여야 한다.

③ 영상정보처리기기운영자는 제1항에 따른 요구를 받았을 때에는 지체없이 필요한 조치를 취하여야 한다. 이때에 영상정보처리기기운영자는 열람등 요구를 한 자가 본인이거나 정당한 대리인인지를 주민등록증·운전면허증·여권 등의 신분증명서를 제출받아 확인하여야 한다.

④ 제3항의 규정에도 불구하고 다음 각 호에 해당하는 경우에는 영상정보처리기기운영자는 정보주체의 개인영상정보 열람등 요구를 거부할 수 있다. 이 경우 영상정보처리기기 운영자는 10일 이내에 서면 등으로 거부 사유를 정보주체에게 통지하여야 한다.

1. 범죄수사·공소유지·재판수행에 중대한 지장을 초래하는 경우(공공기관에 한함)
2. 개인영상정보의 보관기간이 경과하여 파기한 경우
3. 기타 정보주체의 열람 등 요구를 거부할 만한 정당한 사유가 존재하는 경우

⑤ 영상정보처리기기 운영자는 제3항 및 제4항에 따른 조치를 취하는 경우 다음 각 호의 사항을 기록하고 관리하여야 한다.

1. 개인영상정보 열람 등을 요구한 정보주체의 성명 및 연락처
2. 정보주체가 열람 등을 요구한 개인영상정보 파일의 명칭 및 내용
3. 개인영상정보 열람 등의 목적

4. 개인영상정보 열람 등을 거부한 경우 그 거부의 구체적 사유
5. 정보주체에게 개인영상정보 사본을 제공한 경우 해당 영상정보의 내용과 제공한 사유

⑥ 정보주체는 영상정보처리기기 운영자에게 정보주체 자신의 개인영상정보에 대한 파기를 요구하는 때에는 제1항에 의하여 보존을 요구하였던 개인영상정보에 대하여만 그 파기를 요구할 수 있다. 영상정보처리기기 운영자가 해당 파기조치를 취한 경우에는 그 내용을 기록하고 관리하여야 한다.

제124조(개인영상정보 관리대장) 제121조제1항 및 제2항, 제123조제5항 및 제6항에 따른 기록 및 관리는 [별지 제26호 서식]에 따른 '개인영상정보 관리대장'을 활용할 수 있다.

제125조(정보주체 이외의 자의 개인영상정보 보호) 영상정보처리기기운영자는 제123조제2항에 따른 열람등 조치를 취하는 경우, 만일 정보주체 이외의 자를 명백히 알아볼 수 있거나 정보주체 이외의 자의 사생활 침해의 우려가 있는 경우에는 해당되는 정보주체 이외의 자의 개인영상정보를 알아볼 수 없도록 보호조치를 취하여야 한다.

제4절 개인영상정보 보호 조치

제126조(개인영상정보의 안전성 확보를 위한 조치) 영상정보처리기기 운영자는 개인영상정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 법 제29조 및 시행령 제30조제1항에 따라 안전성 확보를 위하여 다음 각 호의 조치를 하여야 한다.

1. 개인영상정보의 안전한 처리를 위한 내부 관리계획의 수립·시행, 다만 「개인정보의 안전성 확보 조치 기준 고시」
2. 개인영상정보에 대한 접근 통제 및 접근 권한의 제한 조치
3. 개인영상정보를 안전하게 저장·전송할 수 있는 기술의 적용 (네트워크 카메라의 경우 안전한 전송을 위한 암호화 조치, 개인영상정보파일 저장시 비밀번호 설정 등)
4. 처리기록의 보관 및 위조·변조 방지를 위한 조치 (개인영상정보의 생성 일시 및 열람할 경우에 열람 목적·열람자·열람 일시 등 기록·관리 조치 등)
5. 개인영상정보의 안전한 물리적 보관을 위한 보관시설 마련 또는 잠금장치 설치

제127조(개인영상정보처리기기의 설치·운영에 대한 점검) ① 학교의 장이 영상정보처리기기를 설치·운영하는 경우에는 이 지침의 준수 여부에 대한 자체점검을 실시하여 한다. 이 경우 다음 각 호의 사항을 고려하여야 한다.

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

② 학교의 장은 제1항과 3항에 따른 영상정보처리기기 설치·운영에 대한 자체점검을 완료한 후에는 그 결과를 홈페이지 등에 공개하여야 한다.

제10장 공공기관 개인정보파일 등록·공개

제1절 총칙

제128조(적용대상) 이 장의 적용대상은 예원예술대학교 및 그에 속한 전 기관을 적용대상으로 한다.

제129조(적용제외) 이 장은 다음 각 호의 어느 하나에 해당하는 개인정보파일에 관하여는 적용하지 아

니한다.

1. 법 제32조제2항에 따라 적용이 제외되는 다음 각목의 개인정보파일
   가. 예원예술대학교의 내부적 업무처리만을 위하여 사용되는 개인정보파일
   나. 다른 법령에 따라 비밀로 분류된 개인정보파일
2. 법 제58조제1항에 따라 적용이 제외되는 다음 각목의 개인정보파일
   가. 공공기관이 처리하는 개인정보 중 「통계법」에 따라 수집되는 개인정보파일
   나. 국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보파일
   다. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우로서 일시적으로 처리되는 개인정보파일
3. CCTV 등 영상정보처리기기를 통하여 처리되는 개인영상정보파일
4. 자료·물품 또는 금전의 송부, 1회성 행사 수행 등의 목적만을 위하여 운용하는 경우로서 저장하거나 기록하지 않고 폐기할 목적으로 수집된 개인정보파일

제2절 개인정보파일의 등록주체와 절차

제130조(개인정보파일 등록 주체) ① 개인정보파일을 운용하는 본교의 개인정보 보호책임자는 그 현황을 행정안전부에 등록하여야 한다.

② 예원예술대학교는 교육과학기술부를 통하여 행정안전부에 등록하여야 한다.

제131조(개인정보파일 등록 및 변경 신청) ① 개인정보파일을 운용하는 본교의 개인정보취급자는 해당 공공기관의 개인정보 보호책임자에게 개인정보파일 등록을 신청하여야 한다.

② 개인정보파일 등록 신청 사항은 다음의 각호와 같다.

1. 개인정보파일을 운용하는 공공기관의 명칭
2. 개인정보파일의 명칭
3. 개인정보파일의 운영 근거 및 목적
4. 개인정보파일에 기록되는 개인정보의 항목
5. 개인정보파일로 보유하고 있는 개인정보의 정보주체 수
6. 개인정보의 처리방법
7. 개인정보의 보유기간
8. 개인정보를 통상적 또는 반복적으로 제공하는 경우에는 그 제공받는 자
9. 본교에서 개인정보 처리 관련 업무를 담당하는 부서
10. 개인정보의 열람 요구를 접수·처리하는 부서
11. 개인정보파일의 개인정보 중 법 제35조제4항에 따라 열람을 제한하거나 거절할 수 있는 개인정보의 범위 및 제한 또는 거절 사유
12. 법 제33조제1항에 따른 개인정보 영향평가를 받은 개인정보파일의 경우에는 그 영향평가의 결과

제132조(개인정보파일 등록 및 변경 확인) ① 개인정보파일 등록 또는 변경 신청을 받은 개인정보 보호책임자는 등록·변경 사항을 검토하고 그 적정성을 판단한 후 행정안전부에 등록하여야 한다.

② 본교의 개인정보 보호책임자는 교육과학기술부에 제1항에 따른 등록·변경 사항의 검토 및 적정성 판단을 요청한 후, 교육과학기술부의 확인을 받아 행정안전부에 등록하여야 한다.

③ 제1항부터 제3항의 등록은 60일 이내에 하여야 한다.

제133조(개인정보파일 표준목록 등록과 관리) ① 본교와 같이 전국적으로 단일한 공통업무를 집행하고 있는 교육기관은 각 중앙행정기관에서 제공하는 '개인정보파일 표준목록'에 따라 등록해야 한다.

② 전국 단일의 공통업무와 관련된 개인정보파일 표준목록은 해당 중앙부처에서 등록·관리해야 한다.

제134조(개인정보파일의 파기) ① 개인정보 보호책임자는 개인정보파일의 보유기간 경과, 처리목적 달성 등 개인정보파일이 불필요하게 되었을 때에는 지체 없이 그 개인정보파일을 파기하여야 한다. 다

만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다.

② 개인정보 보호책임자는 개인정보파일의 보유기간, 처리목적 등을 반영한 개인정보 파기계획을 수립·시행하여야 한다.

③ 개인정보취급자는 보유기간 경과, 처리목적 달성 등 파기 사유가 발생한 개인정보파일을 선정하고, [별지 제27호 서식]에 따른 개인정보파일 파기요청서에 파기 대상 개인정보파일의 명칭, 파기방법 등을 기재하여 개인정보 보호책임자의 승인을 받아 개인정보를 파기하여야 한다.

④ 개인정보 보호책임자는 개인정보 파기 시행 후 파기 결과를 확인하고 [별지 제28호 서식]에 따른 개인정보파일 파기 관리대장을 작성하여야 한다.

제135조(개인정보파일 등록 사실의 삭제) ① 개인정보취급자는 제134조에 따라 개인정보파일을 파기한 경우, 법 제32조에 따른 개인정보파일의 등록사실에 대한 삭제를 개인정보 보호책임자에게 요청해야 한다.

② 개인정보파일 등록의 삭제를 요청받은 개인정보 보호책임자는 그 사실을 확인하고, 지체없이 등록사실을 삭제한 후 그 사실을 행정안전부에 통보한다.

제136조(등록·파기에 대한 개선권고) ① 본교의 개인정보 보호책임자는 제131조제1항에 따라 검토한 개인정보파일이 과다하게 운용되고 있다고 판단되는 경우에는 개선을 권고할 수 있다.

② 본교의 개인정보 보호책임자는 제131조제2항 및 제3항에 따라 검토한 개인정보파일이 과다하게 운용된다고 판단되거나, 등록되지 않은 파일이 있는 것으로 확인되는 경우에는 개선을 권고할 수 있다.

③ 학교의 장은 개인정보파일의 등록사항과 그 내용을 검토하고 다음 각 호의 어느 하나에 해당되는 경우에는 법 제32조제3항에 따라 해당 공공기관의 개인정보 보호책임자에게 개선을 권고할 수 있다.

1. 개인정보파일이 과다하게 운용된다고 판단되는 경우
2. 등록하지 않은 개인정보파일이 있는 경우
3. 개인정보파일 등록 사실이 삭제되었음에도 불구하고 개인정보파일을 계속 보유하고 있는 경우
4. 개인정보 영향평가를 받은 개인정보파일을 보유하고 있음에도 그 결과를 등록사항에 포함시키지 않은 경우
5. 기타 법 제32조에 따른 개인정보파일의 등록 및 공개에 위반되는 사항이 있다고 판단되는 경우

④ 학교의 장은 제3항에 따라 개선을 권고한 경우에는 그 내용 및 결과에 대하여 개인정보 보호위원회의 심의·의결을 거쳐 공표할 수 있다.

⑤ 행정안전부 장관은 공공기관의 개인정보파일 등록·파기 현황에 대한 점검을 실시할 수 있다.

제3절 개인정보파일의 관리 및 공개

제137조(개인정보파일대장 작성) 본교는 1개의 개인정보파일에 1개의 개인정보파일대장을 작성해야 한다.

제138조(개인정보파일 이용·제공 관리) 본교는 법 제18조제2항 각 호에 따라 제3자가 개인정보파일의 이용·제공을 요청한 경우에는 각각의 이용·제공 가능 여부를 확인하고 [별지 제29호 서식]의 '개인정보 목적외 이용·제공대장'에 기록하여 관리해야 한다.

제139조(개인정보파일 보유기간의 산정) ① 보유기간은 전체 개인정보가 아닌 개별 개인정보의 수집부터 삭제까지의 생애주기로서 보유목적에 부합된 최소기간으로 산정하되, 개별 법령의 규정에 명시된 자료의 보존기간에 따라 산정해야 한다.

② 개별 법령에 구체적인 보유기간이 명시되어 있지 않은 경우에는 개인정보 보호책임자의 협의를 거쳐 기관장의 결재를 통하여 산정해야 한다. 다만, 보유기간은 [별표 제3호]의 개인정보파일 보유기간 책정 기준표에서 제시한 기준과「공공기록물 관리에 관한 법률 시행령」에 따른 기록관리기준표를 상회할 수 없다.

③ 정책고객, 홈페이지회원 등의 홍보 및 대국민서비스 목적의 외부고객 명부는 특별한 경우를 제외하고는 2년을 주기로 정보주체의 재동의 절차를 거쳐 동의한 경우에만 계속적으로 보유할 수 있다.

제140조(개인정보파일 현황 공개 및 방법) ① 본교의 개인정보 보호책임자는 개인정보파일의 보유·파기 현황을 주기적으로 조사하여 그 결과를 본교의 개인정보 처리방침에 포함하여 관리해야 한다.
② 학교의 장은 개인정보파일 등록 현황을 누구든지 쉽게 열람할 수 있도록 공개하여야 한다.

부 칙(2000. 3. 2)
1. (시행일) 이 규정은 2000년 3월 2일부터 시행한다.

부 칙(2003. 1. 1)
1. (시행일) 이 규정은 2001년 1월 1일부터 시행한다.

부 칙(2003. 10. 6)
1. (시행일) 이 규정은 2003년 10월 6일부터 시행한다.

부 칙(2007. 3. 15)
1. (시행일) 이 규정은 2007년 3월 15일부터 시행한다.

부 칙(2007. 9. 1)
1. (시행일) 이 규정은 2007년 9월 1일부터 시행한다.

부 칙(2009. 2. 1)
1. (시행일) 이 규정은 2009년 2월 1일부터 시행한다.

부 칙(2009. 12. 1)
1. (시행일) 이 규정은 2009년 12월 1일부터 시행한다.

부 칙(2012. 12. 21)
1. (시행일) 이 규정은 2013년 1월 1일부터 시행한다.

부 칙(2019. 1. 23)
1. (시행일) 이 규정은 2019년 2월 1일부터 시행한다.

[별지 제1호 서식] 신원대장]

신 원 대 장

연번	직급	직위	성명	신원조사				임용 또는 전입일자	비 고
				목 적	의뢰 일자	회보 일자	내 용		

[별지 제2호 서식] 비밀인계인수서]

비 밀 인 계 인 수 서

급 비밀 건

급 비밀 건

계 건

위와 같이 정히 인계 인수 함

20 년 월 일

인 계 자 직 성명 ㊞

인 계 자 직 성명 ㊞

확 인 자 직 성명 ㊞

[별지 제3호 서식] 비밀관리기록부]

비밀관리기록부

부처명 : 보관책임자 :

관리 번호	수량			문서 번호	비밀 등급	형태	건명	사본 번호	예고문	처리 담당	보관 장소	재분류				참조
	연월일	발행처	수신처									등급 변경	파기	파기 확인	근거	영수증

[별지 제4호 서식] 비밀문서발간복제복사업무일지]

비밀문서 발간, 복제, 복사 업무일지

연월일	건 명	비밀등급	수 량	발간, 복제, 복사 인명		비 고
				구 분	성 명	

[별지 제5호 서식] 비밀열람기록전]

비밀열람기록전

( )급 비밀

연월일	소속 및 직책	성 명	인가등급	주민등록번호	열람목적	확인

[별지 제6호 서식] 비밀지출승인신청서]

비 밀 지 출 승 인 신 청 서

1. 지 출 자 : 직책 성명 주민등록번호
2. 지출비밀 관리번호 : 비밀등급 건명
3. 지출목적 :
4. 지출기간 : 20 년 월 일 시부터 20 년 월 일 시까지
5. 지출장소 :
6. 보안대책 :

위와 같이 승인하여 주시기 바랍니다.

20 년 월 일

신청자 ㊞

지 출 자
보안책임자

위와 같이 승인함

20 년 월 일

보안담당책임자 ㊞

[별지 제7호 서식] 비밀취급인가자명부]

비밀취급인가자명부

인가증번호	직책 및 직명	직 책 (비밀취급업무)	성 명	주민등록번호	인 가 해 제				비고
					등 급	연월일	사 유	연월일	

[별지 제8호 서식] 비밀취급인가증교부대장]

비밀취급인가증 교부대장

인가증번호	교부연월일	교 부 자 인 적 사 항				회수사항	결 재			비고
		소속	직위 및 직 급	성 명	주 민 등 록 번 호		담당자	행정지원 팀장	보 안 책임자	

[별지 제9호 서식] 전산장비 관리대장]

전산장비 관리대장

연 번	소 속	취급자(성명)	단말기·PC 및 서버		비 밀 번 호				부여 일자	해제 일자
			관리 번호	기 종 · 성 능	장비별	파일별	망접속시 취급자			
							사용자 계 정	비밀 번호		

[별지 제10호 서식] 서약서]

서 약 서

본인은 년 월 일부로 국가용 보안시스템과 관련한 업무(연구개발, 제작, 입찰, 기타)를 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 나는 국가용 보안시스템과 관련된 소관업무가 국가기밀 사항임을 인정하고 제반 보안관계규정 및 지침을 성실히 수행한다.

2. 나는 이 기밀을 누설함이 국가이익을 침해할 수도 있음을 인식하고 재직중은 물론 퇴직 후에도 알게 된 모든 기밀사항을 일체 타인에게 누설하지 아니한다.

3. 나는 기밀을 누설한 때에는 아래의 관계법규에 따라 엄중한 처벌을 받을 것을 서약한다.
   가. 국가보안법 제4조 제1항제2호·제5호(국가기밀 누설 등)
   나. 형법 제99조(일반이적) 및 제127조(공무상 비밀의 누설)
   다. 군형법 제80조(군사기밀 누설)
   라. 군사기밀보호법 제9조(누설) 및 제13조(업무상 누설)

년 월 일

서약자 소속 직급 주민등록번호
직위 성 명 인

서 약 소속 직급 주민등록번호
집행자 직위 성 명 인

[별지 제11호 서식] 보안적합성 검증 신청서]

보안적합성 검증 신청서

<table>
<tr><td rowspan="4">신청기관</td><td>기 관 명</td><td colspan="2"></td><td>담당부서</td><td></td></tr>
<tr><td>도입목적</td><td colspan="4"></td></tr>
<tr><td>운용환경</td><td colspan="2">□유선망 □무선망 □유·무선통합망</td><td>운용기관</td><td></td></tr>
<tr><td>주요
보안기능
요구사항</td><td colspan="4"></td></tr>
<tr><td rowspan="5">대상
시스템</td><td>개발사
(판매사)</td><td colspan="2">* 개발사와 판매사가 사이한 경우
판권소유자 기재</td><td>대 표 자</td><td></td></tr>
<tr><td>주 소</td><td></td><td>전화번호</td><td colspan="2"></td></tr>
<tr><td>시스템명</td><td></td><td>평가등급</td><td colspan="2"></td></tr>
<tr><td>평가기관</td><td></td><td>인증기관</td><td colspan="2"></td></tr>
<tr><td>담당자</td><td></td><td>E-mail</td><td colspan="2"></td></tr>
<tr><td>비 고</td><td colspan="5"></td></tr>
</table>

* 복수의 시스템을 신청하는 경우, 별도 출력하여 대상 시스템란에만 기재

[별지 제12호 서식] 보조기억매체 관리대장(일반용)]

보조기억매체 관리대장(일반용)

<관리책임자 : >

연번	관리번호 (S/N)	매체 형태	등록일자	취급자	불용처리 일자	불용처리방법 (재사용 용도)	비고
1							
2							
3							
4							
5							

[별지 제13호 서식] 보조기억매체 관리대장(공인인증서용)]

보조기억매체 관리대장(공인인증서용)

<관리책임자 : >

연번	관리번호 (S/N)	형태	등록 일자	취급자	용도	해지일자	해지사유
1							
2							
3							
4							
5							

[별지 제14호 서식] 보조기억매체 점검대장]

보조기억매체 점검대장

<관리책임자 : >

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

[별지 제15호 서식] 보조기억매체(전산장비 포함) 반출·입 대장]

보조기억매체(전산장비 포함) 반출·입 대장

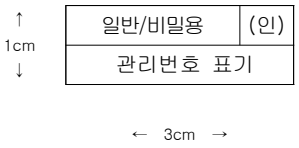
<관리책임자 : >

장비명	관리번호 (시리얼번호)	사용자	용도	전출입 일시 (입·출 구분)	확인

[별지 제16호 서식] 보조기억매체 라벨]

보조기억매체 라벨

<디스켓, 이동형 HDD 서식]>



<USB·CD 등 서식]>

가. 同 서식]을 만들어 보조기억매체 중앙의 적절한 위치에 부착

나. 첫 번째 줄에는 일반/비밀용은 정보보안담당관의 직인을 날인하고 공인인증서용은 관리책임자의 직인을 날인

다. 두 번째 줄에는 보조기억매체 관리번호 표기

라. 세 번째 줄의 '정'란에 관리책임자·'부'란에 취급자 표기
(USB메모리 및 CD의 경우 생략 가능)

마. 보조기억매체의 크기를 고려하여 서식]·글자 크기 조정 가능

[별지 제17호 서식] 예시]

일반용			(인)
총무과-일반-01			
정	이순신	부	홍길동

대외비용			(인)
총무과-대외비-01			
정	이순신	부	홍길동

공인인증서용			(인)
총무과-인증-01			
정	이순신	부	홍길동

일반용	(인)
총무과-일반-01	

Ⅱ급비밀용	(인)
총무과-Ⅱ급-01	

공인인증서용	(인)
총무과-인증-01	

[별지 제18호 서식] 보조기억매체 불용처리 확인서]

보조기억매체 불용처리 확인서

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

연번	관리번호 (S/N)	매체형태	사유	불용처리	재사용
1					
2					
3					
4					
5					

확인일자 : 년 월 일

요 청 자 : 소속・직책 O급 성명 : (인)

확 인 자 : 정보보안담당관 O급 성명 : (인)

[별지 제19호] 정보시스템 저장매체·자료별 삭제방법]

정보시스템 저장매체·자료별 삭제방법

저장매체 \ 저장자료	공개자료	민감자료 (개인정보 등)	비밀자료 (대외비 포함)
플로피디스크	㉮	㉮	㉮
광디스크 (CD·DVD 등)	㉮	㉮	㉮
자기 테이프	㉮·㉯중 택일	㉮·㉯중 택일	㉮
반도체메모리 (EEPROM 등)	㉮·㉰중 택일	㉮·㉰중 택일	㉮·㉰중 택일
	완전포맷이 되지 않는 저장매체는 ㉮ 방법 사용		
하드디스크	㉱	㉮·㉯·㉰중 택일	㉮·㉯중 택일

㉮ : 완전파괴(소각·파쇄·용해) - 비밀이 저장된 플로피디스켓·광디스크 파쇄시에는 파쇄조각의 크기가 0.25mm 이하가 되도록 조치

㉯ : 전용 消磁장비 이용 저장자료 삭제 - 소자장비는 반드시 저장매체의 磁氣力보다 큰 磁氣力 보유

㉰ : 완전포맷 3회 수행 - 저장매체 전체를 '난수'·'0'·'1'로 각각 중복 저장하는 방식으로 삭제

㉱ : 완전포맷 1회 수행 - 저장매체 전체를 '난수'로 중복 저장하는 방식으로 삭제

[별지 제20호 서식] 정보보호시스템 자체 점검결과]

정보보호시스템 자체 점검결과

항목명	점검 항목	결과
인증여부	EAL 2 이상 CC인증서 획득 여부	
	CC 未인증의 경우, 국가용 암호제품 또는 별도 지정제품 목록 등재여부	
	국가정보원장이 검증한 암호모듈 탑재 여부	
일치성	인증보고서 또는 운용정책문서와 도입제품 보안기능 일치성 여부	
	기술제안서(RFP)에서 요구하는 보안기능 구현 여부	
운용환경	도입기관의 시스템관리자 지정여부	
	감사기능 지원 여부	
	도입기관 주요업무 및 최대사용자 등에 대한 가용성 보장 여부	
유지보수	보안적합성 검증결과 반영 가능 여부	
	업체 기술지원 전담조직 운영 여부	
	작동중단 등 긴급상황에 대비한 지원절차 구비 여부	
	업체 유지보수 매뉴얼 제공 여부	
	한글 관리자 설치·운영 매뉴얼 제공 여부	
	업체의 제품운용교육 제공 여부	
	신규취약성에 대한 통보 및 처리절차 구비 여부	

※ 점검결과는 O, X로 표기

[[별지 제21호 서식] 보안적합성 검증 신청서]

보안적합성 검증 신청서

<table>
<tr><td rowspan="8">신청
기관</td><td>기관명</td><td colspan="2"></td><td>운용부서</td><td colspan="2"></td></tr>
<tr><td>도입
목적</td><td colspan="5"></td></tr>
<tr><td rowspan="2">운용환경</td><td>사용자 수</td><td></td><td>망 구성</td><td colspan="2">□유선 □무선</td></tr>
<tr><td>속도(대역폭)</td><td colspan="4"></td></tr>
<tr><td>운용형태</td><td colspan="5">□단독설치·운용 □타보안제품과연동 □대국민배포용</td></tr>
<tr><td>연동
시스템</td><td colspan="5">□ ERP □ KMS □ CRM □ 전자결재 □ 기타 그룹웨어</td></tr>
<tr><td>사업명</td><td colspan="5"></td></tr>
<tr><td rowspan="9">신청
제품</td><td>업체명</td><td colspan="2"></td><td>대표자</td><td colspan="2"></td></tr>
<tr><td>주소</td><td colspan="2"></td><td>전화번호</td><td colspan="2"></td></tr>
<tr><td rowspan="3">제품명</td><td colspan="2" rowspan="3">* 신청제품이 2種 이상인
경우, 추가기재</td><td>CC
인증번호</td><td colspan="2"></td></tr>
<tr><td>암호
검증번호</td><td colspan="2"></td></tr>
<tr><td>용역개발 여부</td><td colspan="2">□ 예 □ 아니오</td></tr>
<tr><td>평가기관</td><td></td><td>인증기관</td><td></td><td>등급</td><td></td></tr>
<tr><td rowspan="3">담당자</td><td>전화번호</td><td colspan="4"></td></tr>
<tr><td>휴대폰번호</td><td colspan="4"></td></tr>
<tr><td>E-mail</td><td colspan="4"></td></tr>
<tr><td>암호모듈</td><td colspan="5">□없음 □있음 (□검증 □미검증)</td></tr>
</table>

[[별지 제22호 서식] 보안관제센터 운영현황]

보안관제센터 운영현황

[앞면]

보안관제센터 개요				
개소		* 개소일자 기재	위치	
규모		* 상황실 면적 등	예산	* 구축예산 및 운영예산
조직 현황				
개요		* 조직구성, 인원 및 임무, 근무형태 등 기술		
1	부서(소속)		센터장	
	직 급		성 명	
	이메일		연락처	전화: HP:
2	부서(소속)		직급/직책	
	담당분야		성 명	
	이메일		연락처	전화: HP:
3	:	* 센터장과 탐지·분석·대응 등 담당분야별 대표자만 기입		
외부인력 현황				
업체명			대표이사	
인원수			근무형태	
계약기간			수행업무	
지침·매뉴얼 현황				
지침			기준	
매뉴얼			기타	
보안관제시스템 현황				
시스템명		* 주요기능 기술	시스템명	
시스템명			시스템명	
시스템명			시스템명	

보안관제센터 운영현황

[뒷면]

<table>
<tr><td colspan="7">보안장비 보유 현황</td></tr>
<tr><td colspan="2">F/W</td><td>* 제품명 및 사용대수 기입</td><td>IDS/IPS</td><td colspan="3"></td></tr>
<tr><td colspan="2">ESM</td><td></td><td>WEB F/W</td><td colspan="3"></td></tr>
<tr><td colspan="2">라우터</td><td></td><td>기타장비</td><td colspan="3">예) NMS 1대
*네트워크 구성도 사본제출</td></tr>
<tr><td colspan="7">보안관제 연동기관 현황</td></tr>
<tr><td colspan="7">* 대상기관 수, 기관명, 대상목표(인터넷 또는 내부망, 홈페이지 등) 기술</td></tr>
<tr><td colspan="7">연동기관 IP할당 현황</td></tr>
<tr><td rowspan="3">1</td><td>연동기관</td><td></td><td rowspan="3">IP
관리자</td><td>성 명</td><td colspan="2"></td></tr>
<tr><td>공인IP</td><td></td><td>연락처</td><td colspan="2">전화: HP:</td></tr>
<tr><td>사설IP</td><td></td><td>전자우편</td><td colspan="2"></td></tr>
<tr><td>2</td><td>:</td><td colspan="5">⋮</td></tr>
<tr><td>3</td><td>:</td><td colspan="5">⋮</td></tr>
<tr><td>4</td><td>:</td><td colspan="5">⋮</td></tr>
<tr><td>5</td><td>:</td><td colspan="5">⋮</td></tr>
<tr><td>6</td><td>:</td><td colspan="5">⋮</td></tr>
</table>

[별지 제23호 서식] 공격정보 이관]

공격정보 이관

탐 지 정 보							
탐지기관명	00 보안관제센터			탐 지 자			
탐지이벤트				탐지방법			
발생일시				이관일시			
연 락 처	전화 :			Fax :			
공 격 정 보							
공격 IP		공격 포트		피해 IP (국적·기관)		피해 포트	
경유 IP (국적·기관)				사고유형			
발생건수 (건/분)							
공격내용							

[별지 제24호 서식]

개인정보 유출신고서

기관명					
정보주체에의 통지 여부					
유출된 개인정보의 항목 및 규모					
유출된 시점과 그 경위					
유출피해 최소화 대책·조치 및 결과					
정보주체가 할 수 있는 피해 최소화 방법 및 구제절차					
담당부서·담당자 및 연락처		성명	부서	직위	연락처
	개인정보 보호책임자				
	개인정보 취급자				

유출신고접수기관	기관명	담당자명	연락처

[별지 제25호 서식]

<table>
<tr><td colspan="5">개인영상정보(□ 존재확인 □ 열람) 청구서
※ 아래 유의사항을 읽고 굵은 선 안쪽의 사항만 적어 주시기 바랍니다.</td><td>처리기한
10일 이내</td></tr>
<tr><td rowspan="3">청 구 인</td><td>성 명</td><td></td><td>전 화 번 호</td><td colspan="2"></td></tr>
<tr><td>생년월일</td><td></td><td>정보주체와의 관계</td><td colspan="2"></td></tr>
<tr><td>주 소</td><td colspan="4"></td></tr>
<tr><td rowspan="3">정보주체의
인적사항</td><td>성 명</td><td></td><td>전 화 번 호</td><td colspan="2"></td></tr>
<tr><td>생년월일</td><td colspan="4"></td></tr>
<tr><td>주 소</td><td colspan="4"></td></tr>
<tr><td rowspan="3">청구내용
(구체적으로 요청하지 않으면 처리가 곤란할 수 있음)</td><td>영상정보
기록기간</td><td colspan="4">(예 : 2011.01.01 18:30 ~ 2011.01.01 19:00)</td></tr>
<tr><td>영상정보
처리기기
설치장소</td><td colspan="4">(예 : 00시 00구 00대로 0 인근 CCTV)</td></tr>
<tr><td>청구 목적 및
사유</td><td colspan="4"></td></tr>
<tr><td colspan="6">「표준 개인정보 보호지침」제52조에 따라 위와 같이 개인영상정보의 존재확인, 열람을 청구합니다.

년 월 일

청구인 (서명 또는 인)

○○○○ 귀하</td></tr>
<tr><td colspan="2">담당자의 청구인에 대한 확인 서명</td><td colspan="4"></td></tr>
</table>

[별지 제26호 서식]

개인영상정보 관리대장

번호	구분	일시	파일명/ 형태	담당자	목적/ 사유	이용· 제공받는 제3자 /열람등 요구자	이용· 제공 근거	이용제 공 형태	기간
1	□ 이용 □ 제공 □ 열람 □ 파기								
2	□ 이용 □ 제공 □ 열람 □ 파기								
3	□ 이용 □ 제공 □ 열람 □ 파기								
4	□ 이용 □ 제공 □ 열람 □ 파기								
5	□ 이용 □ 제공 □ 열람 □ 파기								
6	□ 이용 □ 제공 □ 열람 □ 파기								
7	□ 이용 □ 제공 □ 열람 □ 파기								

[별지 제27호 서식]

개인정보파일 파기 요청서

작성일		작성자	
파기 대상 개인정보파일			
생성일자		개인정보취급자	
주요 대상업무		현재 보관건수	
파기 사유			
파기 일정			
특기사항			
파기 승인일		승인자 (개인정보 보호책임자)	
파기 장소			
파기 방법			
파기 수행자		입회자	
폐기 확인 방법			
백업 조치 유무			
매체 폐기 여부			

[별지 제28호 서식]

개인정보파일 파기 관리대장

번호	개인정보 파일명	자료의 종류	생성일	폐기일	폐기사유	처리담당자	처리부서장

[별지 제29호 서식]

개인정보 목적 외 이용·제공 대장

구분	주요내용
① 개인정보파일명	
② 이용·제공받는 기관	
③ 이용·제공일자	
④ 이용·제공주기	
⑤ 이용·제공형태	
⑥ 이용·제공목적	
⑦ 이용·제공근거	
⑧ 이용·제공항목	
⑨ 비고	

[별표 제1호 정보보안사고 유형]

정보보안사고 유형

조	구 분	세 부 내 용
1	전자정보 (전자문서 및 전자기록물)	(1) 비밀의 유출 (2) 주전산기(주요 서버 등)·대용량 전자기록(DB) 손괴 (3) 전자정보의 위조·변조·훼손 및 유출 (4) PC 등 단말기內 비밀의 평문 보관 및 유통
2	정보시스템 및 정보통신실	(1) 정보통신망에 대한 해킹·악성코드의 유포 (2) 비밀이 저장된 PC, 휴대용 저장매체 등 분실 (3) 정보시스템 및 정보통신실 파괴 (4) 중요 정보시스템 기능 장애 및 정지 (5) 비인가 휴대용 저장매체 및 정보통신장비 사용 (6) 접속이 금지된 P2P, 웹하드 등 접속 (7) 상용메일·메신저 등을 통한 업무자료 무단 소통 (8) 업무자료의 무단 반출 (9) 첨단 정보통신기기를 통한 업무자료 무단 소통
3	암호장비	(1) 암호장비 분실 및 피탈 (2) 암호장비 파손 및 임의파기 (3) 암호장비 복제·복사 (4) 비인가 암호장비 사용 (5) 암호장비 비닉체계 특성 및 제원 노출 (6) 암호장비 키 운용체계 노출
4	보안자재	(1) 암호·음어·약호자재의 분실 및 누설 (2) 암호·음어·약호자재의 파손 및 임의파기 (3) 암호·음어·약호자재의 임의제작 사용 (4) 세부 암호체계 노출

[별표 제2호 정보보호시스템 유형별 도입요건]

정보보호시스템 유형별 도입요건

제품 유형	도입 요건	비 고
침입차단시스템	CC인증(EAL2이상)	
침입탐지시스템	CC인증(EAL2이상)	
침입방지시스템	CC인증(EAL2이상)	
통합보안시스템(UTM)	CC인증(EAL2이상)	검증필암호모듈 탑재필요(VPN기능)
통합보안관리(ESM/TMS)	CC인증(EAL2이상)	
웹방화벽	CC인증(EAL2이상)	
DDoS대응장비	CC인증(EAL2이상)	
인터넷전화 보안제품	CC인증(EAL2이상)	
무선 침입방지시스템	CC인증(EAL2이상)	
가상사설망	CC인증(EAL2이상)	검증필암호모듈 탑재필요
네트워크접근제어시스템	CC인증(EAL2이상)	
스팸메일차단제품	CC인증(EAL2이상)	
바이러스 백신(서버 포함)	CC인증(EAL2이상)	
악성코드 탐지・제거	CC인증(EAL2이상)	
PC용 침입탐지・차단제품	CC인증(EAL2이상)	
PC용 통합보안제품	CC인증(EAL2이상)	
자료유출방지시스템	CC인증(EAL2이상)	
계정・권한관리 제품	CC인증(EAL2이상)	
서버보안제품	CC인증(EAL2이상)	
DB 접근통제 제품	CC인증(EAL2이상)	
다중영역구분 보안	CC인증(EAL2이상)	
스마트카드칩・COS	CC인증(EAL4이상)	
스마트카드 어플리케이션	CC인증(EAL2이상)	
스마트카드 판독기	CC인증(EAL2이상)	
보안토큰	CC인증(EAL2이상)	검증필 암호모듈 탑재필요
보안USB 제품	CC인증(EAL2이상)	검증필 암호모듈 탑재필요
완전삭제제품(복합기용)	CC인증(EAL2이상)	
완전삭제제품(기타)	별도 지정제품	
PKI 제품	국가용 암호제품	검증필 암호모듈 탑재필요
문서 암호화 제품	국가용 암호제품	검증필 암호모듈 탑재필요
DB 암호화 제품	국가용 암호제품	검증필 암호모듈 탑재필요
디스크・파일 암호화 제품	국가용 암호제품	검증필 암호모듈 탑재필요
메일 암호화 제품	국가용 암호제품	검증필 암호모듈 탑재필요
구간암호화 제품	국가용 암호제품	검증필 암호모듈 탑재필요
키보드보안 제품	국가용 암호제품	검증필 암호모듈 탑재필요
문서 위변조 방지제품	국가용 암호제품	검증필 암호모듈 탑재필요
일회용 패스워드	국가용 암호제품	검증필 암호모듈 탑재필요
통합인증 제품	국가용 암호제품	검증필 암호모듈 탑재필요

[별표 제3호 개인정보파일 보유기간 책정 기준표]

개인정보파일 보유기간 책정 기준표

보유기간	대상 개인정보파일
영구	1. 국민의 지위, 신분, 재산을 증명하기 위해 운용하는 개인정보파일 중 영구보존이 필요한 개인정보파일 2. 국민의 건강증진과 관련된 업무를 수행하기 위해 운용하는 개인정보파일 중 영구보존이 필요한 개인정보파일
준영구	1. 국민의 신분, 재산을 증명하기 위해 운용하는 개인정보파일 중 개인이 사망, 폐지 그 밖의 사유로 소멸되기 때문에 영구 보존할 필요가 없는 개인정보파일 2. 국민의 신분증명 및 의무부과, 특정대상 관리 등을 위하여 행정기관이 구축하여 운영하는 행정정보시스템의 데이터 셋으로 구성된 개인정보파일
30년	1. 관계 법령에 따라 10년 이상 30년 미만의 기간 동안 민. 형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일
10년	1. 관계 법령에 따라 5년 이상 10년 미만의 기간 동안 민. 형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일
5년	1. 관계 법령에 따라 3년 이상 5년 미만의 기간 동안 민. 형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일
3년	1. 행정업무의 참고 또는 사실 증명을 위하여 1년 이상 3년 미만의 기간 동안 보존할 필요가 있는 개인정보파일 2. 관계 법령에 따라 1년 이상 3년 미만의 기간 동안 민. 형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일 3. 각종 증명서 발급과 관련된 개인정보파일(단 다른 법령에서 증명서 발급 관련 보유기간이 별도로 규정된 경우 해당 법령에 따름)
1년	1. 상급기관(부서)의 요구에 따라 단순 보고를 위해 생성한 개인정보파일