용역사업 보안관리에 관한 내규

2010. 10. 15 제정

1. 목 적

본 지침은 용역업체에 제공한 내부자료나 용역 결과물 등 보안이 요구되는 제반 자료가 해킹 및 관리 부주의로 인해 유출되는 것을 방지하고자 하는 것을 목적으로 한다.

2. 적용 범위

가. 본교 정보화사업, 정보보안컨설팅, 연구개발 등 용역사업을 민간업체 또는 연구소등에 위탁 시 적용한다.

나. 본교에서 필요 시 또는 업무 효율상 계약에 의해 유지보수업무, 유지관리업무 등 특정 업무를 민간업체에게 외주 용역 의뢰하는 경우에 적용한다.

다. 본 지침에서 명시되지 않은 사항은 대학 정보보호규정 및 세칙과 국내 관계 법령 및 규정을 참조한다.

3. 책임과 권한

가. 용역사업 발주기관의 장은 정보보호담당자로 하여금 용역사업 수행 전반에 대한 인원·장비·자료 등의 보안관리를 담당토록 조치한다.

나. 정보보호관리자는 용역업체의 참여인원·장비·자료에 대한 보안관리와 시스템·네트워크에 대한 보안대책 수립·시행 등 제반사항에 대한 보안업무를 총괄한다.

다. 용역사업과 관련한 보안관리 책임은 용역업체 대표에게 있으며 대표는 용역사업 전반의 보안업무를 수행하는 관리책임자를 지정할 수 있다.

라. 용역업체의 관리책임자는 용역사업과 관련된 인원·장비·자료에 대한 보안업무 및 사업과 관련된 하도급업체의 보안관리 전반을 총괄한다.

4. 용역 입찰 시

가. 중요 외주용역사업은 착수단계부터 적정 등급의 비밀 또는 대외비로 분류, 용역 의뢰하고 '대외주의', '요보안'등의 모호한 표현 사용을 금지한다.

나. 용역의뢰 기관은 입찰공고 이전에 투입이 예상되는 자료, 장비 가운데 보안이 요구되는 사항에 대하여 관련법령 및 자체 규정이 정하는 바에 따라 등급을 분류하고 필요한 보안요구기준을 마련하여 계약부서에 제출하여야 한다.

다. 계약부서는 입찰 공고 시에 용역사업 관련 기밀유지 의무 및 위반 시 불이익 등의 내용을 사전에 고지한다.

라. 용역의뢰 기관은 제안서 제출을 요구하는 경우 평가요소에 문서·시설·장비 등 보안관리계획에 대한 평가 항목 및 배점기준 마련하여야 한다.

마. 용역의뢰기관과 계약부서는 용역업체가 입찰제안서에 제시한 용역사업 전반에 대한 보

안관리계획이 타당한지를 검토하여 사업자 선정 시 이를 반영하여야 한다.

5. 용역 계약 시

가. 용역사업 자체 또는 투입되는 자료・장비 등에 대한 대외보안이 필요한 경우 보안의 범위 및 책임을 명확히 하기 위해 사업수행 계약서와 별도로 비밀유지계약서를 작성할 수 있다.

나. 비밀유지계약서에는 비밀정보의 범위, 보안준수 사항, 위반시 손해배상 책임, 지적재산권 문제, 자료의 반환 등이 포함되도록 명시하여야 한다.

다. 용역사업 참여인원은 용역업체 임의로 교체할 수 없도록 명시하고 신상변동(해외여행 포함) 사항 발생시 발주기관에 즉시 보고하고, 승인을 득하여야 한다.

라. 발주기관의 요구사항을 사업자에게 명확히 전달키 위해 작성하는 과업 지시서(또는 과업내용서)에 자료 보안관리방법, 인원・장비・시설 등에 대한 보안점검・교육 등 보안관련 제반사항을 상세히 기술하여야 한다.

마. 용역업체가 사업에 대한 하도급 계약을 체결할 경우 本 사업계약 수준의 비밀유지 조항을 포함토록 조치하여야 한다.

6. 용역 수행 시

가. 참여인원에 대한 보안관리는 아래 사항을 준수하여야 한다.

①. 용역사업 참여인원에 대해서는 각 개인의 친필 서명이 들어간 정보보호서약서(별지 제 1호서식)를 징구한다.

②. 용역사업 수행 前 참여인원에 대해 법적 또는 발주기관 규정에 의한 비밀유지 의무 준수 및 위반 시 처벌내용 등에 대한 보안교육 실시한다.

③. 용역업체는 보안인식 강화를 위하여 주기적으로 자체 보안교육을 실시하고 정보보호 교육결과서(별지 제 2호 서식)를 발주기관에 제출하여야 하며, 또한 발주기관이 요구하는 보안교육에 반드시 참석하여야 한다.

나. 자료에 대한 보안관리는 아래 사항을 준수하여야 한다.

①. 전산망도・IP현황, 용역사업 산출물 및 개인정보 등 용역업체에 제공하는 비공개자료는 '자료관리대장'을 작성하여 인계자(해당기관 정보보호관리자)와 인수자(용역업체 관리책임자)가 직접 서명한 후 인계・인수한다.

②. 용역사업 관련자료 및 사업과정에서 생산된 모든 산출물은 발주 기관의 파일서버에 저장하거나 정보보호관리자가 지정한 PC에 저장・관리한다.

③. 용역사업 관련자료는 인터넷 웹하드 등 인터넷 자료공유사이트 및 개인메일함에 저장을 금지하고, 전자우편을 이용해 자료전송이 필요한 경우에는 자체 전자우편을 이용, 첨부자료 암호화 후 수・발신 한다. 단, 대외비 이상의 비밀은 전자우편으로 수・발신 금지한다.

④. 발주기관이 제공한 사무실에서 사업을 수행할 경우 제공한 비공개자료는 매일 퇴근 시 반납토록 하며 비밀문서를 제외한 일반문서는 용역업체에 제공된 사무실에 시건장치가

된 보관함이 있을 경우 이에 보관 가능하다.

⑤. 용역사업 수행으로 생산되는 산출물 및 기록은 정보보호관리자가 인가하지 않은 비인가자에게 제공・대여・열람을 금지한다.

⑥. 용역업체는 비공개자료 출력시에는 출력물에 출력자, 출력일시 등을 표시하여야 한다.

다. 사무실・장비에 대한 보안관리는 아래 사항을 준수하여야 한다.

①. 용역사업 수행장소는 발주기관이 시건장치와 통제가 가능한 공간을 제공하거나 협의를 통해 同 환경이 구축된 사무실을 사용하여야 한다.

②. 용역업체 사무실 또는 용역업무를 수행하는 공간에 대한 보안점검을 주 1회 이상 실시하여야 하며, 용역업체는 결과 내용에 대해 발주기관 정보보호담당자의 확인 및 개선조치 요구를 따라야 한다.

③. 발주기관 사무실에서 용역사업을 수행할 경우 용역 참여직원이 노트북 등 관련장비를 반출 또는 반입할 때마다 악성코드 감염여부 및 자료 무단반출 여부를 확인한다.

- 백신 등의 PC 보안프로그램의 설치 여부
- 악성코드 감염여부 및 자료 무단 반출 여부

④. 인가 받지 않은 USB 등의 보조기억매체 사용을 금지하며 산출물 저장을 위해 보조기억매체가 필요한 경우 발주기관 정보보호관리자의 관리하에 사용하여야 한다.

⑤. 용역업체는 노트북 및 PC에 전원기동(CMOS) 패스워드, 윈도우 로그인 패스워드, 화면보호기(10분 간격) 패스워드 등을 영문자 및 숫자가 조합된 8글자 이상으로 설정하여야 한다.

라. 내・외부망 접근시 보안관리는 아래사항을 준수하여야 한다.

①. 용역사업 수행 시 발주기관 전산망 이용이 필요한 경우 사업 참여인원에 대한 사용자 계정(ID)은 외부인력 ID 신청서(별지 제 3호 서식)에 따라 신청하고, 신청된 ID들은 하나의 그룹으로 등록하고 계정별로 정보시스템 접근권한을 부여하고, 계정별로 부여된 접속권한은 불필요시 곧바로 권한을 해지하거나 계정을 폐기하여야 한다.

②. 용역사업 수행시 발주기관 전산망 이용이 필요한 경우 참여인원에게 부여한 패스워드는 발주기관 정보보호담당자가 별도로 기록 관리하고 수시로 해당 계정에 접속하여 저장된 자료와 작업이력을 확인하여야 한다.

③. 용역사업 수행시 발주기관 전산망 이용이 필요한 경우 발주기관 정보보호담당자는 서버 및 장비 운영자로 하여금 내부서버 및 네트워크 장비에 대한 접근기록을 매일 확인하여 이상유무를 정보보호관리자에게 보고하여야 한다.

④. 용역사업 수행시 발주기관 전산망 이용이 필요한 경우 용역업체에서 사용하는 노트북PC는 인터넷 연결을 금지, 다만 사업 수행상 필요한 경우에는 용역업체의 관리책임자가 직접 요청하고 발주기관의 정보보호관리자가 필요성을 인정할 경우 접속할 노트북을 지정하고 필요한 사이트에만 접속토록 방화벽 등을 통해 통제 후 사용 할 수 있도록 하여야

한다.

⑤. 발주기관 및 용역업체 전산망에서 P2P, 웹하드 등 인터넷 자료공유 사이트로의 접속을 방화벽 등을 이용해 원천 차단하여야 한다.

7. 용역 종료 시

가. 사업완료 후 생산되는 최종 산출물 중 대외보안이 요구되는 자료는 대외비로 작성·관리하고 불필요한 자료는 삭제 및 세단 후 폐기한다.

나. 용역업체에 제공한 제반자료, 장비, 서류와 중간·최종 산출물 등 용역과 관련된 제반자료는 전량 회수하고 업체에 복사본 등 별도 보관을 금지한다.

다. 노트북·보조기억매체 등 전자적으로 기록된 자료는 교육과학기술부의 '교육기관 정보보호 기본지침의 제 6장 USB메모리 등 보조기억매체 보안관리'에 따라 보안 조치한다.

라. 용역사업 관련자료 회수 및 삭제조치 후 업체에게 복사본 등 용역사업 관련 자료를 보유하고 있지 않다는 대표 명의 확약서를 징구하여야 한다.

[별지 제1호 서식]

정보보호 서약서 (외부인력용)

본인은 20 년 월 일부터 20 년 월 일까지 POSTECH 업무를 수행함에 있어 다음의 사항을 준수할 것을 서약합니다.

1. 본인은 POSTECH 업무를 수행함에 있어 업무상 취득한 정보의 중요성을 깊이 인식하고, 이에 관련된 소관 업무가 학교 보안에 관한 기밀임을 인정한다.

2. 본인은 POSTECH 업무를 수행함에 있어 아래의 내용을 준수한다.

가 POSTECH내 전반적 정보습득이나 운영상의 기밀을 절대 누설하지 않으며,

나 업무수행을 통해 축적된 정보를 임의 도용하거나 방출하지 않으며,

다 POSTECH 인프라자원을 반드시 업무적 용도로만 활용하며, (email, 전화, 팩스 등)

라 POSETCH내 운영상 불이익을 줄 수 있는 모든 내용을 외부에 유출하지 않으며,

마 허락된 업무 이외의 업무는 일체 행하지 않으며, 현행 보안관련 제반 법령 및 규정을 준수한다.

3. 위의 사항들에 대하여 용역업무 수행시((계약이행기간)는 물론 용역업무 종료(계약만료, 해지) 후에도 직무상 취득한 제반 비밀사항을 제3자에게 일체 누설하지 않을 것을 서약하며 업무종료 후에는 관련 자료 일체를 반납하고 담당자의 확인을 거쳐 퇴거 절차를 진행한다.

4. 업무수행을 통해 생성된 모든 생성물의 소유권은 POSTECH에 있음을 인정하며, 정보의 무단유출 방지를 위하여 POSTECH이 시행중인 통제 및 정기/비정기적인 점검(이메일 모니터링 포함)에 동의한다.

5. 본인은 POSTECH 시스템을 이용함에 있어서 불법소프트웨어를 사용하지 않을 것이며, 만약 본인이 불법 소프트웨어 사용(바이러스 유포를 포함)으로 인하여 POSTECH 시스템에 손해가 발생할 경우 이에 대한 일체의 민•형사상 책임을 진다.

6. 본인은 POSTECH 업무를 수행함에 있어 사용한 전산장비 및 소프트웨어, 데이터 등 유•무형의 자산을 훼손 또는 멸실 시킴으로써 POSTECH에 손해가 발생할 경우 이에 대한 손해배상책임을 진다.

7. 본인은 상기 서약사항을 위반할 경우 관련 법령에 의거 엄중한 처벌을 받을 것이며, 그에 따른 일체의 민•형사상의 일체의 책임을 질 것을 서약한다.

20 년 월 일

서약자 소 속:
성 명: (인)

POSTECH

[별지 제2호 서식]
정보보호 교육결과서 (용역업체용)

1. 목적
용역사업 수행기간 동안 대학의 정보보호 규정에 의거하여, 이행한 정보보호 자체 교육 수행

결
과물을 발주기관에 제출 함

2. 대상
용역 사업에 참여하는 모든 인력을 그 대상으로 함

3. 주관
교육 내용 및 교육 일정은 대학의 정보보호 전담부서의 지원을 받아 용역사업 발주부서와 협의
하여 시행 함.

4. 교육 세부 결과

수강자	소속 및 직위	전화번호	E-mail	비 고
홍길동	경영지원팀/차장	011-9999-8888	security@postech.ac.kr	

외부인력 ID 신청서

승 인 부 서 장

신 청 자 소 속

이 름 (인 또는 서명)

신 청 일 20 년 월 일

신청기간 20 년 월 일 ~ 20 년 월 일

용 도 □ 신규등록 □ 권한변경 □ 사용중지 □ 재사용 □ ID삭제

시 스 템

이 름 1. 4. 7.

2. 5. 8.

3. 7. 9.

ID 이름 초기

패스워드

사 유

및

내 용

1. 최초 로그온 시 반드시 패스워드를 변경하셔야 합니다.
2. 패스워드는 최소8자리 이상이며, 영문자, 숫자는 반드시 포함하고, 특수문자 $,\,',!,&는 사용할 수 없습니다.

정보보호

담당자 부 서 명

이 름 (인 또는 서명)

처 리 일 20 년 월 일

시스템

담당자 부 서 명

이 름 (인 또는 서명)

처 리 일 20 년 월 일

POSTECH