용역사업 보안관리에 관한 지침

2010.10.15 제정
2019. 2.28 개정

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. [2019. 2. 28 삭제]

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 자료·장비·네트워크 보안대책 및 '누출금지 대상정보'관리방안과 문서·시설·장비 등 보안관리계획에 대한 평가

항목 및 배점기준 마련하여야 한다. [2019. 2. 28 개정]

마. 용역의뢰 기관과 계약부서는 용역업체가 입찰제안서에 제시한 용역사업 전반에 대한 보안관리계획이 타당한지를 검토하여 사업자 선정 시 이를 반영하여야 한다.

바. 용역의뢰 기관은 제2조 제 가항과 관련 용역사업을 실시할 경우 시방서와 계약서에 <별첨1>의 「용역 업체 보안 관리 계획」을 참조하여 보안 특약 사항과 이를 위반할 경우에 대한 손해배상 책임 등을 명시해야 한다. [2019. 2. 28 신설]

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 함께 <붙임 1>의 「외주 용역사업 보안특약」을 작성하여야 한다. [2019. 2. 28 개정]

나. [2019. 2. 28 삭제]

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. 용역의뢰 기관은 용역업체가 사업의 일부 또는 전부에 대하여 하도급 계약을 체결하는 경우에 용역업체로 하여금 하도급 계약서에 본 사업계약 수준의 비밀유지 조항을 포함하도록 조치해야 한다. [2019. 2. 28 개정]

6. 용역 수행 시

가. 참여인원에 대한 보안관리는 아래 사항을 준수하여야 한다.

1) 용역사업의 참여인력 및 용역회사 대표에 대하여 각 개인의 친필 서명이 들어간 <별지 1호 서식>의 「보안서약서」를 징구한다. [2019. 2. 28 개정]

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

3) 용역업체는 보안인식 강화를 위하여 주기적으로 자체 보안교육을 실시하고 <별지 4호 서식>의 「용역업체 보안교육 결과서」를 발주기관에 제출하여야 하며, 또한 발주기관이 요구하는 보안교육에 반드시 참석하여야 한다. [2019. 2. 28 개정]

나. 자료에 대한 보안관리는 아래 사항을 준수하여야 한다.

1) 전산망도・IP현황, 용역사업 산출물 및 개인정보 등 용역업체에 제공하는 비공개자료는 <별지 5호 서식>의 「열람·제공자료 관리대장」을 작성하여 인계자(해당기관 정보보호관리자)와 인수자(용역업체 관리책임자)가 직접 서명한 후 인계・인수한다. [2019. 2. 28 개정]

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 <별지 6호 서식>의 「정보시스템 반·출입 관리대장」을 작성하고 악성코드 감염여부 및 자료 무단반출 여부를 확인한다. [2019. 2. 28 개정]

- 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 <별지 7호 서식>의 「외부인력 ID 신청서」에 따라 신청하고, 신청된 ID들은 하나의 그룹으로 등록하고 계정별로 정보시스템 접근권한을 부여하고, 계정별로 부여된 접속 권한은 불필요시 곧바로 권한을 해지하거나 계정을 폐기하여야 한다. [2019. 2. 28 개정]

2) 용역사업 수행시 발주기관 전산망 이용이 필요한 경우 참여인원에게 부여한 패스워드

는 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 노트북 PC는 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.

마. 대학 정보보안책임자는 대학에서 수행 중인 용역사업에 대한 보안관리를 아래와 같이 점검하여야 한다. [2019. 2. 28 신설]

1) 정보보안책임자는 용역사업에 대한 현황을 매년 파악하여 <별첨1>의 「용역 업체 보안 관리 계획」에 따라 발주기관이 용역업체에 대한 관리·감독을 이행하고 있는지 점검하여야 한다.

2) 발주기관은 사업수행 계약서와 함께 <붙임 1>의 「외주 용역사업 보안특약」이 작성되었는지 점검하여야 한다.

3) 발주기관은 용역사업이 안전하게 수행되고 있는지 <별지 8호 서식>의 「용역사업 보안점검 리스트」를 이용하여 연 1회 이상 점검하여야 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 제반 자료는 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 명의의 <별지 2호 서식>의 「보안 확약서」를 징구하여야 한다. [2019. 2. 28 개정]

부칙

1. 이 지침은 2019년 2월 28일부터 시행한다.

[별첨 1] 용역 업체 보안관리 계획

용역 업체 보안관리 계획

□ 개 요

용역사업 수행 업체를 통한 비공개 내부자료(붙임1-별표3 참조) 유출 방지 등을 위해 용역사업 수행 시 용역사업 주관(발주)부서에서는 아래와 같이 보안 관리를 수행해야 함

□ 보안관리 내용

구 분		참고 사항	비 고
인원 보안	보안서약서 징구	개인별 서명 포함 (별지1호서식)	착수 시
	보안교육	보안교육자료(15분 내외) / 교육일지 (별지4호서식)	착수 1달 이내
	보안점검	보안점검 리스트 작성 (별지8호서식)	수시
장비 보안	장비 반·출입 관리	장비 반·출입 대장 / 보안점검 증빙자료 (별지6호서식, 별지9호서식[반출시])	수시
	시스템 접근권한 통제	개인별 계정 생성 / 권한 차등부여	
	보조기억매체 관리	대학 「USB메모리 등 휴대용 저장매체 보안관리 지침」 준수	반입 시
자료 보안	제공자료 관리대장	내부자료 공개 내역 (별지5호서식)	제공/반납 시
	산출물 관리	지정된 PC 또는 서버에만 산출물 저장토록 관리	
	대표명의 확약서 징구	사업관련 자료 미 보유 확약서 (별지2호서식)	사업 종료 후
기타	보안점검	전 분야에 걸쳐 보안점검 실시	분기 1회
	계약서 포함사항	외주 용역사업 보안특약 사항(붙임 참조)	
	원격작업 관리	원격작업 운영 방침 수립	

붙임1. 외주 용역사업 보안특약

[붙임 1] 외주 용역사업 보안특약 (계약용)

외주 용역사업 보안특약

① 사업자는 포항공과대학교의 보안정책을 위반하였을 경우 [별표1]의 위규처리 기준에 따라 위규자 및 관리자를 행정조치하고 [별표2]의 보안 위약금을 포항공과대학교에 납부한다.

② 사업자는 사업 수행에 사용되는 문서, 인원, 장비 등에 대하여 물리적, 관리적, 기술적 보안대책 및 [별표3]의 '누출금지 대상정보'에 대한 보안관리계획을 사업제안서에 기재하여야 하며, 해당 정보 누출시 포항공과대학교는 국가계약법 시행령 제76조에 따라 사업자를 부정당업체로 등록한다.

③ 사업 수행과정에서 취득한 자료와 정보에 관하여 사업수행 중은 물론 사업 완료 후에도 이를 외부에 유출해서는 안되며, 사업종료시 정보보안담당관의 입회하에 완전 폐기 또는 반납해야 한다.

④ 사업자는 사업 최종 산출물에 대해 정보보안전문가 또는 전문보안 점검도구를 활용하여 보안 취약점을 점검, 도출된 취약점에 대한 개선을 완료하고 그 결과를 제출해야 한다.

[붙임 1 - 별표 1] 사업자 보안 위규 처리기준
[붙임 1 - 별표 2] 보안 위약금 부과 기준
[붙임 1 - 별표 3] 누출금지 대상 정보

[붙임 1] 외주 용역사업 보안특약 (입찰공고용)

외주 용역사업 보안특약

1. 본 조항은 대학 발주사업에 참여함에 있어 사업자가 지켜야할 보안에 관한 사항을 규정함을 목적으로 한다.
2. 사업자는 대학의 보안정책을 위반하였을 경우 [별표1]의 위규처리 기준에 따라 위규자 및 관리자를 행정조치하고 [별표2]의 보안 위약금을 대학에 납부한다.
3. 사업자는 사업 수행에 사용되는 문서, 인원, 장비 등에 대하여 물리적, 관리적, 기술적 보안대책 및 [별표3]의 '누출금지 대상정보'에 대한 보안관리계획을 사업제안서에 기재하여야 하며, 해당 정보 누출시 대학은 국가계약법 시행령 제76조에 따라 사업자를 부정당업체로 등록한다.
4. 제안사는 입찰 참여 과정 및 본 사업과 관련하여 취득한 일체의 정보를 제3자에게 유출 또는 누설하여서는 안 되며, 이의 위반으로 인한 문제발생시 민·형사상의 모든 책임을 진다.
5. 사업자는 과업수행 전후를 막론하고 본 과업과 관련하여 업무상 지득한 제반사실과 비공개 자료에 대해 발주기관의 사전승인 없이 공표, 누설 및 제3자에게 제공하여서는 아니 된다.
6. 사업자는 본 과업착수 시 발주기관의 보안관련 규정 양식에 의한 보안서약서[별지 1호 서식]를 제출하여야 하며, 과업 참여자에 대한 보안서약서는 과업수행책임자의 책임 하에 징구하여 발주기관에 제출하여야 한다.
7. 사업 완료시 용역관련 제반자료는 전량회수하고, 저장매체 내 자료삭제 및 사업산출물 복사본 등을 보관하지 않는다는 대표명의의 확약서[별지 2호 서식]를 제출하여야 한다.
8. 사업자는 과업수행 중 과업참여자를 교체할 경우 발주기관의 승인을 받고 인계인수를 철저히 하여 자료의 외부유출을 사전에 방지하여야 한다.
9. 발주기관은 사업자의 보안관리 상태를 수시로 점검할 수 있으며, 사업자는 보안사항을 위반한 경우 즉시 조치하여야 한다.
10. 관련하여 위반사항의 조치가 미진하거나, 조치 후에라도 동일한 보안사항을 재차 위반한 경우, 사업자를 대상으로 손해배상을 청구할 수 있으며, 향후 사업의 입찰참여를 제한 할 수 있다.
11. 발주기관은 보안준수사항을 위반한 참여인력의 교체를 요구할 수 있으며, 사업자는 인력교체요구를 응하여야 한다.
12. 과업참여자 이외의 자에게 부득이한 사정으로 인해 산출물 등 관련 자료를 취급하게 해야 할 경우에는 반드시 보안대책을 마련하고, 과업수행책임자 또는 책임자로부터 위임받은 과업참여자의 책임 하에 취급토록 하여야 한다.
13. 사업자는 과업 사무실을 제한구역으로 지정하여 외부인의 출입을 통제하여야 한다.

14. 사업자는 기타 과업 수행 시 보안상 결함이 없도록 하여야 하며 보안사항 불이행으로 발생되는 모든 책임을 져야한다.
15. 발주사업이 개인정보 처리업무를 사업자에게 위탁하는 경우 [별지 3호 서식]의 개인정보처리 위o수탁 계약서를 작성하여야 한다.

[붙임 1 - 별표 1] 사업자 보안 위규 처리기준
[붙임 1 - 별표 2] 보안 위약금 부과 기준
[붙임 1 - 별표 3] 누출금지 대상 정보
[서식 1] 보안서약서
[서식 2] 보안확약서
[서식 3] 개인정보처리 위·수탁 계약서

[붙임 1 - 별표 1] 사업자 보안 위규 처리기준

사업자 보안위규 처리기준

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

구 분	위 규 사 항	처 리 기 준
보 통	1. 기관 제공 중요정책·민감 자료 관리 소홀 가. 주요 현안·보고자료를 책상위 등에 방치 나. 정책·현안자료를 휴지통·폐지함 등에 유기 또는 이면지 활용 2. 사무실 보안관리 부실 가. 캐비넷·서류함·책상 등을 개방한 채 퇴근 나. 출입키를 책상위 등에 방치 3. 보호구역 관리 소홀 가. 통제·제한구역 출입문을 개방한 채 근무 나. 보호구역내 비인가자 출입허용 등 통제 미실시 4. 전산정보 보호대책 부실 가. 휴대용저장매체를 서랍·책상 위 등에 방치한 채 퇴근 나. 네이트온 등 비인가 메신저 무단 사용 다. PC를 켜 놓거나 보조기억 매체(CD, USB 등)를 꽂아 놓고 퇴근 라. 부팅·화면보호 패스워드 미부여 또는 "1111" 등 단순숫자 부여 마. PC 비밀번호를 모니터옆 등 외부에 노출 바. 비인가 보조기억매체 무단 사용	○ 위규자 및 직속 감독자 등 경징계 ○ 위규자 및 직속 감독자 사유서 / 경위서 징구 ○ 위규자 대상 특별 보안교육 실시
경 미	1. 업무 관련서류 관리 소홀 가. 진행중인 업무자료를 책상 등에 방치, 퇴근 나. 복사기·인쇄기 위에 서류 방치 2. 근무자 근무상태 불량 가. 각종 보안장비 운용 미숙 나. 경보·보안장치 작동 불량 3. 전산정보 보호대책 부실 가. PC내 보안성이 검증되지 않은 프로그램 사용 나. 보안관련 소프트웨어의 주기적 점검 위반	○ 위규자 서면·구두 경고 등 문책 ○ 위규자 사유서 / 경위서 징구

[붙임 1 - 별표 2] 보안 위약금 부과 기준

보안 위약금 부과 기준

1. 위규 수준별로 A~D 등급으로 차등 부과

구 분	위 규 수 준			
	A급	B급	C급	D급
위 규	심각 1건	중대 1건	보통 2건 이상	경미 3건 이상
위약금 비중	계약금액의 20% 이하 및 부정당업자 등록	계약금액의 10% 이하	계약금액의 5%이하	계약금액의 3%이하

※ 위규 수준은 [별표 1] 참조

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

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

3. 사업 종료시 지출금액 조정을 통해 위약금 정산

[붙임 1 - 별표 3] 누출금지 대상 정보

누출금지 대상정보

번호	대 상 구 분	비고
1	정보시스템의 내·외부 IP 주소 현황	
2	정보시스템의 세부 구성현황 및 정보통신망 구성도	
3	사용자계정 및 패스워드 등 정보시스템 접근권한 정보	
4	정보통신망 취약점 분석·평가 결과물	
5	용역사업 결과물 및 프로그램 소스코드	
6	보안시스템 및 정보보호시스템 도입현황	
7	침입차단시스템·방지시스템(IPS) 등 정보보호제품 및 라우터·스위치 등 네트워크 장비 설정 정보	
8	「공공기관의 정보공개에 관한 법률」 제 9 조제 1 항에 따라 비공개 대상 정보로 분류된 기관의 내부문서	
9	「개인정보보호법」 제 2 조 1 호의 개인정보	
10	사업 수행 중 습득・인지한 보안정보	
11	기타 공개가 불가하다고 판단되는 자료	

[별지 1호 서식] 보안서약서

보안 서약서 (업체대표자용)

본인은 20 년 월 일 포항공과대학교와 계약 체결한 _____사업을 시행함에 있어 다음 사항을 준수할 것을 서약서로 제출합니다.

1. 본인은 본 사업을 시행함에 있어 계약서, 과업지시서(제안요청서) 및 사업수행상의 제반 보안사항을 철저히 이행할 것임은 물론 사업 수행전에 사업 참여자 전원에 대하여 보안교육을 실시하겠습니다.

2. 본인은 물론 당사업자의 직원이 보안사항을 외부에 누설 또는 도용한 경우에는 누설 또는 도용한 자가 제법규에 의거 처벌 받음은 물론 당사업자 대한 어떠한 제재조치를 취하여도 이의를 제기하지 않을 것입니다.

3. 포항공과대학교에서 지정한 “누출금지 정보”를 절대 누출하지 않을 것이며, 누출시 지방계약법 시행령 제92조에 의거 부정당업자로 제재함에 이의를 제기하지 않으며, 민·형사상의 책임이 전적으로 당사업자에 있음을 각서합니다.

년 월 일

업체명 :

대표자 성명 : (서명)

포항공과대학교 총장 귀하

[별지 1호 서식] 보안서약서

보안 서약서 (사업참여자용)

본인은 20 년 월 일 포항공과대학교와 계약 체결한 _____사업을 시행함에 있어 다음 사항을 준수할 것을 서약서로 제출합니다.

1. 본인은 본 사업을 시행함에 있어 계약서, 과업지시서(제안요청서) 및 사업수행상의 제반 보안사항을 철저히 이행할 것임은 물론 사업 수행전에 사업 참여자로 보안교육을 받겠습니다.

2. 본인은 보안사항을 외부에 누설 또는 도용한 경우에는 누설 또는 도용한 자가 제법규에 의거 처벌 받음은 물론 사업자 및 참여자에 대한 어떠한 제재조치를 취하여도 이의를 제기하지 않을 것입니다.

3. 포항공과대학교에서 지정한 “누출금지 정보”를 절대 누출하지 않을 것이며, 누출시 지방계약법 시행령 제92조에 의거 부정당업자로 제재함에 이의를 제기하지 않으며, 민·형사상의 책임이 전적으로 당사업자 및 각서인에 있음을 각서합니다.

년 월 일

업체명 :
직위 :
성명 : (서명)

포항공과대학교 총장 귀하

[별지 2호 서식] 보안 확약서

보안 확약서

본인은 귀 기관과 계약한 “ ”의 수행을 완료함에 있어, 다음 각호의 보안사항에 대한 준수 책임이 있음을 서약하며 이에 확약서를 제출합니다.

1. 본 업체(단체)는 업체(단체) 및 사업 참여자가 사업수행 중 지득한 모든 자료를 반납 및 파기하였으며, 지득한 정보에 대한 유출을 절대 금지하겠습니다.

2. 본 업체(단체)는 하도급업체에 대해 상기 항과 동일한 보안사항 준수 책임을 확인하고 보안확약서 징구하였으며, 하도급업체가 위의 보안사항을 위반할 경우에 주사업자로서 이에 동일한 법적책임을 지겠습니다.

3. 본 업체(단체)는 상기 보안사항을 위반할 경우에 귀 기관의 사업에 참여 제한 또는 기타 관련 법규에 따른 책임과 손해배상을 감수하겠습니다.

년 월 일

서약업체(단체) 대표
업체명:
성 명 : (서명)

포항공과대학교 총장 귀하

[별지 3호 서식] 개인정보처리 위·수탁 계약서

개인정보처리 위·수탁 계약서

포항공과대학교(이하 대학)와 계약수행자는 대학의 개인정보 처리업무를 계약수행자에게 위탁함에 있어 다음과 같은 내용으로 본 업무위탁계약을 체결한다.

제 1 조 (목적) 이 계약은 대학의 개인정보처리업무를 계약수행자에게 위탁하고, 계약수행자는 이를 승낙하여 계약수행자의 책임아래 성실하게 업무를 완성하도록 하는데 필요한 사항을 정함을 목적으로 한다.

제 2 조 (용어의 정의) 본 계약에서 별도로 정의되지 아니한 용어는 개인정보보호법, 같은 법 시행령 및 시행규칙, 「표준 개인정보 보호지침」(행정자치부 고시 제 45 호)에서 정의된 바에 따른다.

제 3 조 (위탁업무의 목적 및 범위) 계약수행자는 계약이 정하는 바에 따라 '_____' 목적으로 개인정보 처리(* 본 용역에서는 개인정보를 포함하는 모든 정보시스템에 인가된 접근 행위를 '개인정보 처리'로 본다.) 업무를 이행한다.

제 4 조 (재위탁 제한) ① 계약수행자는 대학의 사전 승낙을 얻은 경우를 제외하고 대학과의 계약상의 권리와 의무의 전부 또는 일부를 제 3 자에게 양도하거나 재위탁할 수 없다.

② 계약수행자가 재위탁받은 수탁회사를 선임한 경우 계약수행자는 당해 재위탁계약서와 함께 그 사실을 즉시 대학에 통보하여야 한다.

제 5 조 (개인정보의 안전성 확보조치) 계약수행자는 개인정보보호법 제 29 조, 같은 법 시행령 제 30 조 및 개인정보의 안전성 확보조치 기준 고시(행정자치부 고시 제 2011-43 호)에 따라 개인정보의 안전성 확보에 필요한 관리적·기술적 조치를 취하여야 한다.

제 6 조 (개인정보의 처리제한) ① 계약수행자는 계약기간은 물론 계약 종료 후에도 위탁업무 이행 목적 범위를 넘어 개인정보를 이용하거나 이를 제 3 자에게 제공 또는 누설하여서는 안 된다.

② 계약수행자는 계약이 해지되거나 또는 계약기간이 만료된 경우 위탁업무와 관련하여 보유하고 있는 개인정보를 「개인정보보호법」 시행령 제16조에 따라 즉시 파기하거나 대학에 반납하여야 한다.

③ 제2항에 따라 계약수행자가 개인정보를 파기한 경우 지체 없이 대학에 그 결과를 통보하여야 한다.

제7조 (수탁자에 대한 관리·감독 등) ① 대학은 계약수행자에 대하여 다음 각 호의 사항을 관리하도록 요구할 수 있으며, 계약수행자는 특별한 사유가 없는 한 이에 응하여야 한다.

1. 개인정보의 처리 현황
2. 개인정보의 접근 또는 접속현황
3. 개인정보 접근 또는 접속 대상자
4. 목적 외 이용·제공 및 재위탁 금지 준수여부
5. 암호화 등 안전성 확보조치 이행여부
6. 그 밖에 개인정보의 보호를 위하여 필요한 사항

② 대학은 계약수행자에 대하여 제1항 각 호의 사항에 대한 실태를 점검하여 시정을 요구할 수 있으며, 계약수행자는 특별한 사유가 없는 한 이행하여야 한다.

③ 대학은 처리위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 년 1회 이상 계약수행자를 교육할 수 있으며, 계약수행자는 이에 응하여야 한다. 또한, 계약수행자가 본 사업에 참여하는 인원에 대하여 전문교육기관 주관의 개인정보보호 교육을 연 1회 이상 이수토록 하여 참여자별 교육이수증 등을 제출한 경우는 대학이 시행하는 교육에 응한 것으로 갈음한다.

④ 제1항에 따른 교육의 시기와 방법 등에 대해서는 대학과 계약수행자가 협의하여 시행한다.

제8조 (손해배상) ① 계약수행자 또는 계약수행자의 임직원 기타 계약수행자의 수탁자가 이 계약에 의하여 위탁 또는 재위탁받은 업무를 이행함에 있어 이 계약에 따른 의무를 위반하거나 계약수행자 또는 계약수행자의 임직원 기타 계약수행자의 수탁자의 귀책사유로 인하여 이 계약이 해지되어 대학 또는 개인정보주체 기타 제3자에게 손해가 발생한 경우 계약수행자는 그 손해를 배상하여야 한다.

② 제 1 항과 관련하여 개인정보주체 기타 제 3 자에게 발생한 손해에 대하여 대학이 전부 또는 일부를 배상한 때에는 대학은 이를 계약수행자에게 구상할 수 있다.

본 계약의 내용을 증명하기 위하여 계약서 2 부를 작성하고, 대학과 계약수행자가 서명 또는 날인한 후 각 1 부씩 보관한다.

20 년 월 일

발주자	과업수행자
위탁기관명 : 포항공과대학교	수탁기관명 :
주 소 : 포항시 남구 청암로 77	주 소 :
대표자 : 총 장 (인)	대표자 : (인)

[별지 4 호 서식] 용역업체 보안교육 결과서

용역업체 보안교육 결과서

용역업체 보안교육 결과서	결재	담당	검 토	승 인

교 육 일 시		교 육 장 소	
대상 / 인원		강 사	

주 요 교 육 내 용

1. 외주 용역사업 보안특약 사항 교육
   가. 사업자 보안위규 처리기준
   나. 보안 위약금 부과 기준
   다. 누출금지 대상 정보
   라. 일별 용역사업 보안점검 리스트

2. 보안지침 소개
   가. PC보안 프로그램(보안USB, 매체제어, V3 등) 설치 안내
   나. 노트북/PC 반·출입 절차 안내
   다. 「사이버보안진단의 날」 행사 안내
   라. 기타 인원/장비/자료 등에 관한 보안관리 사항 안내

3. 기타 필요사항 교육

교육 참석자 확 인 사 항	소속	성명 및 서명	소속	성명 및 서명
		(인)		(인)
		(인)		(인)
		(인)		(인)
		(인)		(인)
		(인)		(인)
		(인)		(인)
		(인)		(인)

포 항 공 과 대 학 교

[별지 5호 서식] 열람·제공자료 관리대장

용역업체 관리책임자	발주기관 관리책임자

열람·제공자료 관리대장

20 년 사업명: 용역업체명:

연번	자료명	인계 및 인수				자료반납	
		인계자	인수자	월일	장소	확인자	월일

[별지 6호 서식] 정보시스템 반·출입 관리대장

정보시스템 반·출입 관리대장

번호	사용자 (소속/성명)	반출·입 대상	사 유	반·출입 일시		확인자 (성명/서명)
				반입	20 . . .	(서명)
				반출	20 . . .	(서명)
				반입	20 . . .	(서명)
				반출	20 . . .	(서명)
				반입	20 . . .	(서명)
				반출	20 . . .	(서명)
				반입	20 . . .	(서명)
				반출	20 . . .	(서명)
				반입	20 . . .	(서명)
				반출	20 . . .	(서명)
				반입	20 . . .	(서명)
				반출	20 . . .	(서명)
				반입	20 . . .	(서명)
				반출	20 . . .	(서명)
				반입	20 . . .	(서명)
				반출	20 . . .	(서명)
				반입	20 . . .	(서명)
				반출	20 . . .	(서명)
				반입	20 . . .	(서명)
				반출	20 . . .	(서명)

① 사용자 : 해당 정보시스템의 반·출입을 요청한 자의 소속과 성명

② 반출·입 대상 : 반출·입 대상 정보시스템 세부 내역(종류/용량 등) 기재

③ 반출·입 일시 : 반입 시에는 반입 일시, 반출 시에는 반출 일시 기재

④ 사유 : 해당 정보시스템 반출·입 사유나 목적 기재

⑤ 확인자 : 해당 정보시스템의 반출·입을 확인하고 관리하는 담당자 성명/서명 기재

[별지 7호 서식] 외부인력 ID 신청서

외부인력 ID 신청서

승인	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

[별지 8호 서식] 용역사업 보안점검 리스트

용역사업 보안점검 리스트

순번	점 검 항 목	확인 (○, X)
1	용역업체 사용 전산망과 기관 전산망의 분리 여부(VLAN 분리 포함)	
2	용역업체 직원 PC의 내부 정보시스템 접근 통제 여부	
3	P2P, 웹하드, 메신저 등 불필요한 인터넷 접속 차단 여부	
4	용역업체 직원에 주요 계정 비밀번호 제공 여부	
5	용역업체 직원에 비밀번호 부여시 관련사항 별도 기록 여부	
6	용역업체 직원에 시스템 관리자 계정 단독 접근 여부	
7	노트북PC 등 휴대형 정보시스템을 시스템 관리용 PC로 활용 여부	
8	용역업체 직원 등에 의한 기관 외부에서의 원격 접속·작업 여부	
9	용역업체 정보시스템 접근시 작업이력 로깅 기능 사용 여부	
10	용역업체 PC 및 휴대형 저장매체에 정보시스템 '계정명/비밀번호' 저장 여부	
11	용역업체 PC에 설치된 운영체제 및 응용프로그램 최신상태 유지 여부	
12	용역업체 PC 백신 프로그램 자동 업데이트 및 실시간 감시기능 사용 여부	
13	용역업체 PC USB·CD-RW·무선랜 등 매체 통제 여부	
14	용역업체 PC 비밀번호 및 화면보호기 설정 여부	
15	용역업체 직원의 비인가 정보통신장비(노트북 등) 휴대·반입 여부	

201 . . .

점검자(용역업체) 부서명 직급 성명 (서명)

확인자(담당자) 부서명 직급 성명 (서명)

[별지 9호 서식] 자료 삭제 및 미보유 확인서

자료 삭제 및 미보유 확인서

본인(당사)은 귀 포항공과대학교 _____ 수행과정에서 취득한 모든 자료를 반납하고, 모든 데이터를 삭제(디스크 초기화)하였음을 확인합니다.

위 내용에 대한 민/형사상 또는 보안상 책임과 관계법규에 의한 조치에 따를 것을 서약하며, 이에 확인서를 제출합니다.

년 월 일

확 인 자 소속 및 직급 :

성 명 : (서명)

연 락 처 :

포항공과대학교총장 귀하