과 업 지 시 서

사업명	한세대학교 개인정보 영향평가 사업

2017. 12

한 세 대 학 교

Ⅰ 과업지시 개요

1. 과업목적

○ 한세대학교에서 운용 중인 개인정보처리시스템에 대한 개인정보 영향평가를 통해 사전에 개인정보 침해 요인을 파악하고 개선방안을 수립, 적용하여 침해사고를 사전에 효과적으로 예방하기 위함.

○ 1차로 입시, 학사행정업무시스템에 대한 개인정보 실태점검을 하였으나 개선사항에 대한 이행점검과 개인정보보호법 제33조에 따른 개인정보 영향평가 의무 수행사항 준수하기 위함.

○ 개인정보처리부서의 개인정보처리에 따른 위법 요인을 파악하고 개선방안을 수립, 적용하여 개인정보보호를 효과적으로 수행하기 위함.

2. 과업개요

○ 사 업 명 : 한세대학교 개인정보 영향평가 사업

○ 사업기간 : 계약일로부터 40일

○ 주요 과업내용

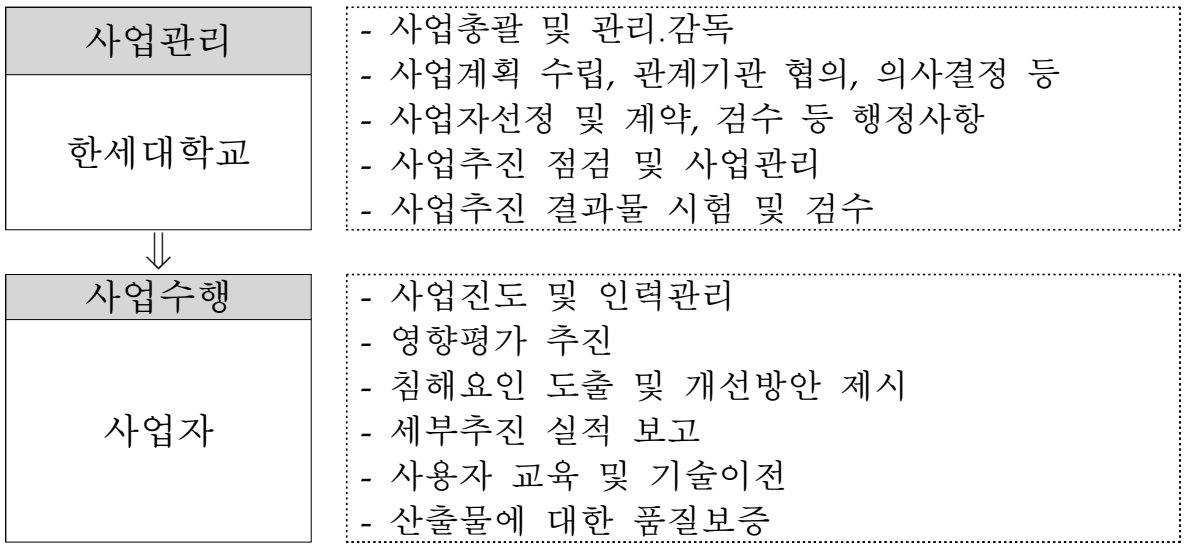
- 입시/학사행정업무시스템에 대한 개인정보 영향평가
- 개인정보처리부서에 대한 개인정보보호 조치
- 대학 개인정보보호 관리체계 현행화
- 각종 정책, 지침, 절차 및 제반 서식의 현행화
- 교육훈련(전 교직원에 대한 개인정보보호 인식제고)

○ 소요예산 : 19,800,000원(부가세 포함)

○ 수행기준 : 개인정보영향평가 수행안내서

3. 추진체계

○ 한세대학교 개인정보 영향평가 추진체계



○ 추진체계별 역할

구 분	주요 역할
개인정보보호책임자	- 개인정보영향평가 총괄 - 사업계획 및 지원예산 검토. 확정 - 평가기관의 지정 및 감독
개인정보보호담당자	- 사업자 선정 등 계약체결 지원 - 사업수행관리, 사업감리, 검사 참여, 사업비 집행 등 - 사업 기본계획 수립 및 제안요청서 작성
분야별책임자	- 사업관리, 요구사항 제시 및 검사 - 결과물 인수 및 사후관리
영상정보기기책임자	- 영상정보기기의 운용 및 관리 방안 검토
평가기관	- 사업추진에 따른 계약 이행 - 개인정보 관련 교육 및 기술 이전 등

4. 기대효과

○ 개인정보보호법에서 요구하는 ①개인정보보호 조직 및 역할의 명확화로 책임의식 고취, ②개인정보 생명주기 프로세스의 준수, ③개인정보의 안정성 확보조치 준수, ④개인정보의 침해 예방으로 대학의 개인정보보호체계 확립

○ 대학이 보유하고 있는 정보보호 관련 정책, 규정, 절차 및 제반 서식을 정비하여 업무처리절차의 명확화 및 간소화

○ 행정자치부와 교육부 등 각종 실태 점검에 효과적 대응

○ 개인정보보호를 위한 각종 H/W, S/W, N/W 등 중복 투자 방지로 예산 절감에 기여

Ⅱ 과업지시 사항

1. 개인정보 영향평가 점검 내용

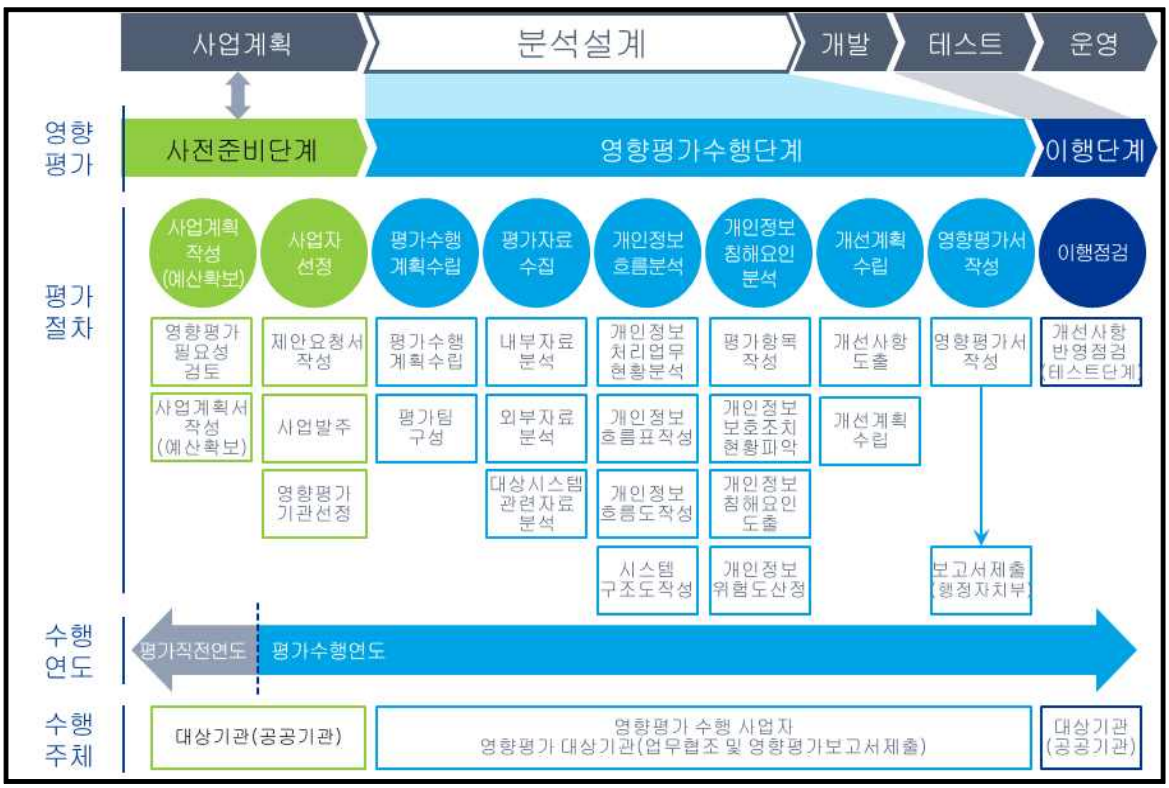
가. 점검 영역

1. 대상기관 개인정보보호 관리체계의 적정성
2. 대상시스템 개인정보보호 관리체계의 적정성 점검
3. 개인정보 처리단계별 관리적·기술적 보호조치의 적정성 점검
4. 특정 IT기술 활용 시 개인정보보호의 적정성 점검
5. 점검 결과에 따른 개선방안 마련 및 후속조치 컨설팅

나. 점검 방법 및 절차

1. 개인정보 영향평가 수행 안내서에 따라 실태점검 수행
2. 전문인력 투입(책임자는 고급기술자 등급 이상인 자이어야 함)

다. 점검 수행절차



라. 점검영역별 평가분야

평가영역	평가분야	세부분야
Ⅰ. 대상 기관 개인정 보보호 관리체계	1. 개인정보보호 조직	개인정보보호책임자의 지정
		개인정보보호책임자 역할수행
	2. 개인정보보호 계획	내부관리계획 수립
		개인정보보호 연간계획 수립
	3. 개인정보 침해대응	침해사고 신고 방법 안내
		유출사고 대응
	4.정보주체권리보장	정보주체 권리보장 절차 수립
		정보주체 권리보장 방법 안내
Ⅱ. 대상시스템의 개인정보보호 관리체계	5.개인정보취급자 관리	개인정보취급자 지정
		개인정보취급자 관리·감독
	6. 개인정보파일 관리	개인정보파일대장 관리
		개인정보파일 등록
	7. 개인정보처리방침	개인정보처리방침의 공개
		개인정보처리방침의 작성
Ⅲ. 개인정보처리 단계별 보호 조치	8. 수집	개인정보 수집의 적합성
		동의 받는 방법의 적절성
	9. 보유	보유기간 산정
	10.이용·제공	개인정보 제공의 적합성
		목적 외 이용·제공 제한
		제공시 안전성 확보
	11. 위탁	위탁사실 공개
		위탁 계약
		수탁사 관리·감독
	12. 파기	파기 계획 수립
		분리보관 계획 수립
		파기대장 작성
Ⅳ. 대상시스템의 기술적 보호 조치	13. 접근권한 관리	계정 관리
		인증 관리
		권한 관리
	14. 접근통제	접근통제 조치

평가영역	평가분야	세부분야
		인터넷 홈페이지 보호조치
		업무용 모바일기기 보호조치
	15. 개인정보의 암호화	저장시 암호화
		전송시 암호화
	16. 접속기록의 보관 및 점검	접속기록 보관
		접속기록 점검
		접속기록 보관 및 백업
	17. 악성프로그램 등 방지	백신 설치 및 운영
		보안업데이트 적용
	18. 물리적 접근방지	출입통제 절차 수립
		반출·입 통제 절차 수립
	19. 개인정보의 파기	안전한 파기
	20. 기타 기술적 보호조치	개발 환경 통제
		개인정보처리화면 보안
		출력시 보호조치
	21.개인정보처리구역보호	보호구역지정
V. 특정 IT기술 활용 시 개인정보보호	22. CCTV	CCTV 설치시 의견수렴
		CCTV 설치 안내
		CCTV 사용 제한
		CCTV 설치 및 관리에 대한 위탁
	23. RFID	RFID 이용자 안내
		RFID 태그부착 및 제거
	24. 바이오정보	원본정보 보관시 보호조치
	25. 위치정보	개인위치정보 수집 동의
		개인위치정보 제공시 안내사항

2. 주요 과업 요건

가. 교육부 개인정보보호 지침 가이드 지원

나. 개인정보 보호법 기반의 법적 요구사항 및 물적·인적자원 현황 분석

다. 개정 개인정보보호법에 따른 대학 개인정보보호 지침 및 제규정 검토 및 현행화(주민등록번호 수집 금지 등 반영)

라. 대학 조직 변화에 따른 개인정보 관리체계 변경 사항 반영

마. 최근 개인정보 침해 동향 반영한 제 지침 검토 및 현행화

바. 내부자, 외부인력에 의한 개인정보 유출 방지 방안 검토 등

사. 정보주체의 개인정보파일 등 개인정보 자산식별 및 중요도 평가

아. 개인정보 흐름분석을 통한 위험분석 및 보호대책 수립

자. 진단결과를 토대로 종합적인 개인정보 보호 관리체계 및 이행과제 도출

차. 개인정보 보호 관련 정책, 지침, 절차서, 매뉴얼 등 관련 규정에 대한 분석 및 제·개정(안) 수립

3. 산출물 및 제출시기

구분	산출물	제출시기	제출수량	비 고
공통	사업수행계획서	계약체결 후 10일 이내	1부	
실태점검	영향평가보고서	영향평가 완료 후 5일 이내	3부	입시,학사행정업무시스템
	실태점검보고서	실태점검 완료 후 5일 이내	3부	개인정보처리부서
	개인정보보호 업무절차서	실태점검 완료 후 5일 이내	10부	대학의 개인정보보호를 위한 업무 절차

※ 산출물 제출 시기는 평가기관과 협의하여 조정할 수 있음

[붙임 1]

외주용역사업 보안특약 조항

① 평가기관은 한세대학교의 보안정책을 위반하였을 경우 [별표1]의 위규처리 기준에 따라 위규자 및 관리자를 행정조치하고 [별표2]의 보안위약금을 한세대학교에 납부한다.

② 사업자는 사업수행에 사용되는 문서, 인원, 장비 등에 대하여 물리적, 관리적, 기술적 보안대책 및 [별표3]의 '누출금지 대상정보'에 대한 보안관리 계획을 사업수행계획서에 기재하여야 하며, 해당 정보 누출 시 한세대학교는 「국가를 당사자로 하는 계약에 관한 법률 시행령 제76조」에 따라 사업자를 부정당업체로 등록한다.

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

④ 사업자는 사업 최종 산출물에 대해 정보보안전문가 또는 전문보안점검도구를 활용하여 보안 취약점을 점검, 도출된 취약점에 대한 개선을 완료 하고 그 결과를 제출해야 한다.

[별표1] 사업자 보안위규 처리기준
[별표2] 보안위약금 부과기준
[별표3] 누출금지 대상정보

[별표1]

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 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 특별보안교육 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 특별보안교육실시

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 특별보안교육 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

[별표2]

보안 위약금 부과 기준

1. 위규 수준별로 A~D 등급으로 차등 부과

구분	위규 수준			
	A급	B급	C급	D급
위규	심각 1건	중대 1건	보통 2건 이상	경미 3건 이상
위약금 비중	부정당업자 등록	총사업비의 5%	총사업비의 2.5%	총사업비의 0.25%

* 위규 수준은 [사업자 보안위규 처리기준] 참고
* 위약금은 사업규모를 감안해서 책정

2. 보안위약금은 다른 요인에 의해 상쇄, 삭감이 되지 않도록 부과
   * 보안사고는 1회의 사고만으로도 그 파급력이 큰 것을 감안하여 타항목과 별도 부과

3. 사업 종료시 지출금액 조정을 통해 위약금 정산

[별표3]

누출금지 대상정보

1. 기관 소유 정보시스템의 내·외부 IP주소 현황
2. 세부 정보시스템 구성현황 및 정보통신망 구성도
3. 사용자계정·비밀번호 등 정보시스템 접근권한 정보
4. 정보통신망 취약점 분석·평가 결과물
5. 용역사업 결과물 및 프로그램 소스코드
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」 제9조제1항에 따라 비공개 대상 정보로 분류된 기관의 내부문서
9. 「개인정보보호법」 제2조제1호의 개인정보
10. 「보안업무규정」 제4조의 비밀 및 동 시행규칙 제16조제3항의 대외비
11. 그 밖에 각급기관의 장이 공개가 불가하다고 판단한 자료

[붙임 2]

비 밀 유 지 계 약 서

제1조 【목 적】

본 계약서는 한세대학교(이하 “갑”이라 한다)이 _____용역사업에 투입되는 자료·장비 등에 대해 보안의 범위·책임을 명확히 하기 위하여 준수하여야 할 비밀유지조건에 합의하였음을 확인하기 위한 계약서이다.

용역사업자(이하 “을”이라 한다)등은 용역사업 수행 중 업무에 관련된 정보나 자료를 제공받기에 앞서서 향후 제공될 정보나 자료를 아래에서 약정한 조건에 따라 비밀을 유지/준수하기로 한다.

제2조 【정보의 사용용도 제한】

“갑”의 모든 정보나 자료는 “용역사업 수행 목적에만 사용되어야 하며 “을”은 누출금지 대상정보에 대한 비밀유지 의무를 성실히 이행하여야 한다. 또한 ‘을’은 누출금지 대상정보의 사용허가를 얻지 아니한 자에게 정보를 제공하거나 목적이외의 용도로 사용해서는 안 된다.

제3조 【제한되는 정보의 범위 및 보안준수 사항】

“을”이 용역사업과 관련하여 비밀유지를 위해 제한되는 누출금지 대상정보와 지켜야할 보안준수 사항은 다음과 같다.

누출금지 대상정보(비밀정보 대상)

1. 한세대학교 _____용역 관련 열람되는 제반 정보
2. 한세대학교 _____용역관련 전산장비, 통신장비, 백업 장비, 보안장비 등 관련 장비 현황
3. 용역사업 결과물
4. 기관 소유 정보시스템의 내·외부 IP주소 현황
5. 세부 정보시스템 구성 현황 및 정보통신망 구성도
6. 사용자계정·비밀번호 등 정보시스템 접근권한 정보
7. 「공공기관의 정보공개에 관한 법률」 제9조 1항에 따라 비공개 대상 정보로 분류된 기관의 내부문서
8. 「개인정보보호법」 제2조 1호의 개인정보
9. 보안업무규정 제4조의 비밀 및 동 시행규칙 제16조 제3항의 대외비
10. 그 밖에 한세대학교에서 공개가 불가하다고 판단한 자료

보안준수 사항

1. 참여인원 보안 준수사항
○ 용역사업 참여인원은 '정보노출' 금지조항 및 개인의 친필 서명이 들어간 보안서약서 제출
○ 용역사업 수행 전 참여인원에 대해 법적 또는 한세대학교 규정에 따른 비밀유지 의무 준수 및 위반 시 처벌내용 등에 대한 보안교육 이행
○ 누출금지 대상 정보의 외부 누출 금지
○ 비밀관련 사업을 수행할 경우 비밀취급인가 취득
○ 사진촬영금지

2. 자료에 대한 보안 준수사항
○ 계약서 등에 명시한 누출금지 대상정보가 필요할 경우 자료관리 대장을 작성, 인계자·인수자가 직접 서명한 후 수령하고 사업완료시 관련자료 반납
○ 용역사업 관련자료 및 사업과정에서 생산된 모든 산출물은 한세대학교의 파일 서버에 저장하거나 보안담당관이 지정한 PC에 저장·관리
○ 용역사업 관련 자료는 인터넷 웹하드·P2P 등 인터넷 자료공유사이트 및 개인 메일함에 저장을 금지하고 용역 발주기관과 용역업체간 전자우편을 이용해 자료 전송이 필요한 경우에는 자체 전자우편을 이용, 첨부자료 암호화 후 수발신
※ 대외비 이상의 비밀은 전자우편으로 송수신 금지
○ 한세대학교에서 제공한 사무실에서 업체가 용역사업을 수행할 경우 제공한 비공개 자료는 매일 퇴근시 반납토록 하며 비밀문서를 제외한 일반문서는 용역업체에 제공된 사무실에 시건장치가 된 보관함이 있을 경우 이에 보관가능
○ 용역사업 수행으로 생산되는 산출물 및 기록은 보안담당관이 인가하지 않은 비인가자에게 제공·대여·열람을 금지

3. 사무실·장비에 대한 보안준수 사항
○ 용역사업 수행장소는 한세대학교 시건장치와 통제가 가능한 공간을 이용하거나 CCTV·시건장치 등 비인가자 출입통제 대책이 마련된 관제센터 사용
○ 한세대학교 내부에서 용역사업을 수행할 경우 용역 참여직원은 노트북 등 관련 장비를 외부에 반출·입 금지 여부 확인
○ 인가받지 않은 USB메모리 등의 휴대용 저장매체 사용을 금지하며 산출물 저장을 위하여 휴대용 저장매체가 필요한 경우 보안담당관의 승인 하에 사용

4. 내·외부망 접근 시 보안준수 사항
○ 용역업체 사용전산망은 업무망과 분리구성하고 필요한 서버에만 제한적 접근허용
○ 용역업체에서 사용하는 PC는 인터넷 연결을 금지하며, 사업수행상 연결이 필요한 경우에는 보안담당관의 보안 통제하에 제한적 허용

5. 용역사업완료 후 준수 사항
○ 제공받은 자료, 장비와 중간·최종 산출물 등 용역사업과 관련된 제반자료 전량 반환하고 복사본 등 별도 보관 금지
○ 업체 소유 PC·서버의 하드디스크·휴대용 저장매체 등 전자기록 저장매체는 국가정보원장이 안전성을 검증한 삭제 S/W로 완전 삭제 후 반출
○ 용역사업 관련자료 회수 및 삭제조치 후 복사본 등 용역사업관련 자료를 보유하고 있지 않다는 대표 명의 확약서 제출

제4조 【정보의 회수】

"을"은 용역사업 완료 시 이미 제공된 정보나 자료의 사본을 남기지 않고 모두 "갑"에게 돌려주기로 한다. "을"이나 관련 당사자들이 이미 제공된 정보를 이용하여 작성한 분석 자료나 보고서 등 기타 어떠한 자료도 모두 반환 및 폐기처분하여야 하며, 사본 등 용역사업관련 자료를 보유하고 있지 않다는 대표 명의의 보안확약서를 제출해야 한다.

제6조 【손해배상】

"을"이 위 사항을 위반하여 "갑" 에 손해를 끼친 경우는 "을"은 그 모든 손해의 배상을 책임진다.

20 년 월 일

(갑) 한세대학교 (인)

(을) 대표이사 (인)

[붙임 3]

보안 서약서

본인은 _____년 __월 __일부로 한세대학교의 다음 사업을 수행함에 있어 아래 사항을 준수할 것을 엄숙히 서약합니다.

사 업 명 : _____
사업기간 : _____

- 아 래 -

1. 본인은 한세대학교 업무 중 알게 될 일체의 내용이 직무상 기밀 사항임을 인정한다.

2. 본인은 이 기밀을 누설함이 국가안전보장 및 국가이익에 위해가 될 수 있음을 인식하여 업무수행 중 지득한 제반 기밀사항을 일체 누설하거나 공개하지 아니한다.

3. 본인이 이 기밀을 누설하거나 관계 규정을 위반한 때에는 관련 법령 및 계약에 따라 어떠한 처벌 및 불이익도 감수한다.

4. 본인은 사업수행 시 반입한 저장장치 반출 시 미디어 소거 후 폐기처분(하드디스크 등 자기장 처리로 사용불가)에 동의한다.

5. 본인은 업무를 함에 있어, 발생하는 위반사항에 대하여 모든 책임을 부담한다.

____년 __월 __일

서 약 자 (근무자)
업 체 명 :
직 위 :
성 명 : (서명)

[붙임 4]

보안 확약서

본인은 귀 기관과 계약한 _____ 사업의 수행을 완료함에 있어, 다음 각 호의 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 보안확약서를 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

소 속 : _____

직 급 : _____

성 명 : _____

한세대학교 총장 귀하