제 안 요 청 서

사 업 명	천안캠퍼스 전산자원 통합 유지보수

2022. 1.

상 명 대 학 교
(교육지원팀)

상명대학교
SANGMYUNG UNIVERSITY

Ⅰ. 일반사항

1. 목적

본 제안요청서는 상명대학교 천안캠퍼스 교육지원팀에서 운영중인 전산자원(네트워크 시스템, 보안시스템 등)에 대한 상명대학교와 유지보수업체간의 유지보수 조건 및 지원사항에 있어 이행되어야 하는 세부 내용을 규정하는데 있다.

2. 사업명

천안캠퍼스 전산자원 통합 유지보수

3. 사업장위치

충남 천안시 동남구 상명대길 31 상명대학교 교육지원팀
문의처 : (041)550-5078, 5480

4. 유지보수 기간

총 유지보수기간: 2022.3.1. ~ 2024.2.29.
1차년도: 2022.3.1. ~ 2023.2.28.(1년)
2차년도: 2023.3.1. ~ 2024.2.29.(1년)
*** 입찰금액은 다년 기본계약 체결 후 년차 별 월지급 금액 협의 (각 차년도 동일금액)**

5. 입찰 참가자격

입찰공고 참조

6. 유지보수대상

"Ⅲ.유지보수대상 내역" 참조

Ⅱ. 제안요청사항

1. 유지보수대상

1) 장비개요

- 위치 : 충남 천안시 동남구 상명대길 31 상명대학교 C305 교육지원팀
- 주요 장비현황("Ⅲ. 유지보수대상 내역" 참조)
  - 유·무선 네트워크 시스템 및 보안시스템 장비 등

2. 유지보수내용

1) 네트워크 시스템 및 보안 시스템

- 유지보수 용역의 총괄 및 장애 신속 처리를 위하여 상주인력 1인을 본 사업기간 동안 교육지원팀 내 상주시켜야 한다.
- 월 1회 이상의 정기점검 및 수시점검을 실시하고 장애 발생 원인을 사전에 제거하여 대상시스템에 대한 안정화를 지원 한다.
- 장애 발생 즉시 필요한 조치 완료 및 안정적 운영을 위한 관리지원 수행
- 장애 발생 시 원인규명과 장애처리 결과에 대하여 보고하여야 한다.
- 장애를 포함한 긴급 요청 시 2시간 이내 조치를 시작하고 이후 4시간 이내에 조치 완료.
- 네트워크 보안장비의 원활한 운영을 위하여 운영 교육을 실시할 수 있다.
- 부품장애 발생 시 무상으로 교체를 유지보수 업체에서 실시한다.
- 장애발생으로 인하여 48시간이상 제품 수리 시 대체장비 설치
- 운영지원 용역의 대상 시스템에 대한 관리지원 및 장애 이력관리 산출물 제출
- 보안시스템을 활용하여 보안 상태를 수시 점검
- 최신 보안 취약점에 대한 자료를 수집하고 관리대상 시스템에 대한 취약점 보안을 하여야 한다.
- 운영 소프트웨어에 대한 가동상태를 점검하고 패치 및 업그레이드를 통하여 최적의 상태를 유지
- 시스템 업그레이드 시 적용 전 사전 연동 테스트를 통하여 작동의 이상 여부 검토
- 정기점검
  - "Ⅲ. 유지보수대상 내역" 참조

2) 네트워크 상주기술지원

- 상주 인력은 CCNA(네트워크관련)와 정보처리기사자격증 이상 소지자의 전문 인력으로 네트워크 및 보안장비에 대한 운영 및 유지관리를 지원하며, 네트워크에 의한 사용자 장애나 보안장비에 의한 사용자 장애 시 본교 내의 사용자를 방문하여 문제 해결을 위한 기술지원 등의 본교 담당자에 대한 보조적인 업무 수행을 지원해야 한다.
- 상주 인력은 주5일 본교 직원과 동일한 출퇴근 시간 근무를 기준으로 하고,

상주 인력은 유지보수 계약기간 중에 업체 임의로 교체할 수 없다. 단, 본교 동의(또는 요청)시 기존 상주인력 이상의 전문 인력으로 변경이 가능하다.

3) 기타사항

- 전산시스템(네트워크장비, 보안장비 등) 유지보수를 위한 필요 보안설정사항 유지 및 보안정책 적용 지원
- 창구의 전화지원 서비스 지원
- 해당 유지보수 대상장비는 예방정비 및 프로그램 PATCH 지원
- 시스템 회복지원과 장애해결 및 분석지원
- 기타 전산시스템 운영을 위한 각종 업무지원
- 유지정비보수의 시간은 본교의 근무시간으로 한다.
- 긴급을 요하는 장애 발생시에는 야간 및 공휴일도 지원하여야 한다.

3. 유의사항

1) 용역 수행은 상기에 제시된 요청사항을 충실히 수행하여야 하며 보다 우수한 용역수행을 위하여 조건의 변경이 필요한 경우 본교 교육지원팀 담당자와 협의 후 수행할 수 있으며 내용에는 제한을 두지 않는다.
2) 본 사업 수행 중 장비나 부품 변경이 필요한 경우 본교의 담당자에게 변경물품에 대한 기술적 타당성을 검증 받아야 한다.
3) 변경으로 인하여 발생할 수 있는 추가 비용은 인정되지 않는다.
4) 유지보수 대상 장비가 시스템 교체 등의 사유로 인하여 제외 또는 증가될 경우 상호 협의에 따라 유지보수 대상품목을 조정하며 그 금액만큼 유지보수비용에서 증감을 조정 한다.
5) 용역 계약 체결 일 이전이라도 수주 기업은 본교의 장애 발생 시 적극적으로 지원하여야 하며, 엔지니어 사전 투입 등과 관련된 제반 비용은 수주 기업이 부담을 한다.

Ⅲ. 유지보수 대상 내역

1. 네트워크 및 보안장비

번호	대상품목	규격	수량	유지보수 기간	지원사항
1	Extreme Switch	Work-Group Switch		22.03.01. ~ 24.02.29.	기술지원 유지보수
		SummitX250-48 10/100BASE-TX, 2 gigabit combo ports	6		
		SummitX250-24 10/100BASE-TX, 2 gigabit combo ports	10		
		Summit200-24 Switch	8		
2	Dell-Force Switch	무선Lan Backbone			H/W RMA 및 점검
		CH-C150-BNA2	1		
		Work-Group Switch			
		S25-01-GE-24T10/100/1000Base-T,SFP-Mini Gbic4port	8		
3	CISCO Switch	유선Lan Backbone			H/W RMA 및 점검
		Nexus 9504	1		
		비공개용 10G스위치			
		Cisco N9K-C9372TX	1		
		무선Lan Controller			
		WLC-C5508-250-K9	1		
		무선Lan AP			기술지원 유지보수
		AP 1262N-K-K9 (실외 AP)	13		
		AP 1142N-K-K9 (실내 AP)	183		
		AP 16021I-K-K9 (실내 AP)	32		
		AP 2802I-K-K9 (실내 AP)	6		
		무선랜 PoE Switch			H/W RMA 및 점검
		WS-C2960S-24PS-L	5		
		무선Lan NMS Switch			기술지원 유지보수
		WCS-Standard-K9+WCS-APBASE-100	1		
		유선 Metro Switch			H/W RMA 및 점검
		WS-C3650-24TS-E Catalyst 3650 24 Port	1		
		DMZ 구간 Switch			
		Cisco WS-C3850-48T-S Catalyst 3850 48 Port Data IP Base	1		
		WS-C3560X-48T-S Catalyst 3560X 48Port Data IP Base	1		
		WS-C3560X-24T-L Catalyst 3560X 24Port Data LAN Base	1		
		WS-C2960S-24TS-L Catalyst 2960S 24 GigE, 4xSFP LAN Base	1		
		WS-C2960X24TS-L Catalyst 2960X 24Port Data LAN Base	1		
		Work-Group Switch			
		C9200L-24T-4X-E	10		
		WS-C4500X-24X-IPB	1		
		WS-C2950G-24-EI	1		기술지원 유지보수
		WS-C2960G-24TC-L	1		
		WS-C2960X-24TS-LL	13		H/W RMA 및 점검
		WS-C2960X-48TD-L	16		
		Catalyst 2960 24 10/100 + 2 1000BT LAN Base Image	8		기술지원 유지보수

번호	대상품목	규격	수량	유지보수 기간	지원사항
4	Juniper Switch	LAN Switch		22.03.01. ~ 24.02.29.	기술지원 유지보수
		24-Port L2 Switch(EX2200-24T-4G)	125		
		24-Port L2 Switch(EX2300-24T-4SFP+)	21		
		48-Port L2 Switch(EX2300-48T-4SFP+)	20		
		무선랜 PoE Switch			H/W RMA 및 점검
		EX2300-24P	16		
		EX2300-48P	3		
5	Extreme 무선랜	무선랜 Manager			H/W RMA 및 점검
		Aerohive Manager(AH-HM-1U)	1		
		무선랜 AP			기술지원 유지보수
		AP 230 (실내 AP)	87		
		AP 250 (실내 AP)	30		
		AP 550 (실내 AP)	5		
		AP 1130(실외 AP)	1		
6	무선Lan 인증	Anyclick AUS ENT3	1		H/W RMA 및 점검
	PC 개인정보	Privacy-I, 150User	1		S/W 점검
	침입탐지 차단	SSG500M/ISG-1000/ISG-2000(방화벽)	3		기술지원 유지보수
	차세대방화벽	차세대방화벽 - SECUI MF2 3100[10G_IPS_DDoS_IPSec모듈포함]	1		H/W RMA 및 점검
	침입탐지 방지	Sniper IPS V7.0.e NE4000	1		기술지원 유지보수
	유해사이트 차단	Webkeeper V10.1	1		H/W RMA 및 점검
	보안 DNS	TE-1410-NS1-AC DNS	1		기술지원 유지보수
	IP 관리시스템	IPScan Probe 600X+/NAC 1000+	1		H/W RMA 및 점검
7	상주지원	네트워크 관리 인력 상주 1명	1		네트워크 점검&장애 상주지원

【붙임】

외주 용역사업 보안특약 조항

① 사업자는 상명대학교의 보안정책을 위반하였을 경우 [별표1]의 위규 처리기준에 따라 위규자 및 관리자를 행정조치하고 [별표2]의 보안 위약금을 상명대학교에 납부한다.

② 사업자는 사업 수행에 사용되는 문서, 인원, 장비 등에 대하여 물리적, 관리적, 기술적 보안대책 및 [별표3]의 '누출금지 대상정보'에 대한 보안관리 계획을 사업제안서에 기재하여야 하며, 해당 정보 누출 시 상명대학교는「국가계약법」시행령 제76조에 따라 사업자를 부정당업체로 등록하고 입찰 참가자격을 제한한다.

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

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

[별표 1] 사업자 보안위약 처리기준
[별표 2] 보안 위약금 부과 기준
[별표 3] 누출금지 대상정보
[별표 4] 보안관리 세부 이행사항

【별표 1】

사업자 보안위약 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
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 연결사용 사. 보안관련 프로그램 강제 삭제 아. 사용자 계정관리 미흡 및 오남용(시스템 불법접근 시도 등)	

구 분	위 규 사 항	처 리 기 준
보 통	1. 기관 제공 중요정책·민감 자료 관리 소홀 가. 주요 현안·보고 자료를 책상 위 등에 방치 나. 정책·현안자료를 휴지통·폐지함 등에 유기 또는 이면지 활용 2. 사무실 보안관리 부실 가. 캐비닛·서류함·책상 등을 개방한 채 퇴근 나. 출입키를 책상 위 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 모니터 옆 등 외부에 노출 바. 비인가 보조기억매체 무단 사용	○ 위규자 교체 ○ 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

【별표 2】

보안 위약금 부과 기준

1. 위규 수준별로 A~D 등급으로 차등 부과

구분	위규 수준			
	A급(심각)	B급(중대)	C급(보통)	D급(경미)
위규	심각 1건	중대 1건	보통 2건 이상	경미 3건 이상
위약금 비중	부정당업자 등록	계약금액의 2%	계약금액의 1%	계약금액의 0.5%

* 위규 수준은 [별표1] 참고

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

* 보안사고는 1회의 사고만으로도 그 파급력이 큰 것을 감안하여 타 항목과 별도 부과

3. 사업 종료 시 지출금액 조정을 통해 위약금 정산

【별표 3】

누출금지 정보

<교육부 정보보안 기본지침 제13조 제2항>

1. 해당 기관의 정보시스템 내·외부 IP 주소 현황
2. 정보시스템 구성현황 및 정보통신망 구성도
3. 개별사용자의 계정·비밀번호 등 정보시스템 접근권한 정보
4. 정보통신망 또는 정보시스템 취약점 분석·평가 결과물
5. 정보화용역사업 용역 결과물 및 관련 프로그램 소스코드(외부에 유출될 경우 국가안보 및 국익에 피해가 우려되는 중요 용역사업에 해당)
6. 암호자재 및 정보보호시스템 도입·운용 현황
7. 정보보호시스템 및 네트워크 장비 설정 정보
8. 「공공기관의 정보공개에 관한 법률」제9조 제1항에 따라 비공개 대상 정보로 분류된 기관의 내부문서
9. 「개인정보보호법」제2조 제1호에 따른 개인정보
10. 「보안업무규정」제4조에 따른 비밀 및 동규정 시행규칙 제16조 제3항에 따른 대외비
11. 그 밖에 해당기관의 장이 공개가 불가하다고 판단한 자료
    1) 계약서상에 상호 비밀 보장에 관련된 내용 명시
    2) 출력물에 대해서는 이면지 사용불가 및 분쇄기 사용 파쇄
    3) E-mail을 통한 인터넷 정보유출 방지

【별표 4】

보안관리 세부 이행사항

❑ **참여 인력에 대한 보안관리**

① 사업 착수 시

- 사업 참여인원 및 업체 대표명의 **보안서약서**를 제출하여야 한다.
- 계약업체는 용역사업 수행 전 참여인원에 대해 법률 또는 보안규정, 지침에 의한 비밀유지의무 준수 및 위반 시 처벌내용 등에 대한 보안교육을 실시하여야 한다.

② 사업 수행 시

- 계약업체는 보안인식강화를 위해 주기적으로 자체 보안교육을 실시해야 하며, 대학이 요구하는 보안교육에 참석하여야 한다.
- 사업 참여인원은 용역사업자가 임의로 교체할 수 없으며, 부득이한 사유로 교체하여야 하는 경우(해외여행 포함) 발생 시 교육지원팀에 즉시 보고
- 용역사업과 관련한 보안관리 책임은 용역업체 대표에게 있으며, 대표는 용역사업 전반의 보안업무를 수행하는 '보안관리책임자'를 지정
  - ■ 보안관리책임자는 용역사업과 관련된 인원.장비.자료에 대한 보안업무 및 사업과 관련된 하도급업체의 보안관리 전반을 총괄

③ 사업 종료 시

- 계약업체는 대학으로부터 제공받는 장비, 서류 및 중간.최종산출물 등 모든 자료를 전량 대학에 반납하고 삭제하여야 한다.
  - ■ 복사본 등 별도 보관 금지
- 노트북.보조기억매체 등 전자적으로 기록된 자료는 「교육부 정보보안 기본지침」제39조 제4항의 규정에 의한 '정보시스템 저장매체 불용처리 지침'에 의한 저장매체·자료별 삭제방법에 따라 삭제 후 반출
- 계약업체는 사업관련 자료를 보유하고 있지 않으며 이를 위반시 향후 법적 책임이 있음을 포함한 "**대표자용 보안확약서**" 및 "**참여자용 보안확약서**"를 작성하여 상명대학교에 제출하여야 한다.

❑ 문서 및 전산자료에 대한 보안관리

① 보안업무규정시행세칙에 의거 정보통신망 구성도, 정보시스템 구성도, IP 현황, 용역사업 산출물 및 개인정보 등은 비밀, 대외비 또는 비공개 자료로 분류하여 관리해야 한다.

② 계약업체는 비공개자료 중 출력물 형태로 제공받는 자료에 대해서는 '제공자료(정보) 관리대장'을 작성하여 인계자(발주부서 담당자)와 인수자(용역업체 보안관리책임자)가 직접 서명한 후 인계·인수해야 한다.

③ 발주부서가 계약업체에 제공한 내부 자료는 복사·외부반출을 금지하며, 내부자료 중 비공개 자료는 매일 퇴근 시 발주부서에 반납토록 하며, 비밀문서를 제외한 일반문서는 시건장치가 된 보관함에 보관하여야 한다.

④ 용역사업 관련자료 및 사업과정에서 생산된 모든 산출물은 발주 부서의 파일서버에 저장하거나 발주부서 담당자가 지정한 PC에 저장·관리하여야 한다.

⑤ 계약업체가 업무상 필요에 의해 부득이하게 외부에서 전자우편 등으로 대학과 자료 송수신이 필요한 경우에는 암호화 등의 보안대책을 마련하여 수발신해야 한다.
다만, 대학 보안업무규정에 의한 비공개 자료, 대외비 자료 및 비밀자료는 전자우편으로 수·발신을 금지한다.

⑥ 계약업체는 인터넷 이용 시 접속이 제한된 사이트 및 인터넷 파일공유(P2P)사이트 등에 접속을 시도하여서는 아니 되며, 사업수행 관련 자료는 인터넷, 웹하드 등 인터넷 자료공유사이트 및 개인 메일함에 저장을 금지한다.

⑦ 사업수행으로 생산되는 산출물 및 기록은 발주부서장의 허가 없이 무단 제공·대여·열람을 금지한다.

❑ 사무실 및 장비에 대한 보안관리

① 용역사업 수행 장소는 시건 장치와 통제가 가능한 사무실을 사용한다.

② 발주부서 담당자는 용역업체 사무실에 대한 정기적인 보안점검을 실시하여야 한다.

③ 반입된 노트북·PC는 사업 종료시까지 반출 금지하며, 다만 부득이하게 외부 반출이 필요한 경우에는 최소한의 장비만 반출승인하고 자료유출에 대비한 발부부서 담당자의 보안조치를 실한 후 반출하여야 한다.

④ 계약업체는 용역사업에 이용되는 노트북·PC에 백신 등의 자체 PC보안프로그램 및 대학에서 제공하는 자료유출방지 등을 위한 PC보안프로그램을 설치하여야 한다.

⑤ 계약업체는 노트북 및 PC에 전원기동(CMOS) 패스워드, 윈도우 로그인 패스워드, 화면 보호기(10분 간격) 패스워드를 영문자 및 숫자가 조합된 9글자이상으로 설정하여야 한다.

❑ 내·외부망 접근시 보안관리

① 용역사업 수행시 발주기관의 전산망 이용이 필요한 경우
- 사업 참여인원에 대한 사용자 계정(ID)은 하나의 그룹으로 등록하고 계정별로 정보시스템 접근권한을 부여한다.
- 계정별로 부여된 접속권한은 불 필요시 곧바로 권한을 해지하거나 계정 폐기
- 계약업체는 정보시스템 사용자 계정(ID) 이용시, 부여된 권한 이외의 접근을 하여서는 아니되며, 부여된 패스워드는 임의 변경 및 타인에게 알려서는 아니된다.
- 발주기관의 전산망을 사용하는 계약업체의 노트북·PC는 인터넷 연결을 금지한다. 다만, 사업 수행 상 필요한 경우에는 계약업체의 보안관리책임자가 직접 요청하고, 발주부서 담당자는 필요성이 인정될 경우 특정 노트북·PC을 지정하고 정보시스템실의 보안담당자에게 필요한 사이트만 접속토록 요청하여야 한다.

② 시스템 유지보수 및 관제는 원격관리를 금지한다.

□ **보조기억매체 제한**

○ 계약업체는 USB 등 이동식 보조기억매체를 대학 내외로 반·출입 할 수 없다. 다만, 분임보안담당관이 그 필요성을 인정한 경우에는 「보안업무규정 등」반·출입 절차에 따라 반·출입 할 수 있다

□ **기타**

○ 상기 내용 중 언급되지 않은 사항은 「보안업무규정」, 「교육부 정보보안 기본지침」,「국가정보보안 기본치침」등 관계법령 및 규정 적용

<서식1>

보안 서약서

(업체 대표자용)

본인은 ____년 __월 __일부로 "천안캠퍼스 전산자원 통합 유지보수" 용역 ____ 관련 사업(업무)을 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 본인은 "천안캠퍼스 전산자원 통합 유지보수" 용역 관련 업무 중 알게 될 일체의 내용이 직무상 기밀 사항임을 인정한다.

2. 본인은 이 기밀을 누설함이 상명대학교에 위해가 될 수 있음을 인식하여 업무 수행 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 하도급업체를 통한 사업 수행시 하도급업체로 인해 발생하는 위반사항에 대하여 모든 책임을 부담한다.

년 월 일

서 약 자 (업체 대표)	업 체 명 :	
	직 위 :	
	성 명 :	(서명)
	생 년 월 일 :	

서약집행자 (담 당 자)	소 속 :	
	직 위 :	
	성 명 :	(서명)

<서식2>

보안 서약서

(업체 직원용)

본인은 ____년 __월 __일부로 "천안캠퍼스 전산자원 통합 유지보수" 용역 ____ 관련 사업(업무)을 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 본인은 "천안캠퍼스 전산자원 통합 유지보수" 용역 관련 업무 중 알게 될 일체의 내용이 직무상 기밀 사항임을 인정한다.

2. 본인은 이 기밀을 누설함이 상명대학교에 위해가 될 수 있음을 인식하여 업무 수행 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.

년 월 일

서 약 자 업 체 명 :
직 위 :
성 명 : (서명)
생 년 월 일 :