『정보통신망 고도화 방화벽 및 무선랜 구축 사업』

과 업 지 시 서

2022. 06

교육지원팀

목 차

정보통신망 고도화 방화벽 및 무선랜 구축 과업 지시서

Ⅰ. 개 요

1. 사 업 명 : 정보통신망 고도화 방화벽 및 무선랜 구축 사업
2. 납품기한 : 계약일로부터 90일
3. 납품 및 설치 장소 : 교육지원팀내 설치장소
4. 주요 내용
   가) 고도화 방화벽 교체 설치 및 정책 이관 작업
   나) 무선랜 시스템(컨트롤러) 업그레이드 구축
   다) 무선랜 시스템(AP_옥외형) 교체 설치
   라) 신규 시스템 연동 작업

Ⅱ. 일반사항

1. 목적

   본 사업은 노후화된 방화벽을 교체하여 보다 안정화 된 보안 상태를 유지하고 확장된 대역폭과 차세대 보안 정책(어플리케이션 제어)의 적용으로 정보통신망을 고도화하여 정보화 시스템의 보안성, 안정성, 신뢰성, 가용성을 확보하기 위함이다. 또한 신규 무선랜 시스템을 업그레이드 구축하여 기존 802.11(a/g/n) 밖에 지원되지 않았던 무선랜 서비스를 802.11ax(Wi-Fi6)가 지원되는 새로운 인프라 서비스를 통해, 보다 확장된 범위와 연결의 안정성, Access point가 밀집된 환경에서 더 많은 Client를 지원할 수 있는 높은 수준의 서비스를 제공함과 동시에 신규 도입 된 시스템의 구축을 통하여 정보통신망의 효율적인 운영을 할 수 있도록 개선한다.

2. 납품조건

   가. 계약자는 납품 시스템 및 부대 장비에 대하여 하드웨어 및 통신망 구성연결 등이 수요자 측의 목적 수행에 지장이 없도록 품질의 신뢰성, 안정성, 시스템 간 호환성 및 연계성을 갖추고 구매 장비 일체를 일괄 납품하여야 한다.

   나. 교체 작업 시 기존 장비는 계약자가 회수하여 교육지원팀에 반납한다.

   다. 시스템의 납품 중 제반 안전사고 및 납품 과정에서 발생하는 행정적, 기술적 제반 비용은 계약자가 부담한다.

3. 구매 및 설치 범위

   본 규격서는 보안 및 네트워크 장비의 설치에 필요한 장비구성 및 운영상 필요로 하는 사항과 기존 시스템과의 연동에 필요한 모든 사항을 포함한다.

   가. 장비 일체의 공급· 설치조립, 장비간 연결, 현장조정, 정책 이관 등

나. 장비 일체의 구축을 위한 제반 사항에 대한 설치

다. 기존 장비 재배치 및 재구성

라. 장비의 운영을 위한 교육 및 기술지원

4. 자격조건

가. 소프트웨어산업진흥법 제24조의 규정에 의한 소프트웨어사업자(컴퓨터관련서비스사업자, 1468)등록업체이며, 정보통신공사업법 제14조에 의한 정보통신공사업(0036) 등록업체

나. 교육 및 공공기관을 대상으로 공고일로부터 3년 내 단일 건 1억원 이상(부가세 포함)의 보안 장비와 네트워크 장비 납품 실적을 제출할 수 있는 업체

다. 안정적인 정책 이관 및 보안장비 구축을 위하여 제조사의 공식 파트너임을 증명하는 서류를 직접 제출할 수 있는 업체(사업명 기재, 입찰 등록 시)

라. 제조사 발행 정품공급확약서 및 기술지원확약서 제출 가능 업체(계약 시 제출)

마. 공동수급 허용되지 않음.

※ 위 각 항목에 해당하는 증빙서류는 입찰 등록 시 첨부하여 제출하여야 한다.
단, 제조사 정품공급 확약서 및 기술지원확약서는 계약 시 제출

5. 사업관리

가. 계약 수행 관리

1) 계약자는 작업내용 및 진행 상황 등을 기록하여 담당자의 승인을 받아야 하며, 특이사항(긴급작업변경 등) 발생 시 지체없이 서면으로 제출해야 한다.

2) 계약자는 참여 인력에 변동이 있을 경우, 사전에 그 변동 사유와 교체 투입인력에 대하여 교육지원팀에 통보하고 승인을 받아야 한다.

3) 교육지원팀은 사업 참여 인력의 자격과 기술 등이 사업 수행에 부적합하다고 판단되는 경우, 일부 교체를 요구할 수 있으며 계약자는 이에 응하여야 한다.

4) 정해진 사업 기간 내 정상적인 과업 수행이 불가능하다고 판단될 경우, 교육지원팀은 인력 추가 투입 등을 요구할 수 있으며, 계약자는 이에 대한 합당한 방안을 제시해야 한다.

5) 계약자는 납품 및 설치하는 물품의 인터페이스 기술 및 어플리케이션은 최종 인계. 인수와 동시에 상명대학교에게 소유권을 이전한다.

6) 작업장소가 필요할 경우 상명대학교와 계약자 간의 상호 협의하여 결정한다.

7) 최소 20일 이상의 기간 동안 기존 보안 장비와 동일하게 운영 구축 후 모니터링을 실시하여 그 결과 값에 따라 최종 적용을 하여야 한다.

나. 책임의 한계

1) 본 사업의 목적달성에 필요한 부품, Cable, 자재 등 제반 비용은 계약자가 부담한다.

2) 계약자는 물품의 납품 및 설치 시 안전관리 및 재해방지에 필요한 안전수칙 준수 및 위험방지대책을 강구하여야 하며, 안전사고 및 재해가 발생 할 경우 모든 책임은 계약자에게 있으며, 계약자는 상명대학교에 민・형사상 책임을 물을 수 없다.

3) 계약자는 과업 수행 중 상명대학교의 자산 손상 및 기타 손실을 끼친 경우, 원상복구 또는 손해배상을 해야 한다.
4) 본 사업 목적에 맞는 요구 성능을 충족하기 위해 계약금액의 10%를 초과하지 않는 범위 내에서 과업 내용이 변경되거나 추가 요구사항이 발생한 경우, 계약자는 별도의 계약변경 없이 이를 수용해야 한다.
5) 본 사업을 수행함에 있어 제3자의 특허권 또는 저작권 침해로 인한 문제 발생 시 이에 대한 모든 책임은 계약자가 진다.
6) 본 시방서에 명시된 사항은 최소한의 사양만을 규정하였으므로 상세히 기술되지 않았거나 누락된 사항은 계약자는 본 사업의 목적달성에 지장이 없도록 현장실사 등 사전에 충분히 검토한 후 사업을 수행하여야 한다.
7) 상명대학교와 계약자 간의 본 규격서에 대한 해석에 차이가 있을 경우에는 관계 법령과 수요기관의 해석에 따른다.
8) 계약자는 [붙임 1] 사업 보안 관리 방안을 준수하여야 하며, 이를 위반할 경우 계약자가 민・형사상 책임을 진다.
9) 본 계약에 관한 소송 관할법원은 상명대학교의 주소지를 관할하는 법원으로 한다.
10) 본 사업 수행과 관련하여 계약서에 명시되지 않은 사항은 상호 합의하여 결정하여야 한다.

6. 무상유지보수

가. 무상 유지보수 기간은 검수일로부터 1년으로 한다. (단, 제조사의 무상 유지보수기간이 상기 기간 이상일 경우에는 제조사의 정책이 우선한다.)

나. 무상 유지보수 기간 내 유지보수 수행내역은 [III. 특수조건 7.유지보수]와 같이 시행하여야 한다.

7. 주요 일정 계획

주 요 사 업 내 용		일 정	비 고
시스템 구축	교체 업체 선정 및 계약	계약 후 15일	상명대학교의 학사, 입시, 행정 일정 등의 사유로 계약자가 제출한 사업수행계획서에 물품의 납품 및 설치 일정을 조정할 수 있다.
	현 시스템 분석 및 교체 세부계획 수립		
	교체 사전 작업(백업) / 광, UTP 케이블 포설		
	방화벽 설치 및 정책 이관 무선 컨트롤러 업그레이드 구축 무선 AP(옥외형) 설치 신규 시스템 연동 작업		
시스템 모니터링	방화벽 시험 운영	구축 완료 후 20일 이내	
	무선랜 서비스 품질 조사		
	신규 시스템 운영 보완 및 품질 개선		
시스템 검수	정보 서비스 정상 가동 완료 및 검수	시스템 서비스 품질 측정 완료 시	

Ⅲ. 특수조건

1. 정의

본 특수조건은 상명대학교 고도화 방화벽 및 무선랜 구축 사업과 관련하여 일반사항에 명시되지 않은 구매조건, 물품의 납품 및 설치, 검사 및 시험운영, 교육 및 기술이전, 유지보수, 보안사항, 제출서류 등 계약 이행에 관한 세부사항을 규정함에 있다.

2. 구매조건

가. 계약자는 본 시방서에 명시된 **물품 일체를 일괄 공급방식으로 납품 및 설치하여야 하며**, 검수 완료 시점을 기준으로 최신의 소프트웨어를 설치하여야 한다.

나. 계약자는 계약 시 납품 및 설치하는 물품의 원 제조사의 기술지원을 인증하는 **물품공급 및 기술지원 확약서를 반드시 제출하여야 하며**, 미제출 시에는 계약을 포기한 것으로 간주 한다.

다. 계약자는 납품 및 설치하는 모든 물품이 현재 운영 중인 네트워크 장비와 완벽하게 호환되어야 하며, 세부규격[Ⅳ. 장비규격서]을 만족해야한다. 또한 해당 제조사가 인증하는 신품이어야 한다.

라. 계약자는 검수 완료 전에 납품 및 설치한 물품에 대하여 하자, 도난, 파손, 장애 등이 발생할 경우 동일 사양 이상의 신품으로 교체하여야 하며, 이에 따른 제반경비는 계약자가 부담한다.

3. 납품 및 설치

가. 계약자는 납품 및 설치하는 모든 물품은 본 장비 구매 규격서에서 규정한 사양과 동등 또는 그 이상의 사양이어야 한다.

나. 물품의 납품 및 설치에 따른 시설물 훼손 및 이동 등은 담당자와 사전에 협의하여야 시행한다.

다. 물품의 납품 및 설치 이후에라도 상명대학교의 사정으로 물품의 이동 시 동일 건물 내에서는 계약자는 무상으로 이동 설치하여야 한다.

라. 물품의 납품 및 설치로 현재 운영되고 있는 시스템의 중단 또는 정지가 필요한 경우 담당자와 충분한 협의 후 납품 및 설치를 한다.

마. 납품 및 설치되는 물품은 고유성능을 최대한 발휘할 수 있어야 하며, 타 시스템과 전체 시스템에 간섭 또는 영향을 주어서는 안 된다.

바. 납품 및 설치되는 물품은 기존에 설치 된 정보 서비스 시스템과 100% 호환되어야 한다.

사. 계약자는 UTP , Fiber Cable 포설 시 담당자의 지시를 따라야 하며, 담당자의 요구 시 케이블 보호를 위하여 트레이 이용 및 PVC 파이프나 몰딩을 이용하여 포설하여야 한다.

아. 계약자는 상명대학교에서 운영 중인 네트워크 환경을 분석하여 담당자가 지시하는 지정

된 위치에 장비를 설치하여야 한다.

-. 무선망 메인 방화벽 : 1 식

-. 내부서버 전담 방화벽 : 1 식

-. 무선랜 시스템(컨트롤러) : 1 식

-. 무선랜 시스템(AP_옥외형) : 4 식

자. 물품의 납품 및 설치에 따라 소요되는 제반비용은 계약자가 부담하여야 한다.
(Optical Patch Cable, UTP Patch Cable, Gbic 등)

차. 상명대학교의 학사, 입시, 행정 일정 등의 사유로 계약자가 제출한 사업수행계획서에 물품의 납품 및 설치 일정을 조정할 수 있다.

카. 납품되는 모든 장비는 상명대학교가 요청한 장소에 설치하여야 한다.

4. 세부 설치 사항

가. 세부교체 계획 수립

1) 계약자는 계약 시부터 상명대학교의 정보시스템 교체설치 사업을 성공적으로 완수할 수 있는 책임 관리자를 본 사업의 완료 시까지 지정하여, 매일 사업 현장을 파악하고 상명대학교의 담당자에게 보고해야 한다.

2) 계약자는 상명대학교의 담당자와 협의한 추진일정에 맞게, 장비 교체에 차질이 발생하지 않도록 다음 사항을 사전 조사 및 준비 작업을 실시한다.

-. 시스템 라벨링, 교체, 설치, 시험운영 방법 및 장애복구 등 세부계획 수립

-. 교체 장비 현황을 사전조사에 의거 재작성하고 각 시스템별 케이블 라벨링 작업, 각 장비별 라벨링 등 해체 준비작업

-. 시간계획, 전산장비 반・출입 허가, 인원배치

-. 시스템별 전기 및 네트워크 케이블 연결 확인 등 사전 환경요인 파악

-. 정보서비스 시스템별 운영 설정 현황 작성

-. 신규 장비별로 시스템의 설치 위치 및 시험운영 점검표 작성

나. 백업 수행 및 전문기술인력 확보

1) 계약자는 상명대학교의 장비 교체에 참여할 전문기술인력(백업 장비포함)을 확보하여야 하며, 확보된 인력을 최대한 활용하여 본 사업의 목적을 달성하도록 하여야 한다.

다. 네트워크 구성 확인 후 교체 작업

1) 계약자는 네트워크, 보안 장비의 현재 시스템 구성과 운영 상태를 충분히 파악하여야 한다.

2) 시스템 교체 전 설치에 필요한 모든 사항을 문서화한 후에 교체하여야 한다.

라. 사업 전 구성도

※ 정보보안 사유로 인터넷 공지는 하지 않습니다.

본교 교육지원팀 담당자에게 개별적으로 열람하여 주시기 바랍니다.

마. 사업 후 구성도

※ 정보보안 사유로 인터넷 공지는 하지 않습니다.

본교 교육지원팀 담당자에게 개별적으로 열람하여 주시기 바랍니다.

※ 주요 사항

1) 무선망 메인 방화벽 설치 시 내부 및 외부 라우팅, NAT 재구성(외부, 무선영역 백본)
2) 내부서버 전담 방화벽 설치 시 내부 및 상단 라우팅 재구성(유선영역 백본, 내부L2)
   * 라우팅 및 NAT 재구성 시 네트워크 정보에 대하여 자체적으로 지원
3) 방화벽 정책 이관 작업(무선망/내부서버 전담 방화벽 정책 모두 포함)
4) 무선랜 시스템(컨트롤러/AP) 업그레이드 구축 시 네트워크 및 정책 구성 적용
   (네트워크, 인증 서비스 연동, DHCP 서버 등)
   * 시스템 구축 시 필요한 네트워크 정보에 대하여 자체적으로 지원
5) 무선인증서버, 신규 무선랜 시스템 연동 구성
6) 무선랜 시스템 업그레이드에 대한 보안 정책 및 네트워크 연동
7) 신규 시스템 및 서비스 정상 동작 모니터링

바. 장비 교체

1) 계약자는 전문기술인력을 통해 안정적으로 장비를 교체하여야 한다.
2) 계약자는 장비 교체 후 계약자는 모니터링(20일 이상)을 수행 하여야 한다.
3) 장비 교체 시 일정은 담당자와 충분한 일정 협의 후 교체 하여야 한다.

사. 시스템실 전산장비 입고 및 설치

1) 시스템실에 장비를 입고 후 상명대학교가 제공하는 시스템 구성도에 따라 시스템을 설치하여야 한다. 다만, 부득이한 사정으로 인하여 정위치에 설치할 수 없을 경우에는 상명대학교와 협의하여 결정한다.
2) 시스템실의 각 시스템 위치는 사전에 설치영역을 표시하여 정위치 확인 후 설치하여야 한다.

아. 시험운영 및 정상동작 확인

1) 전산장비를 교체 설치한 후 다음과 같은 운영을 통하여 정보서비스의 정상적인 동작 여부를 확인한다.
   -. 외부 인터넷과 통신연결 정상 여부
   -. 방화벽 이관 정책 정상 여부(문제 시 보안정책 즉시 수정 지원)
   -. 백본 / 내부 서버 영역의 스위치와 통신 정상 여부
   -. 무선랜 컨트롤러 통신 및 AP 간 통신 정상 여부
   -. 무선랜 시스템, 무선인증서버 간 통신 정상 여부

-. 무선랜 AP(옥외형) 통신 정상 여부

-. 기존 정보시스템 서비스 상태 정상 여부

자. 정보시스템 종합테스트 결과 보고

1) 시스템 시험운영 및 종합테스트 결과보고서를 상명대학교의 담당자에게 제출 하여야 한다.
2) 결과보고서는 서비스 정상 작동 측정, 장애 원인, 조치결과 등을 포함한다.

차. 시스템 안정화

1) 시스템 교체 후 경력 3년 이상의 전문 인력을 안정화 기간(20일) 동안 상주하여야 한다.
2) 시스템 교체 후 검수 완료일까지 전산장비 일일점검 [7.유지보수] 을 실시한다.
3) 시스템 장애를 사전에 예방하여야 하며, 최소 20일 이상의 지속적인 가동상태를 확인하여 서비스 정상 작동 보고서를 제출하여야 한다.
4) 상명대학교의 담당자로부터 서비스 정상 작동 평가 결과에 대하여 완료평가를 득한 날짜를 검수 완료 시점으로 한다.

카. 교체 / 구축 설치 작업 요구사항

1) 고도화 방화벽 설치 방안

1-1) 무선망 메인 방화벽 구축 요구사항

-. 교육지원팀 서버실 내에 설치 된 노후화 무선망 메인 방화벽을 신규 무선망 메인 방화벽으로 교체 설치한다.

-. 네트워크의 Bandwidth는 상단 Metro 스위치와 하단 QoS는 기존 1G로 구성했던 방식으로 구성한다.

-. 기존 방화벽과 연결되어 있는 Metro 스위치와 QoS가 연결 된 1G Muti-mode 광케이블은 그대로 사용한다.

-. 각 장비에 연결 된 광케이블의 커넥터 타입은 LC-LC 타입에 맞게 연결한다.

-. Power Supply는 이중화하여 안정성 있게 구축하고, 담당자가 제공하는 정보를 참고하여 구간 별로 연결 된 Metro 스위치, QoS 장비에 각각 연결한다. 각 구간에 설치된 장비와 방화벽 간 연동 테스트를 완료하여야 한다.

-. 네트워크 물리적 연결은 상단 Metro 스위치, 하단 QoS(Bridge)로 연결 하되 L3구간은 상단 Metro 스위치, 하단 무선망 백본 스위치로 연결이 되므로 해당 상,하단 장비와 L3 라우팅 프로토콜을 적용시켜 담당자의 요구사항에 맞게 네트워크를 적용해야 한다.

-. 신규 무선망 메인 방화벽의 Zone 구성은 인터페이스 별로 상단 Metro 스위치 연결 인터페이스는 외부망, 하단 QoS 연결 인터페이스는 내부망, 2개의 Zone으로 나누

어 적용시킨다.

-. 신규 방화벽 정책은 기존 방화벽의 정책을 이관하고, NAT 정책 설정 시 사설 IP 대역과 공인 IP의 매칭 설정 시 오류가 나지 않도록 정확히 설정 후 연결 테스트를 완료하여야 한다.

-. 기존 방화벽에서 사용 중인 Interface 정보를 담당자의 요구사항에 맞게 신규 방화벽에 적용한다.

-. 기존 방화벽에 설정 되어 있는 각 인터페이스 영역 별 IP 정보를 신규 방화벽으로 이관시킨 후 영역 별로 연동 테스트를 완료 하여야 한다.

-. 상단 Metro 스위치와 연결 된 인터페이스에는 현재 사용 중인 IP를 적용시키고, Gate-way 주소를 적용하여 연동 테스트를 완료 하여야 한다.

-. 하단 L3구간의 무선망 백본과 연결 된 인터페이스에는 현재 사용 중인 IP를 적용시키고, Gate-way 주소를 적용하여 연동 테스트를 완료 하여야 한다.

-. 기존 방화벽과 분리되어 있던 IPS 장비를 제거하고 신규 방화벽에 IPS 서비스 및 Anti-Virus 서비스를 동시에 올려 통합 엔진으로 구축하여 사용한다.

-. IPS와 Anti-Virus의 보안 정책은 제조사 측에서 제공하는 Default 보안 정책을 적용시키고 담당자의 요구에 따라 추가 및 변경에 대한 보안 정책을 적용한다.

-. 웹필터, 애플리케이션 보안 정책은 제조사 측에서 제공하는 Default 보안 정책을 적용시키고 담당자의 요구에 따라 추가 및 변경에 대한 보안 정책을 적용한다.

-. 신규 방화벽의 모든 접속 권한 설정은 관리자 ID와 IP를 모두 충족해야만 장비에 접속할 수 있으므로 담당자의 접속 가능한 IP를 방화벽에 적용하여 사용한다.

-. 정책 설정 완료 후 보안 동작에 따른 로그 기록과 메시지 별, 파일 및 파일 크기 별, 패킷 체크를 통해 정상적으로 방화벽 동작이 이루어지는지 모니터링을 수행한다.

-. 신규 방화벽의 허용 로그, 거부 로그, 세션 로그, 정책별 트래픽 로그 등 테마별 로그 기록을 통하여 불필요한 트래픽이 발생하는 건에 대해서는 차단을 한다.

-. 적용 되어진 정책의 사용량, 세션, 사용 비율, 최근 참조 시각 등의 확인하여 설정된 정책이 적절한지 상시 모니터링을 통해 정책을 최적화 시킨다.

-. 담당자의 요구에 따라 신규 보안 기능 및 설정을 적용한다.

-. 정책 백업은 시스템, 방화벽, IPS/Anti-Virus, 웹필터, 애플리케이션, 모니터링 각 항목 별로 백업을 수행하여 복구 시 각 항목에 맞게 복구가 가능하도록 수행한다.

-. 백업파일 생성 시 Password 설정을 하여 백업 파일에 대한 보안을 강화하고 복구 시 설정한 Password를 입력하여 복구하도록 수행한다.

1-2) 내부서버 전담 방화벽 구축 요구사항

-. 교육지원팀 서버실 내에 설치 된 노후화 내부서버 전담 방화벽을 신규 내부서버 전담 방화벽으로 교체 설치한다.

-. 네트워크의 Bandwidth는 상단 유선망 백본 스위치와 하단 내부서버 Zone, 비공개 서버 Zone은 기존 1G로 구성했던 방식으로 구성한다.
-. 기존 방화벽과 연결되어 있는 유선망 백본 스위치와 내부서버, 비공개 Zone과 연결된 1G Cat.6 규격의 파란색 UTP 케이블은 그대로 사용한다.
-. Power Supply는 이중화하여 안정성 있게 구축하고, 담당자가 제공하는 정보를 참고하여 구간 별로 연결 된 유선망 백본 스위치, 내부서버/비공개 스위치 장비에 각각 연결한다. 각 구간에 설치된 장비와 방화벽 간 연동 테스트를 완료하여야 한다.
-. 상단 유선망 백본 스위치 간 연결은 L3구간으로 라우팅 프로토콜을 적용시켜 네트워크를 연결하고 하단 내부서버 스위치와 비공개 스위치는 L2구간으로 구축하여 담당자의 요구사항에 맞게 네트워크를 적용해야 한다.
-. 신규 내부서버 전담 방화벽의 Zone 구성은 인터페이스 별로 상단 유선망 백본 스위치 연결 인터페이스는 외부망, 하단 연결 인터페이스는 내부망, 2개의 Zone으로 나누어 적용시킨다.
-. 신규 방화벽 정책은 내부서버 Zone과 비공개 Zone을 고려하여 각 영역에 맞게 기존 방화벽의 정책을 이관한다.
-. 기존 방화벽에서 사용 중인 Interface 정보를 담당자의 요구사항에 맞게 신규 방화벽에 적용한다.
-. 기존 방화벽에 설정 되어 있는 각 인터페이스 영역 별 IP 정보를 신규 방화벽으로 이관시킨 후 영역 별로 연동 테스트를 완료 하여야 한다.
-. 상단 유선망 백본 스위치와 연결 된 인터페이스에는 현재 사용 중인 IP를 적용시키고, Gate-way 주소를 적용하여 연동 테스트를 완료 하여야 한다.
-. 하단 L2구간의 내부서버 / 비공개 Zone과 연결 된 인터페이스에는 각각의 Gate-way 주소를 적용하여 연동 테스트를 완료 하여야 한다.
-. 신규 방화벽의 모든 접속권한 설정은 관리자 ID와 IP를 모두 충족해야만 장비에 접속할 수 있으므로 담당자의 접속 가능한 IP를 방화벽에 적용하여 사용한다.
-. 장비 접속권한 외 내부서버 Zone과 비공개 Zone에 있는 서버는 공개적으로 Open이 되면 안되는 구간으로 기본 서비스 포트를 제외한 원격 및 관리 접속 관련 된 Port는 관리자 외 모든 IP는 차단 적용시킨다.
-. 정책 설정 완료 후 보안 동작에 따른 로그 기록과 메시지 별, 파일 및 파일 크기 별, 패킷 체크를 통해 정상적으로 방화벽 동작이 이루어지는지 모니터링을 수행한다.
-. 신규 방화벽의 허용 로그, 거부 로그, 세션 로그, 정책별 트래픽 로그 등 테마별 로그 기록을 통하여 불필요한 트래픽이 발생하는 건에 대해서는 차단을 한다.
-. 적용 되어진 정책의 사용량, 세션, 사용 비율, 최근 참조 시각 등의 확인하여 설정된 정책이 적절한지 상시 모니터링을 통해 정책을 최적화 시킨다.
-. 담당자의 요구에 따라 신규 보안 기능 및 설정을 적용한다.

-. 정책 백업은 시스템, 방화벽 모니터링 각 항목 별로 백업을 수행하여 복구 시 각 항목에 맞게 복구가 가능하도록 수행한다.
-. 백업파일 생성 시 Password 설정을 하여 백업 파일에 대한 보안을 강화하고 복구 시 설정한 Password를 입력하여 복구하도록 수행한다.

2) 무선랜 시스템 설치 방안

2-1) 무선랜 시스템(컨트롤러)

-. 교육지원팀 서버실 내 신규 무선랜 시스템인 컨트롤러 서버를 설치한다.
-. 컨트롤러 구축 시 전용 S/W를 설치를 위한 별도의 H/W 장비로 구축하며, 무선랜 컨트롤러 목적 수행에 지장이 없도록 H/W 서버와 무선랜 시스템 간 호환성 및 연계성을 반영한 충분한 Spec의 서버로 설치 하여야 한다.
-. 컨트롤러 네트워크 연결 케이블은 1G Cat.5e 규격의 회색 UTP 케이블을 사용하여 신규 포설하고 양 종단에 라벨링을 정확하게 한다.
-. Power Supply는 이중화하여 안정성 있게 구축하고, 이중화 테스트를 수행하여 그 결과 값을 제출한다.
-. 네트워크 Interface는 무선 DMZ 스위치에 연결하고, DMZ망 대역의 IP 정보를 요구사항에 맞게 컨트롤러에 적용하여야 한다.
-. 담당자 요구에 따라 컨트롤러의 HostName과 장비 Password를 설정하고 NTP를 지정하여 시간 동기화가 되도록 설정한다.
-. 컨트롤러 장비 구축 시 최신 OS 업그레이드를 수행 및 필요한 License를 등록하여 원활한 정책 적용 및 AP와의 연동 서비스에 지장이 없도록 하여야 한다.
-. 사용자에게 서비스 되는 연결 방식은 인증 방식과 Open 방식의 2가지 방식을 설정하고 각각의 SSID를 다르게 하여 2개의 SSID가 Broadcast 되도록 설정 적용하여야 한다.
-. 각 SSID 별 정책 구축 시 전용 Vlan을 동일하게 적용 시키고, 인증방식의 SSID 정책에 무선인증서버를 등록하여 Open 방식의 SSID와 구분하여 정책을 적용한다.
-. 암호화 인증 방식의 정책 수립 시 담당자의 요구에 따라 표준 Protocol인 WPA/WPA2/WPA3-802.1X와 표준 암호화 방식인 AES방식을 적용하여야 한다.
-. Broadcast Bandwidth는 2.4 GHz와 5 GHz를 동시에 지원 가능해야 하며, 각각의 독립된 채널을 갖게 설정하므로써 각 AP마다 서로의 영향을 받지 않도록 정책을 수립한다.
-. AP에 직접 적용이 되는 각 주파수별 Radio 설정 값 정의 및 QoS, 방화벽 필터링과 같은 부가적인 보안 기능을 필요 시 담당자 요구 사항에 맞게 설정 하여야 한다.
-. 연동 된 각각의 AP는 컨트롤러를 통해 설치 된 위치에 맞게 HostName이 정확하게 설정 되어야 한다.
-. 컨트롤러 서버에 연동 된 AP에 정책을 일괄 적용하여 정상적으로 정책이 변경되었

는지 확인하고 단말기를 통해 정상적으로 서비스되는지 확인하여야 한다.

-. Dashboard를 통한 AP 무선자원에 대한 실시간 관리 기능을 확인하고 담당자의 요구사항에 따라 부족한 정보를 모니터링 할 수 있도록 수동으로 적용한다.

-. AP를 임의로 네트워크 연결을 해제하여 컨트롤러 모니터링 상에서 AP의 장애 상태를 확인하여야 한다.

-. AP의 바운더리 확인 및 관리를 위해 컨트롤러의 Hit Map 설정에 AP가 설치 된 건물의 도면을 등록하여 해당 건물 전체 넓이, 벽의 두께 및 재질을 파악하여 장비에 등록 된 도면에 적용시킨다.

-. 장비의 도면 설정 완료 후 위치에 맞게 신규 AP를 등록하고 AP의 네트워크 연결 모니터링을 함과 동시에 신호 세기를 체크하는 바운더리를 확인할 수 있도록 하여야 한다.

-. 관리 웹UI, Report 항목에서 다양한 통계 분석 정보를 제공해야 하며 담당자의 요구사항에 따라 지정 리포트의 주기적 보고 Report를 제공한다.

-. 컨트롤러의 모든 접속권한 설정은 관리자 ID와 IP를 모두 충족해야만 장비에 접속할 수 있으므로 담당자의 접속 가능한 IP를 컨트롤러에 적용하여 사용한다.

-. 보안 동작에 따른 로그 기록과 메시지 별, 파일 및 파일 크기 별, 패킷 체크를 통해 정상적으로 AP 동작이 이루어지는지 모니터링을 수행한다.

-. 컨트롤러의 테마별 로그 기록을 통하여 불필요한 트래픽이 발생하는 건에 대해서는 담당자의 요구 사항에 따라 차단 한다.

-. 정책 백업을 수행하여 복구 시 각 항목에 맞게 복구가 가능하도록 수행한다.

-. 백업파일 생성 시 Password 설정을 하여 백업 파일에 대한 보안을 강화하고 복구 시 설정한 Password를 입력하여 복구하도록 수행한다.

2-2) 무선랜 시스템(AP)

-. 계당관 및 본관 옥외형 AP 4대를 교체 설치하여 무선 네트워크를 구축한다.

-. AP의 네트워크 연결 케이블은 기존 사용 중인 1G Cat.5e 규격의 회색 UTP 케이블을 사용하여 활용하고 RJ45 및 보호캡이 손상되었으면 교체하고, 새로 라벨링 한다.

-. AP 마운트 시 동봉된 AP 전용 브라켓을 활용하여 설치하며, 장비에 케이블 연결 시 케이블이 보이지 않게 깔끔한 상태로 마감처리를 한다.

-. AP의 Power 공급은 PoE 스위치를 통하여 공급 받고 AP와 PoE 간 연결은 기존 케이블에 연결 된 Port를 활용하여 연결 구축한다.

-. AP 사용 IP 대역은 사설 IP 대역을 사용하고 MGT IP의 확보는 DHCP 서버에서 확보하여야 한다.

-. AP는 컨트롤러 내장형 분산처리 구조로 된 독립형 AP로 MGT IP를 고정으로 설정하여야 한다.

-. MGT IP 외에 관리 Vlan, 컨트롤러 IP 등의 정보를 콘솔로 연결하여 config 설정을

수행하여야 하며 config 적용 후 컨트롤러 장비와 연동시킨다.

-. AP의 수에 따라 필요 시 컨트롤러 서버 장비에 License를 추가 등록하여야 한다.

-. 컨트롤러 장비와 연동시킨 AP는 관리 웹UI를 통해 OS 업그레이드를 수행하여 원활한 정책 적용 및 서비스에 지장이 없도록 한다.

-. AP의 기본 정책은 담당자의 요구에 따라 표준 Protocol인 WPA/WPA2/WPA3-802.1X와, 표준 암호화 방식인 AES방식이 적용되어야 한다.

-. 학내 무선망 IP 대역은 전용 IP 대역을 사용해야 하며, 해당 IP 대역의 정보를 갖고 있는 전용 Vlan에 대한 설정은 AP가 연결 되는 PoE Switch에서 설정 적용한다.

-. AP는 사용자 전용 Vlan과 관리 Vlan이 동시에 적용되야 하므로 계당관 PoE Switch Uplink 및 AP 연결 Interface에 관리 Vlan과 사용자 Vlan을 trunk mode로 설정한다.

-. 본관 PoE 스위치의 경우 기존 Uplink에 trunk mode로 설정 되어 있기 때문에 AP가 연결 된 Interface에 관리 Vlan과 사용자 Vlan을 trunk mode로 설정한다.

-. 무선 백본 스위치에 연결 된 계당관 Interface에 사용자 Vlan을 추가하여 관리 Vlan과 동시에 적용 되도록 access mode에서 trunk mode로 설정 변경하여 적용한다.

-. 무선 백본 스위치의 무선랜 전용 Vlan에 정상적으로 DHCP 서버와 연동이 되도록 설정이 되어 있는지 확인하여야 한다.

-. Broadcast Bandwidth는 2.4 GHz와 5 GHz를 동시에 지원 가능해야 하며, 각각의 독립된 채널을 갖게 설정하므로써 각 AP마다 서로의 영향을 받지 않도록 하여야 한다.

-. 각각의 AP는 설치 된 위치에 맞게 HostName이 정확하게 설정 되어야 한다.

-. 컨트롤러 서버를 통해 AP에 정책을 일괄 적용하여 정상적으로 정책이 변경 되었는지 확인 한다.

-. 무선인증서버에 AP는 각 1대당 무선 컨트롤러와 같은 개념으로 각각의 AP를 NAS 목록에 등록하여 무선인증 서비스를 받게한다.

-. AP 정책 적용 및 무선인증서버에 장비 등록 완료 후 단말기를 이용하여 접속이 가능한지 정상 서비스 테스트를 수행한다.

-. AP에 적용되어 서비스 되어지는 연결 방식은 기존 정책과 동일하게 인증 방식과 Open 방식이 적용 되야 하며, 2개의 SSID를 단말기를 통하여 각각 정상적으로 연결 되는지 확인하여야 한다.

-. AP를 임의로 네트워크 연결을 해제하여 웹UI 상에서 AP의 장애 상태를 확인하여야 한다.

-. 장비의 도면 설정 완료 후 위치에 맞게 신규 AP를 등록하고 AP의 네트워크 연결 모니터링을 함과 동시에 신호 세기를 체크하는 바운더리를 확인할 수 있도록 하여야 한다.

5. 시험 운영 및 서비스 정상 측정평가

가. 계약자는 납품 및 설치한 물품의 정상동작 여부를 검사하고 시험 운영하여야 한다.

나. 계약자는 시험운영을 실시하고 그에 대한 서비스 품질 측정평가를 시행하여야 하며, 상명대학교에게 그 결과물을 제출 하여야 한다.

다. 서비스 품질측정 결과는 만족하여야 한다.

만약, 상명대학교가 정하는 평가지표에 도달하지 못할 경우 원인 분석을 통한 개선 및 보안조치를 해야 한다.

라. 계약자는 물품의 납품 및 설치 후 시험운영 내역, 상태 등 일일 점검보고서[7.유지보수]를 상명대학교에게 제출하여야 한다.

마. 검수 시 납품 및 설치된 물품의 관련기술 및 담당자가 요구 하는 모든 자료(설치완료 보고서, 일일점검보고서, 서비스 정상 측정평가 등)를 상명대학교에게 제출하고 승인을 받아야 한다.

바. 시험운영기간 동안 상명대학교가 수정 및 보완사항을 요청하면 계약자는 즉시 수정 및 보완 조치하여야 한다.

사. 사업기간(구축기간 20일 / 시험운영기간 15일) 이후 서비스 품질측정 보고서 및 구축 자료 제출에 대한 결과를 상명대학교 담당자에게 승인 받지 못한 경우 다음과 같이 손해배상액을 결정하여 지체상금을 입금해야 한다.

지체상금 = 계약금액 * 1.5/1000 * 지체일수

※ 단, 상명대학교의 승인을 받은 경우에는 예외로 한다.

6. 교육 및 기술이전

가. 계약자는 물품의 효율적인 운영과 상명대학교가 자체적으로 경미한 장애 조치를 할 수 있도록 교육 및 기술이전을 무상으로 지원 하여야 한다.

나. 납품 및 설치한 물품을 확장하거나 타 장비와 접속하고자 하는 경우에는 계약자는 인터페이스가 가능하도록 관련기술을 지원하여야 한다.

다. 체계적이고 효율적인 운영을 위하여 상명대학교가 정하는 곳에서 운영자교육을 실시하여야 하며 교육시간 및 교육대상은 상명대학교 담당자가 정한다.

라. 계약자는 물품의 운영에 필요한 교육 및 기술이전을 무상으로 지원하여야 한다.

7. 유지보수

가. 계약자는 하자보증기간 동안 무상으로 유지보수 하여야 한다.

나. 계약자는 납품 및 설치한 물품을 최적의 상태로 운영 및 유지관리 할 수 있도록 지원하여야 한다.

1) 보안장비 및 무선랜 시스템 일일점검 사항

-. System의 운용시간(Uptime) 점검

-. System CPU Utilization 상태 점검

-. System의 Memory 사용량 점검

-. System의 Power Supply 운용상태 점검
-. System의 Temperature 상태점검
-. System의 Fan 상태점검
-. 각 Interface의 Link 상태 점검
-. 각 Interface의 Traffice 상태 점검
-. 각 Interface의 Error 상태 점검
-. 시간 설정 상태 점검
-. Routing 상태점검
-. Log 수집 및 상태점검
-. System에 수집된 Log
-. 단말기를 통한 무선 네트워크 정상 연결 점검
-. 관리 웹UI를 통한 AP 연결 Monitoring 점검
-. 각 AP에 연결 된 Client Counter 점검

다. 계약자는 하자보증기간 동안은 물품 설치에 참여한 인력 중 상명대학교가 지정하는 인력으로 하여금 기능개선, 오류사항 등 지속적인 성능개선을 지원하여야 한다.

라. 납품 및 설치되는 모든 물품의 S/W는 최신판으로 제공하고 검수 후 1년 이내에 상위 버전(Version)이 발표될 경우 무상으로 업그레이드하여야 한다.

마. 납품 및 구축된 시스템 유지보수 시간은 365일 24시간 무휴로 하여야 한다.

바. 계약자는 납품 및 구축된 시스템에 대하여 보안 취약성 발생 시 수집 및 분석하여 결과와 대응책을 담당자에게 보고해야 한다.

사. 계약자는 무상유지보수 기간 중 비상연락 체계를 유지하여 장애발생 통보를 받은 즉시 1시간 이내에 상명대학교에 도착하여, 장애발생 통보 시점으로부터 2시간 이내에 정상적으로 운영될 수 있도록 장애를 복구하여야 한다.

아. 계약자는 장애발생 통보 시점으로부터 48시간 이내에 장애발생 원인을 분석하여 문서로 상명대학교에게 제출하여야 한다. (단, 정확한 원인규명에 많은 시간이 요할 경우, 사전에 상명대학교의 승인을 받아 장애발생 통보 시점으로부터 72시간 이내에 그 사유를 문서로 제출해야 한다.)

자. 계약자는 무상유지보수기간동안 동일한 장애가 2회 이상 발생할 경우 상명대학교의 요구 시 즉시 신품으로 교체하여야 한다.

차. 무상 유지보수기간에 장애발생으로 48시간 이상 정상 서비스가 어렵다고 판단될 경우에는 계약자는 24시간 이내 동급 이상의 물품으로 대체 설치하여 시스템 운영에 지장이 없도록 하여야 한다.

8. 보안사항

가. 계약자는 본 사업의 수행과정에서 취득한 자료와 정보에 관해서는 사업 수행의 전·

후를 막론하고 상명대학교 담당자의 승인 없이 이용 또는 제3자에게 유출 또는 누설하여서는 안 되며, 만일 이를 위반할 경우에는 계약자가 민・형사상의 책임을 진다.

나. 계약자는 물품의 납품 및 설치와 관련하여 보안관련 법규를 위반하는 사례가 발생하지 않도록 각종 보안에 세심한 주의와 의무를 다해야 한다.

9. 제출서류

가. 계약자는 담당자의 승인을 받은 후 아래의 서류를 제출하여야 한다.

1) 계약 후 7일 이내

-. 납품물품 상세 명세서 1부

-. 수행계획서(예정공정표, 제품설치를 위한 출입자 명단 포함) 1부

-. 보안서약서(대표자 명의 및 현장출입자) 각 1부

-. 제조사 물품공급 및 기술지원확약서(상명대학교 명기) 1부

-. 비밀보장계약서는 계약서 작성 시 첨부 1부

2) 검수 요청 시

-. 완료 보고서 및 검수요청서 1부

-. 완료 사진첩 1부

-. 납품내역서 1부

* 사업 수행 중 상명대학교가 필요하다고 판단되는 산출물을 요청할 경우 계약자는 산출물을 추가 또는 보완하여 제출하여야 한다.

[붙임 1] 보안특약

사업 보안특약 조항

① 사업자는 상명대학교의 보안정책을 위반하였을 경우 [붙임 2]의 사업자 보안위규 처리 기준에 따라 위규자 및 관리자를 행정조치하고 [붙임 3]의 보안 위약금을 상명대학교에 납부한다.

② 사업자는 사업 수행에 사용되는 문서.인원.장비 등에 대하여 물리적, 관리적, 기술적 보안대책 및 [붙임 4]의 '누출금지 대상정보'에 대한 보안관리계획을 착수계에 기재하여야 하며, 해당 정보 누출 시 상명대학교는 국가를 당사자로 하는 계약에 관한 법률 시행령 제76조에 따라 사업자를 부정당업체로 등록한다.

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

④ 사업자는 참여인력을 임의로 교체할 수 없으며 부득이 교체할 경우에는 인수인계를 철저히 하여 자료의 외부유출을 사전에 방지하여야 하며, 감독관의 확인을 받아야 한다.

[붙임 2] 용역사업 보안위규 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 OO 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. 보안관련 프로그램 강제 삭제 사. 사용자 계정관리 미흡 및 오남용(시스템 불법접근 시도 등) 아. 노트북, PC 등 전산장비 무단 반·출입 자. 비인가 통신시설(무선공유기, 스마트폰, 테더링 등)의 설치 운용 및 교신	○ 위규자 및 직속 감독자 OO 등 중징계 ○ 재발 방지를 위한 조치계획 제출 ○ 위규자 대상 특별 보안교육 실시

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. 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 단순 숫자 부여 마. PC 비밀번호를 모니터옆 등 외부에 노출 바. 비인가 보조기억매체 무단 사용	○ 위규자 및 직속 감독자 OO 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 3] 보안 위약금 부과 기준

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	500만원 이하	300만원 이하	100만원 이하

* 위규 수준은 [붙임 2] 참고

2. 사업 종료 시 지출금액 조정을 통해 위약금 정산

[붙임 4] 누출금지 대상정보

누출금지 대상정보

1. 기관 소유 정보시스템의 내.외부 IP주소 현황

2. 세부 정보시스템 구성현황 및 네트워크 구성도

3. 사용자계정·비밀번호 등 정보시스템 접근권한 정보

4. 네트워크 취약점 분석·평가 결과물

5. 용역사업 결과물 및 프로그램 소스코드, 상용S/W

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 제7조 제3항의 대외비

11. 그 밖에 상명대학교가 공개 불가하다고 판단한 자료

[붙임 5] 보안서약서

보 안 서 약 서

본인은 년 월 일부로 상명대학교 정보통신망 고도화 방화벽 및 무선랜 구축 사업의 용역사업과 관련한 업무를 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 나는 상명대학교 정보통신망 노후 방화벽 교체 및 무선랜 시스템 구축 사업과 관련된 소관업무가 국가기밀 사항임을 인정하고 제반 보안관계규정 및 지침을 성실히 준수한다.
2. 나는 이 기밀을 누설함이 국가이익을 침해할 수도 있음을 인식하고 재직 중은 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. 전자정부법 제35조(금지행위) 및 제76조(벌칙)

년 월 일

서 약 자	업 체 명 :		
	직 위 :		
	성 명 :		(서명)
서약집행자	소 속 :		
	직 위 :		
	성 명 :		(서명)

[붙임 6] 비밀보장계약서

비 밀 보 장 계 약 서

상명대학교(이하 "갑"이라 함)와 (주)○○○○○○○(이하 "을"이라 함)는 상명대학교 정보통신망 고도화 방화벽 및 무선랜 시스템 구축 사업 (이하 "본건"이라 함)을 위해 "갑"이 "을"에게 개시하는 갑의 비밀사항 취급에 관해 다음과 같이 계약을 체결한다.

제1조(비밀사항) 본 계약에서 비밀사항이란 문서, 도면, 그 밖의 서류에 기재되거나 혹은 전자적 또는 광학적으로 기록된 "갑"이 보유한 갑의 업무상 모든 지식 및 정보를 말한다. 단, 다음의 각호의 하나에 해당하는 것을 제외한다.

1. "을"이 "갑"으로부터 개시를 받은 시점에서 이미 공지로 되어있는 것
2. "을"이 "갑"으로부터 개시를 받은 후에 을의 고의 또는 과실에 의하지 않고 공지로 된 것을 을이 증명할 수 있는 것
3. "을"이 "갑"으로부터 개시를 받기 전에 을이 스스로 얻거나 정당한 권리를 가진 제3자로부터 정당한 수단으로 입수하였다는 것을 증명할 수 있는 것

제2조(비밀유지의무) ①"을"은 비밀사항을 엄중히 지키며 사전에 "갑"으로부터 서면에 의한 승낙 없이 이것을 제3자에게 개시 혹은 누설해서는 안 된다.
②"을"은 앞항의 "갑"의 승낙을 얻은 경우라도 해도 제3자가 계약상 을의 의무와 동등한 의무를 "갑"에게 지울 것을 확약하는 서면을 제3자가 "갑"에게 제출하기까지는 제3자에게 비밀사항을 개시해서는 안 되며, 제3자에게 비밀사항을 개시한 후는 제3자의 "갑"에 대한 의무이행에 대해 제3자와 연대하여 책임을 진다.
③"을"은 하도급업체를 통하여 사업 수행시, 하도급업체와 계약을 체결할 경우 비밀유지 조항을 포함하여야 한다.
④"을"은 계약한 하도급업체의 비밀유지의무 이행의무에 대하여 연대하여 책임을 진다.

제3조(사용목적) "을"은 비밀사항을 본건의 목적을 위해서만 사용하고 그 밖의 목적으로 사용해서는 안 된다.

제4조(개시범위) ①"을"은 비밀사항을 본건에 종사하고 또한 해당 비밀사항을 알 필요가 있는 "을"의 담당자 또는 종업원에 한해 필요한 범위 내에서만 개시할 수가 있다. 단, "을"은 해당 담당자 또는 종업원의 행위에 대해서 모든 책임을 지며 또한 해당 담당자 또는 종업원에 대해 본 계약상 "을"의 의무를 준수시켜야 한다.
②"을"은 앞항에 기초하여 "을"의 담당자 또는 종업원에 대해 비밀사항을 개시하려고 할 때는 사전에 해당 담당자 또는 종업원의 성명 및 해당 담당자 또는 종업원에게 개시할 비밀사항의 범위를 서면으로 "갑"에게 통지해야 한다. "갑"에게 통지한 사항을 변경할 경우도 동일하다.

제5조(복사) ①"을"은 비밀사항이 기재 또는 기록된 모든 문서, 도면, 기타 서류 또는 전자적, 광학적 기록매체를 사전에 "갑"으로부터 서면에 의한 승낙 없이 복사해서는 안 된다.
②"을"은 본건이 완료하였을 때 또는 중지 혹은 중단되었을 때 혹은 갑의 청구가 있는 경우는 곧바로 비밀사항이 기재 또는 기록된 모든 문서, 도면, 기타서류 혹은 전자적 또는 광학적 기록매체를 모든 복사물과 함께 "갑"에게 인도해야 한다.

제6조(조사권) "갑"은 "을"의 영업시간 중 언제라도 "을"의 사무소에 들러 "을"의 본 계약상의 의무이행 상황을 조사할 수 있다.

제7조(손해금액) ①비밀사항이 제3자가 알게 된 경우 "을"은 "갑"에게 손해배상금을 지불하여야 한다. 단, "을"이 본 계약상의 의무이행에 대해 나태하지 않았음을 증명하였을 때는 이에 해당되지 않는다.
②손해배상금액은 "갑"과 "을" 상호간에 합의하여 결정 한다. 단, 손해배상금은 최소 계약금액의 10%이상이어야 한다.
③손해금액에 대하여 합의가 이루어지지 않을 경우 해석은 관할법원의 판결에 따른다.

제8조(분쟁의 해결) ①본 계약서에 명시되지 아니한 사항은 "갑"과 "을"은 서로 협의하여 결정함을 원칙으로 하고 협의가 이루어지지 않을 경우의 해석은 갑의 해석에 따른다.
②이 계약과 관련하여 분쟁이 있는 경우 관할법원은 갑의 소재지를 관할하는 지방법원으로 한다.

제9조(유효기간) 본 계약은 본건이 완료하거나 중지 혹은 중단된 후라고 하더라도 5년간은 효력을 갖는다.

제10조(제재조치) "을"은 본 계약을 이행하지 않았을 경우 국가를당사자로하는계약에관한법률 시행령 제76조에 의거 부정당업자로 제재조치를 실시하고 관련사항을 관계기관에 통보한다.

이상 본 계약의 성립을 증명하기 위해 본서 2통을 작성하고 "갑"·"을" 기명날인 후 각각 1통씩을 보유한다.

2022년 06월 일

갑 천안시 안서동 상명대길 31
상명대학교
총장 홍 성 태

을 ○○시○○구○○동○○번지 ○호
○○회사
대표이사 ○○○