‘19년 전산장비 교체/도입 제안요청서

2019. 01. 29.

정보지원센터

1. 목적

- 본 시방서는 국제대학교와 계약업체간의 정보보안 장비등 구축을 위하여 계약사항 과 제반 지원사항 등 이행되어야 할 세부내용을 규정함에 있다

2. 사업명

- 국제대학교 전산장비 교체/도입 사업

3. 납품 및 설치 장소

- 국제대학교 정보지원센터 시스템실 및 실습실

4. 납품 및 설치 기한

- 2019년 02월 28일 이전까지

5. 사업범위 및 규격

- 침입방지(IPS) 시스템 외 1식

※ 세부사항 [별첨] 정보보안시스템 도입 규격표 참조

6. 참가 자격

가. 소프트웨어산업진흥법 제 24조에 규정에 의한 소프트웨어사업자(컴퓨터관련 서비스사업) 등록을 필한 업체

나. S/W 및 H/W의 경우 제조사(외국산일 경우 한국지사)의 제품공급 및 기술지원 확약서를 제출 할 수 있는 업체

7. 일반조건

가. 본 시스템을 납품 시 반드시 제조사 정품을 사용하고 규격서에 명기된 제품을 납품한다.

나. 설치 중 장비가 손상될 우려가 있다고 판단될 경우 필요한 방지책을 세워 야 하며 피해 발생 시 응급조치를 취하고 그 비용을 부담하며 손상된 장비는 원상복구 하여야 한다.

다. 납품업체는 납품 시 안전대책을 수립하며, 납품과 설치 중 제반 안전사고 또는 납품과정에서 발생하는 행정적, 기술적 제반비용과 그 문제처리를 모두 부담한다.

라. 납품업체는 목적달성을 위한 세부규격에 명시된 품목 외 추가적인 품목과 비용이 요구된다면 해당 품목과 비용이 이미 포함된 것으로 본다.

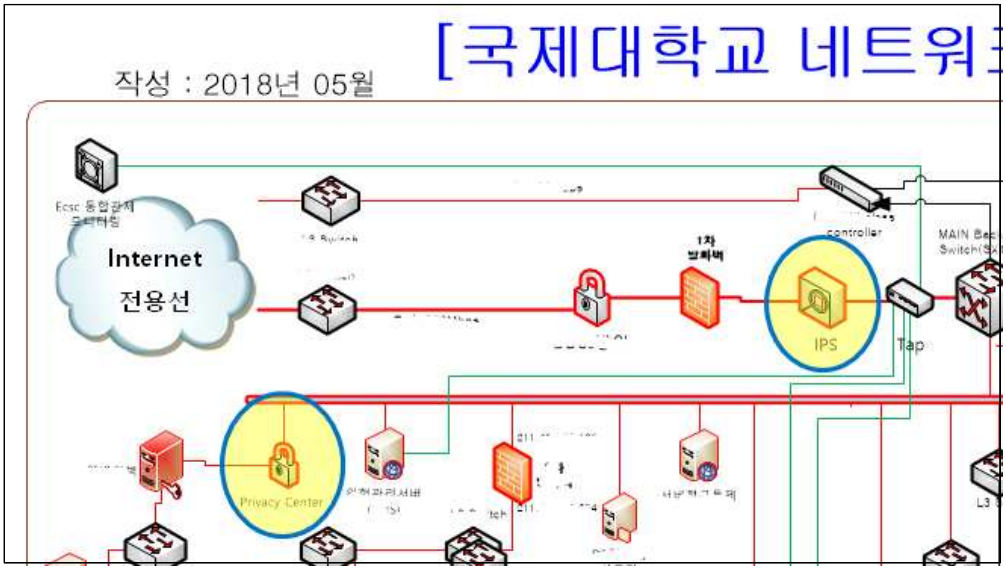
마. 본 시방서에 대하여 해석 간 차이가 있을 경우 관련법령이나 일반관례에 따르며, 소송담당법원은 발주자의 주소를 담당하는 법원으로 한다.

바. 과업수행 중에 발생한 고의 또는 과실 등 사고의 책임은 사업자에 있으며 발생한 손해에 대하여 배상책임을 진다.

사. 교체대상 장비 리스트

용도	품명 및 사양(제조사)	수량	도입시기
침입차단(IPS)	Sniper IPS E2000(나우콤)	1	2009.03
전산 실습	컴퓨터 SET(HP Pro6200MT+HP LE2202X)	20	2012.03

아. 시스템 네트크워크 구성도(일부 캡춰)



8. 기기공급 및 설치

가. 계약업체는 계약 후 5일 이내 납품 일정 및 세부 작업에 대한 공정표를 제출한다.

나. 납품업체의 납품 및 설치는 납기일 내 설치하지 못 할 경우 학교에서 정 해진 지체상금을 납부한다.

다. 계약업체는 장비설치 및 개통에 필요한 통신시설, 전원설비 등에 대한 환경조성 등 모든 필요한 사항을 조치하며, 설치 시 필요한 일체의 부품 및 부대비용을 부담한다.

라. 도입된 장비와 소프트웨어는 기 설치된 시스템의 원활한 운영과 관리에 지장이 없도록 설치한다.

마. 계약업체는 무상유지보수 기간 내 납품시스템의 보안상 문제점이 발견되면 즉각 그 대책을 수립하여 해결하여야 한다.

9. 대가지급

본 물품의 구매는 일괄구매 방식으로, 납품설치를 완료하고 검수완료 후 30일내 금액을 지급한다.

10. 보안유지

가. 설치 중 취득한 보안사항과 서버의 내부자료 구성, 구현기법, 통신망 구성 등에 대하여 보안을 유지하여야 하며, 해당 자료를 타 기관 제공, 유출등 일체 행위를 할 수 없다. 만일 보안사항을 유출 시 부정당업자의 제제조치를 취할 수 있으며, 낙찰업체는 민.형사상 책임을 진다.

나. 계약업체는 본 계약에 따른 제반업무를 처리함에 있어 모든 인원에 대하여 국제대학교 정보보안에 관한 규정에 의하여 처리한다.

다. 본 사업에 투입된 인원은 임의로 교체 할 수 없으며 불 가피 한 경우 교체 시 제반 보안조치 이후 학교의 승인을 받아야 한다.

라. 계약업체는 본 사업기간 취득한 정보는 사업기간 이후라도 보안준수사항 위반 시 민.형사상 책임을 진다.

II. 특수사항

1. 교육훈련과 기술지원

가. 계약업체는 납품한 장비와 솔루션에 대하여 효율적인 운영과 가벼운 장애조치를 위하여 국제대학교 자체적으로 유지관리 능력을 갖출 수 있도록 관리자와 사용자에 대한 교육을 해야 하며, 교육에 따른 일체의 비용은 계약업체가 부담한다.

나. 계약업체는 시스템 설치 완료 후 국제대학교에서의 업무협조 요청 시 이에 응해야 하고 다음과 같은 사항을 지원 하여야 하며 필요한 경우 교육기간을 협의하에 연장할 수 있다.

1) 안정화 기간동안 시스템운영 부분 등 관련 업체와의 최적화 보완작업 수행
2) 시스템 관리자에게 운영에 관련된 실질적인 기본 교육 지원
3) 납품한 시스템에 전문적인 Admin 교육 지원

2. 하자보증 및 유지보수

가. 무상하자보증기간은 구축완료 검수일로부터 1년으로 하고 정상운영이 되도록 매월 정기점검을 실시하고 보고서를 제출하여야 한다.

나. 무상보증기간 이후 유상유지보수기간에는 H/W는 도입가에 8%, S/W는 12%를 넘을 수 없다. 또한 제품에 대한 유상유지보수는 5년 이상을 유지할 수 있어야 한다.

다. 하자보증기간 중 발생한 하자에 대하여 계약업체는 신속하게 수리 또는 교체하여 운영의 중단을 초래하지 않아야 하며, 하자로 인한 피해가 발생할 시는 계약업체가 부담 변상조치 하여야 한다.

라. 계약업체는 24시간 비상연락체제를 유지하여 장애복구에 책임을 져야 한다.

마. 장애 발생 시 24시간(일과 후 시간포함)이상 정상운영이 불가능한 경우에는 즉시 동일 규격의 장비로 대체 설치하여 업무에 지장이 없도록 하여야 한다.

바. 모든 납품 H/W, S/W에 대해 월3회 이상 동일한 장애가 발생하였을 경우 국제대학교 요청에 따라 계약업체는 납품한 전 품목을 신규로 교체하여 제공하야 한다. 월3회라 함은 최초발생기준 30일 이내 3회 이상을 의미한다.

사. 국제대학교는 추후 무상 유지보수기간동안 시스템을 확장하거나 이설, 타 기종으로 교체 등이 발생할 경우 계약업체는 이에 적극 지원하여야 한다.

아. 일과 후 및 공휴일에도 기술팀과 항시 연락될 수 있도록 비상연락망을 구축하고 변동 발생 시 수시로 그 명단과 연락처를 제출하여야 한다.

3. 검수

가. 시스템 관련 기본교육과 운용에 필요한 기술자료를 국제대학교 시스템 관리자에게 충분히 제공하여야 한다.

나. 시스템 검수 시 발견되는 에러나 불합리한 문제점에 대하여 정상 가동될 수 있도록 즉시 조치하여야 하며, 수정 또는 보완 요구사항이 제기되면 이를 전면 수용하여야 한다.

다. 최종 검수결과 시스템 운영이 불가하다고 판단되거나 장비의 하자 발생으로 계약조건을 이행하지 못하는 것으로 판단될 시 계약업체는 납품과 설치한 모든 장비를 철거 회수해야 하며 그 비용은 계약업체가 부담한다.

라. 본 제안요청서에 명시된 모든 사항이 준수되어야만 검수가 완료된 것으로 하며 지체상환금은 국제대학교 기준에 따른다.

4. 제출서류

가. 계약업체는 아래 산출물을 문서로 만들어 학교에 제출하여야 하며 사업수행 중 국제대학교에 필요하다고 판단되는 산출물은 추가 또는 보완 제출하여야 한다.

1) **계약 시 제출 서류**

- 각 제품별 제조사(외산인 경우 한국지사)의 제품공급 및 기술지원 확약서 각 1부.
- 기타 입찰공고에 게시된 등록서류 일체

2) **계약일로부터 5일 이내 제출서류**

- 납품설치 계획서(설치계획서, 납품장비규격과 수량, 설치인력현황 및 명단 등)
- 보안확약서(업체대표) 및 보안서약서(설치인원) 각 1부

3) **설치 완료 후**

- 유지보수요원 재직증명서 각 1부.
- 시스템 설치완료 보고서 1부.
- 기술지원 인력현황 및 비상연락망이 포함된 유지보수 체계도 1부
- 관리운영자 매뉴얼 1부.
- S/W, H/W 라이센스가 발급되는 경우 라이센스 각 1부.
- 물품납품 명세서(낙찰가 기준 물품별 세부 납품금액)
- 국가정보원 CC 인증서 1부(인증 제품인 경우)

5. 설치 시 공통준수 사항

가. 납품업체는 학교에서 지정한 위치에 설치하고 정상동작하도록 설치하여야 한다.

나. 납품업체는 기 운영 중인 관련장비 및 시스템운영에 어떠한 하자도 발생하지 않도록 하고 연계장비와 100% 완벽한 호환성 및 연계성을 확보 하며, 납품과정 중 발생하는 기술적, 구조적 문제점을 전적으로 책임지며 정상가동 될 수 있도록 한다.

다. 납품 업체는 목적 수행에 전혀 지장이 없도록 품질의 신뢰성 및 안정성을 가지고 규격에 맞는 시스템 일체를 납품.설치하여야 한다.

라. 설치 시스템의 내용이 시방서에 요구되는 성능, 규격을 수용할 수 없다고 판단되면 설치 변경 등을 요구할 수 있으며 납품업체는 이에 즉시 응하여야 한다.

마. 검수 완료 후에라도 본 구매.설치에 있어 납품업체의 책임으로 발생되는 모든 사고와 그로 인한 우리대학교의 손해데 대하여 납품업체가 전적으로 변상조치 하여야 한다.

바. 납품업체는 모든 Interface는 Giga급 이상으로 설치한다.(managing port 제외)

[별첨 1]

정보보안시스템 도입 시방서

1. 침입차단 시스템(IPS) 1식

구분	규 격	비 고
H/W	○ IPS 성능 : 2~4Gbps ○ 동시 세션 처리 : 5,000,000 이상 ○ CPU : 2.4GHz 8Core ○ Memory : 32GB (최대 64GB) ○ HDD : 2TB ○ SSD : 64GB ○ NIC : 1G 4port (최대 8port) ○ Power : 이중화	
세부 기능	○ IT인증사무국 침입방지시스템 보안요구사항 V1.0 이 적용된 하드웨어 일체형 장비로 CC인증(EAL4) 이상을 획득한 제품 ○ 자체 CERT 보유를 통한 취약성 DB 구축 및 지속적 업데이트 지원 ○ 공격발생 시 신속한 대처를 위해 최신 해킹패턴 및 공격에 대한 시그니처 업데이트 제공 ○ 국가사이버안전센터(NCSC) 및 상위기관에서 제공한 탐지규칙(PCRE, YARA) 차단 적용 ○ 어플리케이션 인지 및 제어기능 제공(2,000개이상) ○ 시그니처 제공(7,000개이상) 및 보안관제 서비스 제공 ○ 국가/IP/URL/URI별 유형에 따라 탐지/차단 및 시간별 정책 설정 기능 제공 ○ 사용자 정의 시그니처 설정 및 실시간 차단 기능 제공 ○ 자동학습 기능을 통한 정책 생성 및 적용으로 Zero-day 공격 대응 지원 ○ SSL 세션 복호화 기능으로 유해 트래픽 탐지/차단 기능 제공 ○ 유해트래픽(해킹, 바이러스, 웜 등)에 대한 양방향 탐지/차단 ○ 프로 토콜 anomaly(변조된 패킷헤더, 비정상패킷), 변종 공격코드 탐지/차단 ○ 트래픽 anomaly(어플리케이션별 트래픽 패턴 분석), Unkown 공격코드 탐지/차단 ○ 어플리케이션 제어 기능 및 예외 IP설정 기능 제공 ○ 어플리케이션/사용자/악성코드 인지 분석을 통한 위협탐지 기능 제공 ○ 패킷차단 및 트래픽 대역폭 제어기능 제공 ○ 프로 토콜/서비스별 네트워크 트래픽 분석기능 제공 ○ Packet/Session/Payload/Application의 Multi-layer 분석 기능 제공 ○ Raw Data저장 및 Packet Dump를 통한 상세분석기능 및 추적기능 제공 ○ 파일 다운로드 추이파악을 위한 이벤트 추적 기능 제공 ○ 네트워크 패킷분석을 통한 사용자별 보안위험도 판별 및 공격 위험도 정보 제공 ○ 악성코드 평판분석(패턴, AV, YARA 등) 및 분석결과 악성코드DB 갱신기능 제공 ○ 어플리케이션을 이용한 악성코드 감염경로 추적기능 제공 ○ 파일 재구성으로 악성코드 탐지 분석을 위한 파일 수집기능 제공	

	○ 세션내 트래픽 분석을 통한 내부 자산(OS, 브라우저, 어플리케이션 등) 자동인식 및 자동/수동 등록기능 제공 ○ 자산관리 시스템 연동, 네트워크 트래픽 분석을 통한 자산인식 기능 제공 ○ 원격 접속 시 암호화 통신(SSH, HTTPS 등) 기능 제공 ○ 보안정책 및 장비상태, 장애감지, 보안감사 등 관리환경(GUI) 제공 ○ 실시간 탐지/차단 현황 및 트래픽, 패턴 업데이트, 시스템정보를 확인하는 상황판 제공 ○ 실시간 네트워크 트래픽의 정보 모니터링 및 시스템 자체의 부하량 정보 제공 ○ IP Pool기능에 의한 네트워크 분할관리 및 이벤트 통계, 정책설정, 보고서 출력 등 각 영역별 관리기능 제공 ○ 사용자 제어를 위한 자체 사용자 등록기능 및 자산관리시스템 연동기능 제공 ○ 다운로드 된 악성코드 정보(악성코드파일, 악성코드명, 출발지, 목적지)에 따른 추이 통계정보 제공 ○ 각종 트래픽 및 이벤트에 대한 통계, 분석, 리포트 기능을 지원 ○ 관리자용 도움말의 한글화를 제공하여 보안정책 적용에 용이한 접근성 제공 ○ 시스템 자체 저장장치(HDD) 보유 Log 저장 및 백업, 복구 가능, 별도 서버 없이 운영 가능 ○ SNMP, Syslog 정보 전송기능 제공 ○ 통합보안관리 시스템과 연동을 위한 IAP, WEAP 프로 토콜 지원 ○ 동일 제조사의 위협관리시스템(TMS)의 연동 센서역할 기능 제공	
설치 상세	○ In-Line Bridge(Transparent) 모드 구성 지원 ○ 기존 네트워크의 구성 및 설정값(Routing 정보등) 변경 없이 구축 및 적용 가능 ○ 기본 서비스 및 네트워크 구성변경 없이 자체 장비로 HA기능 지원 ○ HA구성시, Active/Active 및 Active/Standby 구성 지원 ○ 내장형 Bypass 기능을 통해 시스템 장애발생 시 통신망 유지기능 및 장애원인 분석을 위한 IDS기능 지원 ○ Virtual IPS Zone별 멀티라이선스 선택 기능 및 Virtual IPS Rule-set 기능 제공 ○ 기존 보안정책의 이관작업 및 상/하단 장비와의 연동가능	

2. 컴퓨터 SET 20대

구분	규 격	비 고
H/W	○ HP EliteDesk 800 G4 Tower PC ○ Intel Core i7 8700 3.2 2666MHz 6C 65W CPU ○ 16GB (2x8GB) DDR4 2666 DIMM Memory APJ ○ 256GB SATA Three Layer Cell Solid State Drive ○ NVIDIA GeForce GTX1060 3GB ○ 9.5mm DVD-Writer G3 800/600 Tower ○ Windows 10 Pro 64 KOR	

	○ 3/3/3 (material/labor/onsite) TWR Warranty SING ○ HP Optical Wired Mouse USB ○ HP USB Business Slim Wired Keyboard KOR ○ 500W active PFC / 80 PLUS Gold ○ HP Prodisplay P232LED(23인치형) 16:9, 1920*1080(FHD)	
설치 상세	- 지정하는 전산 실습실에 본체 교체 설치 - 기존 사용중인 본체는 지정된 장소로 이동 - 패션디자인 3D프로그램(CLO 4.1) 동작에 문제가 없도록 설치지원. - 학내에 지정된 소프트웨어 설치(OA, 백신, 인터넷 설정 등)	