University Innovation 대학혁신지원사업

건국대학교 GLOCAL캠퍼스 가상화 시스템 구축
제 안 요 청 서

2020. 09.

GLOCAL캠퍼스 정보운영팀

목 차

Ⅰ. 사업 개요

1. 사업내용

❍ 사 업 명 : 건국대학교 GLOCAL캠퍼스 가상화 시스템 구축

❍ 사업기간 : 계약일로부터 30일 이내

❍ 입찰방식 : 경쟁 입찰(최저가)

❍ 문의처

가. 전산담당 : 기획처 정보운영팀 **조남주** (043-840-3967)

나. 구매담당 : 총무처 총 무 팀 **이선호** (043-840-3118)

2. 사업목적

❍ 통합과 확장이 용이한 서버 인프라 환경 구축

❍ H/W 운영의 효율성 및 서비스 가용성 확보

❍ 시스템 관리비용 절감 및 Green IT 기반 마련

3. 사업범위

분 야	내 용
H/W 도입 및 인프라 환경 구축	가상화 기반의 통합운영 인프라 환경 구축 - 서버(노드) 2식
가상화 S/W 설치 및 구성	가상화 S/W 설치 및 가상 머신 생성
서비스	현 운용중인 가상화시스템과의 연동 및 분리작업 지원 포함

4. 기대효과

가 시스템 안정성 및 서비스의 고가용성 확보

❍ 시스템 이중화(HA) 구성으로 서비스의 다운타임 최소화 및 고가용성 확보

❍ 기존 노후 시스템들을 가상서버로 이관하여 시스템 성능 및 안정성 확보

나. 서비스의 민첩성 향상

❍ 빠른 서버 Provisioning이 가능하므로 업무의 유연성이 증대 됨

❍ 서버 IT자원에 대한 통합모니터링 가능으로 시스템의 운영 편의성 및 효율성 제고

❍ 가상화 구성으로 인한 비용절감으로 다른 분야에 대한 기회비용이 증대 됨

다. 비용절감

❍ 신규 서버 구매 및 유지비용 예산절감

❍ 시스템 안정성 확보를 위한 이중화 구성 확보

❍ 에너지비용 절감(서버 소비전력, 냉·난방 비용 등)으로 Green IT 구현

Ⅱ. 추진 계획

1. 추진 배경

가. 운영 서버의 노후화에 따른 안정성 확보 및 성능 개선 필요

나. 정보 서비스의 신뢰성 향상을 위한 서비스 이중화(HA) 구성 필요

다. 사용자 요구사항에 신속하게 대응할 수 있는 유연한 IT환경 구축 필요

2. 추진 방향

가. 자원 활용의 효율성 및 시스템 확장을 고려한 가상화 기반의 시스템 구축

❍ 자원 활용을 극대화하기 위해 자원의 이동 및 확장이 용이한 시스템 구조로 설계

나. 논리적·물리적 이중화(HA) 구성을 기본으로 하는 안정된 시스템 구축

❍ 보다 안정적이고 성능이 우수한 인프라 도입으로 서비스의 고가용성을 확보

다. 최신 IT 정보기술을 적용한 자동화된 통합 관리 시스템 구축

❍ 자동화된 관리 기능을 사용하여 위험요소를 예측하고, 가상 머신에 할당된 자원의 효율성을 분석하여 효율적인 자원 할당을 이룰 수 있는 지능형 관리 시스템 구축

Ⅲ. 제안요청 내용

1. 제안요청 개요

❍ 서버 가상화 시스템 구축을 통하여 시스템의 신뢰성과 안정성을 확보하고, 유연한 IT 인프라 환경 구축이 가능토록 제안

❍ 본 사업에 대한 충분한 이해로 전체적인 가상화 시스템 구축과 통합 대상 서버의 이관방안을 제시하여야 하며, 제안요청서에서 추구하는 목표를 달성하기 위해 추가해야 할 사항이 있을 경우 제안서에 추진방안과 제안업체의 역할을 명확히 제시

2. 도입 장비 규격

가. 물품 세부 규격

구 분	세 부 규 격	수량
가상화 서버 (노드)	CPU : Intel Skylake 6148 제품군 이상 - Processor & Core : 2CPU, CPU당 20Core 이상 제공 - Clock speed: 2.4GHz 이상 제공 메모리 : 서버(노드)당 DDR4 512GB 이상 제공 내장 디스크 : 1.92TB SSD 2개 및 4TB HDD 10개 이상 제공 NIC : 10GbE Dual SFP+ Network Adapter 이상 제공	2식
가상화 S/W	가상화 소프트웨어 기능 - Bare-metal 기반의 Hypervisor 방식 - 통합 서버 장애 시 가상 머신이 가용한 다른 서버에서 자동 Re-start 해 주는 HA기능 제공 - 운영 중인 가상머신을 서비스 중단 없이 다른 호스트로 이동하는 라이브 마이그레이션 기능을 제공 - 업그레이드시 가상머신의 서버간 무중단 마이그레이션 자동화 제공 - 지원OS : Windows, Linux, CentOS 등 - 다양한 하이퍼바이저(VMware vSphere, Microsoft Hyper-V, Citrix XenServer)와 호환 제공 - 스토리지 컨트롤러는 하이퍼바이저와 별개의 형태로 제공 - 인라인/포스트방식의 데이터 중복제거 및 압축을 제공해야 하며, 기능을 On/Off 할 수 있는 기능 제공 - 가상머신의 스토리지 I/O는 같은 서버(노드)안에서 처리되는 구조 제공 - OS와 상관없는 동일한 관리 GUI 제공 - 물리·가상 머신에 대한 중앙관리 및 모니터링 가능 - 관리 콘솔로 가상머신을 마이그레이션, 모니터링, 자원 할당 관리 및 재해복구 관리 기능을 제공 - 작업에 대한 진행경과, 장애 및 자원 사용률에 대한 경고기능 포함 - 문제 발생 전 관리자에게 장애가능성 통보 기능 제공 - 서버 가상화 상태 모니터링 기능 제공	1식
기타	제안하는 장비의 구성을 위해 필요한 추가 장비(케이블 등) 일체	-

※ 제안 조건

❍ 컴퓨팅/스토리지/통합관리도구가 통합된 어플라이언스 형태의 하이퍼 컨버지드 시스템(HCI)제품으로 제안

❍ 도입되는 모든 부품은 제조사 정품으로 제안(OEM 제품 제외)

❍ 제안 물품은 제안요청서에 명시된 규격과 유사한 사양으로 제안하여야 하며 특이

경우에는 제안서 제출 전 사전 협의를 통해 승인된 부분에 한해 제안

❍ 제안물품은 물품 규격서의 세부사양의 동급 또는 그 이상의 제품이어야 함. 모든 물품은 인지도, 성능, 유지보수 및 관리에 문제가 없는 제품이어야 하며 정품 및 신품으로 공급

❍ 해당 물품은 현장설치기준이며 별도의 표기가 없는 한 검수일로부터 3년 무상 유지보수를 실시

3. 상세 요구사항

가. 시스템 구성・설치 및 서비스 이전

❍ 가상화 서버의 하드웨어 오류로 인한 서비스 중단이 발생한 경우, 즉시 다른 하드웨어에서 해당 서비스를 가동할 수 있어야 한다.

❍ 하드웨어 (CPU, Memory 등) 자원의 사용량에 따라 운영 중인 가상머신의 부하를 적정 수준으로 분산 할 수 있어야 한다.

❍ 다수의 호스트 서버와 가상서버를 중앙에서 일원화된 콘솔을 사용하여 성능, 장애 상황을 통합 관리해야 한다.

❍ 자동화된 관리 기능을 사용하여 위험요소를 예측하고, VM에 할당된 자원의 효율성을 분석하여 관리자에게 알려주어 효율적인 자원 할당이 이루어지도록 하여야 한다.

❍ 서비스의 원활한 제공을 위해 가상 머신의 환경은 완벽하게 호환되도록 구성하여야 하며, 이를 위한 제반 라이선스 및 부품 등이 제공되어야 한다.

❍ 도입 장비(H/W, S/W) 납품장소는 건국대학교 GLOCAL캠퍼스에서 지정한 장소에 설치하여 구성 한다.

❍ 제안하는 모든 S/W는 운영 및 제안 장비 규격(장비모델, CPU, Core 등)에 적법한 라이선스를 제공해야 한다.

❍ 도입되는 소프트웨어에 대하여 커스터마이징이 필요하다고 판단되는 경우 사업기간 내에 완료하여 납품해야 한다.

❍ 제안하는 물품의 설치 및 구성을 위해 필요한 자재는 모두 포함하여 제안해야 한다.

❍ 시스템 오픈 후 안정화 기간을 1개월 이상 두고 추가되는 모든 비용은 제안사에서 부담하여야 한다. 단, 시스템 성능 등 문제가 있다고 판단 될 때는 연장 지원해야 한다.

❍ 도입 장비는 일체형으로 구성가능하며, 물리적 논리적 이중화 구성으로 제안 할 수 있다.

❍ 도입 장비 설치 시 H/W의 펌웨어, 드라이버 및 기타 지원 S/W는 최신 버전으로 업그레이드 하여야 한다.

❍ 도입 장비, 주요 구성품과 부품은 물품 규격서를 만족시키는 정품, 완제품으로 공급

해야 하고, 모든 S/W는 원소유자의 저작권을 침해하지 않는 최신 버전의 라이선스를 제공해야하며, 최신 버전으로 업그레이드 및 구성하여야 한다.

❍ 제시한 규격은 최소한의 요구조건으로 시스템 구축을 위해 명시되지 않은 H/W 및 S/W가 추가되거나 기존 시스템 업그레이드가 필요한 경우 제안에 포함하고 추가되는 비용은 제안사에서 부담해야 한다.

❍ 제안한 제품에 성능저하, 장애발생, 기능미비, 중대한 결함 등의 문제가 발생한 경우 해결방안을 제시하고 이에 대한 비용은 제안사에서 부담해야 한다.

❍ 납품되는 제품은 기존 건국대학교 GLOCAL캠퍼스의 장비 및 시스템(H/W, S/W, 네트워크 등)에 대하여 품질의 신뢰성, 안정성, 호환성, 연계성을 확보해야 한다.

❍ 검수완료 후에라도 제안사의 책임으로 발생되는 사고와 그로 인한 건국대학교 GLOCAL캠퍼스의 손해에 대하여는 제안사가 변상 조치해야 한다.

나. 검수

❍ 제안사는 검수 개시 일까지 제안요청서의 요구조건을 포함하는 시험항목 및 방법등을 기술한 검수계획서를 건국대학교 GLOCAL캠퍼스에 서면으로 제출하여 승인받아야 한다.

❍ 제안사는 감독관의 입회하에 각종 현장시험을 실시하여 정상 가동함을 입증해야 하며 규격확인이 어렵거나 미흡한 경우 관련 증빙서류 제출 및 기타 확인 과정을 통해 입증해야 한다.

❍ 현장시험에서 발견되는 에러나 문제점에 대하여 건국대학교 GLOCAL캠퍼스의 수정 및 보완 요구 사항이 제기되면 이를 수용해야 한다.

❍ 시험 운영에 필요한 장비 및 기기는 검수 기간 동안 무상으로 제공해야 한다.

❍ 검수 후 납품된 장비의 결함 등으로 인한 가동 중단횟수가 월 3회 이상 발생할 경우 제안사는 장비 일체를 동급의 신규제품으로 교체 지원해야 한다.

다. 품질보증

❍ 품질보증을 보장하기 위한 방안을 제시해야 한다.

❍ 제안사는 S/W에 대해서 해당 제조사와 개발사가 보증하는 정품 보증서와 S/W 원본(라이선스 포함)을 H/W 사양에 맞추어 검수 전까지 제출하여야 한다.

❍ 납품 완료된 시스템에 사용된 구성품(기능모듈, 이미지, 폰트 등) 중 라이선스가 존재하는 경우 각 구성품별로 라이선스를 제공하여야 한다.

❍ 규격의 누락 또는 기준 미달의 경우 계약해지의 사유가 될 수 있다.

❍ 시스템 구축에 사용되는 장비, 소프트웨어, 자료 등은 지적 재산권 침해 등 법적 문제가 없어야 하고, 향후 업그레이드가 가능하도록 구축하여야 한다.

라. 사업관리

❍ 사업 수행 조직 구성

- 제안사는 사업을 수행할 추진조직, 인력구성(약력 포함), 일정 단계별 인력투입 계획, 업무분장 내역 등을 제시하여야 한다.

- 투입된 인원의 변경이 필요한 경우 건국대학교 GLOCAL캠퍼스에 즉시 보고 및 승인을 얻어 동급 이상의 대체인력으로 변경하여야 한다.

❍ 사업 일정 수립

- 제안업체는 제시한 추진 일정을 참고하여 최적의 시스템이 구축될 수 있도록 추진 일정계획을 전체일정과 세부일정으로 구분하여 상세하게 제시하여야 한다.
- 일정계획 수립 시에는 지연가능 요소를 미리 파악·분석하여 일정 내에 사업 수행이 가능하도록 하여야 한다.

❍ 제출서류 및 산출물 관리

- 계약 시 제출 서류
  - ○ 장비납품 일정 및 세부작업 공정표를 계약 체결 후 10일 이내에 제출해야 한다.
  - ○ 보안서약서를 계약 후 10일 이내에 제출해야 한다.
- 납품 시 제출서류
  - ○ 각 납품 물품 상세명세서(소비자가, 납품단가) 1부를 제출해야 한다.
  - ○ 교육 지원 계획서, 시스템 설명서, 장비별 운영 방법 각 1부를 제출해야 한다.
- 검수 시 제출서류
  - ○ 납품업체는 납품 소프트웨어에 대하여 다음 서류 각 1부를 검수 개시 일까지 제출 해야 한다.
    . 사용설명서 1부
    . 사업 관련 산출물 1부
    . 사업수행계획서, 물품 상세명세서, 검수계획서 등 사업진행 시 작성된 모든 문서 (검수자료 책자 3부)
    . 시험항목 및 방법 등을 기술한 검수계획서 3부를 검수 개시 일까지 제출해야한다.

마. 유지보수

❍ 유지관리 운영체계

- 유지관리에는 제안사가 제안한 모든 제안 내역을 포함해야 한다.
- 유지관리는 검수완료일로부터 3년(24시간×365일)으로 하며, 제조사 정책상 상기 기간보다 긴 경우 그 기간을 적용해야 하며 무상 유지관리를 원칙으로 한다.
- 유지관리 관리방안 및 지원체계를 제시하고 유지관리 기간 중 년 2회 이상 예방점검 등을 실시해야 하여 그 결과를 건국대학교 GLOCAL캠퍼스에 제출해야 한다.

❍ 비상대응 체계 구축

- 제안사의 파업 등 다수의 인력 변동으로 유지관리에 지장을 초래하는 경우를 대비한 긴급 유지관리방안을 제시해야 한다.
- 바이러스 및 사이버공격 등으로 인하여 장비의 일부 또는 전체 장애가 발생된 경우에 대비한 비상 유지관리 방안을 제시해야 한다.

❍ 장애처리 및 지원

- 유지관리 대상 장비의 장애발생시 장애통보를 받은 즉시 정보시스템 서비스가 정상 수행 되도록 조치를 취한 후 4시간 이내에 도착하여 4시간 이내에 정상 가동 되도록 하여야 한다. 또한, 장애원인 및 해결방법을 제시하여 재발방지책을 강구해야 한다.
- 장애원인 분석결과 장애원인이 타 업체의 장애로 판단될 경우에도 구체적인 근거 자료를 제출하여야 하며, 타 업체의 장애조치에 최대한 협조해야 한다.
- 장애처리 및 복구는 제안사의 전문 인력을 투입해야 하며, 건국대학교 글로컬 캠퍼스와 24시간 비상연락체계를 항상 유지하여 신속한 장애복구가 가능하도록 해야 한다.
- 시스템 장애 발생 시 정상상태로 복구가 불가능하다고 판단될 경우 동종동급이상의 기기로 임시 대체하여 정상 가동되도록 해야 하며, 이를 위하여 대체장비를 사전에 보유해야 한다.
- 장애발생이 예상되거나 대상 장비 운용에 필요하다고 판단되는 경우 건국대학교 GLOCAL캠퍼스는 특별 점검을 요구할 수 있으며, 제안사는 점검계획을 수립하여 시행해야 한다.
- 제안사는 유지관리 대상 장비의 기능 및 성능이 최적의 상태로 가동될 수 있는 방안을 제시해야 한다.
- 반복적인 시스템 과부하 발생 또는 시스템 성능진단 및 과부하 테스트 요청 시 지원 및 개선방안을 제시해야 한다.
- 각 장비의 성능향상(Upgrade) 및 기능보완(Patch) 방안을 제시해야 한다.

바. 기술지원 및 교육

- 제안사는 검수 전 시스템 관련 기본교육 및 운용에 필요한 기술 자료를 건국대학교 GLOCAL캠퍼스의 관리자에게 충분히 제공하여야 한다.

❍ 제안사는 시스템 운영에 필요한 교육을 무료로 실시해야 하여야 한다.

❍ 신기술 및 선진사례 도입 등 각종 정보시스템의 효율적인 관리방안을 제시하여야 한다.

❍ 제안사는 납품된 장비 및 소프트웨어 관련분야의 정보기술에 대하여 지속적으로 정보를 제공하고 기술자문에 응해야 한다.

❍ 본 시스템을 확장하거나 타 장비와 연동이 필요한 경우 제안사는 필요한 제반 기술사항을 지원해야 한다.

사. 보안유지

❍ 물리적 보안대책, 관리적 보안대책, 기술적인 보안대책 등 보안 관리에 대한 운영규정을 마련하여 제시하고 비상사태에 대비하여야 한다.

❍ 사업 수행에 따른 투입요원의 출입통제, 자료의 누설 및 외부 유출 금지를 위한 대책을 수립하여야 한다.

- ❍ 시스템이 설치된 장소 및 시스템에 대한 접근은 인가받은 담당자에 한하여 접근하여야 한다.
- ❍ 납품되는 모든 장비는 보안취약점을 사전에 분석·제거한 후에 구축해야 한다.
- ❍ 제안사는 본 사업수행 중은 물론 완료 이후라도 사업수행 과정에서 취득한 시스템 구성, 데이터 내용 등에 대해 보안을 유지해야 하며 취득 자료의 정보 제공 및 누설로 인하여 발생되는 제반사항에 대한 모든 책임을 져야 한다.
- ❍ 사업 수행 완료 후 개발 장비 및 개인용PC에 저장된 건국대학교 GLOCAL캠퍼스 관련 데이터를 파기해야 한다.
- ❍ 본 과업에 참여하는 모든 제안사는 건국대학교 GLOCAL캠퍼스 정보보호 준수사항을 이행하여야 하며, 준수사항 위반 시에는 **[붙임1]**의 「정보화사업 용역업체 정보보호 준수사항」을 이행하여야 하며 준수사항 위반 시에는 **[별표1]**의 「사업자 보안 위규 처리기준」에 따라 책임을 져야 한다.

【붙임1】

정보화사업 용역업체 정보보호 준수사항

건국대학교 GLOCAL캠퍼스 가상화 구축 사업에 참여하는 용역업체는 다음 사항을 참고하여 정보보호 요구사항을 준수하여야 한다.

1. 일반사항
   가. **건국대학교 글로컬캠퍼스의 정보보호 정책, 지침 및 매뉴얼을 준수하여야 한다.**
   나. 본교의 자산에 접근하기 위해서는 본교의 접근 통제 절차를 준수하여야 한다.
   다. 본교는 계약서의 보안사항을 준수하고 있는지를 감사할 권한을 가진다.
   라. 본교의 감사 시 필요한 근거 자료를 제공하고 현장 실사에 적극 협조하여야 한다.
   마. 사업 수행에 사용되는 문서, 인원, 장비 등에 대하여 물리적, 관리적, 기술적 보안 대책 및 '누출금지 대상정보'에 대한 보안관리 계획을 제안서에 기재하여야 한다.
   바. 본교의 보안정책을 위반하였을 경우 「[별표1] 사업자 보안위규 처리기준 및 [별표2] 보안 위약금 부과 기준」에 따라 위규자 및 관리자를 행정조치하고 민형사상의 책임을 진다.

< 누출금지 정보 >

① 기관 소유 정보시스템의 내·외부 IP주소 현황
② 세부 정보시스템 구성현황 및 정보통신망구성도
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 네트워크장비 설정 정보
⑧ '공공기관의 정보공개에 관한 법률' 제9조1항에 따라 비공개 대상정보로 분류된 기관의 내부문서
⑨ '개인정보 보호법' 제2조1호의 개인정보
⑩ 그 밖의 발주자가 공개가 불가하다고 판단한 자료

2. 제3자의 직원에 대한 보안관리
   가. 참여직원에 대해서 각 개인의 친필 서명이 들어간 보안서약서를 제출한다.
   나. 참여직원은 임의로 교체할 수 없으며, 교체 시 본교의 승인을 받는다.

3. 내부 자료에 대한 보안관리

가. 업무 수행을 위해 제공하는 내부 자료는 자료관리대장을 작성하여 인수·인계 시 직접 서명한다.
나. 제공된 내부 자료에 대해 복사 및 외부반출을 할 수 없으며, 업무 완료 후 본교에 반환한다.
다. 제공된 내부 자료는 매일 퇴근 시 반납하여야 한다. 다만, 비밀문서를 제외한 일반문서는 제3자에 제공된 사무실에 시건장치가 된 보관함이 있을 경우 이를 보관함에 보관할 수 있다.
라. 본교는 제3자에 제공된 사무실에 보관된 자료에 대해서는 수시로 확인할 수 있다.

4. 장비에 대한 보안관리
가. PC(노트북 포함)는 반입시마다 최신 바이러스 백신프로그램 설치와 바이러스 감염여부를 확인하여야 한다.
나. 업무 수행을 위해 반입된 PC는 업무 종료 시까지 반출 할 수 없다. 다만, 불가피한 경우 본교의 승인 후 반출할 수 있다.
다. USB 등의 보조기억매체는 사용할 수 없다. 다만, 불가피한 경우는 본교의 승인 후 사용할 수 있다.
라. 업무 종료 시 PC 및 사용된 보조기억매체는 Format하고 본교의 승인 후 반출한다.

5. 내·외부망 접근에 대한 보안관리
가. 사용자 계정(ID)은 하나의 그룹으로 등록하고 사용자계정별로 정보시스템에 접근권한을 부여토록 한다.
나. 사용자계정별로 부여된 권한은 불필요 시 곧바로 권한을 해지하거나 계정을 폐기토록 한다.
다. 본교는 사용자별로 부여한 계정에 접속하여 저장된 자료와 작업 이력을 확인할 수 있다.
라. 담당자는 서버 관리자로 하여금 내부 서버에 대한 접근기록을 확인하도록 한다.
마. PC(노트북 포함)는 인터넷 연결을 금지한다. 다만, 불가피한 경우는 필요한 보안조치를 실시하고 본교의 확인 후 사용한다.

6. 기타 산출물에 대한 보안관리 등
가. 업무 수행 시 생산되는 모든 산출물은 담당 부서의 파일서버에 저장하거나, 본교에서 지정한 PC에 저장한다.
나. 업무 수행으로 생산되는 모든 산출물 및 기록은 본교가 인가하지 않은 자에게 제공·대여·열람을 금지한다.
다. 업무 수행으로 생산되는 모든 산출물 및 기록의 소유권 및 지적재산권은 본교에 있다.
라. 제3자에 의한 보안사고 발생 시 민·형사상의 모든 법적 책임은 제3자에게 있다.
마. 보안사고 발생 시 또는 인지 시에는 즉시 본교에 통보하여야 한다.

【별표1】

사업자 보안위규 처리기준

구 분	위 규 사 항	처 리 기 준
심각	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	◦ 사업 참여 제한 ◦ 위규자 및 직속감독자 등 중징계 ◦ 재발 방지를 위한 조치계획 제출 ◦ 위규자 대상 특별보안교육 실시
중대	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 수·발신 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 직속감독자 등 중징계 ◦ 재발 방지를 위한 조치계획 제출 ◦ 위규자 대상 특별보안교육 실시
보통	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 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	◦ 위규자 및 직속 감독자 등 경징계 ◦ 위규자 및 직속 감독자 사유서 / 경위서 징구 ◦ 위규자 대상 특별보안교육 실시

구 분	위 규 사 항	처 리 기 준
	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	
경미	1. 업무 관련서류 관리 소홀 가. 진행 중인 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	계약금액의 5%	계약금액의 3%	계약금액의 1%

* 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