

제 안 요 청 서

- 협의체 플랫폼 정보보안 및 네트워크 장비
유지보수 -



2024. 5.

한 국 항 공 우 주 연 구 원

목 차

I. 사업개요	3
II. 세부수행내용	4
III. 계약특수조건	16
IV. 입찰참가자격 및 계약방법	23
[부록] 제안서 작성요령 및 평가방법	24

I. 사업개요

1. 용역명

협의체 플랫폼 정보보안 및 네트워크 장비 유지보수

2. 용역기간

계약일로부터 2024년 12월 13일까지

3. 소요금액(추정)

66,842,000원(부가세포함)

4. 배경 및 목적

- 현재 한국항공우주연구원은 국가 수요의 위성정보를 안정적으로 공급하기 위하여 위성정보활용협의체 위성정보 서비스 플랫폼을 구축·운영하고 있음
- 이와 관련하여, 위성정보 서비스 플랫폼의 체계적인 관리와 안정적인 운영을 위해서는 정보보안 및 네트워크 장비 등에 대한 유지보수가 반드시 요구됨
- 따라서, 정보보안 및 네트워크 장비 등의 체계적인 유지보수를 통하여 위성정보 서비스 플랫폼의 안정적인 운영과 서비스 제공

5. 용역내용

- 원활한 통신환경 유지 및 고속 네트워크 사용 지원
- 각종 정보보안 장비의 안정적 운영을 위해 분석 등을 통한 불법침입·훼손 탐지 및 방지
- 서비스 관련 이슈 발생 시 전반적인 원인분석을 통해 예상되는 장비 진단 후 해결방안 제시 및 조치

- 대상 장비의 장애발생시 신속한 대응 및 복구
- 장비 및 통신의 서비스 문제 및 장애발생 방지를 위한 매월 정기 점검 실시 및 보고
- 장비의 주기적인 펌웨어 업그레이드 및 보안 패치를 통한 시스템 및 중요자료의 보호
- 시스템 취약점 진단 및 개선조치 수행
 - 대상장비 전체 시스템 취약점 진단
 - 개선조치 수행 이후에도 지속적인 취약점 모니터링 수행 및 조치수행
- 사용자 운영교육 및 교육매뉴얼 제공

II. 세부수행내용

1. 유지보수 대상 장비

구분	모델명	용도	수량	비고
보안 장비	SECUI MF2 2100	방화벽#1	1	
	SECUI MF2 2100	방화벽#2	1	
	Secuway U7000	VPN	1	
	SNIPER ONE-i 5000	IPS	1	
	AIWAF-2000	웹방화벽	1	
솔루션	Ahnlab EPP Patch	패치관리	1	
	카보나이트	DB 백업	1	
	WatchAll V11	서버/네트워크 관리	1	
서버 장비	HP DL380 G10	웹서버#1	1	
	HP DL380 G10	웹서버#2	1	
	HP DL380 G10	자료처리서버	1	

	HP DL380 G10	자료배포서버	1	
	HP DL380 G10	DB서버#1	1	
	HP DL380 G10	DB서버#2	1	
스토리지	QSAN XN8016R	NAS 스토리지	1	
네트워크 장비	PIOLINK PAS-K 3200	L4 스위치 #1	1	
	PIOLINK PAS-K 3200	L4 스위치 #2	1	
	ALE OS6900-X20	L2 스위치 #1	1	
	ALE OS6900-X20	L2 스위치 #2	1	
	ALE OS6900-X20	L2 스위치 #3	1	
	ALE OS6860-24	VPN 용 L2	1	
망연계 장비	i-oneNet 4.0	망연계서버#1	1	
	i-oneNet 4.0	망연계서버#2	1	
기타	SEIKO TS-2560	NTP 서버	1	
	m-Station	문자발송기	1	
KVM	ATEN CL-5780AN-AX-ATA-kk	KVM 스위치#1	1	
	ATEN KL-1516AN-AX-K	KVM 스위치#2	1	

2. 일반사항

- 신속한 유지보수를 위하여 유지보수 업체는 현장책임자를 지정하여 접수창구를 일원화하고 네트워크, 보안장비, 서버 등 엔지니어 참여인력들의 통합관리를 통해 점검 및 유지보수와 장애처리에 있어 발주처와 긴밀하게 협조 할 수 있도록 한다.
- 유지보수 인력은 설정사항 변경 및 기능개선 요청 시 신속히 처리하여야 하고, 그 사항에 대하여 기록 및 제출을 통해 이력관리를 수행 하여야 한다.

- 유지보수 인력에 대한 업무능력, 기술숙련도 등이 부적합하다고 판단되어 교체를 요구할 경우 이에 응해야 한다.
- 유지보수 인력은 필요시 야간근무 및 휴일근무를 수행해야 하며, 인력지원에 대한 부대장비 및 비용은 제안사가 부담한다.
- 유지보수 대상 장비에 대한 운영 매뉴얼을 숙지하고, 최초 점검 시 파일 및 문서형태로 제출하여야 한다. 또한 기능 업그레이드 등 매뉴얼 수정사항 발생 시 추가 배포해야 한다.
- 대상 장비의 정상적인 기능수행 및 성능개선
 - 장비의 구성내용과 설치내역을 완전히 숙지한다.
 - 장비의 환경설정, 설치, 변경, 성능측정 및 평가, 내·외부 모니터링 등의 포괄적 기능을 수행한다.
 - 관련 소프트웨어의 커스터마이징 및 업그레이드를 수행한다.
- 기술지원이 필요한 대상장비의 관련 증빙서류(제조사 기술지원 약속서 혹은 제조사 유지보수 계약서)를 제출하여야 한다.
- 모든 작업내용 및 처리사항 등은 지정양식에 의거 작성하며 작업 종료 시 제출하여야 한다(통합 유지보수 이력 관련 일지 작성 및 제출).
- 효율적인 장비 운영을 위하여 장비(네트워크, 보안장비, 서버 등) 재구성 등 발주처의 요청이 있는 경우 각 부문의 지원 방안을 제시한다.
 - 장비의 신·증설에 따른 작업을 무상으로 지원하여야 한다.
 - 장비 및 시스템 이전 시, 무상으로 지원하여야 한다.
- 대상 장비에 대한 정기점검은 매월 1회 이상 현장책임자와 담당 엔지니어가 함께 실시하며, 시스템의 상태 및 데이터 백업 수행의 일련의 행위를 수행하고 문서화 하여 제출한다.
- 과업기간 내 시스템 취약점 진단 및 개선조치 수행을 각각 1회 수행하고 결과보고서를 바탕으로 실제 취약점을 조치 후 수행내용 및 개선조치 결과를 정리하여 함께 제출하여야 한다.

- 대상 장비와 네트워크가 외부의 위협으로부터 문제발생 시 이에 대한 대응과 조치를 즉시 이행하고 지원해야 한다.

3. 대상 장비별 유지보수 내용

가. 네트워크 장비관리

- 네트워크 장비(라우터, 백본 스위치, 워크그룹 스위치 등)에 대한 환경설정, 가동상태 점검 등을 실시하여 정상적으로 가동될 수 있도록 하여야 한다.
- 네트워크 장비에 대해 24시간 관리운영기능(회선, 장애, 성능 등)을 지원하여야 한다.
 - KISTI 회선에 대한 상태관리 등을 포함하여 지원하여야 한다.
- 네트워크 장비의 운영체제 등에 대한 버전(version)을 업그레이드 하여 최신버전을 유지한다.
- 계약기간 중 1회 이상 내·외부 네트워크 트래픽 분석·점검하고 필요시 개선대책(속도 등) 방안을 보고하여야 한다.
- 네트워크 장비는 한국인터넷진흥원(KISA) 기술안내서 가이드를 참고하여 아래 예시 점검표 형식으로 점검항목에 대한 점검 수행 후 결과 및 조치사항을 보고 하여야 한다.

분류	점검항목
계정관리	패스워드 설정
	패스워드 복잡성 설정
	암호화된 패스워드 사용
	사용자, 명령어별 권한 수준 설정
접근관리	VTY 접근 (ACL) 설정
	Session Timeout 설정
	VTY 접속 시 안전한 프로토콜 사용
	불필요한 보조 입출력 포트 사용 금지
	로그온 시 경고 메시지 설정
패치관리	최신 보안 패치 및 벤더 권고사항 적용
로그관리	원격 로그서버 사용
	로그 버퍼 크기 설정
	정책에 따른 로깅 설정

기능관리	NTP 서버 연동
	timestamp 로그 설정
	SNMP 서비스 확인
	SNMP community string 복잡성 설정
	SNMP ACL 설정
	SNMP 커뮤니티 권한 설정
	TFTP 서비스 차단
	Spoofing 방지 필터링 적용
	DDoS 공격 방어 설정
	사용하지 않는 인터페이스의 shutdown 설정
	TCP keepalive 서비스 설정
	Finger 서비스 차단
	웹 서비스 차단
	TCP/UDP small 서비스 차단
	Bootp 서비스 차단
	CDP 서비스 차단
	Directed-broadcast 차단
	Source Routing 차단
	Proxy ARP 차단
	ICMP unreachable, Redirect 차단
	identd 서비스 차단
	Domain lookup 차단
	pad 차단
	mask-relay 차단
	스위치 허브 보안 강화

나. 정보보안 장비관리

- 협의체 기관과 위성정보 서비스 플랫폼 간 상호 운영하는 방화벽 등을 활용, 인터넷 서비스 접속을 차단함에 있어 발주처의 요청이 있는 경우 각 부문의 방안 수립 및 지원하여야 한다.
 - 협의체 기관 간 방화벽 정책설정을 위한 기술지원을 수행하여야 한다.
 - 위성정보 서비스 플랫폼 접속 및 관련문제 발생 시, 기관방문 등을 통해 무상으로 기술지원 업무를 수행하여야 한다.
- 신기술 적용이나 운영체제의 변화 등으로 발생하는 불일치를 조정하여야 한다.

- 방어정책 변경 시 망 운영에 지장이 없는 경우 업무시간에 진행하나, 지장이 있는 경우는 업무시간외에 수행한다.
- 최신의 보안패턴 및 엔진 업데이트를 제공·적용하여야 한다.
- KISTI 보안관제 및 회선에 대한 상태관리 등을 포함하여 지원하여야 한다.
- 각 보안시스템의 트래픽 통계 및 위성정보 서비스 플랫폼으로 유출·입 되는 다양한 침입유형에 따른 트래픽 분석을 계약기간 중 1회 이상 보고서를 제출해야한다.
- 정보보안 장비는 한국인터넷진흥원(KISA) 기술안내서 가이드를 참고하여 아래 예시 점검표 형식으로 점검항목에 대한 점검 수행 후 결과 및 조치사항을 보고 하여야 한다.

분류	점검항목
계정관리	보안장비 Default 계정 변경
	보안장비 Default 패스워드 변경
	보안장비 계정별 권한 설정
	보안장비 계정 관리
	로그인 실패 횟수 제한
접근관리	보안장비 원격 관리 접근 통제
	보안장비 보안 접속
	Session Timeout 설정
패치관리	벤더에서 제공하는 최신 업데이트 적용
로그관리	보안장비 로그 설정
	보안장비 로그 정기적 검토
	보안장비 로그 보관
	보안장비 정책 백업 설정
	원격 로그 서버 사용
	로그 서버 설정 관리
	NTP 서버 연동
DB 관리	정책 관리
	NAT 설정
	DMZ 설정
	최소한의 서비스만 제공
	이상 징후 탐지 경고 기능 설정
	장비 사용량 검토
	SNMP 서비스 확인
	SNMP Community String 복잡성 설정
	부가 기능 설정
	유해 트래픽 차단 정책 설정

다. 서버관리

- 매월 정기점검 시에 서버의 자원(Memory, CPU, Disk) 등에 대한 현황 및 성능을 파악하여 개선사항을 포함한 결과보고서를 제출하여야 한다.
- 서버 운영에 필요한 유지보수 업무수행 절차와 지침서를 마련하고 주기적으로 백업, 수시로 최신 버전으로 관리 및 각종 로그점검과 패치 등을 하여야 한다.
- 서버장비 백신 업데이트를 점검 기간내에 수행하여야 하며 KISA 사이버위협 경보단계 주의 이상 및 주요 보안 이슈 발생 시에도 비정기적으로 수행 하여야 한다.
- 서버 장비는 한국인터넷진흥원(KISA) 기술안내서 가이드를 참고하여 아래 예시 점검표 형식으로 점검항목에 대한 점검 수행 후 결과 및 조치사항을 보고 하여야 한다.

분류	점검항목
계정관리	Administrator 계정 이름 바꾸기
	Guest 계정 상태
	불필요한 계정 제거
	계정 잠금 임계값 설정
	해독 가능한 암호화를 사용하여 암호 저장
	관리자 그룹에 최소한의 사용자 포함
	Everyone 사용 권한을 익명 사용자에게 적용
	계정 잠금 기간 설정
	패스워드 복잡성 설정
	패스워드 최소 암호 길이
	패스워드 최대 사용 기간
	패스워드 최소 사용 기간
	마지막 사용자 이름 표시 안함
	로컬 로그인 허용
	익명 SID/이름 변환 허용
	최근 암호 기억
	콘솔 로그인 시 로컬 계정에서 빈 암호 사용 제한
	원격터미널 접속 가능한 사용자 그룹 제한

서비스관리	공유 권한 및 사용자 그룹 설정
	하드디스크 기본 공유 제거
	불필요한 서비스 제거
	IIS 서비스 구동 점검
	IIS 디렉토리 리스팅 제거
	IIS CGI 실행 제한
	IIS 상위 디렉토리 접근 금지
	IIS 불필요한 파일 제거
	IIS 웹 프로세스 권한 제한
	IIS 링크 사용 금지
	IIS 파일 업로드 및 다운로드 제한
	IIS DB 연결 취약점 점검
	IIS 가상 디렉토리 삭제
	IIS 데이터 파일 ACL 적용
	IIS 미사용 스크립트 매핑 제거
	IIS Exec 명령어 쉘 호출 진단
	IIS WebDAV 비활성화
	NetBIOS 바인딩 서비스 구동 점검
	FTP 서비스, 구동 점검
	FTP 디렉토리 접근 권한 설정
	Anonymouse FTP 금지
	FTP 접근 제어 설정
	DNS Zone Transfer 설정
	RDS (RemoteDataServices) 제거
	최신 서비스팩 적용
	터미널 서비스 암호화 수준 설정
	IIS 웹서비스 정보 숨김
	SNMP 서비스 구동 점검
	SNMP 서비스 커뮤니티스트링의 복잡성 설정
	SNMP Access Control 설정
	DNS 서비스 구동 점검
	HTTP/FTP/SMTP 배너 차단
	Telnet 보안 설정
	불필요한 ODBC/OLE-DB 데이터 소스와 드라이브 제거
	원격터미널 접속 타임아웃 설정

	예약된 작업에 의심스러운 명령이 등록되어 있는지 점검
패치관리	최신 HOT FIX 적용
	백신 프로그램 업데이트
	정책에 따른 시스템 로깅 설정
로그관리	로그의 정기적 검토 및 보고
	원격으로 액세스할 수 있는 레지스트리 경로
	이벤트 로그 관리 설정
	원격에서 이벤트 로그 파일 접근 차단
보안관리	백신 프로그램 설치
	SAM 파일 접근 통제 설정
	화면 보호기 설정
	로그온하지 않고 시스템 종료 허용
	원격 시스템에서 강제로 시스템 종료
	보안 감사를 로그할 수 없는 경우 즉시 시스템 종료
	SAM 계정과 공유의 익명 열거 허용 안 함
	Autologon 기능 제어
	이동식 미디어 포맷 및 꺼내기 허용
	디스크 볼륨 암호화 설정
	DoS 공격 방어 레지스트리 설정
	사용자가 프린터 드라이버를 설치할 수 없게 함
	세션 연결을 중단하기 전에 필요한 유희시간
	경고 메시지 설정
	사용자별 홈 디렉터리 권한 설정
	LAN Manager 인증 수준
	보안 채널 데이터 디지털 암호화 또는 서명
	파일 및 디렉토리 보호
	컴퓨터 계정 암호 최대 사용 기간
	시작프로그램 목록 분석
DB 관리	Windows 인증 모드 사용

4. 성능관리

- 유지보수 대상 장비의 자원(Memory, CPU, Disk, I/O Channel, DB Space 등)이 적정 수준의 여유율을 가지도록 수시로 점검하여

조치하여야 한다.

- 대상 장비 자원의 사용량 실태를 분석 및 조치하고, 그 결과를 보고하여야 한다.
- 주기적인 장비 및 OS 업그레이드 및 패치(보안패치 포함), Kernel, 환경파일 Parameter 수정 등 시스템 Performance 튜닝을 하여야 한다.
- 위성정보 서비스 플랫폼 특성상 인터넷을 이용한 업데이트가 불가하기 때문에 외부PC에서 파일을 준비하여 오프라인 형태로 패치 업데이트를 진행한다.

5. 장애관리

- 야간 및 공휴일의 장애에 대비하여 비상대응체계 수립해야 한다.
- 장애조치 요구 시에는 신속한 장애극복 및 대응을 위하여 유지보수 지원조직에서 2시간 이내에 현장에 도착하여야 하며, 장애발생 후 4시간 이내에 필요한 조치를 완료하여 정상 복구해야 한다. 복구 후 발생한 장애와 동일 유형의 장애가 24시간 이내에 다시 발생한 경우 미처리된 것으로 한다.
- 대상 장비의 장애/고장 발생 시 지체 없이 보고 후 신속히 조치해야 하며 장애처리완료 후 장애원인 분석, 해결 방법, 재발 방지책 등을 포함한 장애처리보고서를 제출하여야 한다.
- 장애발생에 따른 장비의 부속품 교체 시 교체부품은 동질 또는 그 이상의 부품으로 하며, 정상상태로 복구가 불가능하다고 판단될 경우 동종 기기로 임시 대체하여 정상가동을 보장해야 한다.
- 다른 유지보수업체가 관리하는 전산장비의 장애 발생 시 현장책임자와 관련 사항을 상호 협력하여 신속히 조치하여야 한다.
- 유지보수 기간 중 동일 장비에서 3회 이상 장애가 발생할 경우 동종 또는 그 이상의 장비로 교체하여야 한다.

6. 취약점 분석

- 시스템 주요장비에 대하여 취약점 점검 실시하고 이에 대한 보완

조치를 수행하여야 하며, 그 중 1회 이상은 정보시스템에 대한 기술적 취약점 진단 및 이행점검을 아래와 같이 실시 하여야 하며 조치결과 및 보안강화 방안 등을 포함하는 결과보고서를 제출 하여야 한다.

- 현황분석(취약점 대상 분석)
- 현황진단(장비별 취약점 진단, 전체 시스템 종합진단)
- 취약점 조치 (취약점 조치 지원)
- 취약점 분석을 통한 결과조치 완료 후에는 반드시 재점검을 수행 하여 발견된 취약점의 제거 여부를 확인하여야 한다.
- 이행점검 (취약점 조치여부 점검)

7. 헬프데스크 운영

- 유지보수 계약 체결 업체는 대상 장비 문제해결 요청에 원활하게 지원할 수 있도록 헬프데스크를 운영하여야 하며 접수담당 1인을 지정, 다른 유지보수업체가 관리하는 전산장비를 포함하는 각 부문별 상호 협력을 통해 신속한 상황 전파 및 조치가 될 수 있어야 한다.
- 즉시 처리가 가능한 건은 방문지원을 통하여 즉시 처리하고, 그렇지 않은 경우 담당 유지보수 지원팀과 연락하여 처리한다.
- 유지보수 업체는 유지보수 전담인원과 전담인원 부재 시 대체할 수 있는 인원을 지정하여야 하며, 전담 및 대체인력은 정보보안 및 네트워크에 대한 전문기술을 갖춘 자로 장비 관리, 운영, 장애 예방점검, 긴급복구 및 개선방향 수립 등의 업무를 수행할 수 있어야 한다.
- 유지보수 전담인원에 대한 교체는 발주처의 사전승인을 통해서만 교체가 가능하며, 인원교체 시에는 최소 동급 또는 그 이상의 기술자로 교체함을 원칙으로 한다.
- 유지보수 업체는 문제에 대한 해결책을 제시해야 하고 발주처 담당자와 협의하여 해결방안을 결정한다.

- 유지보수 업체는 문제접수에서부터 처리종료까지 상황을 보고하며 처리 지연 시 사유 및 처리예상가능 시간을 통보한다.
- 모든 유지보수 관련 요청 및 처리내역은 이력으로 문서화 관리하며 발주처 담당자에게 제출 및 보고한다.

8. 교육 및 기술지원

- 유지보수 업체는 네트워크장비, 정보보안장비 등에 대한 사용자운영교육을 연 2회 무상으로 지원하여야 하며, 이를 위해 필요한 교육매뉴얼은 별도로 작성하여 제공하여야 한다.
- 유지보수 업체 참여인력은 담당장비(네트워크장비, 정보보안장비 등)별 전문성을 바탕으로 기술 지원 업무를 수행하여야 하며 현장 책임자는 시스템 전체에 대한 이해를 바탕으로 종합적인 기술지원 업무를 수행해야 한다.

Ⅲ. 계약특수조건

1. 총 칙

이 특수조건은 한국항공우주연구원과 계약대상업체 간에 체결하는 “협업체 플랫폼 정보보안 및 네트워크 장비 유지보수” 계약에 적용한다.

2. 용 어

이 특수조건에서 사용하는 용어의 정의는 다음과 같다.

가. 한국항공우주연구원을 “발주기관”이라 한다.

나. 계약대상업체를 “수탁업체”이라 한다.

3. 계약기간

본 계약의 계약기간은 계약일로부터 2024년 12월 13일까지로 한다.

4. 수행범위

“수탁업체”는 본 제안요청서에 명시되어 있는 모든 내용을 차질 없이 수행하고 “발주기관”에게 그 결과를 보고한다.

5. 계약문서

가. 계약문서는 다음의 문서들로 구성되며 상호보완의 효력을 갖는다.

- 1) 계약서
- 2) 예산산출내역서
- 3) 제안요청서 및 제안업체제안서

나. 계약문서상 상이한 조항이 있을 경우 본 특수조건에 정하는 바를 우선하여 따른다.

6. 사업시행계획서

가. “수탁업체”는 계약체결 후 2주 이내에 계약서에 명시된 사항을 바탕으로 세부 추진일정표, 인력 및 자원 투입계획, 산출물의 종류/제출시기/매체 및 부수, 자체 추진계획 등이 포함된 사업시행계획서를 “발주기관”에게 제출하여 승인 받아야 한다.

- 나. “발주기관”이 지적하는 문제점 및 수정/보완 사항 등에 대하여 “수탁업체”는 신속한 대책 강구 등과 같은 성공적인 사업 수행을 위한 모든 조치를 취하여야 한다.
- 다. “발주기관”은 “수탁업체”에 대하여 용역업무 진행 및 확인을 위하여 필요한 자료를 요구할 수 있으며 “수탁업체”는 특별한 사유가 없는 이상 “발주기관”이 요구한 기일 내에 응하여야 한다.
- 라. 본 계약조건에 명시되어 있지 않은 사항은 “수탁업체”가 제출한 사업시행계획서에 따르되 계약문서와 사업시행계획서의 내용이 불일치 시에는 계약문서가 우선한다.

7. 인력투입 및 관리

- 가. “수탁업체”는 사업기간 중 원칙적으로 현장책임자, 실무작업자를 교체할 수 없으며, 부득이 교체하여야 할 경우에는 그 사유와 교체인원 명단 및 경력 등에 관한 서류를 “발주기관”에게 제출하여 승인을 받아야 한다.
- 나. “수탁업체”는 사업을 수행하는 과정에서 “수탁업체”의 직원의 부주의로 인하여 “발주기관”이 손해를 입었을 경우에는 이에 대한 모든 책임을 져야 한다.

8. 사업보고

- 가. “수탁업체”는 제안요구 내용에 따라서 작업을 수행하며, 사업수행과 관련된 제반 변동사항을 수시로 “발주기관”에게 보고한다.
- 나. “수탁업체”는 “발주기관”의 요구에 따라 사업의 시작과 중간 그리고 최종보고회를 개최하여야 한다.
- 다. “수탁업체”는 “발주기관”의 주관하여 월 1회 정기점검과 동시에 그 결과를 논의하는 회의를 개최하여야 하며, 필요시 상호합의에 따라서 수시로 회의를 개최할 수 있다.

구분	보고명	주요내용
정기보고	월간보고	월간실적, 차월계획, 문제점보고
수시 및 기타 보고	변경보고	업무의 수행방법 및 이에 따른 변경내역 보고
	위험관리 보고	잠재적 위험요소 발견 시 위험요소에 대한 조치방안 논의 및 처리 후 보고

9. 자료제공

- 가. “발주기관”은 사업수행과 관련하여 보유하고 있는 자료를 “수탁업체”에게 제공할 수 있으며, “수탁업체”는 사업종료와 함께 모든 자료를 반납하여야 한다.
- 나. “수탁업체”는 “발주기관”이 제공한 자료를 복제·복사 또는 제3자에게 제공·공개할 수 없으며, 기타 목적으로 사용할 수 없다.
- 다. “수탁업체”가 본 사업을 수행하면서 수집한 자료 및 생산한 모든 자료의 소유권은 “발주기관”에게 있고, 사업수행 완료 후 모든 자료는 “발주기관”에 제출하여야 하며, “발주기관”의 승인 없이 대외공개, 유통 등을 할 수 없다.

10. 사업수행 및 관리

- 가. “수탁업체”는 “발주기관”과의 계약에 따른 용역업무 수행을 위하여 각 파트별로 제3의 업체와 하도급 계약을 체결할 수 있으나, 이 경우 “발주기관”의 사전 승인이 요구되며 이를 어길 시에는 “발주기관”과 체결한 본 용역계약은 무효가 된다.
- 나. “수탁업체”는 사업수행에 있어 불가피한 일정조정 등의 사유가 발생할 시에는 지체 없이 “발주기관”에 통보하고 “발주기관”의 지시에 따른다.
- 다. 사업수행 장소는 “발주기관”과 “수탁업체”가 상호 협의하여 결정한다.

11. 설계변경

- 가. “발주기관”은 성공적인 과업완료를 위해서 필요에 따라서 설계

- 변경을 “수탁업체”에게 요청할 수 있으며, 이 경우 “수탁업체”는 “발주기관”과의 협의를 통하여 가능한 범위 내에서 이를 따른다.
- 나. “수탁업체”는 “발주기관”의 사전 동의 없이 임의대로 설계 변경하여 작업을 진행할 수 없으며, 사전승인 없이 진행된 작업에 대해서는 “발주기관”의 지시에 따라서 새로 작업하여야 한다.

12. 책임 및 의무사항

- 가. “수탁업체”는 “발주기관”과의 용역계약에 따른 성공적인 과업완수를 위한 책임을 갖는다.
- 나. “수탁업체”는 사업수행 중 계약서에 명시되어 있지 않다 하더라도, “발주기관”의 요구규격을 보장하기 위하여 추가적인 조치를 취하여야 한다.
- 다. “수탁업체”는 사업을 수행함에 있어 국내 제반법규 및 규정을 준수하여야 하며, 이에 대한 모든 책임은 “수탁업체”에 있다.
- 라. “수탁업체”는 “발주기관”이 제공하는 시설, 장비, 자료 등에 대하여 훼손하지 않도록 주의하여야 하며, 만약 “발주기관”의 시설, 장비, 자료 등을 훼손할 경우 이를 원상 복구하여야 한다.

13. 감독/검사

- 가. “수탁업체”는 제안된 작업을 종료하기 전에 최종 품질검사(인수검사)에 임해야 하며, 품질검사 시험절차는 “발주기관”에서 제시하는 방법에 따른다.
- 나. “수탁업체”는 매월 하드웨어 및 소프트웨어에 대한 이상 유무를 점검하여야 하며, 문제가 있는 장비 및 소프트웨어에 대해서는 “발주기관”에 보고 후 즉시 보완조치 하여야 한다.

14. 납품

- 가. “수탁업체”는 사업종료(납기만료) 전까지 “발주기관”의 최종품질검사를 득하여야 하며 “발주기관”이 요구하는 사항에 따라서 최종 산출물을 정리하여 사업종료(납기만료) 전까지 납품을 완료하여야 한다.

나. “수탁업체”는 아래의 산출물들을 반드시 포함하여 “발주기관”에게 최종 납품하여야 한다.

1) 보고서 : 2부(월별 유지보수 및 취약점 보고서 포함)

2.) 보고서 전자파일 : 1식(CD 제출)

15. 자료제출 및 반납

가. “수탁업체”는 “발주기관”이 사업진행 상태 점검 및 품질검사 등에 있어 필요로 하는 각종 자료를 제공하여야 한다.

나. “수탁업체”는 “발주기관”이 사업기간 동안 제공하는 모든 자료에 대하여 사업종료와 함께 원상태로 반납하여야 하며 이를 위반함으로써 발생하는 모든 책임은 “수탁업체”에게 있다.

다. “수탁업체”의 부주의로 “발주기관”이 제공한 자료에 대하여 파손·훼손 등이 발생한 경우에는 원상 복구하거나 실비로 보상하여야 한다.

16. 지식재산권

가. 사업완료와 함께 사업에 관련된 제반자료, 산출물 및 사업수행과정에서 획득되는 지식재산권은 「기획재정부 계약예규 제468호, 2019. 12. 18.(용역계약일반조건)」에 의거하여 공동으로 소유하며 “수탁업체”는 발주처의 동의 없이 지식재산권을 사용할 수 없다.

나. “수탁업체”는 본 사업과 관련된 내용을 “발주기관”의 승인 없이 대외적으로 발표·공개할 수 없다.

다. “수탁업체”는 본 사업으로 인하여 산출되는 제반자료, 산출물 및 기술정보 등 계약과 관련된 권리와 의무를 “발주기관”의 승인 없이 제3자에게 공개·양도할 수 없다.

라. “수탁업체”가 납품한 본 사업의 최종성과물에 대해 “발주기관”은 타 기관과 공동으로 활용할 수 있는 권한을 가진다.

17. 보안관리

- 가. “수탁업체”는 사업을 수행함에 있어 『국가공간정보 기본법』 “발주기관”의 『국가공간정보보안관리지침』을 준수하여야 하며, 이를 위반함으로써 발생하는 문제에 대한 모든 책임은 “수탁업체”에 있다.
- 나. “수탁업체”는 사업에 참여하는 임직원을 대상으로 보안각서를 작성 및 서명날인 후 “발주기관”에 제출하며, “수탁업체”는 사업에 참여하는 임직원을 대상으로 보안교육을 수행하여야 한다.
- 다. “수탁업체”는 사업을 수행함에 있어 “발주기관”이 제공한 자료에 대한 보안관리 대책을 수립하여 이행하여야 한다.
- 라. “수탁업체”는 “발주기관”이 제공하는 자료를 사전 승인 없이 복제·복사 및 유출하였을 경우에는 관계법률 및 규정에 따라 모든 책임을 진다.
- 마. “수탁업체”는 “발주기관”의 사전 승인 없이 “수탁업체”의 장비(PC, 노트북, USB 등)를 무단으로 반입할 수 없으며, “수탁업체” 직원 소유의 장비가 “발주기관” 근무지내로 반입되는 것을 차단하여야 한다.
- 바. “수탁업체”는 “수탁업체”의 직원이 “발주기관”의 시설에 불법으로 침입하였을 경우에는 “수탁업체”는 해당 직원을 사업에서 즉시 제외시켜야 한다.
- 아. “수탁업체”는 본 사업의 성과 및 품질을 비롯하여 기타 관련된 사항에 대하여 비밀을 유지하여야 하며 이를 위반함으로써 발생하는 모든 책임은 “수탁업체”에게 있다.

18. 계약해지

- 가. “발주기관”은 다음과 같은 사유가 발생한 때에는 계약을 해지할 수 있다.
 - 1) “수탁업체”가 계약내용 또는 관계법령을 위반하는 등의 사유로

원활한 사업수행이 곤란하다고 인정될 경우

- 2) “수탁업체”가 기술 및 품질요구사항을 만족시키지 못하며, 이를 만족시키기 위한 대책 및 노력 등이 부족하여 정상적인 사업수행이 불가능 하다고 판단될 경우
- 3) “수탁업체”의 사정으로 사업수행이 불가능한 경우, 이 경우 “수탁업체”는 최소 1개월 전에 사업수행이 불가능하다는 것을 “발주기관”에 통보하여야 한다.

나. “수탁업체”는 계약해지를 통보받은 즉시 그 동안의 모든 작업성과물을 “발주기관”에게 인도하여야 한다.

19. 과업심의위원회

가. (과업내용 확정 심의 여부) 본 사업은 「소프트웨어 진흥법」 제50조에 따른 과업내용 확정을 위하여 과업심의위원회를 (✓)개최 또는 ()미개최 한 사업임

나. (과업내용 변경) 본 사업은 「소프트웨어 진흥법」 제50조, 같은법 시행령 제47조 제1항 제2호, 제3호에 따른 과업내용 변경 및 그에 따른 계약금액·계약기간 조정이 필요한 경우, 계약상대자는 국가기관등의 장에게 소프트웨어사업 과업변경요청서*를 제출하여 과업심의위원회 개최를 요청할 수 있으며, 국가기관등의 장은 과업심의위원회 개최요청에 대해서 특별한 사정이 없으면 수용해야 함 (*「소프트웨어사업 계약 및 관리감독에 관한 지침」 별지 13호서식 참조)

20. 기타

가. 본 사업은 하도급을 불허하는 사업임

나. 본 사업을 시행함에 있어 작업내용이 상이하여 해석의 차이가 있는 경우에는 “수탁업체”는 “발주기관”의 지시에 따라야 한다.

다. 본 계약특수조건에 명시되지 않은 사항은 “발주기관”과 “수탁업체”가 협의하여 결정한다.

IV. 입찰참가자격 및 계약방법

1. 입찰참가자격

- 가. '국가종합전자조달시스템 입찰참가등록규정'에 따라 입찰접수마감일 전일까지 소프트웨어사업자(컴퓨터 관련 서비스사업)(업종코드: 1468) 와 정보통신공사업(업종코드: 0036)으로 입찰참가자격 등록을 완료한 자
- 나. '중소기업제품 구매촉진 및 판로지원에 관한 법률'제8조의 중소기업자로서'중소기업 범위 및 확인에 관한 규정'에 따라 발급된 중소기업/소기업/소상공인 확인서를 소지하고 동 법률 제9조에 의한 직접생산확인증명서(정보시스템유지관리서비스)를 소지한 업체
- 다. 대전광역시에 주된 영업소 업무 신고를 한 자

2. 계약방법

- 가. 「국가를 당사자로 하는 계약에 관한 법률 시행령」 제43조에 의거 “협상에 의한 계약체결” 방식으로 선정한다.
- 나. 입찰가격이 예정가격 이하인 자로서, 제안서 평가를 통해 기술점수의 85%이상을 득한 자를 협상적격자로 선정하며, 기술평가점수(90%)와 가격점수(10%)를 합산하여 협상적격자 중 고득점 순에 따라 우선협상대상자를 선정한다.

[부록]

제안서 작성요령 및 평가방법

I. 제안서 작성요령

1. 제안서 제출

- 가. 마감일 : 입찰공고문 참조
- 나. 접수처 : 입찰공고문 참조
- 다. 제안서 수량 : 총 6부(전자파일 CD 1식)

2. 제안서 작성요령

- 가. 제안서는 반드시 제안서 작성 목차 및 순서에 따라서 간단명료하게 작성한다.
- 나. 제안서는 한글 작성을 원칙으로 하며, 사용된 영문약어에 대해서는 설명을 하여야 한다.
- 다. 제출된 제안서의 내용은 수정 또는 추가할 수 없다. 단, 발주처가 추가자료 또는 보완을 요청할 경우에는 그 자료는 제안 당시의 내역으로서 효력을 갖는다.
- 라. 제안서 내용에 “가능하다”, “할수있다”, “고려한다” 등의 모호한 표현은 불가능한 것으로 해석하여 처리한다.
- 마. 제안사가 제시하는 기술 및 품질확보 측면의 가능성에 대해서는 명확한 근거자료를 함께 제시하여야 하며, 그렇지 않은 경우에는 불가능한 것으로 판단하여 처리한다.
- 바. 제안사가 본 제안요청서의 요구사항 이상의 규격을 제안하는 경우 별도의 제안내용과 함께 객관적 근거자료를 발주처에 제출할 수

있다. 한편 그 반대의 경우에도 그러하다.

아. 제안서는 A4 종방향 작성을 원칙으로 작성하여 3 hole 바인더를 사용하여 제출한다.

3. 유의사항

가. 제안서 내용에는 제안가격과 관련된 내용이 포함되어서는 안 된다.(제안가격은 별도로 밀봉하여 구매(계약)부서에 제출)

나. 제안서의 내용을 객관적으로 입증할 수 있는 관련 자료는 제안서에 포함하여 작성하되, 부득이한 경우에는 별첨 자료로 제출한다.

다. 제안서는 허위나 단순한 추측으로 작성해서는 안 되며, 모든 기재사항은 객관적으로 입증할 수 있어야 하고, 향후 허위로 작성된 사실이 발견될 경우에는 심사대상에서 제외한다.

라. 제출된 제안서는 일체 반환하지 않으며, 본 제안과 관련된 일체의 소요비용은 제안사의 부담으로 한다.

마. 발주처가 제안내용 확인을 위한 추가 자료요청 및 현지실사를 요구할 경우 제안사는 이에 반드시 응하여야 한다.

바. 계약된 업체의 제안서는 본 제안요청서와 함께 계약서의 일부로 한다.

4. 제안서 목차 및 작성순서

목 차	작성순서	작성내용	비고
1. 제안업체 일반현황	전문 인력 현황	조직 및 보유인력 현황 작성(전문분야별로 작성)	
	유사용역 수행실적	유사용역 수행실적 작성 및 실적증명서 첨부	
	재정상태	신용평가서 제출	
2. 사업이해	사업의 이해도	제안요청 내용에 대한 구체적 분석내용 작성	
	사업의 범위 및 내용	제안내용에 대한 이해를 바탕으로 제안사의 제안범위 및 내용작성	
3. 사업수행	사업목표 실현방안	제안사의 구체적인 실현계획 작성 및 제안	
	사업 추진체계 및 전략	전체 및 세부내용별 구체적 사업 추진체계 및 추진전략 작성	
4. 시스템 관리	장비점검 및 관리방안	전체 장비에 대한 점검 및 관리를 위한 세부적인 방안 제시	
	장애대응 및 위기관리방안	장애발생에 따른 대응 및 위기관리 방안 제시	
	시스템 취약점 진단 및 개선조치 방안	시스템 대상장비별 취약점 진단 방법과 개선조치 방안 제시	
5. 사업관리	사업수행 일정 및 계획	전체사업일정 및 항목별 추진일정과 계획 작성	
	조직구성 및 인력운영 방안	제안사의 인력투입 계획 및 효율적 인력운영 방안 제시	
	참여자의 보안교육 및 관리	참여인력의 보안의식 재고 방안 등 구체적 보안관리 대책 제시	
	사용자교육 지원	발주기관 사용자에게 대한 교육지원 방안 제시	
별첨자료	증빙 및 근거자료		

II. 제안서 평가기준 및 방법

제안서 평가항목 및 배점한도

목 차	평가항목	평가기준		비고
제안업체 일반현황 (15)	전문 인력 현황	산정방식 참고	5	
	유사용역 수행실적	산정방식 참고	5	
	재정상태	산정방식 참고	5	
사업이해 (10)	사업의 이해도	사업의 목표, 특성 및 환경 등에 대한 이해	5	
	사업의 범위 및 내용	사업의 주요업무 범위 및 수행 업무에 대한 이해	5	
사업수행 (15)	사업목표 실현방안	성공적 사업수행을 위한 제안사의 구체적 방안	7.5	
	사업 추진체계 및 전략	추진전략의 타당성 및 실현 가능성	7.5	
시스템관리 (30)	장비점검 및 관리방안	장비점검 및 관리에 대한 구체적인 방안	10	
	장애대응 및 위기관리방안	장애대응 및 위기관리 시나리오의 구체성 및 타당성	10	
	시스템 취약점 진단 및 개선조치 방안	시스템 대상장비별 취약점 진단 방법과 개선조치 방안	10	
사업관리 (20)	사업수행 일정 및 계획	추진일정 합리성 및 계획의 타당성	5	
	조직구성 및 인력운영 방안	투입 인력의 적정성 및 인력운영의 효율성	5	
	참여자의 보안교육 및 관리	보안체계의 적정성 및 보안대책의 확신성	5	
	사용자교육 지원	사용자 교육내용의 적절성 및 효율성	5	
입찰가격 평가	협상에 의한 계약체결 기준의 입찰가격 평점산식 적용		10	
합계			100	

※ 기술부문 평가점수는 기술평가위원들 점수 중에서 최고점수와 최저점수를 제외한 평균점수로 산정

[산정방식]

제안업체 일반현황 평가기준

1. 전문인력 현황

- 가. 정보보안 및 네트워크장비 관리 분야에 종사하는 전문 인력(일반사무, 영업 인력은 제외)에 한하여 평가하며 이를 증명하기 위한 기술경력증서본 또는 국가기술자격증 사본을 제출하여야 한다.
- 나. 입찰공고일 현재 당해업체에 재직 중이어야 하며, 재직 중임을 객관적으로 입증할 수 있는 4대 보험(국민연금, 의료보험, 고용보험, 산재보험) 중 1개가 첨부된 인원에 대하여 평가한다.
- 다. 증빙서류 미첨부시 평가에서 제외한다.

구 분	10명 이상	10명 미만 5명 이상	5명 미만
배 점(5)	5	4	3

2. 유사용역 수행실적

- 가. 최근 5년간(공고일 기준) 국가, 지방자치단체, 정부투자기관, 출연연구원, 민간기업 등에서 발주하여 수행한 용역실적을 기재한다.
- 나. 유사용역의 범위는 정보보안 및 네트워크장비 유지보수 용역으로 제한한다.
- 다. 총괄(장기계속계약)에 따른 연차별 준공실적은 단일 건으로 평가한다.
- 라. 발주처 발행 실적증명서가 첨부된 실적에 대해서만 평가하며 실적건수와 실적금액의 점수를 합산한다.

1) 실적건수

구 분	10건 이상	10건 미만 5건 이상	5건 미만
배 점(2.5)	2.5	2	1.5

2) 실적금액

구 분	1억 이상	5천 이상 1억 미만	5천 미만
배 점(2.5)	2.5	2	1.5

3. 재정상태

가. 신용평가등급에 의한 재정상태 평가

회사채에 대한 신용평가등급	기업어음에 대한 신용평가등급	기업신용평가 등급	배 점
AAA	-	AAA (회사채에 대한 신용평가등급 AAA에 준하는 등급)	5.0
AA+, AA0, AA-	A1	AA+, AA0, AA- (회사채에 대한 신용평가등급 AA+, AA0, AA-에 준하는 등급)	4.8
A+	A2+	A+ (회사채에 대한 신용평가등급 A+에 준하는 등급)	4.6
A0	A20	A0 (회사채에 대한 신용평가등급 A0에 준하는 등급)	4.4
A-	A2-	A- (회사채에 대한 신용평가등급 A-에 준하는 등급)	4.2
BBB+	A3+	BBB+ (회사채에 대한 신용평가등급 BBB+에 준하는 등급)	4.0
BBB0	A30	BBB0 (회사채에 대한 신용평가등급 BBB0에 준하는 등급)	3.8
BBB-	A3-	BBB- (회사채에 대한 신용평가등급 BBB-에 준하는 등급)	3.6
BB+, BB0	B+	BB+, BB0 (회사채에 대한 신용평가등급 BB+, BB0에 준하는 등급)	3.4
BB-	B0	BB- (회사채에 대한 신용평가등급 BB-에 준하는 등급)	3.2
B+, B0, B-	B-	B+, B0, B- (회사채에 대한 신용평가등급 B+, B0, B-에 준하는 등급)	3.0
CCC+ 이하	C 이하	CCC+ 이하 (회사채에 대한 신용평가등급 CCC+에 준하는 등급)	2.8

【별지 제2호 서식】

주요사업실적(최근 5년)

사 업 명	발주처	사업기간	총사업금액	계약금액	수행분야	비고

- 최근 5년간(공고일 기준) 국가, 지방자치단체, 정부투자기관, 출연연구원, 민간기업 등에서 발주하여 수행한 용역실적을 기재한다.
- 유사용역의 범위는 정보보안 및 네트워크장비 유지보수 용역으로 제한한다.
- 총괄(장기계속계약)에 따른 연차별 준공실적은 단일 건으로 평가한다.
 - 공공도급계약일 경우에는 계약금액란에 제안사의 지분만을 기재
- 실적증명서 등 증빙자료 첨부

【별지 제3호 서식】

참여인력 이력사항

성명		소속		직책		연령	세
학력	대학교		전공	해당분야근무경력		년	개월
	대학원		전공	자 격 증			
본사업참여임무			사업참여기간			참여율	%

경 력				
사 업 명	참여기간 (년월~년월)	담당업무	발주처	비고

【별지 제4호 서식】

제안서 표지 규격(A4)

『협의체 플랫폼 정보보안 및 네트워크 장비
유지보수』 용역사업

제 안 서

2024. 5.



[별첨 1]

용역 계약업체 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 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 마. 참여인원에 대한 보안서약서 미징구 및 교육 미실시 2. 사무실(작업장) 보안관리 허술 가. 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, USB 등 보조기억매체 기술적 통제 미흡 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. 제공된 계정관리 미흡 및 오남용(시스템 불법접근 시도 등) 자. 바이러스 백신 정품 S/W 미설치	○ 위규자 및 직속감독자 등 중징계 ○ 재발 방지를 위한 조치계획 제출 ○ 위규자 대상 특별보안교육 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 다. 중요정보에 대한 자료 인수·인계 절차 미 이행 2. 사무실 보안관리 부실 가. 캐비넷·서류함·책상 등을 개방한 채 퇴근 나. 출입키를 책상위 등에 방치 3. 보호구역 출입 소홀 가. 통제·제한구역 출입문을 개방한 채 근무 나. 보호구역내 비인가자 출입허용 등 통제 불순응 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 단순 숫자 부여 마. PC 비밀번호를 모니터옆 등 외부에 노출 바. 비인가 보조기억매체 무단 사용 사. 정보시스템 반입시 바이러스 백신 미검사 또는 반출시 자료 삭제 미확인 아. 바이러스 백신 최신 업데이트 또는 정밀점검 미실시	○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 다. PC 월 1회 보안 점검 미이행	○위규자 서면·구두 경고 등 문책 ○위규자 사유서 / 경위서 징구

※ 용역 계약업체 보안위규 처리 절차



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	총 사업비의 8%	총 사업비의 5%	총 사업비의 2%

※ A급은 국가계약법 시행령 제76조에 따라 부정당업자로 지정하여 입찰참가를 제한

* 위규 수준은 보안위규 처리기준 참고

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

3. 용역 종료시 지출금액 조정을 통해 위약금 정산

보안 준수사항 - 사업수행업체

1. 공통사항

- 사업 수행과정에서 취득한 자료와 정보에 관하여 사업수행중은 물론 사업완료 후에도 이를 외부에 유출해서는 안되며, 사업종료시에는 완전 폐기 또는 반납해야 한다.
- 사업자는 사업 수행에 사용되는 문서, 인원, 장비 등에 대하여 물리적, 관리적, 기술적 보안대책 및 '누출금지 대상정보'에 대한 보안관리 계획을 수행계획서 또는 계약서에 기재하여야 하며, 해당 정보 누출시 발주기관은 국가계약법 시행령 제76조에 따라 사업자를 부정당업체로 등록한다.

< 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 국가용 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 대상 정보로 분류된 기관의 내부분서
- ⑨ '개인정보 보호법' 제2조1호의 개인정보
- ⑩ '보안업무규정' 제4조의 비밀, 동 시행규칙 제7조3항의 대외비
- ⑪ 그 밖의 발주자가 공개가 불가하다고 판단한 자료

- 사업자는 연구원의 보안정책을 준수하여야 하며, 이를 위반하였을

경우 위규처리기준(별첨1)에 따라 관련자에 대하여 조치하고 보안
위약금 부과기준에 따라 손해배상 책임을 진다.

- 정보시스템 신규 구축사업의 경우, 최종산출물(정보시스템, 홈페이지 등)에 대해 정보보안 전문가 또는 전문 보안점검도구를 활용하여 보안 취약점을 점검하고, 도출된 취약점에 대해 개선 완료한 결과를 제출해야 한다.

※ 사업에서 자체점검이 어려운 경우, IT정보보안실과 협의하여 추진

2. 참여인원에 대한 보안관리

- 용역사업 참여인원중 보안책임관을 지정하여 연구원의 승인을 받아야 한다.
- 용역사업 참여인원은 보안서약서(별첨2-2)에 자필서명 후, 연구원에 제출하여야 한다.
- 용역사업 참여인원은 업체 임의로 교체할 수 없으며, 신상변동(해외여행 포함)사항 발생 즉시 보고하여야 한다.
- 참여인원에 대하여 월1회 정보보안교육을 수행하고, 교육결과에 대하여 발주기관의 확인을 받아야 한다.

3. 자료에 대한 보안관리

- 사업수행으로 생산되는 산출물 및 기록은 보안책임관이 인가하지 않은 자에게 제공.대여.열람을 금지한다.
- 사업관련 자료 및 사업과정에서 생산된 산출물은 보안책임관이 지정한 PC 등(반드시 인터넷과 분리)에 저장.관리하여야 하며, 계정관리 및 계정별 접근권한 부여 등을 통하여 접근을 제한하여야 한다.
- 과업지시서 등에 명시한 누출금지 대상정보를 사용할 경우 자료관리 대장을 작성하여 인계.인수자가 직접 서명한 후 사용하고, 사업완료시 관련 자료는 반드시 반납하여야 한다.
- 사업관련 자료는 인터넷 웹하드.P2P 등 인터넷 자료공유사이트 및 개인메일함 저장을 금지하고 발주기관과 사업수행업체간 자료전송이 필요한 경우는 자사 전자우편을 이용하여 송.수신하고

메일을 확인하는 즉시 삭제하여야 한다.

※ 다만, 대외비 이상의 비밀은 전자우편으로 송수신 금지

- 사업완료 후 생산된 최종 산출물은 인수·인계서를 통하여 발주기관에 반납하고, PC 완전삭제 등 보안조치를 통해 사업관련 산출물(중간산출물 포함)을 모두 삭제하여야 하며, **대표자 명의 확약서(별첨2-1)**를 연구원에 제출하여야 한다.

※ 확약서 제출 시 산출물 인수·인계서와 자료삭제기록(날짜가 포함된 증빙사진 등)을 제출하여야 한다.

4. 사무실·장비에 대한 보안관리

- 사업을 수행하는 장소(이하 사업장)는 CCTV·시건장치 등 비인가자 출입통제대책이 마련된 사무실을 사용하여야 한다.
- 사업장에서 사용하는 모든 정보시스템에 대하여 정보시스템 관리대장을 작성하고 변경사항에 대해 현행화하여야 한다.
- 사업장의 정보시스템에 바이러스 백신 정품 S/W를 설치하고, 자동 업데이트, 실시간 점검을 수행하는 지 수시로 점검하여야 한다.

5. 내·외부망 접근에 대한 보안관리

- 연구원 내부망에 대한 접속은 반드시 연구원의 승인을 득한 후 사용하여야 한다.
- 사업 참여인원이 연구원의 정보시스템에 접근하는 경우
 - 사용자 계정은 하나의 그룹으로 등록하고 계정별로 접근권한을 차등 부여하되 기관내부문서의 접근을 금지하여야 한다.
 - 계정별로 부여된 접근 권한은 불필요시 즉시 권한을 해지하거나 계정을 폐기하여야 한다.
 - 계정별 패스워드는 보안정책(숫자, 영문자, 특수문자 등을 혼합하여 9자리 이상)에 부합되어야 하며 보안책임자가 별도로 기록 관리하여 변경이력을 수시로 확인하여야 한다.

[별첨 2-1]

보안확약서

본인은 귀 기관과 계약한 _____ 사업의 수행을 완료함에 있어, 다음 각 호의 보안사항에 대한 준수 책임이 있음을 서약하며 이에 확약서를 제출합니다.

1. 본 업체는 업체 및 사업 참여자가 사업수행 중 지득한 모든 자료를 반납 및 파기하였으며, 지득한 정보에 대한 유출을 절대 금지하겠습니다.
2. 본 업체는 하도급업체에 대해 상기 항과 동일한 보안사항 준수 책임을 확인하고 보안확약서 징구하였으며, 하도급업체가 위의 보안사항을 위반할 경우에 주사업자로서 이에 동일한 법적 책임을 지겠습니다.
3. 본 업체는 상기 보안사항을 위반할 경우에 귀 기관의 사업에 참여 제한 또는 기타 관련 법규에 따른 책임과 손해배상을 감수하겠습니다.

이월

이

서약업체 대표

소속 :

직 급 :

성명 :

(서명)

한국항공우주연구원장 귀하

[별첨 2-2]

보안서약서

본인은 ____년 ____월 ____일부로 _____관련 용역(업무)을 수행함에 있어 다음사항을 준수할 것을 엄숙히 서약합니다.

1. 본인은 _____관련 업무 중 알게 될 일체의 내용(개인 정보 포함)이 직무상 기밀 사항임을 인정한다.
2. 본인은 이 기밀을 누설함이 국가안전보장 및 국가이익에 위해가 될 수 있음을 인식하여 업무수행 중 취득한 제반 기밀사항을 일체 누설하거나 공개하지 아니한다.
3. 본인이 이 기밀을 누설하거나 관계 규정을 위반한 때에는 관련 법령 및 계약에 따라 민형사상의 책임을 지고 어떠한 처벌 및 불이익도 감수한다.

년 월 일

서 약 자	업 체 명 :	
	직 위 :	
	성 명 :	(서명)

서약집행자	소 속 :	
(부서장)	직 위 :	
	성 명 :	(서명)

[별첨 2-4]

외주 용역 보안특약

1. 용역 수행 업체는 용역 수행 전후를 막론하고 한국항공우주연구원의 보안정책을 위반하였을 경우 민.형사상의 책임을 면할 수 없다.
2. 용역 수행 업체는 용역 수행에 사용되는 문서, 인원, 장비 등에 대하여 물리적, 관리적, 기술적 보안대책 및 [별표1]의 ‘누출금지 대상정보’에 대한 보안관리계획을 용역제안서에 기재하여야 하며, 해당 정보 누출시 한국항공우주연구원은 국가계약법 시행령 제76조에 따라 용역 수행 업체를 부정당업체로 등록한다.
3. 용역 수행과정에서 취득한 자료와 정보에 관하여 용역수행 중은 물론 용역 완료 후에도 이를 외부에 유출해서는 안 되며, 용역 종료시 정보보안담당자의 입회하에 완전 폐기 또는 반납해야 한다.
4. 용역 수행업체는 용역 최종 산출물에 대해 정보보안전문가 또는 전문보안 점검도구를 활용하여 보안 취약점을 점검, 도출된 취약점에 대한 개선을 완료하고 그 결과를 제출해야 한다.

일 일 일
월 월 월
년 년 년

회 사 명 :

대 표 자 : (서명)

[별첨 3]

소프트웨어 과업변경요청서

※ []에는 해당되는 곳에 √ 표를 합니다.

접수번호		접수일		처리기간 14일	
변경요청 번호					
사 업 명					
계약번호					
변경요청 유형		[] 과업내용 변경 [] 과업내용변경 및 계약금액 조정			
과업내용서 관련사항		기 존		변 경	
변경요청 내용		(※ 필요한 경우 별지 사용)			
변경요청 사유		(※ 필요한 경우 별지 사용)			
변경 영향평가		(※ 필요한 경우 별지 사용)			
변경 소요 비용		소요비용		변경규모	
		산출근거	(※ 필요한 경우 별지 사용)		

「소프트웨어 진흥법」 제50조제3항에 따라 위와 같이 소프트웨어사업 과업 내용변경을 요청합니다.

111 112 113

신청인

(서명 또는 인)

발주기관의 장 귀하

처리 절차

신청서 작성	→	접 수	→	과표심의위원회 개최	→	심의·의결	→	심의결과 및 조치계획 통보
신청인				처리 기관: 발주 기관				

210mm×297mm[백상지 80g/m²]

주 의 사 항

1. 본 제안요청서의 내용을 임의로 수정하여서는 아니 된다.
2. 본 제안요청서는 복제하여 제3자에게 배포·제공해서는 아니 된다.
3. 본 제안요청서에 의문사항이 있는 경우, 국가위성정보활용지원센터 위성활용부 담당자에게 문의하여야 한다.