제 안 요 청 서

「2027~2029년 초록우산 하이브리드 보안관제 및 정보보호시스템 운영 용역」

2026. 10.

초록우산

목 차

Ⅰ. 사업개요 02

Ⅱ. 사업 범위 05

Ⅲ. 제안요청 내용 08

Ⅳ. 사업 수행 지침 28

Ⅴ. 제안 안내 사항 30

Ⅵ. 제안서 작성 요령 31

Ⅶ. 제안서 평가 및 선정 32

[별지1 서식] 용역사업 제안서

[별지2 서식] 일반현황 및 주요 연혁

[별지3 서식] 사업 실적

[별지4 서식] 사업수행 조직도

[별지5 서식] 참여인력 현황

[별지6 서식] 제안요청서 수용여부 참조표

[별표1] 기술인력의 자격기준

Ⅰ 사업개요

❍ 사 업 명: 2027~2029년 초록우산 하이브리드 보안관제 및 정보보호시스템 운영 용역

❍ 사업기간: 2027. 1. 1. ~ 2029. 12. 31. (36개월) / 장기계속계약

❍ 사업금액: 금840,000,000원(금팔억사천만원, VAT포함)

* 본 사업은 장기계속계약으로 차수계약을 체결하며, 3년치 총액기준으로 투찰하여야 함

* 재단 사정에 따라 사업범위 및 예산은 변동될 수 있음

❍ 입찰방법: 일반(총액)협상에의한계약

1. 사업목적

❍ 24시간 365일 원격 보안관제와 상주 보안관제를 연계한 하이브리드 보안관제 체계를 구축·운영하여 지능화·고도화되는 사이버위협에 대한 상시 대응체계 확보

❍ 정보보호시스템의 전문적이고 체계적인 운영을 통해 시스템 안정성과 보안정책의 일관성을 확보하고 침해사고 대응역량 강화

❍ 취약점 진단, 모의해킹, 정보보호 관리체계 점검 및 교육 등 예방·개선 활동을 통해 재단의 정보보호 수준 지속 향상

2. 주요 사업내용

❍ **하이브리드 보안관제 운영**

- 24시간 365일 원격 보안관제와 평일 주간 상주 보안관제를 연계한 상시 보안관제 수행
- 관제대상 정보보호시스템 및 정보시스템의 보안이벤트·로그 모니터링, 이상징후 탐지·분석 및 대응
- 관제 연계·로그수집 상태 관리, 정기·비정기 보고 및 최신 사이버위협 정보 제공

❍ **정보보호시스템 운영**

- 기존 및 신규 구축되는 정보보호시스템의 운영·관리, 보안정책 관리·최적화 및 장애 대응
- 정보보호시스템의 신규 구축·교체·증설·구성변경 지원과 운영 전환 및 안정화

❍ **침해사고 분석 및 대응**

- 침해사고 및 침해사고 의심 상황에 대한 분석, 초동대응 및 피해확산 방지
- 사고원인 분석, 복구 및 재발방지 대책 수립 지원

○ **취약점 진단 및 모의해킹**

- 정보시스템 및 정보보호시스템에 대한 기술적 취약점 진단과 주요 웹·앱 서비스 모의해킹
- 발견된 취약점에 대한 조치방안 제시 및 이행점검

○ **홈페이지 위·변조 모니터링**

- 주요 홈페이지 위·변조 탐지 및 알림
- 이상 발생 시 원인분석 및 대응 지원

○ **정보보호 관리체계 점검 및 개선 지원**

- 정보보호 관리체계 현황에 대한 GAP 분석 및 미흡사항 식별
- 정보보호 수준 향상을 위한 개선과제 도출

○ **정보보호 교육 및 훈련**

- 임직원 및 관련 직무자를 대상으로 한 직무별 정보보호 교육
- 임직원 대상 악성메일 모의훈련 및 훈련결과 분석·개선 지원

3. 사업의 기대효과

○ 24시간 365일 상시 보안관제를 통한 사이버위협의 조기 탐지·대응 및 침해사고 피해 최소화

○ 정보보호시스템의 체계적인 운영·관리와 신속한 장애·변경 대응을 통한 운영 안정성 및 업무 연속성 확보

○ 지속적인 취약요인 식별·개선과 교육·훈련을 통한 재단의 정보보호 관리수준 및 자체 대응역량 향상

4. 추진 일정

구 분	~ 2026. 11.	2026. 12.	2027. 1. ~ 12.	2028. 1. ~ 12.	2029. 1. ~ 12.
사업자 선정 및 계약 체결	●				
업무 인수인계 및 착수 준비		●			
1차년도 사업 수행			●		
2차년도 사업 수행				●	
3차년도 사업 수행					●

※ 추진 일정은 사업 추진상황에 따라 변경될 수 있음

5. 사업 주요사항

❍ 제안서 작성 비용은 제안사의 부담이며, 제출된 제안서는 반환하지 않음

❍ 제안평가 결과에 대하여는 이의를 제기할 수 없음

- 본 입찰 및 평가 관련 사항은 "Ⅶ. 제안서 평가 및 선정" 참조

❍ 제안서는 명시된 제출기한까지 도착하여야 하며, 기한 내에 제안서를 제출하지 않는 경우에는 제안 의사가 없는 것으로 간주함

❍ 본 사업의 제안과 관련하여 관련문서 또는 그 내용을 대외에 누설할 수 없으며, 이를 어길 경우 해당업체가 모든 책임을 부담함

❍ 제안된 내용은 재단 필요에 따라 상호협의 하에 조정될 수 있음

❍ 제안서 작성에 필요한 자료 열람은 사전 요청을 통해 재단에 방문하여 보안서약서 작성 및 담당자 입회하에 열람 가능

- 기　　간: 입찰공고 익영업일 ~ 입찰공고 마감 전일까지
  ※ 마감전일이 휴일(공휴일)인 경우 전 영업일까지
- 장　　소: 사회복지법인 어린이재단 4층 DT서비스본부(서울시 중구 무교로 20)
- 신청방법: 방문 희망일 최소 1영업일 전 담당자 이메일(cube@chorogusan.or.kr)로 연락 및 일정 조율 후 방문
- 예약자 정보(방문업체명, 방문자명, 방문자 수 및 연락처) 필수
- 자료 열람 시 열람자는 해당 업체 소속임을 증명할 수 있어야 하며(재직증명서 등) 열람 자료의 촬영은 불가함
- 자료열람은 본 사업에 입찰 참여 의사가 있는 업체로 제한
- 열람인원은 5인 이내, 1회 열람시간은 3시간 이내로 제한(최대 3회 열람 가능)
- 열람일정은 접수 순서대로 배정하여 통지 예정

Ⅱ 사업 범위

※ 세부 수행내용 및 요구조건은「Ⅲ. 제안요청 내용」참조

※ 세부 대상 현황은 보안상 공개하지 않으며, 자료 열람에 관한 사항은「Ⅰ. 사업개요 5. 사업 주요사항」참조

1. 하이브리드 보안관제 운영

가. 원격 보안관제

1) 관제대상 정보보호시스템 및 주요 정보시스템에 대한 24시간 365일 실시간 원격 보안관제 수행
2) 보안이벤트·로그 실시간 모니터링 및 이상징후 탐지·분석·대응
3) 침해사고 의심 이벤트에 대한 초동분석·보고·전파 및 대응 지원
4) 재단의 정보보호 환경과 사업자 관제시스템 간 연동 및 로그수집 상태 관리
5) 관제대상 정보보호시스템의 가용성 및 운영상태 모니터링

나. 보안관제 운영 및 대응 연계

1) 원격관제에서 탐지·분석된 주요 보안이벤트에 대한 상주인력 연계 및 현장 대응
2) 정보시스템 및 정보보호시스템의 신규 구축·교체 등 운영환경 변경에 따른 관제 대상 현행화
3) 보안관제 수행결과에 대한 정기·비정기 보고 및 최신 정보보호 이슈·위협 인텔리전스 정보 제공

2. 정보보호시스템 운영

가. 상주인력 운영

1) 전문인력 3명(중급 1명, 초급 2명)을 투입하여 평일 09:00~18:00 상주 운영
   ※ 인력 자격요건은 [별표1] 참고
2) 정보보호시스템 운영·관리를 중심으로 원격 보안관제와 연계한 현장 대응 및 정보보호 업무 수행

나. 정보보호시스템 운영·관리

1) 기존 및 신규 구축 정보보호시스템의 운영·관리 및 보안정책 관리·최적화
2) 정보보호시스템 운영상태 점검 및 장애 발생 시 원인분석·초동조치·복구 대응
3) 정보보호시스템 신규 구축·교체·증설·구성변경에 따른 구축 지원, 보안정책 적용, 관련 시스템 연동 및 운영 안정화
4) 정보보호시스템 운영에 필요한 현황관리·기술지원 등 제반 정보보호 업무 수행

3. 침해사고 분석 및 대응

가. 침해사고 분석 및 대응

1) 침해사고 및 의심 상황에 대한 보안이벤트·로그 분석 및 사고 영향범위 파악
2) 침해사고 발생 시 초동대응 및 피해확산 방지를 위한 대응조치 수행·지원
3) 사고원인 분석, 시스템 복구·정상화 및 재발방지 대책 수립 지원

4. 취약점 진단 및 모의해킹

가. 기술적 취약점 분석·평가

1) 운영 중인 정보시스템 및 정보보호시스템을 대상으로 연 1회 이상 기술적 취약점 분석·평가 수행
2) 신규 구축·도입되거나 주요 변경되는 정보시스템 및 정보보호시스템에 대한 추가 기술적 취약점 분석·평가 수행
3) 발견된 취약점에 대한 조치방안 제시 및 조치 후 이행점검 수행

나. 모의해킹

1) 주요 웹·앱 서비스를 대상으로 연 1회 이상 모의해킹 수행
2) 신규 구축·도입되거나 주요 변경되는 웹·앱 서비스에 대한 추가 모의해킹 수행
3) 발견된 취약점에 대한 조치방안 제시 및 조치 후 이행점검 수행

5. 홈페이지 위 · 변조 모니터링

가. 홈페이지 위·변조 모니터링

1) 재단 주요 홈페이지에 대한 위·변조 및 이상징후 모니터링
2) 위·변조 또는 이상징후 탐지 시 알림 및 원인분석·대응 수행·지원

6. 정보보호 관리체계 점검 및 개선 지원

가. 정보보호 관리체계 점검 및 개선 지원

1) ISO/IEC 27001 또는 ISMS-P 요구사항을 기준으로 한 정보보호 관리체계 GAP 분석 연 1회 수행
2) GAP 분석을 통한 미흡사항 및 개선 필요사항 식별
3) 정보보호 수준 향상을 위한 개선과제 및 이행방안 제시

7. 정보보호 교육 및 훈련

가. 정보보호 교육

1) 정보보호 및 IT 관련 업무담당자를 대상으로 직무 및 업무 특성을 고려한 정보보호 차등교육을 연 1회 이상 실시
2) 교육은 재단의 교육환경을 고려하여 온·오프라인 방식으로 실시

나. 악성메일 모의훈련

1) 재단이 보유·운영 중인 악성메일 모의훈련 솔루션을 활용한 임직원 대상 모의훈련 수행
2) 훈련 시나리오·콘텐츠 구성 및 훈련대상 설정 등 모의훈련 운영
3) 훈련결과 분석 및 결과 보고

Ⅲ 제안요청 내용

1. 제안서 내용과 순서

가. 제안사업의 과업 범위 전체를 포괄하는 제안내용으로 양식에 구애 없이 기술하되, 아래 내용을 반드시 포함하여야 함.

구 분	내 용
Ⅰ. 제안업체 일 반	1. 일반현황 및 주요 연혁 [별지2 서식] 2. 사업 실적 [별지3 서식] * 최근 3년 이내 이행이 완료된 **보안관제 사업** 중 단일 계약금액 280,000,000원(부가가치세 포함) 이상인 사업의 실적 3. 사업수행 조직도 [별지4 서식] 4. 참여인력 현황 [별지5 서식] 5. 제안요청서 수용여부 참조표 [별지6 서식]
Ⅱ. 제안내용	본 제안요청서의 요구사항별 수행방안 및 이행계획
Ⅲ. 기 타	본 사업의 효과적인 수행을 위한 추가 제안 및 지원사항

※ 세부 목차 및 작성방법은「Ⅲ 제안요청 내용 2. 제안서 목차 및 작성방법」참조

나. 하나의 제안내용이 둘 이상의 요구사항과 관련되는 경우 해당 요구사항 고유번호를 함께 표시하고, 제안요청서에서 요구하지 않은 추가 제안사항은 [추가제안]으로 구분하여 명시하여야 함

다. 제안요청서의 요구사항이 제안서에 누락되지 않도록 작성하여야 하며, 요구사항별 수용여부 및 제안서 해당 페이지를 확인할 수 있도록「[별지6 서식] 제안요청서 수용여부 참조표」를 작성하여 제안서에 포함하여야 함

라. 제안사는 본 사업의 목적 및 과업범위와 관련된 사항에 대하여 추가제안을 할 수 있으며, 추가제안의 내용, 기대효과 및 수행방안을 구체적으로 제시하여야 함. 추가제안에 필요한 비용 및 인력은 본 사업의 제안금액 및 수행범위에 포함하여야 함

2. 제안서 목차 및 작성방법

작성항목	작성방법	비고
Ⅰ. 제안업체 일반		
1. 일반현황 및 주요 연혁	제안업체의 일반현황 및 주요 연혁을 명확하게 제시	[별지2 서식]
2. 사업 실적	최근 3년 이내 이행이 완료된 보안관제 사업 수행실적을 제시	[별지3 서식]
3. 사업수행 조직도	본 사업 수행을 위한 조직체계 및 역할을 제시	[별지4 서식]
4. 참여인력 현황	본 사업에 투입할 인력의 구성, 경력 및 역할 등을 제시	[별지5 서식]
5. 제안요청서 수용여부 참조표	제안요청서의 요구사항별 수용여부 및 제안서 해당 페이지를 작성	[별지6 서식]
Ⅱ. 제안내용		
1. 사업 이해 및 추진전략		
1.1. 사업이해도	사업목적, 환경 및 과업범위와 제안요청사항에 대한 이해도를 구체적으로 제시	
1.2. 수행전략	사업목표 달성을 위한 수행전략 및 방법론을 구체적으로 제시	
2. 보안관제 수행	보안관제 요구사항 전반에 대한 수행방안, 운영체계 및 전문성을 구체적으로 제시	
3. 상주인력 및 정보보호 시스템 운영	상주인력 운영 및 정보보호시스템 운영·관리 요구사항에 대한 수행방안과 운영체계를 구체적으로 제시	
4. 정보보호 진단 및 개선	취약점 분석·평가, 모의해킹, 정보보호 관리체계 점검 및 개선에 대한 수행방안을 구체적으로 제시	
5. 사업관리·품질관리 및 보안관리	사업관리체계, 일정·보고·산출물·위험관리, 품질관리, 보안관리, 인수인계 및 업무연속성 확보, 관련 법령 및 계약조건 등 제약사항에 대한 준수·이행방안을 구체적으로 제시	
6. 전문지원체계	사업수행 전반에 대한 분야별 기술지원 조직 및 지원체계를 구체적으로 제시	
7. 정보보호 교육 및 훈련	정보보호 교육 및 훈련에 대한 수행계획과 방법을 구체적으로 제시	
Ⅲ. 기타	위 항목에서 제시되지 않은 기타 내용 혹은 추가제안 사항을 기술(선택)	추가제안

3. 요구사항 정의

요구사항 구 분	고 유 번 호	요구사항 설 명	개 수
보안관제 요구사항 (Security Monitoring Requirement)	SMR	하이브리드 보안관제, 침해사고 분석·대응, 취약점 진단·모의해킹, 홈페이지 위·변조 모니터링, 정보보호 관리체계 점검 및 정보보호 교육·훈련 등 보안관제 관련 업무에 관한 요구사항	10
정보보호시스템 운영 요구사항 (Operation Requirement)	OPR	상주인력 운영, 정보보호시스템 운영·관리, 보안정책 관리·최적화, 장애 대응 및 신규·변경 시스템의 운영 안정화 등에 관한 요구사항	4
사업관리 요구사항 (Project Management Requirement)	PMR	사업수행 조직 및 인력, 사업수행계획, 일정·보고·위험관리, 업무 인수인계 등 사업의 체계적인 수행 및 관리에 관한 요구사항	8
품질 요구사항 (Quality Requirement)	QUR	서비스 수준, 품질관리, 성과관리 및 지속적인 서비스 개선에 관한 요구사항	1
보안 요구사항 (Security Requirement)	SER	사업수행 과정에서의 인적·물리적·관리적 보안, 자료·시스템 접근통제 및 정보유출 방지 등에 관한 요구사항	4
제약사항 (Constraint Requirement)	COR	관련 법령·규정·지침, 계약조건 및 기타 사업수행 시 준수하여야 할 제약사항	2
합 계			29

4. 요구사항 목록

요구사항 구분	요구사항 ID	요구사항 명칭
보안관제 요구사항	SMR-001	24시간 365일 실시간 원격 보안관제
	SMR-002	보안이벤트 탐지·분석 및 대응
	SMR-003	관제시스템 연동 및 로그·탐지정책 관리
	SMR-004	침해사고 분석 및 대응
	SMR-005	사이버위협정보 수집·전파
	SMR-006	기술적 취약점 분석·평가
	SMR-007	웹·앱 모의해킹
	SMR-008	홈페이지 위·변조 모니터링
	SMR-009	정보보호 관리체계 점검 및 개선 지원
	SMR-010	정보보호 교육 및 훈련
정보보호시스템 운영 요구사항	OPR-001	상주인력 운영
	OPR-002	정보보호시스템 운영·관리
	OPR-003	장애 대응 및 유지관리
	OPR-004	정보보호시스템 구축·변경 및 운영 안정화
사업관리 요구사항	PMR-001	사업수행 조직 및 관리체계
	PMR-002	투입인력 자격 및 구성
	PMR-003	투입인력 관리 및 변경
	PMR-004	사업수행계획 및 일정 관리
	PMR-005	보고 및 의사소통 관리
	PMR-006	산출물 및 문서 관리
	PMR-007	위험 및 이슈 관리
	PMR-008	업무 인수인계
품질 요구사항	QUR-001	서비스 수준 및 품질관리
보안 요구사항	SER-001	보안관리 일반
	SER-002	참여인력 보안관리
	SER-003	자료 및 정보 보안관리
	SER-004	장비·매체 및 업무환경 보안관리
제약사항	COR-001	사업수행 관련 법령 및 계약조건 준수
	COR-002	손해배상 책임

5. 상세 요구사항

가. 보안관제 요구사항

요구사항 분류	보안관제 요구사항
요구사항 ID	SMR-001
요구사항 명칭	24시간 365일 실시간 원격 보안관제
요구사항 상세설명	○ 사업자의 보안관제센터를 통한 24시간 365일 실시간 원격 보안관제 수행 ○ 관제대상 정보보호시스템 및 정보시스템에서 수집되는 보안이벤트 및 로그에 대한 실시간 모니터링 ○ 관제대상 정보보호시스템의 가용성 및 운영상태 상시 모니터링 ○ 관제대상 정보보호시스템의 장애 또는 운영상 이상상태 발생 시 재단에 신속히 상황을 전파하고 원인 파악 및 대응 지원 ○ 보안관제 수행현황 및 결과에 대한 일일·주간·월간·연간 정기보고 실시
산출정보	일일·주간·월간·연간 보안관제 보고서

요구사항 분류	보안관제 요구사항
요구사항 ID	SMR-002
요구사항 명칭	보안이벤트 탐지·분석 및 대응
요구사항 상세설명	○ 보안관제 과정에서 수집되는 보안이벤트 및 로그에 대한 실시간 탐지·분석 ○ 탐지된 보안이벤트에 대한 정·오탐 분석 및 위협 수준·영향도 판단 ○ 유해트래픽, 악성 IP·도메인, 비정상 접근, 해킹시도 등 이상징후 분석 ○ 침해사고 의심 이벤트 발생 시 초동분석을 실시하고 분석결과 및 대응 필요사항을 재단에 신속히 보고·전파 ○ 분석결과에 따른 차단, 정책변경 등 필요한 대응방안 제시 및 조치 지원 ○ 주요 보안이벤트 발생 시 상주인력과 연계한 현장 확인 및 대응 ○ 탐지·분석·전파·조치 결과에 대한 이력 및 통계 관리
산출정보	보안이벤트 분석·대응 이력, 주요 보안이벤트 분석자료

요구사항 분류	보안관제 요구사항
요구사항 ID	SMR-003
요구사항 명칭	관제시스템 연동 및 로그·탐지정책 관리
요구사항 상세설명	○ 재단의 정보보호 환경과 사업자 관제시스템 간 안정적인 연동을 통한 원격 보안관제 수행 ○ 관제대상 정보보호시스템 및 정보시스템의 연동 현황을 관리하고, 신규 구축·교체·변경·폐기 등 운영환경 변경사항을 관제대상 및 연동 구성에 반영

	○ 보안이벤트 및 로그의 수집·연동상태를 지속적으로 관리하고, 수집 중단·누락 등 이상상태 발생 시 원인분석 및 정상화 ○ 재단과 사업자 보안관제센터 간 보안이벤트 및 로그의 전송구간은 암호화 등 안전한 통신방식을 적용하여야 함 ○ 사업자 관제시스템에 수집·연계되는 보안이벤트 및 로그는 1년 이상 보관·관리하여야 하며, 재단의 요구 또는 관련 법령·지침에 따라 로그 유형별 보관기간을 추가로 연장하여 적용할 수 있음 ○ 신규 시스템 도입 또는 기존 시스템 변경 시 관제에 필요한 로그수집 항목 및 연동방안을 검토하고 적용 지원 ○ 최신 사이버위협, 공격기법 및 보안관제 결과를 반영하여 탐지정책 및 경보 기준을 지속적으로 개선·최적화 ○ 탐지정책 및 경보에 대한 지속적인 분석을 통해 오탐을 최소화하고 탐지 정확도를 향상 ○ 보안관제 이벤트의 미처리·누락 방지를 위한 이벤트 처리현황 및 이력 관리 ○ 보관 중인 보안이벤트 및 로그는 보관기간 동안 조회·검색·분석이 가능하도록 관리
산출정보	관제 연동·로그수집 현황, 탐지정책 변경·관리내역

요구사항 분류	**보안관제 요구사항**
요구사항 ID	SMR-004
요구사항 명칭	침해사고 분석 및 대응
요구사항 상세설명	○ 침해사고 발생 시 관련 보안이벤트·로그 등 사고자료에 대한 상세 분석 수행 ○ 사고원인, 공격경로, 피해·영향범위 및 추가 피해 가능성 분석 ○ 침해사고 발생 시 초동대응 및 피해확산 방지를 위한 대응방안 제시 및 조치 지원 ○ 필요 시 현장조사 및 디지털 포렌식 등 침해사고 정밀분석 지원 ○ 피해시스템의 복구방안 제시 및 정상화 지원 ○ 사고원인 분석결과를 기반으로 재발방지 대책 및 보안 강화방안 제시 ○ 침해사고 유형별 대응절차 마련·현행화 ○ 중대한 침해사고 등 기존 관제인력만으로 대응이 어려운 경우 사업자의 침해사고 대응 전문인력 지원 ○ 침해사고 분석·대응 및 조치결과 보고
산출정보	침해사고 분석·대응 결과보고서(발생 시)

요구사항 분류	보안관제 요구사항
요구사항 ID	SMR-005
요구사항 명칭	사이버위협정보 수집·전파
요구사항 상세설명	○ 국내·외 최신 사이버위협 동향, 정보보안 관련 이슈 및 언론동향 등을 상시 모니터링·분석하여 제공 ○ 사이버공격 피해 예방을 위한 악성 IP, URL, IOC 등 주요 사이버위협정보를 일 1회 이상 제공하고 정보보호시스템 등에 대한 적용 방안 제시 ○ 재단과 관련되거나 영향이 예상되는 주요 보안이슈에 대한 영향도 분석 및 대응방안 제시 ○ 긴급 대응이 필요한 사이버위협정보 발생 시 재단에 신속히 상황을 전파하고 대응방안 제시 ○ 최신 악성코드에 대한 분석보고서 월 1회 이상 제공
산출정보	보안동향 및 사이버위협정보, 악성코드 분석보고서

요구사항 분류	보안관제 요구사항
요구사항 ID	SMR-006
요구사항 명칭	기술적 취약점 분석·평가
요구사항 상세설명	○ 운영 중인 정보시스템 및 정보보호시스템을 대상으로 연 1회 이상 기술적 취약점 분석·평가 수행 ○ 서버, WEB/WAS, DBMS, 네트워크 및 정보보호시스템 등 대상별 특성을 고려한 기술적 취약점 분석·평가 수행 ○ 신규 구축·도입되거나 주요 변경되는 정보시스템 및 정보보호시스템에 대한 추가 기술적 취약점 분석·평가 수행 ○ 「주요정보통신기반시설 기술적 취약점 분석·평가 방법 상세가이드」를 준용하여 대상별 기술적 취약점 분석·평가 수행 ○ 대상 시스템의 특성을 고려하여 자동화 도구 및 수동점검 등 적정한 방법으로 분석·평가 수행 ○ 발견된 취약점에 대한 위험도·영향도 분석 및 구체적인 조치방안 제시 ○ 취약점 조치에 따른 시스템 영향도 검토 및 조치 지원 ○ 취약점 조치 후 이행점검을 수행하여 조치여부 확인 ○ 취약점 진단 및 조치·이행점검 결과에 대한 이력 관리 ○ 현장·원격 등 세부 수행방법은 재단과 협의하여 결정
산출정보	취약점 분석·평가 계획서, 취약점 분석·평가 결과보고서, 취약점 조치가이드, 이행점검 결과보고서

요구사항 분류	보안관제 요구사항
요구사항 ID	SMR-007
요구사항 명칭	웹·앱 모의해킹
요구사항 상세설명	○ 주요 웹·앱 서비스를 대상으로 연 1회 이상 모의해킹 수행 ○ 신규 구축·도입되거나 주요 변경되는 웹·앱 서비스에 대한 추가 모의해킹 수행 ○ 대상 서비스의 특성, 실제 공격 가능성 및 영향도를 고려한 모의해킹 계획 및 시나리오 수립 ○ OWASP Top 10 등 국내·외 취약점 진단기준과 최신 취약점 및 실제 공격 기법을 활용한 침투테스트 수행 ○ 운영 중인 서비스에 미치는 영향을 최소화할 수 있도록 재단과 사전 협의 후 수행 ○ 발견된 취약점에 대한 위험도·영향도 분석 및 구체적인 조치방안 제시 ○ 취약점 조치 후 이행점검을 수행하여 조치여부 확인 ○ 모의해킹 및 조치·이행점검 결과에 대한 이력 관리
산출정보	모의해킹 계획서, 모의해킹 결과보고서, 취약점 조치가이드, 이행점검 결과보고서

요구사항 분류	보안관제 요구사항
요구사항 ID	SMR-008
요구사항 명칭	홈페이지 위·변조 모니터링
요구사항 상세설명	○ 재단 주요 홈페이지에 대한 위·변조 및 이상징후 실시간 모니터링 수행 ○ 홈페이지 위·변조 또는 이상징후 탐지 시 재단에 신속히 상황 전파 ○ 탐지된 위·변조 및 이상징후에 대한 원인 및 영향범위 분석 ○ 악성코드 은닉·유포 등 홈페이지를 통한 악성행위 여부 확인 ○ 분석결과에 따른 대응방안 제시 및 홈페이지 정상화를 위한 조치 지원 ○ 위·변조 탐지·분석 및 조치결과에 대한 이력 관리
산출정보	위·변조 모니터링 결과(정기 보안관제 보고서에 포함), 위·변조 분석·조치 결과자료(발생 시)

요구사항 분류	보안관제 요구사항
요구사항 ID	SMR-009
요구사항 명칭	정보보호 관리체계 점검 및 개선 지원
요구사항 상세설명	○ ISO/IEC 27001 또는 ISMS-P 요구사항을 기준으로 연 1회 정보보호 관리체계 GAP 분석 수행

	○ 재단의 정보보호 관리체계 운영현황 및 관련 정책·지침·절차·증적자료 등에 대한 점검 ○ GAP 분석을 통한 미흡사항 및 개선 필요사항 식별 ○ 미흡사항의 중요도 및 우선순위를 고려한 개선과제 도출 ○ 개선과제별 개선방향 및 구체적인 이행방안 제시 ○ GAP 분석은 현장 방문을 통해 수행
산출정보	정보보호 관리체계 GAP 분석 결과보고서

요구사항 분류	**보안관제 요구사항**
요구사항 ID	SMR-010
요구사항 명칭	정보보호 교육 및 훈련
요구사항 상세설명	○ 정보보호 및 IT 관련 업무담당자를 대상으로 직무 및 업무 특성을 고려한 정보보호 차등교육 연 1회 이상 실시 ○ 교육대상별 업무특성 및 요구역량을 고려한 교육내용 구성 ○ 최신 사이버위협, 침해사고 사례, 정보보호 기술동향 및 실무 대응사항 등 교육내용 반영 ○ 교육은 재단의 교육환경을 고려하여 온·오프라인 방식으로 실시 ○ 재단이 보유·운영 중인 악성메일 모의훈련 솔루션을 활용하여 임직원 대상 악성메일 모의훈련 수행 ○ 악성메일 모의훈련을 위한 시나리오·콘텐츠, 훈련대상 및 일정 등 세부 훈련계획을 수립하고 재단과 협의하여 수행 ○ 훈련결과 분석 및 개선 필요사항 제시
산출정보	정보보호 교육계획 및 교육자료·결과자료, 악성메일 모의훈련 계획서 및 결과보고서

나. 정보보호시스템 운영 요구사항

요구사항 분류	정보보호시스템 운영 요구사항
요구사항 ID	OPR-001
요구사항 명칭	상주인력 운영
요구사항 상세설명	○ 정보보호시스템의 안정적인 운영·관리를 위하여 전문인력 3명(중급 1명, 초급 2명, [별표1] 참고)을 재단이 지정한 장소에 상주 배치하여 운영 ○ 상주인력의 근무시간은 평일 09:00부터 18:00까지를 원칙으로 하며, 재단의 운영환경 및 업무여건에 따라 협의하여 조정 가능 ○ 상주인력은 정보보호시스템의 운영상태 확인, 보안정책 관리, 보안이벤트 확인·분석, 장애 대응 등 일상적인 운영업무 수행 ○ 원격 보안관제 과정에서 주요 보안이벤트 및 이상징후가 탐지된 경우 원격 관제 인력과 연계하여 현장 확인 및 대응 수행 ○ 정보보호시스템의 신규 구축·교체·변경 등 운영환경 변경 시 관련 작업 및 안정적인 운영전환 지원 ○ 정보보호시스템 운영과 관련한 사용자 문의 및 기술지원 요청에 대한 응대·지원 ○ 장애, 침해사고 등 긴급상황 발생 시 재단과 협의하여 필요한 비상 대응 지원 ○ 상주인력의 근무장소 및 기본 사무집기(책상, 의자)는 재단이 제공하며, 업무용 PC(노트북 포함) 및 그 밖의 업무 수행에 필요한 장비·사무용품·기타 비품은 제안사가 부담하여야 함
산출정보	상주인력 업무수행 내역

요구사항 분류	정보보호시스템 운영 요구사항
요구사항 ID	OPR-002
요구사항 명칭	정보보호시스템 운영·관리
요구사항 상세설명	○ 기존 및 신규 구축된 정보보호시스템의 안정적인 운영·관리 및 운영상태 점검 ○ 정보보호시스템별 보안정책의 등록·변경·삭제 및 재단의 업무 요청에 따른 정책 적용 ○ 보안위협 및 운영현황 등을 고려한 보안정책 점검·최적화 ○ 정보보호시스템의 성능·용량·구성 등 운영상태 관리 ○ 정보보호시스템의 주요 설정정보 및 보안정책 등에 대한 백업·복구 관리 ○ 정보보호시스템 사용자 문의에 대한 응대 및 기술지원 ○ 정보보호시스템 운영과 관련한 기술적 문제의 원인 확인 및 해결 지원 ○ 정보보호시스템 현황, 구성정보, 운영절차 및 매뉴얼 등 운영 관련 자료 현행화
산출정보	정보보호시스템 운영내역, 보안정책 변경·관리내역, 정보보호시스템 현황 및 운영 관련 자료

요구사항 분류	정보보호시스템 운영 요구사항
요구사항 ID	OPR-003
요구사항 명칭	장애 대응 및 유지관리
요구사항 상세설명	○ 정보보호시스템의 장애 및 비정상 상태 발생 시 원인 확인, 초동조치 및 정상화 대응 ○ 장애 원인 및 영향범위 파악과 복구 후 시스템 정상동작 여부 확인 ○ 장애 대응을 위해 제조사 또는 유지보수업체의 기술지원이 필요한 경우 관련 업체와 협업하여 장애 분석 및 복구 수행 ○ 유지보수업체가 수행하는 정기점검, 보안패치·업데이트·업그레이드 등 유지관리 작업에 대한 기술지원 및 작업 협조 ○ 유지관리 작업에 따른 시스템 영향도 및 적용사항 사전 확인 ○ 유지관리 작업 전 주요 설정정보 및 보안정책 등의 백업 여부 확인과 작업 후 시스템·보안정책 정상동작 여부 점검 ○ 장애 대응 및 유지관리 관련 작업내역 관리
산출정보	장애 조치내역(발생 시), 유지관리 작업내역

요구사항 분류	정보보호시스템 운영 요구사항
요구사항 ID	OPR-004
요구사항 명칭	정보보호시스템 구축·변경 및 운영 안정화
요구사항 상세설명	○ 정보보호시스템의 신규 구축·교체·증설·이전·구성변경 등에 따른 기술지원 ○ 신규·변경 정보보호시스템에 대한 보안정책 검토 및 적용 ○ 신규·변경 정보보호시스템과 관련 정보시스템 및 정보보호시스템 간 연동 적용 ○ 원격 보안관제를 위한 관제시스템 연동 및 로그수집 적용 ○ 운영환경 변경에 따른 기존 보안정책·설정정보 등의 이관 및 적용 ○ 구축·변경 작업 전 운영 영향도를 검토하고 필요한 경우 주요 설정정보·보안정책 등의 백업 및 복구방안을 확인하며, 작업 후 정상동작 여부 점검 ○ 구축·변경 과정에서 발생하는 기술적 이슈에 대하여 재단 및 관련 사업자와 협업하여 원인 확인 및 조치 지원 ○ 신규·변경 정보보호시스템의 운영전환 및 안정화 수행 ○ 구축·변경사항을 반영한 시스템 현황, 구성정보 및 운영 관련 자료 현행화
산출정보	구축·변경 및 운영 안정화 내역(해당 시), 시스템 현황·구성정보 현행화 자료

다. 사업관리 요구사항

요구사항 분류	사업관리 요구사항
요구사항 ID	PMR-001
요구사항 명칭	사업수행 조직 및 관리체계
요구사항 상세설명	○ 사업의 원활한 수행을 위한 사업수행 조직체계 및 관리체계 구성 ○ 상주인력, 원격 보안관제센터 및 사업자의 전문지원 조직 등 본 사업에 참여하는 조직과 인력의 구성 및 역할 제시 ○ 조직별·업무별 책임과 역할을 명확히 하고 업무분장 체계 수립 ○ 사업수행책임자(PM)를 지정하여 상주인력, 원격 보안관제센터 및 전문지원 조직 등 본 사업에 참여하는 조직과 인력의 업무를 총괄하고, 재단과의 업무협의 창구를 일원화하여야 함 ○ 원격 보안관제, 정보보호시스템 운영, 침해사고 대응 등 업무 간 유기적인 연계 및 협업체계 마련 ○ 침해사고 등 전문적인 기술지원이 필요한 경우 사업자의 전문지원 조직을 활용할 수 있는 지원체계 마련
산출정보	사업수행 조직도 및 업무분장표

요구사항 분류	사업관리 요구사항
요구사항 ID	PMR-002
요구사항 명칭	투입인력 자격 및 구성
요구사항 상세설명	○ 본 사업의 안정적인 수행을 위하여 업무수행에 필요한 전문성과 경험을 갖춘 인력을 투입하여야 함 ○ 상주인력의 기술등급은 「보안관제 전문기업 지정 등에 관한 공고」(과학기술정보통신부 공고 제2019-441호) [별표 1] '기술인력의 자격기준'을 적용하며, 총 3명(중급 1명, 초급 2명)을 배치하여야 함 ○ 사업수행책임자(PM)는 상주인력 3명과 별도로 제안사 소속 인력으로 지정하여야 하며, 본 사업의 상주 운영, 원격 보안관제 및 전문지원 업무 전반을 총괄할 수 있는 전문성과 사업수행 경험을 보유하여야 함 ○ 투입인력은 정보보호시스템 운영, 보안관제 등 담당업무 수행에 적합한 경력과 기술능력을 보유하여야 함 ○ 원격 보안관제, 침해사고 대응, 취약점 진단·모의해킹 등 비상주 업무에 대해서도 해당 업무를 수행할 수 있는 전문인력을 확보하여야 함 ○ 투입인력의 자격, 경력 및 재직 여부 등을 객관적으로 확인할 수 있는 증빙자료 제출
산출정보	투입인력 현황, 참여인력 이력사항, 자격·경력 및 재직 증빙자료

요구사항 분류	사업관리 요구사항
요구사항 ID	PMR-003
요구사항 명칭	투입인력 관리 및 변경
요구사항 상세설명	○ 투입인력의 전문성 및 업무 연속성이 유지될 수 있도록 인력을 관리하고, 사업기간 중 투입인력의 변경을 최소화 ○ 상주인력의 휴가·교육 등 사전에 예상 가능한 부재는 재단과 사전 협의하고 업무공백이 발생하지 않도록 조치 ○ 휴가·교육·질병·사고 등의 사유로 상주인력이 연속 3일을 초과하여 업무를 수행할 수 없는 경우 동급 이상의 대체인력을 투입 ○ 퇴직 등 부득이한 사유로 투입인력의 교체가 필요한 경우 교체 예정일 14일 전까지 재단의 승인을 받아야 하며, 동등 이상의 자격과 경력을 보유한 인력으로 교체 ○ 투입인력 교체 시 최소 10일 이상의 인수인계 기간을 두어 업무공백이 발생하지 않도록 하고, 인수인계 결과를 재단에 제출 ○ 재단은 투입인력이 계약상 업무를 적정하게 수행하지 못하거나 업무수행 능력이 부족하다고 판단되는 경우 사업자에게 인력교체를 요구할 수 있으며, 사업자는 특별한 사유가 없는 한 이에 응하여야 함 ○ 대체·교체인력은 투입 전에 해당 인력의 자격·경력 등 관련 자료를 제출하고 재단의 승인을 받아야 함
산출정보	인력 변경·대체 승인자료, 인수인계서

요구사항 분류	사업관리 요구사항
요구사항 ID	PMR-004
요구사항 명칭	사업수행계획 및 일정 관리
요구사항 상세설명	○ 계약 체결 후 7일 이내 제안요청서, 제안서 및 계약내용을 반영한 사업수행계획서를 작성하여 재단의 검토·승인을 받아야 함 ○ 사업수행계획서에는 사업목적 및 범위, 사업수행 조직 및 인력, 세부 과업별 수행방안, 추진일정, 보고·품질·보안관리 방안 등 사업수행에 필요한 사항을 포함 ○ 사업수행계획에 따라 세부 과업별 추진일정 및 진행상황을 지속적으로 관리하고 일정 지연이 예상되는 경우 원인 및 대응방안을 마련하여 재단에 보고 ○ 사업수행 중 과업내용 또는 일정의 변경이 필요한 경우 사전에 재단과 협의하고 승인된 변경사항을 사업수행계획 및 관련 일정에 반영 ○ 사업수행계획서의 내용은 사업기간 동안 지속적으로 관리하고 주요 변경사항 발생 시 현행화
산출정보	사업수행계획서, 세부 추진일정

요구사항 분류	사업관리 요구사항
요구사항 ID	PMR-005
요구사항 명칭	보고 및 의사소통 관리
요구사항 상세설명	○ 사업수행책임자(PM)를 중심으로 재단과의 원활한 업무협의 및 의사소통 체계를 마련하여 운영 ○ 장애, 침해사고, 일정 지연 등 사업수행에 중대한 영향을 미치는 사항이나 주요 현안 발생 시 해당 내용과 대응방안을 재단에 신속히 보고 ○ 재단이 사업수행 현황 또는 주요 현안에 대한 보고를 요청하는 경우 관련 내용을 수시로 보고 ○ 사업수행과 관련하여 협의가 필요한 사항은 재단과 사전에 협의하고 주요 협의·결정사항을 기록·관리 ○ 사업 종료 시 사업수행 내용, 주요 성과 및 개선사항 등을 종합한 사업 완료보고서 제출
산출정보	수시 보고자료, 회의·협의 결과자료, 사업완료보고서

요구사항 분류	사업관리 요구사항
요구사항 ID	PMR-006
요구사항 명칭	산출물 및 문서 관리
요구사항 상세설명	○ 본 제안요청서의 각 요구사항에서 정한 산출정보를 기준으로 사업수행 과정에서 발생하는 산출물을 작성·관리 및 제출 ○ 사업 착수 시 산출물의 종류, 주요 내용 및 제출시기 등을 포함한 산출물 목록을 작성하여 사업수행계획서에 반영 ○ 산출물의 세부 양식 및 작성방법은 재단과 협의하여 결정하며, 재단이 보완을 요구하는 경우 이를 반영하여 제출 ○ 운영절차, 매뉴얼, 시스템 현황 등 지속적으로 관리되는 문서는 변경사항을 반영하여 현행화하고 최신본을 유지 ○ 산출물의 작성·수정 이력 및 최종본을 식별할 수 있도록 체계적으로 관리 ○ 사업 종료 시 사업수행 과정에서 작성·관리한 최종 산출물을 정리하여 재단에 제출
산출정보	산출물 목록 및 관리내역, 최종 산출물

요구사항 분류	사업관리 요구사항
요구사항 ID	PMR-007
요구사항 명칭	위험 및 이슈 관리
요구사항 상세설명	○ 사업기간 중 발생 가능한 위험요소를 사전에 식별하고 사업수행에 미치는 영향을 최소화할 수 있도록 대응방안 마련 ○ 보안관제 서비스 중단, 상주인력 공백, 정보보호시스템 장애·침해사고, 사업자의 파업·도산, 재난·감염병 등 비상상황에 대비한 업무연속성 및 비상대응체계 마련 ○ 위험요소 또는 사업수행에 영향을 미치는 주요 이슈 발생 시 재단에 신속히 보고하고 필요한 대응조치 수행 ○ 주요 위험 및 이슈에 대한 발생원인, 영향, 대응·조치사항 및 처리결과를 관리 ○ 업무별 정·부 담당자를 지정하고 재단 및 사업자 간 비상연락망을 구성하여 상시 현행화
산출정보	비상연락망, 위험·이슈 관리내역

요구사항 분류	사업관리 요구사항
요구사항 ID	PMR-008
요구사항 명칭	업무 인수인계
요구사항 상세설명	○ 사업자는 계약체결 후 기존 사업자로부터 보안관제 및 정보보호시스템 운영업무 전반에 대한 인수인계를 수행하여야 함 ○ 업무 인수인계 기간은 1개월을 원칙으로 하며, 세부 일정 및 수행방법은 재단과 협의하여 결정 ○ 업무 인수에 필요한 인력 투입 등 인수인계에 소요되는 제반 비용은 사업자가 부담 ○ 기존 사업자로부터 보안관제 대상 및 연동현황, 정보보호시스템 현황·구성정보, 보안정책 및 변경이력, 관리자 계정·접근권한 현황, 유지관리·기술지원 연락체계, 운영절차 및 매뉴얼, 장애·침해사고 대응이력 및 미결사항, 주요 수행업무 등 사업수행에 필요한 사항을 빠짐없이 인수하여야 함 ○ 사업수행책임자(PM) 및 주요 투입인력은 인수인계에 참여하여 업무내용 및 운영환경을 충분히 숙지하고 사업 개시일부터 정상적인 업무수행이 가능하도록 하여야 함 ○ 인수인계 항목 및 일정 등을 포함한 인수인계 계획을 수립하고, 항목별 인수 여부를 확인할 수 있도록 체크리스트를 작성·관리하여야 함 ○ 인수인계 과정에서 발생 가능한 업무공백, 자료누락, 운영오류 등 위험요소를 사전에 식별하고 이에 대한 방지대책을 마련하여야 함

	○ 인수인계 완료 후 인수사항, 미결사항 및 후속조치 사항 등을 포함한 인수인계 결과를 재단에 제출하고 재단의 확인을 받아야 함 ○ 사업 종료 시 사업자 관제시스템에 보관 중인 보안이벤트 및 로그의 이관·보존 및 파기 방안은 잔여 보관기간을 고려하여 재단과 협의하여 처리하여야 함 ○ 사업 종료 시 차기 사업자가 업무를 차질 없이 수행할 수 있도록 관련 자료를 정리·현행화하고, 재단이 요청하는 경우 차기 사업자에 대한 업무 인계에 성실히 협조하여야 함
산출정보	인수인계 계획서, 인수인계 체크리스트, 인수인계 결과보고서

라. 품질 요구사항

요구사항 분류	**품질 요구사항**
요구사항 ID	QUR-001
요구사항 명칭	서비스 수준 및 품질관리
요구사항 상세설명	○ 보안관제 및 정보보호시스템 운영 서비스의 품질 확보 및 향상을 위하여 서비스 수준 관리체계를 운영하여야 함 ○ 사업자는 사업개시 전까지 서비스 수준 관리방안 및 관리지표(안)를 마련하여 재단과 협의하여야 함 ○ 사업자는 사업개시 후 1개월 이내에 서비스 수준 관리기준을 최종 확정하고 재단과 서비스수준협약(SLA)을 체결하여야 함 ○ 재단은 용역수행 중 중간점검을 위해 측정결과를 요구할 수 있으며, 요구받은 경우 서비스 수준 측정결과서(중간점검용)를 제출하여야 함. ○ 서비스 수준이 목표수준에 미달하거나 서비스 품질 저하가 확인된 경우 원인을 분석하고 개선방안을 마련하여 필요한 조치를 수행하여야 함 ○ 서비스 수준 측정·평가 결과 및 개선조치 내역을 지속적으로 관리하여야 함 ○ 사업자는 사업 종료 시 서비스 수준에 대한 최종 성과측정을 실시하고 그 결과를 재단에 제출하여야 함
산출정보	서비스수준협약서(SLA), 서비스 수준 측정·평가 결과 및 개선조치 내역

마. 보안 요구사항

요구사항 분류	보안 요구사항
요구사항 ID	SER-001
요구사항 명칭	보안관리 일반
요구사항 상세설명	○ 사업자는 사업수행 기간 중 관련 법령 및 재단의 정보보호 관련 규정·지침을 준수하여야 함 ○ 사업수행계획서 작성 시 참여인력, 문서·자료, 정보시스템 및 장비 등에 대한 관리적·기술적·물리적 보안대책을 포함한 보안관리계획을 수립하고, 재단의 검토 및 시정·보완 요구사항을 반영하여야 함 ○ 사업수행에 대한 보안관리 책임자를 지정하고 사업기간 동안 보안관리 업무를 총괄하도록 함 ○ 사업수행 과정에서 취득한 재단의 정보 및 자료는 본 사업의 목적 외 용도로 사용하거나 외부에 누설·유출하여서는 아니 되며, 사업 종료 후에도 동일하게 적용 ※ 누출금지 정보 1. 재단 소유 정보시스템의 내·외부 IP주소 현황 2. 세부 정보보호시스템 구성 현황 및 정보통신망 구성도 3. 사용자계정·비밀번호 등 정보시스템 접근권한 정보 4. 정보시스템 취약점 분석·평가 결과물 5. 용역사업 결과물 및 프로그램 소스코드 6. 정보보호시스템 도입·운용 현황 7. 방화벽·IPS 등 정보보호시스템 및 라우터·스위치 등 네트워크 장비 설정 정보 8. 비밀, 대외비 및 비공개 등으로 분류된 재단 내부 정보 9.「개인정보 보호법」에 따른 개인정보 10. 사이버위협 분석자료 및 침해사고 대응 정보 11. 그 밖에 재단이 공개할 수 있다고 지정한 자료 이외의 자료 ○ 보안사항 또는 누출금지 정보의 누설·유출로 문제가 발생한 경우 사업자 및 사업 참여인력은 관련 법령 및 계약조건에 따른 제재를 받을 수 있으며, 이에 따른 손해배상 및 민·형사상 책임을 부담하여야 함 ○ 재단은 사업자의 보안관리 현황을 점검할 수 있으며, 보안상 필요한 시정·보완사항을 요구하는 경우 사업자는 이를 이행하여야 함 ○ 사업수행 중 보안사고 또는 정보유출 등 보안위반 사항이 발생하거나 발생이 의심되는 경우 즉시 재단에 보고하고 필요한 조치를 수행하여야 함 ○ 사업수행 과정에서 개인정보를 처리하는 경우「개인정보 보호법」및 재단과 체결하는 개인정보 처리위탁 계약의 제반사항을 준수하고, 이에 따른 관리적·기술적·물리적 보호조치를 이행하여야 함
산출정보	보안관리계획, 보안관리 책임자 지정 내역

요구사항 분류	보안 요구사항
요구사항 ID	SER-002
요구사항 명칭	참여인력 보안관리
요구사항 상세설명	○ 사업에 참여하는 모든 인력은 재단의 정보보호 관련 규정·지침 및 보안 수칙을 준수하여야 함 ○ 사업 참여인력은 업무 투입 전에 재단이 정한 보안서약서를 제출하여야 하며, 신규·대체·교체인력의 경우에도 업무 투입 전에 동일하게 적용 ○ 사업자는 참여인력을 대상으로 비밀유지, 정보유출 방지, 정보시스템 및 자료의 안전한 취급 등 사업수행에 필요한 보안교육을 실시 ○ 사업수행에 필요한 출입권한과 정보시스템 및 정보보호시스템에 대한 접근권한은 업무수행에 필요한 최소한의 인력 및 범위로 제한하여야 함 ○ 참여인력은 업무수행을 위하여 부여된 출입권한과 정보시스템 및 정보보호시스템에 대한 접근권한을 업무 목적에 한하여 사용하고 타인에게 공유·양도하여서는 아니 됨 ○ 참여인력의 퇴직·교체·업무변경 등으로 업무수행이 종료되는 경우 출입권한, 정보시스템 및 정보보호시스템의 계정·접근권한 등이 즉시 회수·해지될 수 있도록 재단에 관련 사실을 통보하고 필요한 조치 수행 ○ 사업수행 과정에서 취득한 재단의 정보 및 업무상 비밀에 대한 비밀유지 의무는 해당 인력의 사업 참여 종료 및 본 사업 종료 후에도 적용 ○ 참여인력의 보안규정 위반 또는 정보유출 등 보안사고 발생 시 즉시 재단에 보고하고 재단의 요구에 따른 필요한 조치를 수행
산출정보	참여인력 보안서약서, 보안교육 실시내역

요구사항 분류	보안 요구사항
요구사항 ID	SER-003
요구사항 명칭	자료 및 정보 보안관리
요구사항 상세설명	○ 사업수행 과정에서 재단으로부터 제공받거나 취득·생산한 정보, 자료 및 산출물은 안전하게 관리하여야 함 ○ 사업수행 과정에서 취득한 정보 및 자료는 본 사업의 목적 외 용도로 사용하거나 재단의 승인 없이 외부에 제공·공개·누설하여서는 아니 됨 ○ 정보 및 자료의 복사·전송·반출 등이 필요한 경우 사전에 재단의 승인을 받아야 하며, 업무수행에 필요한 최소한의 범위에서 취급 ○ 정보시스템 구성정보, IP정보, 보안정책 및 설정정보, 보안로그, 취약점 및 침해사고 분석자료 등 주요 정보는 인가된 인력만 접근할 수 있도록 관리

	○ 재단으로부터 제공받은 자료 및 사업수행 과정에서 생산된 자료는 분실·훼손·무단복제 및 유출되지 않도록 관리 ○ 사업 종료 또는 자료의 이용목적이 달성된 경우 재단의 요구에 따라 관련 자료를 반환하거나 복구할 수 없는 방법으로 파기하고 그 결과를 재단에 제출 ○ 자료의 분실·유출 등 보안사고가 발생하거나 의심되는 경우 즉시 재단에 보고하고 사고조사 및 후속조치에 협조 ○ 재단의 사전 승인 없이 사업 관련 정보 및 자료를 개인 이메일, 외부 클라우드 서비스, 생성형 인공지능 서비스 또는 국외 서버 등에 저장·전송·입력하여서는 아니 됨
산출정보	자료 반출 승인·관리내역, 자료 반환·파기 확인자료

요구사항 분류	**보안 요구사항**
요구사항 ID	SER-004
요구사항 명칭	장비·매체 및 업무환경 보안관리
요구사항 상세설명	○ 사업수행에 사용하는 PC, 노트북 등 정보통신장비는 재단이 지정하거나 승인한 장비를 사용하고 재단의 보안정책을 준수하여 관리 ○ 업무용 PC 등에는 백신 및 재단이 요구하는 보안프로그램을 설치하고 운영체제·응용프로그램의 보안상태, 비밀번호 및 화면보호기 등 필요한 보안조치를 적용 ○ PC, 노트북, USB 등 정보통신장비 및 보조기억매체의 반출·입은 원칙적으로 제한하며, 업무상 필요한 경우 재단의 사전 승인을 받아 정해진 절차에 따라 수행 ○ 보조기억매체는 재단이 승인한 매체에 한하여 사용하고 비인가 보조기억매체의 사용을 금지 ○ 장비 및 매체의 반출·입 시 악성코드 감염 여부 및 사업 관련 자료의 무단 반출 여부 등을 확인하고 필요한 보안조치 수행 ○ 재단 정보시스템에 대한 외부 원격접속이 필요한 경우 사전에 재단의 승인을 받고 재단이 지정한 보안접속 방식과 접근권한 범위 내에서 수행하며 접속 및 작업이력을 관리 ○ 사업수행 장소 및 업무용 장비는 비인가자의 접근·사용을 방지할 수 있도록 관리하고 자리 이석 시 화면잠금 등 필요한 보호조치 수행 ○ 사업 종료 또는 장비 반출 시 해당 장비·매체에 저장된 재단 관련 자료를 복구할 수 없는 방법으로 삭제하고, 재단이 요구하는 경우 그 결과를 제출하여 확인받아야 함
산출정보	장비·매체 반출입 및 사용 관리내역

바. 제약사항

요구사항 분류	제약사항
요구사항 ID	COR-001
요구사항 명칭	사업수행 관련 법령 및 계약조건 준수
요구사항 상세설명	○ 사업자는 본 사업 수행에 적용되는 관련 법령, 계약조건 및 재단의 관련 규정을 준수하여야 함 ○ 사업기간 중 본 사업에 적용되는 법령·규정 등이 제·개정되는 경우 변경사항을 확인하고, 필요한 사항은 재단과 협의하여 사업수행에 반영 ○ 제안요청서, 제안서 및 계약서 등에 명시되지 않은 사항은 재단과 협의하여 처리
산출정보	-

요구사항 분류	제약사항
요구사항 ID	COR-002
요구사항 명칭	손해배상 책임
요구사항 상세설명	○ 사업자는 사업수행 시 선량한 관리자로서의 주의의무를 다하여야 함 ○ 사업자의 고의 또는 과실로 재단의 정보시스템, 정보보호시스템, 장비 및 기타 재산 등에 손해를 발생시킨 경우 이에 대한 책임을 부담하고 해당 손해를 배상하여야 함 ○ 사업자의 귀책사유로 사업수행 과정에서 발생한 사고 또는 계약상 의무 위반으로 재단에 손해가 발생한 경우 관련 법령 및 계약조건에 따라 책임을 부담하여야 함
산출정보	-

Ⅳ 사업 수행 지침

1. 일반지침

가. 사업자는 본 사업 전체의 이행에 대한 포괄적인 책임을 지며, 제안요청서, 제안서, 계약내용 및 재단의 승인을 받은 사업수행계획서에 따라 사업을 성실히 수행하여야 한다.

나. 사업자는 계약체결 후 7일 이내에 착수계, 사업수행계획서 등 사업수행에 필요한 제반 서류를 제출하여 재단의 검토·승인을 받아야 한다.

다. 사업자는 본 사업 수행에 적용되는 관계 법령·규정·지침 및 재단의 관련 규정을 준수하여야 하며, 사업기간 중 관련 법령·규정 등이 제·개정되는 경우 재단과 협의하여 필요한 사항을 사업수행에 반영하여야 한다.

라. 과업 목적 달성을 위해 필요한 사항은 본 제안요청서에 명시되지 않은 경우에도 재단이 요청할 수 있으며, 사업자는 이를 수행하여야 한다. 다만, 과업범위 또는 계약조건의 중대한 변경이 필요한 사항은 상호 협의하여 처리한다.

마. 사업수행 중 사업계획 변경, 불가항력, 과업 추가 또는 과업범위 변경 등 계약내용의 조정이 필요한 경우에는 재단과 사전에 협의하고 관계 법령 및 계약조건에 따라 처리한다.

바. 본 제안요청서의 문구·용어 및 과업범위 등에 대하여 해석상 이견이 있는 경우에는 재단의 해석에 따른다.

사. 사업자가 정당한 사유 없이 재단의 업무지시를 이행하지 아니하거나 계약조건을 위반하는 경우 재단은 시정·개선을 요구할 수 있으며, 사업자가 정당한 사유 없이 이를 이행하지 않는 경우 관계 법령 및 계약조건에 따라 계약의 해제·해지 등 필요한 조치를 할 수 있다.

아. 해당 과업은 「중대재해 처벌 등에 관한 법률」의 안전 및 보건 확보 의무사항에 따라 사업장에서 종사자의 안전·보건상 유해 또는 위험을 방지하기 위하여 그 사업 또는 사업장의 특성 및 규모 등을 고려하여 다음과 같이 조치사항을 이행하여야 한다.

<계약업체의 안전 및 보건 확보 의무사항(제4조, 제9조)>

① 재해예방에 필요한 인력·예산·점검 등 안전보건관리체계의 구축 및 그 이행
② 재해 발생 시 재발방지 대책의 수립 및 그 이행
③ 중앙행정기관·지자체가 관계 법령에 따라 개선, 시정 등을 명한 사항 이행
④ 안전·보건 관계 법령에 따른 의무이행에 필요한 관리상의 조치

2. 소유권 및 지식재산권 귀속 등

가. 본 사업 수행 과정에서 새로 작성·생산된 보고서, 분석자료, 운영절차서, 매뉴얼, 현황자료 등 사업수행 산출물에 대한 소유권 및 저작재산권 등 지식재산권은 재단에 귀속한다. 다만, 사업자가 본 사업 수행 이전부터 보유한 기술, 프로그램, 도구 등 기존 지식재산권은 사업자에게 귀속한다.

나. 사업자는 본 사업을 수행함에 있어 제3자의 특허권, 저작권 등 지식재산권을 침해하여서는 아니 되며, 이와 관련한 분쟁이 발생한 경우 사업자의 책임과 비용으로 이를 해결하여야 한다. 이로 인하여 재단에 손해가 발생한 경우 사업자는 그 손해를 배상하여야 한다.

다. 사업자는 본 사업 수행을 위하여 제3자의 프로그램, 소프트웨어, 기술 등을 사용하는 경우 이에 필요한 사용권 등 적법한 권리를 사전에 확보하여야 한다.

Ⅴ 제안 안내 사항

1. 입찰 참가 자격

가. 「지방자치단체를 당사자로 하는 계약에 관한 법률 시행령」 제13조 및 같은 법 시행규칙 제14조에 의한 경쟁입찰 참가자격을 갖추고, 아래의 자격을 모두 갖춘 업체

1) 「보안관제 전문기업 지정 등에 관한 공고」에 따라 지정된 보안관제 전문기업(업종코드 6526)

2) 「정보보호산업의 진흥에 관한 법률」에 따라 지정된 정보보호 전문서비스 기업(업종코드 1542)

※ 입찰서 제출 마감일 전일까지 조달청 나라장터(G2B)에 해당 업종으로 입찰참가자격 등록을 마치고, 입찰서 제출 마감일 현재 각 지정이 모두 유효하여야 함

나. 「지방자치단체를 당사자로 하는 계약에 관한 법률」 제31조 및 같은 법 시행령 제92조, 같은 법 시행규칙 제76조에 따른 부정당업자로 입찰참가자격 제한 중이지 아니한 업체

다. 공동수급 및 하도급 불가

2. 입찰 참가 등록 및 제안서 제출

가. 제출서류: 입찰공고문에 의함

나. 제출기한: 입찰공고문에 의함

다. 제안내용 문의

○ 입찰문의: 운영지원실 입찰 담당자 (02-398-0152 / glass@chorogusan.or.kr)

* 과업문의는 메일로 질의

VI 제안서 작성 요령

1. 제안서 작성 및 제출

가. 제출부수: 제안서 및 제안요약서 각 3부, 동 내용이 수록된 USB 1개 별도 제출
 * 제안요약서는 제안설명(PT) 발표자료로 활용함

나. 분　　량: 제안서 본문 100페이지 이내(표지·목차 및 별첨 증빙자료 제외),
제안요약서 30페이지 이내(표지·목차 제외)

다. 규　　격: A4(210×297mm)를 원칙으로 하며, 전자파일은 PDF 형식으로 제출

2. 제안서의 효력

가. 제안서에 제시된 내용과 재단의 요구에 따라 수정, 보완, 변경된 제안 내용은 계약서에 명시하지 아니하더라도 계약서와 같은 효력을 가진다. 다만, 계약서에 명시된 경우는 계약서를 우선으로 한다.

나. 재단은 필요시 제안사에 대하여 추가 제안 또는 자료를 요구할 수 있으며, 이에 따라 제출된 자료는 제안서와 같은 효력을 가진다.

다. 제출된 제안서의 내용은 재단이 요청하지 않는 한 수정·추가·대체할 수 없다.

라. 제안서 또는 제출자료의 중요 내용이 허위로 확인되거나, 계약 후 제안내용을 정당한 사유 없이 이행하지 않는 경우 재단은 계약의 해제·해지, 손해배상 청구 등 관계 법령 및 계약조건에 따른 필요한 조치를 할 수 있다.

3. 제안서 작성 유의 사항

가. 표지와 목차를 제외한 제안서의 각 페이지 하단 중앙에 연속된 일련번호를 부여하여야 한다.

나. 제안서는 국문 작성이 원칙이며, 사용된 영문약어에 대해서는 약어표를 제공하여야 한다.

다. 제안서의 내용을 객관적으로 입증할 수 있는 관련 자료는 제안서의 별첨으로 제출하여야 한다.

라. 제안서의 내용은 명확한 용어를 사용하여 표현하여야 하며, '할 수 있다', '가능하다', '고려하고 있다' 등 모호한 표현은 해당 요구사항을 수용하지 않은 것으로 간주할 수 있다. 계량화가 가능한 사항은 가능한 한 계량화하여 제시하여야 한다.

마. 제안서에는 주민등록번호, 외국인등록번호, 여권번호, 운전면허번호 등 고유식별정보를 기재하여서는 아니 되며, 재단의 비공개 정보 및 본 제안요청서에서 정한 누출금지 정보를 포함하여서는 아니 된다.

바. 제안요약서는 제안서의 주요 내용을 요약하여 작성하여야 하며, 제안서에 포함되지 않은 내용을 추가하여서는 아니 된다.

Ⅶ 제안서 평가 및 선정

1. 선정방법

가. 입찰종류: 일반경쟁(총액)

나. 낙찰자 결정방법: 협상에 의한 계약

다. 제안서 심사: 제안서 평가위원회 구성하여 평가

※ 제안서 심사위원별 평가 점수 및 평가내용은 공개하지 않습니다.

2. 제안서 평가

가. 평가기준 및 배점

구분		평가부문	평가항목	배점	비고
기술능력평가(90점)	정량평가분야(20점)	일반부문(20)	■ **참여업체 수행실적** - 최근 3년간 보안관제 사업 수행실적	10	사업부서 또는 입찰담당자 평가
			■ **경영 및 재무 상태** - 재무상태의 건전성("신용평가등급확인서"를 통해 평가)	10	
	정성평가분야(70점)	전략 및 방법론(10)	■ **사업이해도** - 사업목적·환경 및 제안요청사항에 대한 이해도	5	평가위원 평가
			■ **수행전략** - 사업 수행전략 및 방법론의 적정성과 실현가능성	5	
		사업수행능력(40)	■ **보안관제 수행** - 보안관제 요구사항 전반에 대한 수행방안의 적정성 및 전문성	10	
			■ **상주인력 및 정보보호시스템 운영** - 상주인력 및 정보보호시스템 운영 요구사항에 대한 수행역량 및 적정성	15	
			■ **정보보호 진단 및 개선** - 취약점 분석·평가, 모의해킹, 정보보호 관리체계 점검 및 개선 수행방안의 적정성 및 전문성	15	
		프로젝트 관리(10)	■ **사업관리, 품질관리 및 보안관리** - 사업관리 체계와 품질 및 보안관리 방안의 적정성 - 인수인계 및 업무연속성 확보방안의 적정성	10	

		프로젝트 지원 (10)	■ **전문지원체계** - 사업수행 전반에 대한 분야별 기술지원 조직 및 지원 체계의 적정성	5	
			■ **정보보호 교육 및 훈련** - 정보보호 교육 및 훈련 수행방안의 적정성	5	
가격평가 (10점)		입찰가격 (10)	■ **제안 가격 평가** - 행정안전부 [지방자치단체 입찰 시 낙찰자 결정기준] 협상에 의한 계약산식	10	* 산식에 의한 평가
합계				100	-

※ 보안관제 및 정보보호시스템 운영의 전문성과 사업수행 역량에 중점을 두어 평가

나. 정량적 평가 분야 배점 기준

1) 참여업체 수행실적(10점)

- 입찰공고일 기준 최근 3년 이내(2023. 9. ~ 입찰공고일) 이행이 완료된 보안관제 사업 중 단일 계약금액 280,000,000원(부가가치세 포함) 이상인 사업에 한함

평가항목	평가등급	평점
유사 사업 수행실적 (최근 3년)	10건 이상	10
	7 ~ 9건	9
	5 ~ 6건	8
	3 ~ 4건	7
	1 ~ 2건	6
	실적 없음	0

※ 동일 발주기관의 실적이라도 각각 별도의 계약으로 체결되어 이행이 완료된 경우 각각 1건으로 인정함

※ 보안관제를 포함한 정보보호시스템 운영 및 유지관리 등 통합사업은 실적증명서에서 보안관제 수행내용이 확인되는 경우 인정함

※ 수행실적의 세부 인정기준 및 증빙방법은 [별지3 서식]에 따름

※ 실적증명서 발급이 부득이하게 어려운 경우(예: 발주처 폐업 등)에 한하여 해당 용역계약서 사본과 세금계산서 제출로 대체할 수 있으며, 단순 편의에 따른 용역계약서 사본 제출은 실적으로 인정하지 않음

2) 경영상태 평가(10점)

회사채	기업어음	기업신용평가	평점
AAA, AA+, AA0, AA-, A+, A0, A-, BBB+, BBB0	A1, A2+, A20, A2-, A3+, A30	AAA, AA+, AA0, AA-, A+, A0, A-, BBB+, BBB0	10
BBB-, BB+, BB0, BB-	A3-, B+, B0	BBB-, BB+, BB0, BB-	9.5
B+, B0, B-	B-	B+, B0, B-	9
CCC+ 이하	C 이하	CCC+ 이하	7

① 신용평가등급은「신용정보의 이용 및 보호에 관한 법률」제4조 제4항 제1호 또는 제4호의 업무를 영위하는 신용정보업자가 동 세부기준 제5조의 적용기준일 이전 가장 최근에 평가한 유효기간 내 회사채(또는 기업어음)에 대한 신용평가등급 또는 기업신용평가 등급으로 하며, 위의 신용정보업자가 신용평가등급, 등급 평가일 및 등급 유효기간 등을 명시하여 작성한 "신용평가등급 확인서"(이하 "등급확인서"라 한다)를 기준으로 평가한다.

② 회사채(또는 기업어음)에 대한 신용평가등급 또는 기업신용평가등급은 입찰공고일 전일 이전에 평가한 것으로서 유효기간 내에 있는 것이어야 한다. (유효기간 만료일이 입찰공고일인 경우도 인정)

③ 회사채(또는 기업어음)에 대한 신용평가 등급 및 기업신용평가에 따른 평점이 다른 경우에는 높은 평점으로 평가하며, "등급확인서"를 제출하지 않은 경우에는 최저등급으로 평가한다.

3. 평가 및 선정방법

가. 제안서 및 설명(프레젠테이션)을 통하여 평가 실시

1)「Ⅶ 제안서 평가 및 선정 2-가. 평가기준 및 배점」중 기술능력 평가 기준에 따라 사업담당부서 내부 심사위원 구성 후 서면심사(입찰가격 평가 제외), 이를 통해 상위 3순위까지 선정하여 PT(프레젠테이션) 실시

* 제안서 제출 업체가 3개 이하일 경우 서류심사는 생략하고 모두 프레젠테이션 평가 참여자격 부여

2) 제안서 설명(PT) 방법

① 제안서 설명 시간은 30분 내외(제안설명발표 20분, 질의응답 10분)

② 제안설명은 제출한 제안요약서를 발표자료로 활용하여 진행함

3) 제안서 설명 발표순서

입찰 마감일 제안서 등록 제출 역순으로 자동 순서 배정

4) 유의사항

① 제안발표회는 제안사의 발표자를 포함하여 3인 이내로 제한하며, 제안설명은 제안사의 사업수행책임자(PM)가 직접 발표해야 한다.

② 발표내용이 제안서와 상이한 사항이 있는 경우 이를 별도로 명기하여야 한다.

③ 제안서 평가는 재단의 평가 기준에 의하여 평가하며, 제안사는 제안서 평가 결과에 대해 일체의 이의를 제기할 수 없다.

④ 제안발표회에 참가하지 않은 업체는 협상적격자 대상에서 제외한다.

나. 우선협상 대상자 선정

1) 제안서 평가 결과, 입찰가격이 해당 사업 예산 이하인 자로서, 기술능력 평가점수가 기술능력 평가분야(정량평가+정성평가) 배점한도의 85% 이상이고, 기술능력 평가점수와 가격평가 점수의 합산점수가 70점 이상인 자를 협상적격자로 선정한다.
2) 1)에 따른 협상적격자가 없는 경우에는 재공고 입찰에 부칠 수 있다.
3) 협상 순서는 기술능력평가 점수와 가격평가 점수를 합산한 고득점순으로 결정한다.
4) 다만, 합산 점수가 동일한 제안자가 2인 이상일 경우에는 정성적 평가 분야 항목의 세부 평가항목 중 배점이 큰 항목에서 높은 점수를 얻은 자를 우선순위로 한다.

다. 협상 절차

1) 협상은 재단이 정하는 절차와 일정에 따라 진행하며, 기술조건 합의 및 재단이 요구하는 사항에 근거하여 진행한다.
2) 결정된 협상 순위에 따라 협상대상자와 협상을 실시하며, 협상이 성립된 경우 최종 낙찰자로 선정하고 다른 협상적격자와 협상을 실시하지 아니한다.
3) 협상대상자와 협상이 성립되지 않으면 같은 기준과 절차에 따라 순차적으로 차 순위 협상자와 협상을 시행하며, 모든 협상자와 협상이 결렬되면 재공고 입찰에 부칠 수 있다.
4) 협상기간은 협상대상자 통보일로부터 15일 이내로 하고, 상호협의 하에 협상기간을 조정할 수 있다. 정한 기한 내에 협상이 이루어지지 않을 경우에는 10일의 범위 내에서 연장할 수 있다. 그러나 협상대상자가 협상에 불성실하게 임하거나, 협상을 지연시키는 경우 재단은 협상이 결렬된 것으로 간주한다.

[별지1 서식]

<table>
<tr><td colspan="6">용역사업 제안서</td></tr>
<tr><td>사업명</td><td colspan="5"></td></tr>
<tr><td rowspan="2">용 역
업 체</td><td>업체명</td><td colspan="4"></td></tr>
<tr><td>주 소</td><td colspan="4"></td></tr>
<tr><td rowspan="3">사 업
수 행
책임자
(PM)</td><td>성 명</td><td></td><td>직위/전공</td><td colspan="2"></td></tr>
<tr><td>소 속</td><td></td><td>전 화</td><td colspan="2"></td></tr>
<tr><td>e-mail</td><td colspan="4"></td></tr>
<tr><td>사 업
기 간</td><td colspan="2"></td><td>참 여
인 력</td><td colspan="2">명</td></tr>
<tr><td colspan="6">「2027~2029년 초록우산 하이브리드 보안관제 및 정보보호시스템 운영 용역」 사업에 대한 제안서를 제출합니다.

상기 사업 과제가 귀 재단의 용역사업비에 의하여 수행될 경우 이에 따른 모든 편의를 제공할 것이며 소정의 기관책무를 이행하겠습니다.

2026년 월 일

용역사업 기관 대표: (직인)</td></tr>
<tr><td colspan="6">사회복지법인 어린이재단 귀중</td></tr>
<tr><td colspan="6">구비서류: 증빙자료</td></tr>
</table>

[별지2 서식]

일반현황 및 주요 연혁

1. 기본사항

회사명		대표자명	
주소		회사설립년월	년 월
전화번호		팩스번호	
사업자번호		업종	
면허/허가 등록증보유현황	* 보유 사항이 있는 경우 작성		
종업원수		자본금 (단위:천원)	
매출액 (단위: 천원)	2023년	2024년	2025년

2. 주요 연혁

일자	내용	비고

* 제안서 내에 해당 내용을 포함할 경우 별도 제출 불필요

[별지3 서식]

사업 실적

※ 단위: 백만원, 부가가치세 포함

사업명	사업기간[1)]	계약 금액	발주처	용역수행 범위	비고

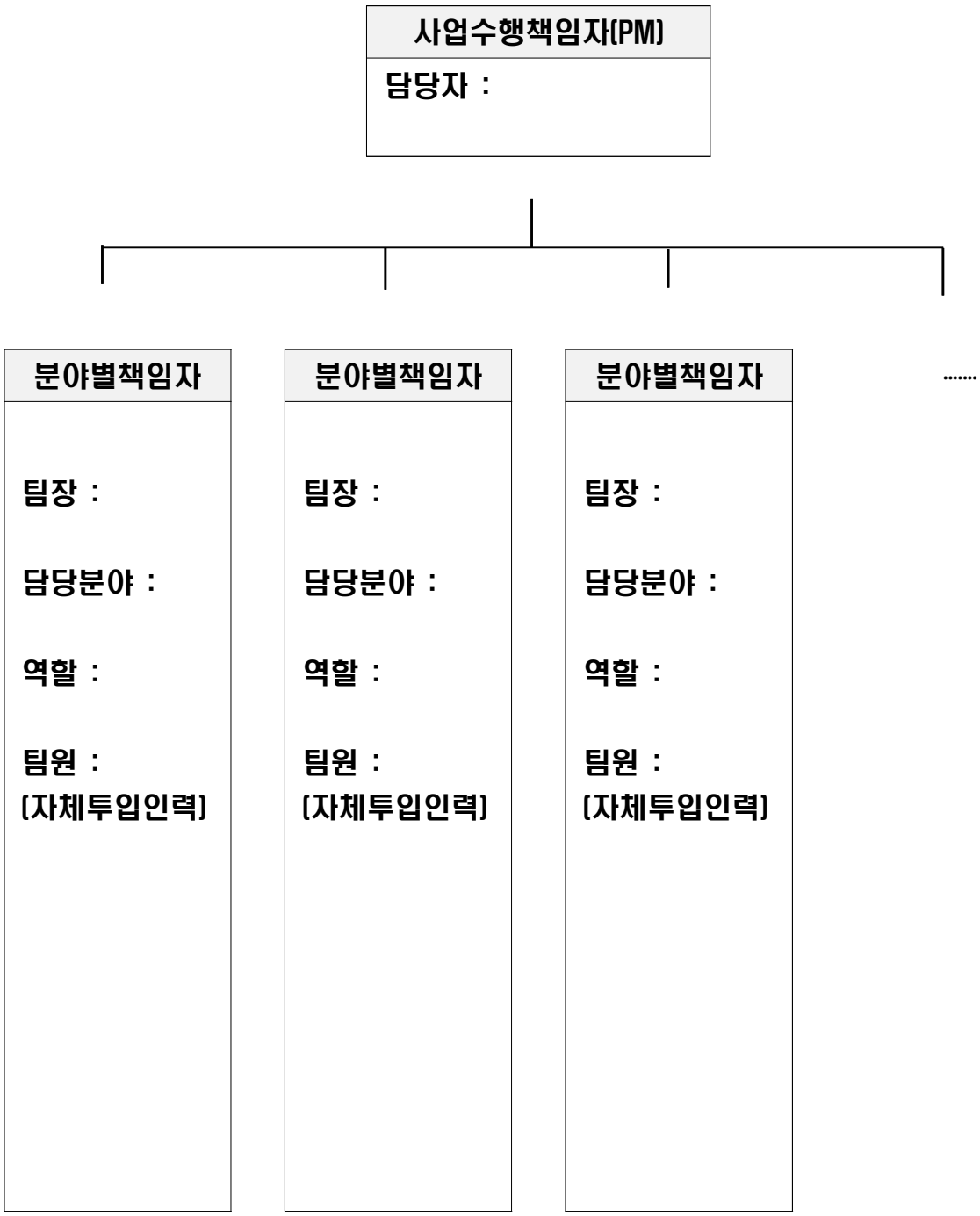
주 1) 입찰공고일 기준 최근 3년 이내 이행이 완료된 실적을 최근 연도순으로 기재하여야 함

< 작성 시 참고사항 >

- 입찰공고일 기준 최근 3년 이내 이행이 완료된 보안관제 사업 중 단일 계약금액 280,000,000원(부가가치세 포함) 이상인 실적을 건별로 작성하여야 함
- 보안관제를 포함한 정보보호시스템 운영 및 유지관리 등 통합사업의 경우 실적증명서에서 보안관제 수행내용이 확인되어야 함
- 동일 발주기관에서 수행한 실적이라도 각각 별도의 계약으로 체결되고 이행이 완료된 경우 각각 구분하여 작성하고, 해당 실적증명서를 첨부하여야 함
- 수행실적은 발주기관이 발급한 실적증명서 또는 조달청 나라장터에서 발급한 용역이행실적증명서로 증빙하여야 함
- 수행실적에 대한 입증책임은 제안사에 있으며, 제출한 증빙자료로 사업내용, 계약금액 또는 이행완료 여부 등을 확인하기 어려운 경우 해당 실적은 인정하지 않음
- 반드시 발주처의 확인을 받은 실적증명서를 기준으로 작성하며(조달청 용역이행실적증명서로 대체 가능), 실적증명서 미제출 시 사업 실적으로 인정하지 않음. 단, 실적증명서 발급이 부득이하게 어려운 경우(예: 발주처 폐업 등)에 한하여 해당 용역계약서 사본과 세금계산서 제출로 대체할 수 있으며, 단순 편의에 따른 용역계약서 사본 제출은 실적으로 인정하지 않음

[별지4 서식]

사업수행 조직도



※ 지원조직이 있을 경우에는 추가하여 작성
※ 분야별 책임자는 분야별 팀장을 말함
※ 제안사 자체양식 제출 가능

[별지5 서식]

참여인력 현황

1) 참여인력 명단

분야 [1]	성명	연령	근무경력 [2]	직위	주요담당업무	보유기술

주 1) 업무구분

2) 해당 분야 경력기간만 기재

1-1) 참여인력 이력사항

성 명		소 속		직 책		연 령	세
학 력	대학교		전공	해당분야근무경력			
	대학원		전공	자 격 증			
참여업무(분야)		사업참여기간				참여율	%

주 요 경 력				
사 업 명	참 여 기 간 (년/월 ~ 년/월)	담당업무	발주처	비 고

< 작성 시 참고사항 >

- 투입인력은 반드시 본 사업에 투입 가능한 제안사 소속 인력으로 구성하여야 함
- 개인별 자격, 경력 및 재직 여부를 객관적으로 확인할 수 있는 증빙자료를 제출하여야 하며, 허위 작성이 확인되는 경우 관계 법령 및 계약조건에 따라 필요한 조치를 할 수 있음
- 투입인력의 재직 여부 확인을 위하여 4대 사회보험 사업장 가입자 명부로 객관적인 증빙자료를 제출하여야 함
- 투입인력의 자격 및 경력 확인을 위하여 자격증 사본, 경력증명서 또는 관련 협회·기관에서 발급한 경력확인서 등 객관적인 증빙자료를 제출하여야 함
- 경력증명서 또는 경력확인서의 발급이 곤란한 경우에는 국민연금 가입증명서, 건강보험 자격득실확인서 등 근무기간을 확인할 수 있는 자료와 해당 분야 업무 수행경력을 확인할 수 있는 자료를 함께 제출하여야 함
- 제출된 증빙자료로 자격, 경력 또는 재직 여부를 확인하기 어려운 경우 해당 사항은 인정하지 않음
- 증빙자료에 포함된 주민등록번호 등 본 사업의 확인에 불필요한 개인정보는 마스킹하여 제출하여야 함

[별지6 서식]

제안요청서 수용여부 참조표

요구사항 ID	요구사항 명	수용여부	제안서 페이지
SMR-001	*24시간 365일 실시간 원격 보안관제*	*O/X*	*25*
추가제안	*추가제안 내용*	*-*	*82*

※ 본 참조표는「Ⅰ. 제안업체 일반」에 포함하여 작성하여야 함

※ 추가제안 사항이 있는 경우 '요구사항 ID'란에 '추가제안'으로 표기하고, '요구사항명'란에 추가제안 내용을 간략히 기재하여야 함

[별표1]

기술인력의 자격기준

<table>
<tr><th>구 분</th><th>관련 자격 또는 관련 학력을
보유한 사람</th><th>관련 자격 또는 관련 학력을
보유하지 않은 사람</th></tr>
<tr><td>초 급
기술자</td><td>· 학사 이상의 학위, 기사 또는 정보보호 관련 국내외 자격을 취득한 사람
· 전문대학 졸업 또는 산업기사 자격을 취득한 후 2년 이상의 정보통신 관련 경력이 있는 사람
· 기능사 자격을 취득한 자로서 4년 이상의 자격을 취득한 자</td><td>· 학사 이상의 학위를 취득한 후 2년 이상의 정보통신 관련 경력이 있는 사람
· 전문대학을 졸업한 후 4년 이상의 정보통신 관련 경력이 있는 사람
· 정보통신 관련 경력 6년 이상 있는 사람</td></tr>
<tr><td rowspan="2">중 급
기술자</td><td>· 1년 이상의 정보보호 관련 경력이 있고 석사학위를 취득한 사람
· 학사학위, 기사 또는 정보보호 관련 국내외 자격을 취득한 후 3년 이상의 정보보호 관련 경력이 있는 사람
· 전문대학 졸업 또는 산업기사 자격을 취득한 후 5년 이상의 정보보호 관련 경력이 있는 사람</td><td>· 학사 이상의 학위를 취득한 후 5년 이상의 정보보호 관련 경력이 있는 사람
· 전문대학을 졸업한 후 7년 이상의 정보보호 관련 경력이 있는 사람</td></tr>
<tr><td colspan="2">· 초급 자격 기준 취득 후 3년 이상 정보보호 경력이 있는 사람</td></tr>
<tr><td rowspan="2">고 급
기술자</td><td>· 박사학위 또는 기술사 자격을 취득한 사람
· 4년 이상의 정보보호 관련 경력이 있고 석사학위를 취득한 사람
· 학사학위, 기사 또는 정보보호 관련 국내외 자격을 취득한 후 6년 이상의 정보보호 관련 경력이 있는 사람
· 전문대학 졸업 또는 산업기사 자격을 취득한 후 8년 이상의 정보보호 관련 경력이 있는 사람</td><td>· 학사 이상의 학위를 취득한 후 8년 이상의 정보보호 관련 경력이 있는 사람
· 전문대학을 졸업한 후 10년 이상의 정보보호 관련 경력이 있는 사람</td></tr>
<tr><td colspan="2">· 중급 자격 기준 취득 후 3년 이상 정보보호 경력이 있는 사람</td></tr>
</table>

<table>
<tr><td rowspan="2">특 급
기술자</td><td>· 3년 이상의 정보보호 관련 경력이 있고 박사학위 또는 기술사 자격을 취득한 사람
· 7년 이상의 정보보호 관련 경력이 있고 석사학위를 취득한 사람
· 학사학위, 기사 또는 정보보호 관련 국내외 자격을 취득한 후 9년 이상의 정보보호 관련 경력이 있는 사람
· 전문대학 졸업 또는 산업기사 자격을 취득한 후 11년 이상의 정보보호 관련 경력이 있는 사람</td><td>· 학사 이상의 학위를 취득한 후 11년 이상의 정보보호 관련 경력이 있는 사람
· 전문대학을 졸업한 후 13년 이상의 정보보호 관련 경력이 있는 사람</td></tr>
<tr><td colspan="2">· 고급 자격 기준 취득 후 3년 이상 정보보호 경력이 있는 사람</td></tr>
<tr><td>기 타</td><td colspan="2">※ 정보통신유관경력은 정보보호유관경력 50%로 인정한다(단, 정보보호유관경력은 정보통신유관경력과 중복인정 안됨).
※ 자격 및 학위 취득 이전의 정보보호유관경력은 50%를 인정한다.
※ 한국인터넷진흥원의 정보보호전문가(SIS) 2급 자격을 취득한 자는 유관 자격 또는 유관 학력의 보유 여부와 관계없이 초급 기술자로 인정하며, SIS 1급은 기사 자격에 준하여 인정한다(단, 비고 "5호"의 "가" 항목과 중복인정 안됨).
※ 국내외 해킹방어대회 입상자는 전문위원회 심의를 통하여 유관 자격 또는 유관 학력의 보유 여부와 관계없이 중급 기술자 이상으로 인정할 수 있다.</td></tr>
</table>

<비고>

1. "관련자격"이란「국가기술자격법 시행규칙」별표 7에 따라 과학기술정보통신부장관 또는 방송통신위원회 검정의 소관으로 하는 전자계산기, 정보통신, 통신설비, 통신기기, 통신선로, 정보기기운용, 전파통신, 전파전자, 무선설비, 방송통신, 정보관리, 정보처리, 사무자동화 및 전자계산조직응용 종목의 기술자격을 말한다.

2. "관련학력"이란「고등교육법」에 따른 해당 학교에서 다음 각 목에 해당하는 학과에서 소정의 과정을 이수하고 졸업하거나 그 밖의 관계법령에 따라 국내 또는 외국에서 이와 같은 수준 이상으로 인정되는 학력을 말한다.

가. 전자 관련 학과: 정보전자, 전자, 전자계산, 전기전자제어, 전자정보, 전자제어, 전기전자, 전자전기정보, 전자컴퓨터전기제어, 컴퓨터과학, 전기전자정보, 전자컴퓨터, 메카트로닉스, 전자재료, 제어계측, 반도체

나. 정보통신 관련 학과: 전기통신설비, 국제정보통신, 방송설비, 방송통신, 이동통신, 전자통신, 컴퓨터네트워크, 통신, 컴퓨터정보기술, 전파통신, 전기전자통신, 전기전자정보통신, 전자정보통신, 전자제어통신, 전자통신, 전파, 전파통신, 정보통신, 컴퓨터통신, 항공통신정보, 전자정보통신반도체, 전기전자전파, 통신컴퓨터, 무선통신

다. 정보처리기술 관련 학과: 시스템, 전산, 정보전산, 컴퓨터제어, 컴퓨터응용제어, 컴퓨터응용, 컴퓨터응용설계, 구조시스템, 컴퓨터정보, 멀티미디어, 정보시스템, 전산통계, 정보처리

라. 그 밖에 교육부장관이나 해당 교육기관의 장으로부터 전자·통신 및 정보처리기술·정보보호 관련 학과로 인정받은 학과

3. "정보통신 유관경력"이란 공공기관, 민간기업, 교육기관 등에서 정보통신서비스(기간통신, 별정통신, 부가통신, 방송서비스 등을 말한다), 정보통신기기(정보기기, 방송기기, 부품 등을 말한다) 또는 소프트웨어 및 컴퓨터 관련 서비스(패키지 소프트웨어, 컴퓨터 관련 서비스, 디지털콘텐츠, 데이터베이스 제작 및 검색 등을 말한다)에 해당되는 분야에서 계획·분석·설계·개발·운영·유지보수·컨설팅·감리 또는 연구개발 업무 등을 수행한 기간을 말한다.

4. "정보보호 유관경력"이란 공공기관, 민간기업, 교육기관 등에서 정보보호를 위한 공통기반기술(암호 기술, 인증 기술 등을 말한다), 시스템·네트워크 보호(시스템 보호, 해킹·바이러스 대응, 네트워크 보호 등을 말한다) 또는 응용서비스 보호(전자거래 보호, 응용서비스 보호, 정보보호 표준화 등을 말한다)에 해당되는 분야에서 계획·분석·설계·개발·운영·유지보수·컨설팅 또는 연구개발 업무 등을 수행한 기간을 말한다.

5. 다음 각 목에 해당하는 자격증을 보유한 자는 정보보호 유관경력 1년으로 인정하되, 중복 인정은 할 수 없다.(정보보호 관련 국내외 인정 자격 또한 다음 각 목과 같으며, 정보보호 유관경력과는 중복 인정되지 아니한다.)

가. 정보시스템감리사
나. 공인정보시스템감사사(CISA: Certified Information Systems Auditor)
다. 공인정보시스템보호전문가(CISSP: Certified Information Systems Security Professional)
라. 정보보호전문가(SIS: Specialist for Information Security)
마. 정보보안기사, 정보보안산업기사
바. 정보보호관리체계(ISMS: Information Security Management System) 인증심사원
사. 전자정부정보보호관리체계(G-ISMS: Government Information Security Management System) 인증심사원
아. 개인정보보호관리체계(PIMS: Personal Information Security Management System) 인증심사원

6. 제7조제1항제1호에 따른 기술인력은 신원조사에서 국가 안전보장에 유해한 정보가 있음이 확인되면 기술인력으로 인정되지 아니한다.