정보보호시스템 구축을 위한 실무가이드

2018. 6.

과학기술정보통신부

KISA 한국인터넷진흥원

CONTENTS

CONTENTS

제1장
정보보호사업 개요

제 1 장 정보보호사업 개요

제 1 절 정보보호사업 정의

1. 정보보호시스템의 의미

○ ‘정보보호시스템’은 정보보호를 위한 관리적·기술적·물리적 수단을 의미하므로, 웹 방화벽 구축, 침입탐지시스템 설치 등과 같이 정보보호 관련 하드웨어(관련 소프트웨어의 설치 포함)의 구축에 한정되지 않습니다. 즉, 정보보호시스템은 「전자정부법」에 따른 정보시스템, 정보보호진흥법 시행령에 따른 구매정보시스템, 전자공시시스템 등과 같이 ‘하드웨어와 소프트웨어의 조직화된 체계’로서의 시스템 개념보다는 넓은 범위의 개념에 해당한다고 할 수 있습니다.

○ 한편, 「국가정보화 기본법」 및 시행령은 정보보호시스템의 성능과 신뢰도에 관한 기준 고시 및 정보보호시스템 평가·인증에 관한 사항을 규정하면서 ‘정보보호시스템’이라는 용어를 동일하게 사용하고 있으나, 정보보호시스템 정의와는 달리 ‘하드웨어와 소프트웨어의 조직화된 체계’라는 제한된 의미를 가집니다.

○ "사업자"라 함은 정보보호사업 계약(이하 "계약"이라 한다) 조건하에서 정보보호제품 또는 정보보호 관련 서비스(이하 "정보보호시스템 등"이라 한다)의 공급을 위해 발주자와 계약을 체결하는 자를 말합니다.
※「소프트웨어사업 관리감독에 관한 일반기준」의 “공급자”와 같은 의미

● **정보보호시스템**
정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 발생할 수 있는 정보의 훼손, 변조, 유출 등을 방지 및 복구하거나 또는 암호·인증·인식·감시 등의 보안기술을 활용하여 재난·재해·범죄 등에 대응하거나 관련 장비·시설을 안전하게 운영하기 위한 관리적 · 기술적 · 물리적 수단

● **정보보호사업**
정보보호기술 및 정보보호제품을 개발 · 생산 또는 유통하거나 정보보호 서비스를 제공하는 산업(정보보호산업)과 관련된 경제활동

▹ 사업 : 사업 추진 준비 단계부터 사업이행 및 관리단계까지 전 단계에 걸쳐 추진되는 대상을 의미한다.
▹ 프로젝트 : “사업” 중 사업자 선정 시점부터 인수 및 사업 종료까지 걸쳐 추진되는 대상을 의미한다. 즉, “사업”은 “프로젝트”를 포함하는 개념으로 사용한다.
※ 출처 : 소프트웨어사업 요구사항 분석 적용 가이드 (NIPA, ‘12.12)

관련근거

정보보호산업의 진흥에 관한 법률
제2조(정의) ① 이 법에서 사용하는 용어의 뜻은 다음과 같다.

1. **"정보보호"**란 다음 각 목의 활동을 위한 관리적·기술적·물리적 수단(이하 "정보보호시스템"이라 한다)을 마련하는 것을 말한다.
   가. 정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 발생할 수 있는 정보의 훼손, 변조, 유출 등을 방지 및 복구하는 것
   나. 암호·인증·인식·감시 등의 보안기술을 활용하여 재난·재해·범죄 등에 대응하거나 관련 장비·시설을 안전하게 운영하는 것
2. **"정보보호산업"**이란 정보보호를 위한 기술(이하 "정보보호기술"이라 한다) 및 정보보호기술이 적용된 제품(이하 **"정보보호제품"**이라 한다)을 개발·생산 또는 유통하거나 이에 관련한 서비스(이하 **"정보보호서비스"**라 한다)를 제공하는 산업을 말한다.
3. "정보보호기업"이란 정보보호산업과 관련된 경제활동(이하 **"정보보호사업"**이라 한다)을 영위하는 자를 말한다.

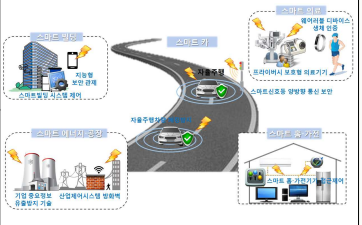
2. 정보보호의 범위

○ '정보보호'는 ① 사이버보안(네트워크·시스템 보안, 관제, 디지털 포렌식 등), ② 물리보안(영상감시, 바이오 인식, 무인전자경비 등), ③ 사이버 보안과 타 산업이 융합된 융합보안(제조, 에너지, 교통, 의료, 홈·가전 등에 대한 보안)으로 분류할 수 있습니다. 종래의 정보보호가 해킹, 바이러스 대응을 위한 사이버보안 중심이었다면 최근에는 전 산업이 ICT 기술과 연계·융합되면서 기존 사이버공간의 위험이 현실세계로 전이(轉移)되어 대부분의 제품에 보안이 필요한 시대가 도래함에 따라, 점차 물리보안과 융합보안으로 그 범위가 확장되고 있는 상황입니다.

○ ICT 기술의 발전에 따른 정보보호의 범위 확장을 반영하여 정보보호의 범위에 사이버보안 외에 물리보안을 포함하여 규정하고 있습니다. 즉, 사이버보안과 관련해서는 ① 정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 발생할 수 있는 정보의 훼손, 변조, 유출 등을 방지하는 것 및 ② 정보의 훼손, 변조, 유출 등이 발생한 경우 이를 복구하는 것을 규정하고 있으며, 물리보안과 관련해서는 암호·인증·인식·감시 등의 보안기술을 활용하여 ③ 재난·재해·범죄 등에 대응하거나 ④ 관련 장비·시설을 안전하게 운영하는 것을 규정하고 있습니다.

3. 정보보호 서비스의 특징

○ 정보보호 서비스에는 보안성 지속 서비스, 보안컨설팅, 보안관제, 교육훈련, 인증(공인/사설인증, CC평가인증)서비스 등이 포함되는데 다음과 같은 특징을 가지고 있습니다.

사이버 보안	물리보안	융합보안
		
네트워크·시스템 보안 관제·디지털 포렌식 등	영상감시, 바이오인식 무인전자경비 등	제조, 에너지, 교통, 의료, 홈·가전 등에 대한 보안

[그림 1-1] 정보보호/정보보호산업 분류

〈 정보보호서비스의 특징〉
- 정보시스템에 대한 해킹, 신규 악성코드 감염, 정보유출 등 내·외부 보안 위협에 대한 사후 대응 중심의 서비스
- 무장애, 성능 업그레이드 외에 보안 위협에 대비 대응하기 위한 수시적 업그레이드 등 보안 조치가 수반되는 서비스
- 무결성·기밀성·가용성이 담보되어야 하는 서비스
- 발전소, 항공관제 해킹 등 사회적 안전과 긴밀한 관련이 있는 서비스

※ 정보보호 서비스 대가 산정 가이드 (2015), KISA

4. 정보보호 솔루션의 특징

○ 정보보호 솔루션은 정보보호 제품, 그 제품의 기능 유지를 위한 일반적 유지관리, 외부 위협요인(공격)으로부터 보안성 유지를 위한 보안성 지속 서비스로 구성됩니다.

○ 정보보호 제품은 신규 취약점에 대응하기 위한 패턴/시그니쳐 등의 적시 업데이트가 필요하며, 해당 업데이트 패턴을 사용자 상황에 맞추어 유효한 정책으로 반영하는 과정도 지속적으로 요구됩니다.

○ 정보보호 제품은 국가정보화기본법 제38조(정보보호시스템에 관한 기준 고시 등)와 과학기술정보통신부 고시 정보보호시스템 평가·인증 지침, 전자정부법에 따라 국내용 CC인증 또는 암호화 모듈인증(KCMVP) 획득이 필수 조건으로 적용되고 있습니다.

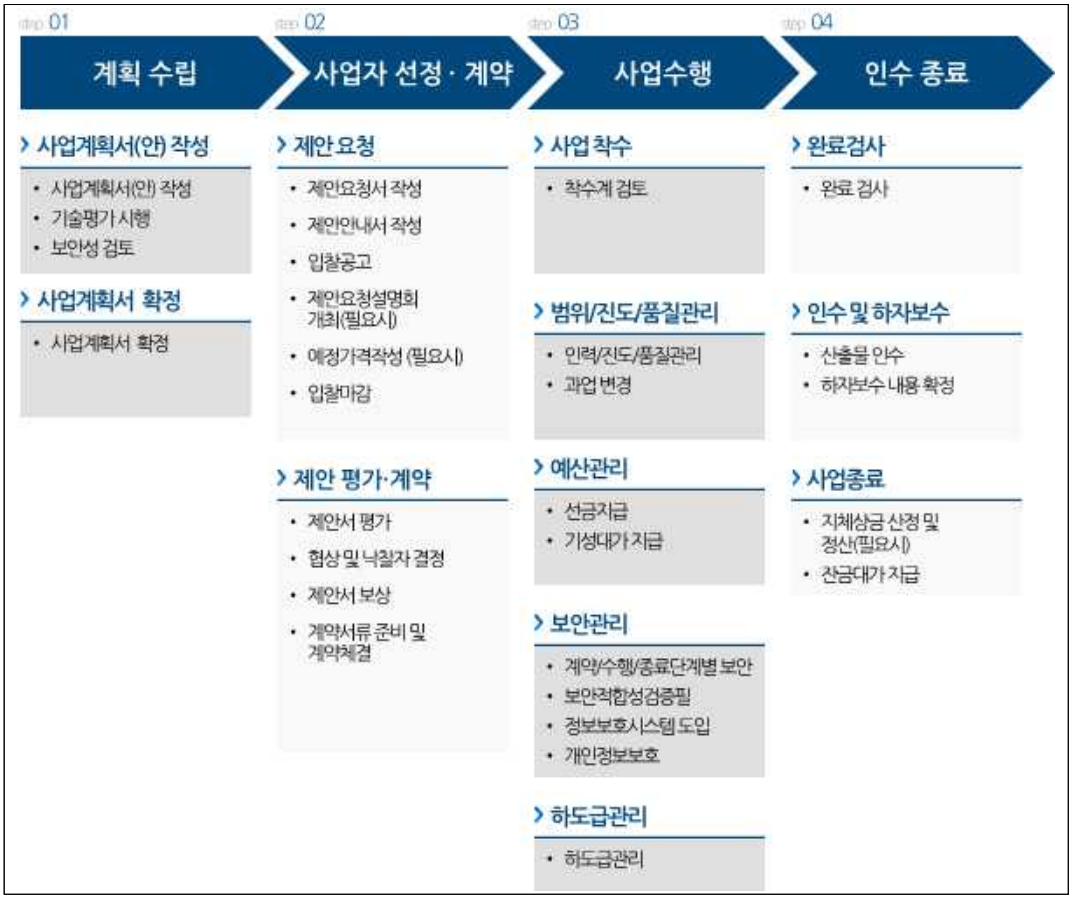
[표 1-1] 정보보호 제품의 특징

구 분	정의	비고
정보보호 제품	정보의 수집 · 가공 · 저장 · 검색 · 송신 · 수신 중에 정보의 훼손 · 변조 · 유출 등을 방지하기 위한 관리적 · 기술적 수단	보안성지속서비스 적용 제품은 형태에 따라 SW와 일체형(SW+HW)로 구분
유지관리	구매한 제품을 최적의 상태에서 활용 · 유지하기 위해 제공되는 활동	예) 제품지원, 기술지원, 사용자지원 등
보안성 지속 서비스	정보보호제품을 활용하여 정보의 훼손, 변조, 유출 등을 방지하기 위한 기술 기반의 서비스	예) 보안업데이트, 보안정책관리, 위협/사고분석, 보안성 인증효력 유지, 보안기술자문 등

제 2 절 정보보호사업 발주 단계

1. 정보보호사업 발주 프로세스

❍ 정보보호사업 발주 프로세스는 ①계획 수립, ②사업자 선정/계약, ③사업 수행, ④검사의 4단계로 나눌 수 있습니다. 이중 사업자 선정/계약 단계에는 제안요청서 작성과 사업자 선정을 위한 기술평가 등이 포함되어 있습니다.



[그림 1-2] 발주 프로세스

❍ 제안요청서의 기술제안 요구사항을 명확하고 상세하게 기재하기 위해서는 위의 발주 프로세스를 바탕으로 상세한 정보보호 요구사항과 관계 법령을 적용하여 제안요청서를 작성하고 본 요건을 충족하는 사업자 제안서를 기술 평가하여 선정, 계약 업무를 진행합니다.

- 발주 준비 과정에서는 사업계획서를 작성하고 이를 토대로 제안요청서를 작성하는 것이 일반적인 사업추진 절차입니다. 본 가이드에서는 제안요청서의 상세 정보보호 요구사항 도출을 위한 세부 절차와 방법을 설명하고 있으며 이 내용은 사업계획서에도 동일하게 적용될 수 있습니다.

  - 사업계획서는 사업의 추진 배경 및 필요성, 현황 및 문제점과 주요 사업내용, 일정 및 소요예산 등을 내부 품의용으로 작성하고 있으며 기관별로 자체적인 정보화사업 관리 지침을 정하여 수행하고 있습니다.

  - 정보보호사업 발주 프로세스의 4 단계 중 발주준비와 사업자 선정 · 계약의 2단계에 대해서는 정보보호사업 특성을 고려한 활동과 요령에 따라 수행하고 사업 수행 및 인수 종료는 일반 소프트웨어 사업의 착수단계부터 검사 단계까지 준용할 수 있습니다.

  - 정보보호사업 요구사항 분석 · 적용 프로세스는 발주 준비와 사업자 선정 · 계약 단계를 세부 절차로 구분한 것으로 일반 소프트웨어사업과 유사한 절차로 복합 사업의 경우에도 동일 절차를 적용할 수 있습니다.

[그림 1-3] 정보보호사업 요구사항 분석·적용 프로세스

2. 정보보호사업 발주 단계별 수행활동

❍ 정보보호사업의 범위 및 방향성을 수립하고 현황 분석 및 개선방향을 도출하여 제안요청서 작성과 사업자 선정·계약 단계를 체계적으로 수행할 수 있습니다.

[표 1-2] 정보보호사업 요구사항 분석·적용 단계별 수행활동

구분	수행 단계	수행활동	
계획 수립	1. 사업범위 및 방향성 수립단계	1.1 사업에 대한 개념 정의 및 시스템 구축 목적	
		1.2 관련 이해관계자 정의	
		1.3 사업추진 범위 및 방향성 수립	
	2. 사업 추진 준비단계	2.1 사업수행 내부 조직 구성	
		2.2 사업 추진체계 수립	
	3. 현황 분석 및 개선사항 도출단계	3.1 업무 현황 분석	업무체계 분석
			핵심 프로세스 분석
			법제도 현황 분석
		3.2 보유 기술 현황 분석	어플리케이션 분석
			데이터 분석
			기술구조 분석
			내·외부 연계분석
		3.3 사업 동향 분석	공공부문 유사사례 조사·분석
			민간부문 시장조사·분석
		3.4 위험 평가	
		3.5 시사점 및 개선사항 도출	
		3.6 사업추진 범위 및 방향성 검토/보완	
사업자 선정·계약	4. 제안요청서 요구사항 정의단계	4.1 정보보호 준거성, 위험관리 방안 도출	
		4.2 요구사항 분석 및 도출	공통 및 선택 요구사항
			정보보호 제품 사업 요구사항
			정보보호 서비스 사업 요구사항
		4.3 요구사항 상세내역 작성 및 검토	
	5. 사업 발주계획 수립 및 발주단계	5.1 사업 발주계획 수립	
		5.2 사업자 선정기준 및 절차 수립	
		5.3 제안요청서 작성 및 법제도 요건 반영여부 검토	
		5.4 입찰공고	
		5.5 제안서 평가 및 사업자 선정	
사업 수행	6. 사업이행 및 관리단계	6.1 사업수행계획서 검토 및 승인	
		6.2 요구사항 관리체계 수립	
		6.3 사업관리 및 인수전략 수립	
		6.4 요구사항별 충족여부 확인	
		6.5 인수 및 사업종료	

제 3 절 사업 계획 수립

1. 사업범위 및 방향성 수립단계

○ 사업범위 및 방향성 수립 단계에서는 구축하고자 하는 정보보호사업에 대한 개념을 명확히 하고, 관련 이해관계자들이 기대하고 있는 목표 시스템의 이미지를 고려하여 사업추진 범위와 구축 방향을 설정하는 단계입니다.

○ 정보보호사업은 정보보호 대상 자산, 업무 프로세스, 적용기술, 적용 법령, 조직에 따라 범위가 달라지며, 이에 따라 현황 분석 및 위험 평가, 요구사항 도출 업무에 영향을 받게 되므로 초기에 사업에 대한 명확한 방향과 구축 범위가 결정되어야 합니다.

가. 사업에 대한 개념 정의 및 시스템 구축 목적

○ 정보보호사업 전략 및 추진 방향성 검토

- 정보보호 정책, 지침 등에 따라 정보보호사업 추진 전략을 결정하며 기 운영 중인 정보시스템의 정보보호 강화 또는 신규 정보보호시스템 구축 등에 따라 사업 추진 방향을 설정합니다.

○ 사업 예산 확인 및 검토

- 사업계획 수립 시 해당 정보보호시스템 구축 사업에 할당되어 있는 예산금액을 확인하고, 목표 시스템 구축 및 정보보호 서비스 운영에 적정한지의 여부에 대한 검토를 수행합니다. 따라서 사전에 사업 예산을 확인하고, 차후 제안 요구사항들이 구체화될 경우 필요한 추가 예산을 확보할 수 있도록 사전에 예측하고, 예산 증액 방법과 절차를 알아두는 것이 필요합니다.

  ※ 기획재정부 예산편성 지침에는 정보화사업 추진 시 낙찰 차액을 정보시스템의 보안 강화 사업에 우선 활용할 수 있음

ㅇ 정보화사업의 낙찰차액은 원칙적으로 불용 처리한다.
- 다만, 정보시스템의 보안 강화, 감리비, 조달수수료를 지원하는데 사용할 수 있다. 이 경우 중앙관서의 장은 낙찰차액 사용내역을 기획재정부장관에게 통보하여야 한다.

ㅇ 국무회의 등 정책결정을 거쳐 수립된 중장기계획에 따라 추진 중인 계속 사업의 당해 연도 계획대비 예산 부족분을 지원하거나, SW사업 과업 확대에 따른 추가과업 수행을 위해 사용하고자 하는 경우 등 낙찰차액을 다른 용도로 사용하고자 하는 경우에는 기획재정부장관과 사전협의하여야 한다.
- 이 경우에도 낙찰차액을 활용하여 신규 사업을 추진할 수 없으나, 법령개정 등으로 인하여 불가피한 경우에는 그러하지 아니한다.

출처 : 예산 및 기금운용계획 집행지침, 기획재정부

나. 관련 이해관계자 정의

○ 시스템 주 사용자 및 관련 이해관계자 파악

- 사업은 수행조직 및 이해관계자들과의 공통된 목표와 추진방향을 공유하고 그 목표를 달성하고자 하는 의지를 확인하여야 합니다. 정보보호사업의 범위 및 목적을 토대로 사용자 및 관리자 그룹을 정의하고 연관된 조직 및 실무자를 선정합니다.
  ※ 개인정보보호 관련 사업의 경우 개인정보취급자를 포함한 현업 실무자 참여가 필수적임

○ 이해관계자별 상위개념의 요구사항 도출

- 사업 수행 내부 조직은 이해관계자를 대상으로 사업을 추진하기에 앞서 사업의 추진배경 및 필요성, 시스템 구축 목표 및 대략적인 정보보호 기능 등 사업계획을 기반으로 이들이 언제 참여해야 할지에 대한 정보를 공유합니다. 시스템 주 사용자 및 이해관계자 부서에서 해당 사업에 요구하거나 기대하는 보안 요구사항, 반드시 고려해야 할 요인, 사업의 방향성을 서로 협의하여 사업의 전체적인 방향과 범위를 구체화시켜 나가도록 합니다.
- 또한 상위관리자 중 정보보호 사업의 방향을 제시해 줄 수 있는 정보보호 임원이나 책임자, 이해관계자 들을 대상으로 인터뷰하여 정보보호 사업에 대한 업무 목표 및 방향을 파악합니다.

다. 사업추진 범위 및 방향성 수립

○ 사업추진 범위 및 방향성 수립

- 발주기관 실무자, 정보보호 실무자, 관련 과제별 담당자, 이해관계자 등 사업 수행 조직을 중심으로 사업의 추진방향과 주요 추진범위에 대하여 협의하고, 정보보호 사업을 통해 제공하고자 하는 정보보호 서비스의 범위를 결정합니다. 또한 정보보호 사업과 관련된 사용자 및 관리자 그룹을 명확하게 정의하고, 정보보호 정책 방향과 이해관계자의 기대사항을 고려하여 정보보호 사업을 통해 달성하고자 하는 목표 및 추진 방향을 정의합니다.
- 정보보호 사업은 사용자의 직접 요구사항 이외에도 정보보호 대상 자산을 설정하고 위험평가 또는 취약점 분석 등을 수행하고 발견된 취약점에 대한 대비책 마련이나 법적 정보보호 요구사항에 따라 사업의 추진범위가 결정될 수 있습니다.

2. 사업 추진 준비단계

○ 사업 추진 준비단계에서는 해당 사업의 요구사항 분석부터, 제안요청서 작성, 사업의 발주계획 업무를 담당할 내부조직을 구성하며, 사업에 대한 방향성을 수립하고, 추진력을 얻기 위해 주요 의사결정권자의 지원을 확보하도록 합니다.

○ 일반적으로 사업 추진 준비단계를 당연한 것으로 생각하고 과업 수행을 경시할 수 있으나, 추진하고자 하는 사업을 성공적으로 발주하기 위한 조직 구성과 역할 정의는 매우 중요합니다.

가. 사업수행 내부 조직구성

1) 내부 조직 구성 및 역할 정의

○ 본 사업의 제안요청서 작성 및 발주계획 업무에 참여할 실무자들과 관련된 조직 구성원들을 중심으로 사업 수행 내부조직을 구성하고, 주요 참여자들을 대상으로 수행 역할 및 책임범위를 정의합니다.
- 의사결정권자
- 사업총괄책임자
- 사업 담당부서(담당자)
- 관련부서
- 외부 전문가

○ 조직의 규모에 따라 정보화 담당부서에서 정보보호 직무를 총괄하여 수행할 수 있으나 정보보호 전담 부서를 설치하여 운영하는 조직에서는 정보보호 전담부서가 주도하여 사업 추진조직을 구성하고 있습니다.

2) 의사결정권자의 지원 확보

○ 의사결정권자는 정보보호 사업 지원 및 수행 방향 등에 대한 의사결정 권한을 가지게 됩니다. 일반적으로 의사결정권자는 조직의 비전 및 정보보호 정책과 전략을 이해하고 있고, 의사소통 능력이 뛰어나며 적극적이고 변화에 대해 긍정적인 자질이 필요합니다. 사업 수행에 실무자의 참여가 필요한 업무를 파악하고, 관련 부서로 부터 실무자의 참여를 확약 받도록 해야 합니다.

○ 정보보호사업의 경우에는 정보보호 정책 및 정보보호책임자(CISO, DPO)의 관리 하에 정보보호 전담조직을 구성하여 추진하도록 하여야 합니다.

나. 사업 추진체계 수립

1) 사업 일정 및 추진체계 수립

○ 사업을 성공적으로 수행하기 위해 필요한 사업 추진 업무와 계획을 수립하며, 사업 수행조직이 이에 따라 업무를 수행할 수 있도록 계획을 공유하도록 합니다.

2) 의사소통 및 보고체계 수립

○ 실무자들과 부서 간 발생하는 업무·기술 협의 및 의견 수렴, 관련된 정보를 전달하기 위해 중요한 업무 정보 전달 시점, 전달 수단 및 관련된 담당자를 명확하게 정의하며 의사소통 계획을 수립합니다.

3. 업무 및 기술 현황 분석 단계

○ 업무 및 기술 현황 분석단계에서는 정보보호 시스템과 관련된 업무 프로세스, 정보화 수준, 연계 시스템, 시스템 운용환경, 운영 현황, 전사 아키텍처 구조 등 정보시스템 전체 환경과 특성을 파악하고, 정보시스템과 관련된 기술 현황을 파악함으로써 보다 정확한 정보보호 요구사항 및 개선사항을 도출하기 위한 활동을 수행합니다.

○ 또한 구축하고자 하는 정보보호시스템을 운영하고 있는 유사사례를 조사하여 시스템이 제공하는 기능 및 문제점, 구축 시 유의사항 등을 파악하여 요구사항에 빠짐없이 반영하도록 합니다.

가. 업무 현황 분석

1) 업무체계 분석

○ 전사 조직구성과 업무 프로세스 등 전체 업무에 대한 현황을 이해하고, 목표 시스템에 영향을 받는 조직과 프로세스를 선별합니다. 이를 기반으로 정보보호 시스템의 구축으로 영향을 받는 서비스와 업무 프로세스를 파악하여 현재의 업무 처리의 문제점을 식별합니다.

2) 핵심 프로세스 분석

○ 정보보호시스템의 개선사항 및 요구사항을 도출하기 위해서는 정보보호 대상 업무 프로세스와 시스템에 대한 이해가 우선적으로 이루어져야 하며, 업무 프로세스를 수행하는 과정에서 발생되는 정보보호 이슈나 문제점은 사용자 인터뷰나 보안진단 등을 통해 도출해 낼 수 있습니다.

3) 법제도 현황 분석

○ 정보보호 대상 업무나 정보시스템에 적용해야 하는 정보보호 법적 조치 요구사항은 관계 법령 검토를 통하여 파악하여야 합니다.

[표 1-3] 정보보호 관련 주요 법령

부문	법령명
정보통신망 및 정보시스템의 안전한 이용	국가정보화 기본법, 정보통신기반 보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 전자정부법, 전자서명법, 국가사이버안전관리규정 등
침해행위의 처벌	정보통신기반 보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 전자무역 촉진에 관한 법률, 형법 등
국가기밀보호 및 중요 정보 국외유출 방지	군사기밀보호법, 보안업무규정, 군형법, 산업기술의 유출방지 및 보호에 관한 법률, 기술의 이전 및 사업화 촉진에 관한 법률, 민·군겸용기술사업 촉진법 등
정보보호 여건 구축	정보보호산업의 진흥에 관한 법률, 정보통신기반 보호법, 국가사이버안전관리규정 등
개인정보보호	개인정보 보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 신용정보의 이용 및 보호에 관한 법률 등

※ 출처 : 국가정보보호백서

나. 보유 기술 현황 분석

1) 어플리케이션 분석

○ 구축하고자 하는 정보보호시스템이 기 구축되어 있어 정보보호 기능을 강화하거나 개선하는 사업에 해당되는 경우 현재 구축되어 있는 정보시스템의 기능과 운영 현황을 정확하게 이해하는 것이 가장 중요합니다.

○ 정보시스템의 시스템 구성도와 취약점 분석 결과 등을 통해 현재 부족한 정보보호 기능을 도출합니다. 그리고 정보보호 대상 시스템 관련된 시스템 정보, DB 정보, 처리 프로세스 등의 내용과 현재 운영 중인 정보보호시스템 기능을 어떻게 활용하고 있는지, 부족한 정보보호 기능 개선 사항이나 추가 정보보호 기능 등에 대한 내용을 파악합니다.

2) 데이터 분석

○ 현재 저장된 데이터에 대하여 암호화 여부를 파악하고 데이터 항목별 암호화 수준 등의 요건을 확인합니다.

○ 특히, 개인정보 중 주민번호, 고유식별정보, 민감정보 등에 따른 안전조치 의무를 이행하고 있는지 확인하여 미 적용된 부분을 파악하여 개선조치 요구사항을 파악합니다.

관련근거

개인정보보호법

제23조(민감정보의 처리 제한)

② 개인정보처리자가 제1항 각 호에 따라 민감정보를 처리하는 경우에는 그 민감정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 제29조에 따른 안전성 확보에 필요한 조치를 하여야 한다.

제24조(고유식별정보의 처리 제한)

③ 개인정보처리자가 제1항 각 호에 따라 고유식별정보를 처리하는 경우에는 그 고유식별정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다.

제24조의2(주민등록번호 처리의 제한)

② 개인정보처리자는 제24조제3항에도 불구하고 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하여야 한다. 이 경우 암호화 적용 대상 및 대상별 적용 시기 등에 관하여 필요한 사항은 개인정보의 처리 규모와 유출 시 영향 등을 고려하여 대통령령으로 정한다.

제29조(안전조치의무)

개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

[표 1-5] 개인정보 항목별 암호화 적용기준 요약표 (사례)

<table>
<tr><th colspan="4">구분</th><th>암호화 기준</th></tr>
<tr><td>정보통신망,
보조저장매체를
통한 송신 시</td><td colspan="3">비밀번호, 바이오정보, 고유식별정보</td><td>암호화 송신</td></tr>
<tr><td rowspan="4">개인정보처리
시스템에
저장 시</td><td colspan="3">비밀번호</td><td>일방향(해쉬 함수) 암호화 저장</td></tr>
<tr><td colspan="3">바이오정보</td><td>암호화 저장</td></tr>
<tr><td rowspan="2">고유
식별
정보</td><td colspan="2">주민번호</td><td>암호화 저장
※ 2017.12.31.까지 암호화 저장:
100만 명 이상 정보주체</td></tr>
<tr><td>여권번호,
외국인등
록번호,
운전면허</td><td>인터넷 구간,
인터넷 구간과 내
부망의 중간 지점
(DMZ)</td><td>암호화 저장</td></tr>
</table>

구분				암호화 기준
		번호	내부망에 저장	암호화 저장 또는 다음 항목에 따라 암호화 적용여부·적용범위를 정하여 시행 ① 개인정보 영향평가 대상이 되는 공공기관의 경우, 그 개인정보 영향평가의 결과 ② 암호화 미적용 시 위험도 분석에 따른 결과
업무용 컴퓨터, 모바일 기기에 저장 시	비밀번호, 바이오정보, 고유식별정보			암호화 저장 ※ 비밀번호는 일방향 암호화 저장

※ 출처 : 개인정보의 암호화 조치 안내서 (2017.1), KISA

○ 실 데이터를 테스트용 데이터로 활용하거나 빅데이터 분석 기초자료로 이용하기 위해서는 비식별화 조치가 필요하며 비식별화 기법 적용방안을 검토하여야 합니다.

3) 기술구조 분석

○ 목표 시스템 구성을 위해서는 필요한 정보보호 장비를 추가적으로 구매하거나 기존의 사용 장비를 활용하기 위해 현재 전사 또는 기 구축된 정보보호시스템의 시스템 운용환경 구성현황을 파악해야 합니다. 현재 구성되어 있는 정보보호 하드웨어, 소프트웨어, N/W, OS 등의 현황을 파악합니다.

○ 정보보호 기능 및 성능 요구사항, 기술 요구사항 등은 전사 아키텍처 관점에서 기술표준 부합여부를 파악하여야 합니다. 우선 정보보호시스템 하드웨어, 소프트웨어, 지원 도구의 관점에서 시스템의 기반 구조를 파악한다. 또한 전사 정보보호 아키텍처 현황을 기준으로 기술표준 현황을 분석합니다.

4) 내·외부 연계분석

○ 최근 구축되는 정보시스템은 단독적으로 업무를 처리하기 보다는 각 시스템들 간의 수많은 데이터와 기능들이 서로 연계되어 있다는 것이 특징입니다. 따라서 정보보호 대상 시스템과 연계되는 업무와 시스템을 파악하고, 어떤 기능과 데이터들이 연계되어야 하는지에 대한 분석이 필요합니다.

○ 현재 연계되어 있는 업무, 시스템 기능, 데이터 등을 분석하고, 향후 사업 추진 시 추가적으로 연계가 필요한 부분에 대한 정보보호 요구사항을 도출합니다. 서로 연계된 시스템 간 기술 현황(개발언어, 플랫폼, 보안문제 등)을 파악하여 송수신 과정에서 적용해야 할 정보보호 요구사항에 대하여 사전 검토가 필요합니다.

다. 사업 동향 분석

1) 공공부문 유사사례 조사·분석

○ 공공 부문에서는 정보보호시스템 구축에 대하여 법령 개정에 맞춰 유사한 시기에 발주되는 경향이 있고 적용되는 법규도 동일한 경우에 타 기관의 발주 및 구축 사례를 조사하고 기관별 고유 업무나 시스템과 관계없이 공통적으로 적용해야 하는 요구사항을 파악하여 활용할 수 있습니다.

○ 유사사례 조사 수행 시 조사항목에 집중하여 직접 방문하거나 자료 분석을 통해 타 기관의 정보보호시스템 활용 및 제공 기능, 구축 시 유의사항, 실패요소 등을 조사합니다.

2) 민간부문 시장조사·분석

○ 민간 부분에서는 특정 정보보호 제품이나 서비스 발주 시 법적 요건보다는 해당 기업의 취약점에 대비하여 정보보호 제품이나 서비스를 구축하고 있어 이에 대한 기술적인 요건을 파악하여 참조할 수 있습니다.

○ 시장 내 존재하는 상용 제품의 경우 성능이나 기 도입하여 운영하고 있는 기관들의 사례를 찾아 구체적인 적용 사례와 만족도 수준 등을 조사합니다.

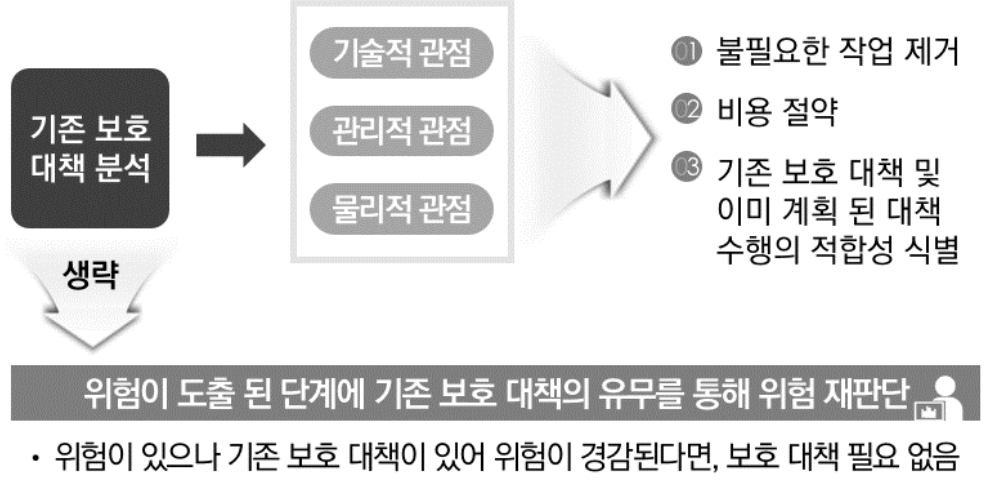
라. 위험평가

○ 정보보호 대책을 선택하는 방법으로 위험평가 절차를 적용할 수 있습니다. 정보자산을 식별하고 유사한 자산을 그룹핑하여 위험을 평가하고 수용 가능한 위험 수준을 결정하여 정보보호 대책을 선택합니다.

○ 기존 정보보호대책에 대하여 관리적, 기술적, 물리적 관점에서 현황을 조사하고 불필요한 대책의 제거와 비용 절약, 기존 대책의 적합성을 평가하여 추가 대비책이 필요한지 판단합니다.

마. 시사점 및 개선사항 도출

○ 조직 및 업무 프로세스 현황 분석 결과, 기술 및 정보보호 대상 시스템 현황 분석 결과, 유지관리 현황 분석 결과와 유사사례 조사결과를 바탕으로 정보보호시스템 구축 사업을 위한 시사점과 개선사항을 도출하도록 합니다.



바. 사업추진 범위 및 방향성 검토/보완

1) 이해관계자 검토 및 보완

○ 사업 내부 조직에서 검토회의를 통해 정보시스템 주요 시사점 및 개선사항 도출결과를 반영하여 앞서 수립된 사업추진 범위 및 방향성을 수정합니다. 내부 업무현황 분석 및 내부 기술현황 분석 활동을 거치면서 수정된 범위 및 방향성에 대해서 이해관계자들과 검토하고 보완사항을 반영합니다.

2) 사업 추진범위 확정 및 의사결정권자 승인

○ 사업범위 및 방향성을 수립하고, 이해관계자들뿐 아니라 본 사업의 최고 의사결정권자가 사업의 추진목표와 상위 개념의 사업추진 범위에 대해 공식적으로 승인하는 절차가 필요합니다. 이러한 과정을 거치지 않을 경우 사업 진행과정에서 추진 범위에 대한 조정과 논란으로 인해 진행에 차질이 발생할 뿐만 아니라 사업 예산과 기간에도 직결되는 문제이기 때문에 사전에 충분한 이해 과정을 거치도록 합니다.

제2장
제안요청서 작성

제 2 장 제안요청서 작성

제 1 절 제안요청서 작성 개요

1. 제안요청서의 정의

○ 『제안요청서(Request For Proposal)』란? “행정기관 등의 장이 입찰에 참가하고자 하는 자에게 제안서의 제출을 요청하기 위하여 교부하는 서류”이며, 제안서 작성 및 평가, 업체선정의 기준이 됩니다.

○ 또한, 공공기관이 정보보호 사업을 발주할 때 세부적인 요구사항을 정하여 공개하여야 합니다.

관련근거

정보보호산업의 진흥에 관한 법률
제7조(공공기관 등의 정보보호시스템 구축 계약 등) ① 공공기관 등의 장은 정보보호시스템 구축을 위한 사업계약을 체결하는 경우 「국가를 당사자로 하는 계약에 관한 법률」 제10조제2항제3호 및 「지방자치단체를 당사자로 하는 계약에 관한 법률」 제13조제2항제4호에 따른 입찰자를 낙찰자로 하는 계약방식을 우선적으로 적용하여 계약을 체결하여야 한다. 다만, 계약을 체결하려는 정보보호시스템의 특성상 필요하다고 판단되는 경우에는 다른 방식으로 계약을 체결할 수 있다.
② 과학기술정보통신부장관은 제1항의 계약을 위하여 정보보호시스템의 요구사항을 분석·적용할 수 있는 기준과 정보보호시스템의 사업자 선정을 위한 기술평가 기준을 정할 수 있다.
③ 과학기술정보통신부장관은 공공기관 등의 장이 제1항에 따른 사업계약을 체결하거나 사업자 선정을 위한 기술평가를 실시하는 경우에는 제2항에 따른 기준을 적용하도록 권장할 수 있다.
④ 제1항부터 제3항까지의 규정에 따른 계약 체결의 세부 절차와 기준은 과학기술정보통신부장관이 정하여 고시한다.

2. 제안요청서 기재사항

○ 제안요청서에는 과업내용, 요구사항, 계약조건, 평가요소와 평가방법, 제안서의 규격, 기타 필요한 사항 등을 기술하여야 합니다.

[표 2-1] 제안요청서 기재사항

▫ 과업내용 및 요구사항
▫ 계약조건
▫ 평가요소, 평가방법
▫ 제안서 규격 · 제출방법 · 제본형태

- □ 제안서 보상에 관한 사항
- □ 사업자가 준수해야 하는 사항
  - 하도급 대금지급 등
  - 과학기술정보통신부장관이 고시한 " 정보보호시스템 구축 사업의 하도급 승인 및 관리 지침"에 따른 하도급 계약 승인 절차 및 하도급 계약 적정성 판단기준
  - 기술적용계획표
  - "소프트웨어 개발보안" 적용
  - 사업관리자의 제안서 발표 의무화
  - 표준산출물 작성 및 제출
- □ 그밖에 필요한 사항

관련근거

행정기관 및 공공기관 정보시스템 구축·운영지침 (행정안전부 고시)
제16조(제안요청서 작성) ① 행정기관 등의 장은 사업자를 선정하기 위하여 제안요청서를 작성하여야 한다.
② 제안요청서에는 다음 각 호의 사항을 명시하여야 한다.
1. 과업내용, 요구사항
2. 계약조건
3. 평가요소, 평가방법
4. 제안서의 규격 · 제출방법 · 제본형태
5. 제안서 보상에 관한 사항
6. 사업자가 준수해야 하는 다음 각 목에 관한 사항
   가. 제19조에 따른 하도급 대금지급 등
   나. 과학기술정보통신부장관이 고시한 “소프트웨어사업 하도급계약의 적정성 판단기준”에 따른 하도급 계약 승인 절차 및 하도급 계약 적정성 판단기준
   다. 제7조제1항에 따른 기술적용계획표
   라. 제50조 내지 제53조에 따른 “소프트웨어 개발보안” 적용
   마. 제20조에 따른 사업관리자의 제안서 발표 의무화
   바. 제45조에 따른 표준산출물 작성 및 제출
7. 과학기술정보통신부장관이 고시한 "소프트웨어사업 관리감독에 관한 일반기준" 제6조에 따른 적정 사업기간 산정에 관한 사항
8. 그 밖에 필요한 사항

협상에 의한 계약체결기준 (기획재정부 예규)
제5조(제안요청서의 교부 또는 열람 등) ① 계약담당공무원은 입찰에 참가하고자 하는 자에게 제안요청서를 교부하여야 한다.
② 계약담당공무원은 제안요청서 등 필요한 서류를 시행령 제14조 제3항의 규정에 의한 지정정보처리장치에 게재함으로써 제1항에 따른 제안요청서 등 필요한 서류의 교부에 갈음할 수 있다.
③ 계약담당공무원은 사업내용이 비교적 단순하여 제1항 및 제2항의 규정에 의한 제안요청서의 교부 또는 열람이 불필요하다고 인정되는 경우에는 제안요청서의 교부 또는 열람을 생략하고, 바로 제안서를 제출하게 할 수 있다. 이 경우 입찰공고에 사업내용 등 제안서 작성에 필요한 사항을 명시 하여야 한다.
④ 계약담당공무원은 계약의 성질·규모 등을 고려하여 필요하다고 인정하는 경우에는 제안요청서 등에 대한 설명을 할 수 있으며, 설명을 실시하는 경우에는 설명에 참가한 자에 한하여 계약에 참가하게 할 수 있다.
⑤ 제안요청서에는 다음 각 호의 사항을 명시하여야 한다.

1. 과업내용
2. 요구사항
3. 계약조건
4. 평가요소와 평가방법
5. 제안서의 규격

3. 제안요청서의 표준 목차

○ 제안요청서의 표준 목차는 6개의 장으로 구성되어 있으며, 사업유형별로 목차를 조정하여 작성할 수 있습니다.

[표 2-2] 정보보호사업 제안요청서 표준 목차

목 차	
1. 사업 개요	**5. 제안서 작성요령**
가. 추진배경 및 필요성	가. 제안서의 효력
나. 서비스 내용	나. 제안서 작성지침 및 유의사항
다. 사업 범위	다. 제안서 목차
라. 기대효과 및 성과지표	**6. 안내 사항**
2. 업무 및 시스템 현황	가. 입찰방식
가. 업무 현황	나. 제안서 평가방법
나. 정보시스템 현황	다. 기술성 평가기준
3. 사업 추진방안	라. 제출서류
가. 추진목표	마. 제안서 제출 일정 및 방법
나. 추진전략	바. 제안요청 설명회
다. 추진체계	사. 제안설명회 개최
라. 추진일정	아. 입찰시 유의사항
마. 추진방안	
4. 제안요청내용	[붙임 서식]
가. 제안요청 개요	[붙임1] 일반현황 및 연혁
나. 용어 정의	[붙임2] 자본금 및 매출액
다. 목표시스템 개념도	[붙임3] 참여인력 현황
라. 상세 요구사항	[붙임4] 기술적용계획표
1) 정보보호제품 요구사항	[붙임5] 하도급 대금지급비율 명세서
2) 정보보호 서비스 요구사항	[붙임6] 하도급 계약승인신청서
3) 공통/선택 요구사항	[별지1] 사업수행업체 보안 준수사항
	[별지2] 사업자 보안 위규 처리기준
	[별지3] 보안 위약금 부과 기준

4. 제안요청서 작성 요청

가. 정보보호사업 관련 법제도 원칙 준수

○ 제안요청서는 과학기술정보통신부·기획재정부·행정안전부 소관 법령, 고시, 계약예규 등의 관련 법규에서 정한 내용을 준수하여 작성하여야 합니다.

[표 2-3] 정보보호사업 관계 법령

관계 법령	준수 사항
• 국가(지방)를 당사자로 하는 계약에 관한 법률 관련 계약예규 등	입찰, 계약, 사업수행 과정의 준수사항 규정
• 전자정부법 • 행정기관 및 공공기관 정보시스템 구축·운영지침 • 전자정부지원사업 관리요령 등	사업추진과정의 준수사항 규정
• 정보보호산업의 진흥에 관한 법률 • 정보보호시스템 구축 사업의 하도급 승인 및 관리 지침 • 국가 사이버 안전관리 규정 • 정보보호시스템 공통평가기준 • 정보보호시스템 평가·인증 지침 • 정보보호 전문서비스 기업 지정 등에 관한 고시 • 보안관제 전문기업 지정 등에 관한 공고 • 정보보호 관리체계 인증 등에 관한 고시 • 정보보호 사전점검에 관한 고시 • 클라우드컴퓨팅서비스 정보보호에 관한 기준 • 집적정보 통신시설 보호지침 • 정보보호조치에 관한 지침 • 개인정보 영향평가에 관한 고시 • 개인정보의 기술적.관리적 보호조치 기준 • 개인정보의 안전성 확보조치 기준 • 주요정보통신기반시설 취약점 분석·평가기준 • SW사업 대가산정 가이드	정보보호 사업 관련 준수사항 규정

나. 세부적인 요구사항을 상세히 기술

○ 정보보호사업 요구사항별 필요한 기술수준에 대한 명확한 분석을 통하여 상세하게 기술하여야 합니다.

● 제안요청서는 발주기관의 명확한 요구사항이 기재되어야 하며, 요구사항을 명확하게 정의하기 위해서는
① 요구하는 사항에 대해 시스템 구축 후, 그 결과가 확실할 것
② 현재의 기술수준으로 실현 가능할 것
③ 검사 등으로 기술적인 검증이 가능할 것
④ 의미가 불명확한 용어나 표현은 사용하지 않을 것
⑤ 특정 제품이나 스펙을 명시하지 않을 것

다. 제안서 작성에 필요한 모든 정보를 상세히 제공

○ 정보보호사업 수행에 필요한 모든 정보를 제공함으로써 제안사가 제안서를 작성하는데 도움을 줄 수 있도록 합니다.

○ 그러나 정보시스템의 보안이나 안정성에 직접적인 관련이 있는 사항은 제공하지 않도록 하고, 제안에 필요한 정보는 연락처만을 기재하고 방문하여 열람하는 것으로 대체할 필요가 있습니다.

라. 애매모호한 요구사항을 배제하여 기술

○ 애매모호한 문구나 현실적이지 않은 과도한 요구조건이 기재되어 있는 경우 향후 제안업체와의 분쟁이 우려되므로, 과업이행여부가 검증될 수 있도록 기술하여야 합니다.

마. 개방적인 표준에 근거한 요구조건의 기재

○ 기술적 요구조건의 내용이 중립적인지 여부를 확인하여 특정 하드웨어, 소프트웨어 기술을 명시하거나, 특정 사업자만 참여가 가능한 제안요청서 작성은 지양하여야 합니다.

○ 다만, 소프트웨어 분리발주에 따른 상호호환성 확보 등을 위하여 특정 제품명을 기재할 필요가 있는 등 합리적인 이유가 있는 경우 제안요청서에 그 사유를 명시하여야 합니다.

● 개방적 표준이란?
① 오픈된 참가 프로세스 하에서 합의되고, 구체적 사양이 실현 가능한 레벨에서 공개되고 있는 것
② 누구나 채택 가능한 것
③ 기술표준이 실현된 제품이 시장에 다수 있는 것이라는 모든 조건을 충족하고 있는 기술표준을 의미

제 2 절 사전 준비

1. 사업 유형 정의

가. 사업 유형

○ 본 가이드에서는 기 발주된 공공부문 정보보호사업의 현황을 분석하여 [부록1] 사업유형 분류표의 7개 유형으로 정의하였습니다. 그러나 다수의 사업유형이 하나의 사업에 포함되어 있거나, 하나의 사업이라도 다양한 기술, 사업내용이 포함될 수 있습니다.

○ 따라서, 사업유형을 명확하게 정의하고 분류하는 것은 입찰참가자격 및 적용 법제도 등을 결정하는 요인일 뿐만 아니라 정보보호 사업의 통계 및 제안요청 내용의 명확화, 상세화를 위해서도 중요한 의미가 있습니다.

○ 본 가이드에서 제공하는 사업유형별 제안요청서 표준 템플릿을 활용하기 위해서는 먼저 발주하고자 하는 정보보호 사업의 유형을 결정하여야 합니다.

나. 사업 유형 분류

○ 발주 예정사업이 정보보호 제품 사업 인지 정보보호 서비스 사업인지를 고려하여 사업유형을 결정합니다.

○ 정보보호 사업은 [표 2-4] 정보보호 사업 유형 분류표의 사업유형 Level 3에서 해당되는 세부 사업유형을 선택합니다.

○ 복수의 사업유형을 포함하는 경우 사업비가 크거나 더 많은 사업범위 비중을 차지하는 사업을 중심으로 사업유형을 선택합니다.

○ 비중이 큰 사업유형에 해당되는 제안요청서 표준 템플릿을 선택하고 이를 기준으로 제안요청서를 작성하면서 다른 유형의 사업에 해당되는 제안요청서 표준 템플릿의 요구사항을 활용하거나 별도로 제공된 [부록2] 요구사항 표준 패키지 및 [부록3] 사업유형별 요구사항 매핑표 등을 활용하여 작성합니다.

> 정보보호 제품 구입과 관제 상황실을 구축하며 내부 관제 절차와 체크리스트 등을 작성하여 사이버안전센터를 구축하는 사업의 경우에는 정보보호 사업 유형 중 “정보보호시스템 개발사업”으로 분류함

[표 2-4] 정보보호 사업 유형 분류표

Level 1	Level 2	Level 3	세부항목 (예시)
정보보호제품	보안관리	• 접근통제 • 암호/인증관리 • 데이터·콘텐츠 보안 • 네트워크 보안 • 모바일 보안 • 바이오 인식 • 보안운영	· 통합보안시스템(UTM) · 통합보안관리(ESM) · 시스템접근통제(PC방화벽 포함) · DB보안 · 접근통제시스템 · 웹 방화벽 · 네트워크(시스템) 방화벽 · 네트워크접근제어(NAC) · 통합접근관리(EAM) · 통합계정관리(IM/IAM) · 디지털 포렌식(부분, 기능) · 보안운영체제(Secure OS) · 서버보안 제품 및 시스템 · 가상사설망 시스템(VPN) · 모바일 보안 제품(MDM, MAM 등) · 자산관리시스템(RMS) · 유·무선 네트워크 보안 제품 · 싱글사인온(SSO) · 보안스마트카드 · H/W토큰(HSM) · 일회용비밀번호(OTP) · 모바일인증(m-OTP, QR) · 공개키기반구조(PKI) · DB암호 · 보안 USB · 얼굴인식시스템 · 홍채인식시스템 · 지문인식시스템 · 음성인식시스템 및 기타(수기서명) · 디지털저작권관리(DRM) · 네트워크 DLP, 단말 DLP · 가상화 망분리 · 카드&리더(번호/마그네틱) · 시큐리티게이트 및 S/W · 패치관리시스템(PMS)
	침입탐지	• 침입탐지·방지 • 모니터링	· 침입탐지·방지시스템(IDS, IPS) · DDoS 차단 시스템 · 로그 관리/분석 시스템 · 위협관리시스템(TMS) · APT 대응 시스템 · 스팸 차단 제품(HW, SW) · Anti 멀웨어(바이러스, 웜, 스파이웨어 등) · 알람/모니터링(적외선/레이저/진동/장력 센서, 모션디텍터/침입 탐지장비)
	분석·대응 및 복구	• 침해 관리 • 복구 및 백업	· 취약점 분석 시스템 · 백업/복구 관리시스템 · 디지털 포렌식 시스템(통합)
	물리보안 및 기타	• 물리보안제품 • 기타제품	· CCTV 시스템(저장장치, 카메라, 지능형/관제 Solution,주변장비) · 영상보안(DVR, 카메라, IP영상장치 등) · ICT 신기술(Iot, 클라우드, 블록체인 등) 적용 제품 및 엔진/칩셋 · 기타장비 및 주변장치
정보보호서비스	정보보안 컨설팅	• 취약점 분석 평가	주요기반시설 및 전자금융 관련 취약점 분석·평가, 진단 및 모의해킹
		• 정보보호 관리체계	정보보호 관리체계(ISMS, ISO/IEC 27001) 인증
		• 개인정보보호	개인정보보호(PIMS, PIA) 등 인증체계컨설팅
		• 기본·종합컨설팅	기본·종합 보안 컨설팅(보안기술 자문, 교육 및 훈련 등) 및 보안 감사
		• 개발보안 컨설팅	시스템 개발 보안 컨설팅(보안결함 제거, 단계별 보안기능 구현 등)
	보안성 지속 서비스	• 유지 관리	유지·보수 서비스(보안업데이트, 기술지원 등), 보안정책관리
		• 사고 분석	위험·사고분석
		• 인증 및 자문	보안성 인증효력유지(CC, KCMVP 등), 보안기술자문
	보안관제	• 기본 서비스	원격관제, 파견관제, 하이브리드관제(원격+파견) 서비스 등
		• 부가 서비스	보안관제 부가서비스(기획, 진단, 분석, 운영, 개별 서비스)
		• 훈련 서비스	모의훈련 서비스(침해사고, DDoS, 악성메일(파일) 유입/전파 대응 등)
	SI 서비스	• 시스템기획·개발	보안 솔루션 통합 및 신규 구축, 융합보안시스템 설계 및 구축 정보보호 인프라 개발·구축
			개발보안(시큐어코딩), 시스템 설계·운영·기술이전 등 ※ 정보보호시스템(레거시시스템) 추가개발 및 고도화
	물리보안 및 기타	• 물리 보안	영상보안 서비스, 출동보안서비스
		• 교육·훈련	정보보안 및 개인정보보호 등 관련 교육 서비스
		• 기타 보안	신규 서비스(Iot, 클라우드관련 등), 기타보안 서비스

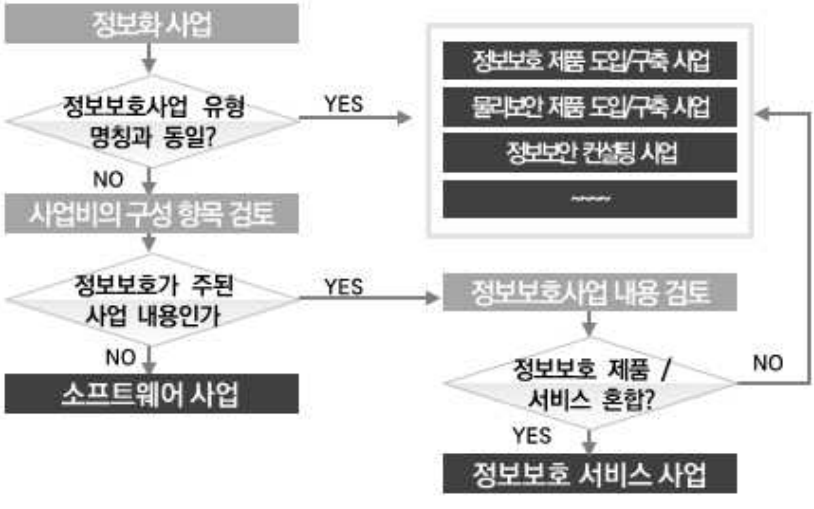
다. 정보보호사업 유형의 선택

○ 정보보호 제품 도입, 정보보호 서비스 구축 등 정보보호 사업의 특성을 고려하여 정보보호 사업 유형을 선정합니다.

- 정보보호 관련 사업 내용이 포함된 정보화 사업으로 주된 사업내용이 정보보호 제품 도입이나 정보보호 서비스 구축 사업의 특정 사업 유형과 매핑되는 경우에는 해당 정보보호사업 유형으로 선택합니다.
- 정보보호 제품과 정보보호 서비스 구축이 혼재된 경우에는 정보보호 서비스 구축사업 유형을 선택합니다.

○ 정보보호시스템 구축 이외에 일반적인 소프트웨어 개발 또는 DB 구축 등이 포함된 경우에는 세부 과제별 비중을 검토하여 사업유형을 결정합니다.

- 사업비의 규모에 관계없이 정보시스템 개발에 수반되는 정보보호 제품 도입이나 정보보호 기능 구현은 소프트웨어 구축사업으로 분류하고 해당 제안서 템플릿과 요구사항 유형을 적용합니다. 여기에 정보보호 관련 제품과 보안 기능 요구사항을 추가하는 방식으로 작성합니다.
- 정보보호시스템 구축에 필요한 DB 전환이나 보조적 기능 구현을 위한 솔루션 도입(예, 리포트 솔루션, 전자문서 솔루션 등) 등이 포함된 사업은 정보보호시스템 개발 사업 유형을 적용합니다. 여기에 소프트웨어 개발이나 일반 상용소프트웨어 도입 요구사항을 추가하는 방식으로 작성합니다.



[그림 2-1] 정보보호사업 유형 선택 절차

2. 제안요청서 표준 템플릿 선택

가. 제안요청서 표준 템플릿

○ 사업유형은 정보보호산업진흥법에 의한 제안요청서 요구사항 분석 적용여부 및 구축 내용, 형식적 요건에 따라 2가지 유형으로 구분할 수 있습니다.

[표 2-5] 제안요청서 표준 템플릿

구분	해당 사업유형	비고
유형 I	정보보호 제품 도입 · 구축 사업 물리보안 제품 도입 · 설치 사업	
유형 II	정보보안 컨설팅 사업 보안성지속서비스 사업 보안관제 사업 물리보안 서비스 사업	
	정보보호시스템 개발 사업	소프트웨어사업 제안요청서 템플릿 참조

나. 제안요청서 표준 템플릿의 선택

○ 발주예정 사업의 사업내용을 분석하여 사업유형이 결정되면, 본 가이드의 별첨으로 별도 제공된 [부록5] 사업유형별 제안요청서 표준 템플릿 중에서 해당 사업유형의 제안요청서 표준 템플릿을 선택합니다.

○ 비중이 큰 사업유형에 해당되는 제안요청서 표준 템플릿을 선택하고 이를 기준으로 제안요청서를 작성하면서 다른 유형의 사업에 해당되는 제안요청서 표준 템플릿의 요구사항을 활용할 수 있습니다.

3. 정보보호사업 유형별 요구사항 정의

가. 정보보호사업 유형별 요구사항 패키지 선택 및 요구사항 정의

○ 정보보호사업 유형별로 기본적으로 과업에 포함해야 할 상세 요구사항에 대하여 “사업유형별 요구사항 매핑표”를 활용하여 요구사항 목록을 추출합니다.

- 정보보호 제품, 정보보호 서비스 사업 유형별로 제품 선택요구사항과 서비스 선택 요구사항을 매핑하여 필수 요구사항을 선택하고 사업 내용에 따라 선택 요구사항을 선정합니다.

- 일반적인 공공 정보화사업으로서 프로젝트 기밀성 요구사항과 함께 프로젝트관리, 프로젝트지원, 제약사항, 품질요구사항을 적용합니다.

- 또한, 사업 유형에 따라 자산관리 기능 요구사항, 제품컨설팅 요구사항과 함께 일반 소프트웨어 사업에서 적용하고 있는 성능 요구사항, 테스트 요구사항, 데이터 요구사항, 인터페이스 요구사항을 선별적으로 선택합니다.

[표 2-6] 정보보호 제품과 서비스 선택 요구사항 매핑표

요구사항 유형			정보보호제품		정보보호서비스				
			정보보호제품 도입 및구축	물리보안제품 도입 및구축	보안 컨설팅	보안성 지속서비스	보안 관제	정보보호 시스템 개발	물리보안 서비스
제품 선택 요구사항	시스템 장비 구성	보안관리 장비구성	●						
		침입탐지 장비구성	●						
		대응 및 복구 장비구성	●						
		기타 장비 구성		●					
	보안 기능	보안관리 기능	●						
		침입탐지 기능	●						
		침해관리 기능	●						
		기타 기능 구성		●					
서비스 선택 요구사항	정보 보안 컨설팅	보안컨설팅 공통 일반			●	○	○	○	○
		정보보호관리체계 인증			●				
		개인정보보호관리체계 구축			●				
		개인정보영향평가			●				
		정보보호 마스터 플랜 수립			●				
		교육체계 및 콘텐츠 개발			●				
		모의해킹			●				
		보안취약점 진단			●				
	보안성 지속 서비스				○	●	○	○	○
	보안 관제	원격 파견관제 서비스			○	○	●	○	○
		보안관제 부가서비스			○	○	●	○	○
	SI 서비스 사업 요구사항				○	○	○	●	○
	물리보안 및 기타 정보보호서비스				○	○	○	○	●

[표 2-7] 공통/선택 요구사항 매핑표

요구사항 유형		정보보호제품		정보보호서비스				
		정보보호제품 도입 및구축	물리보안제품 도입 및구축	보안 컨설팅	보안성 지속서비스	보안 관제	정보보호 시스템 개발	물리보안 서비스
공통 요구사항	프로젝트 기밀성 유지 요구사항	●	●	●	●	●	●	●
	프로젝트 관리	●	●	●	●	●	●	●
	프로젝트 지원	●	●	●	●	●	●	●
	제약사항	●	●	●	●	●	●	●
	품질 요구사항	●	●	●	●	●	●	●
선택 요구사항	자산관리 기능 요구사항	●	●				●	○
	성능 요구사항	●	○				●	○
	테스트 요구사항	●	○				●	○
	데이터 요구사항	●	○				●	○
	인터페이스 요구사항	●	○				●	○
	제품 컨설팅 요구사항	●	●				●	○

○ 각 요구사항별 상세 요구사항은 “정보보호 요구사항 표준 패키지”를 참조하여 본 사업의 대상 시스템이나 업무 환경 등을 고려하여 상세 요구사항을 작성합니다.

[표] 2-8 정보보호 요구사항 패키지 목록 (예시)

Level 1		Level 2		Level 3		상세 요구 기능	
code	요구기능명	code	요구기능명	code	요구기능명	code	요구기능 명
ECR	시스템 장비 구성 요구기능	P/M	보안관리 (Protection& Management) 장비구성	PAM	암호/인증기관리	01	싱글사이온(SSO)
						02	보안스마트카드
						03	H/W토큰(HSM)
						04	일회용비밀번호(OTP)
						05	DB암호
				DCS	데이터·콘텐츠보안	01	데이터 콘텐츠 보안
				NWS	네트워크 보안	01	가상사설망 시스템
						02	유·무선 네트워크 보안 제품
						03	네트워크 DLP, 단말 DLP
						04	가상화 망분리
				MOS	모바일 보안	01	모바일 보안 제품(MDM, MAM 등)
						02	모바일 인증 (m-OTP, QR)
				BIO	바이오인식	01	얼굴인식시스템
						02	지문인식시스템
				SSM	보안운영	01	DB보안
						02	통합계정관리(IM/IAM)
						03	보안운영체제(Secure OS)
						04	서버보안 제품 및 시스템
						05	보안USB
						06	패치관리시스템(PMS)
						07	통합로그관리시스템

○ 정보보호 관련 법령, 규정의 적용여부와 정보보호 대상에 대한 위험평가 결과를 활용하여 정보보호사업의 특성을 고려한 정보보호 상세 요구사항을 추가 도출하여 반영합니다.

○ 제안요청서에 작성하는 정보보호 요구사항은 사업계획 수립 단계에서 파악된 시사점 및 개선사항, 사업범위 및 방향성을 토대로 공통 요구사항, 정보보호 제품 요구사항, 정보보호 서비스 요구사항 등 정보보호 요구사항 분류기준 항목 각각에 대해서 상세하게 정의합니다.

○ 정보보호 사업은 정보보호 대상 자산과 위험평가에 따라 구축 방향성이나 기능이 달라질 수 있고, 예상 취약점을 모두 대응할 수 있는 구체적인 목표 시스템(To-be System)을 정의하기 어렵기 때문에 요구사항을 명확하게 도출하는 것이 핵심 요소입니다. 정보보호 대상 시스템이나 정보들이 지속적으로 운영 및 유지 관리되고, 기술적 환경의 변화로 인한 새로운 취약점에 노출될 수 있어 구축 이후 운영 및 기술지원 요구사항 또한 상세하게 정의되어야 합니다.

[표 2-9] 정보보호 상세 요구사항 작성표 (예시)

요구사항 고유번호	ECR-PAM-04
요구사항 명칭	일회용비밀번호(OTP)

요구사항 세부내용	◦ *도입 품목 : OPT S/W 및 HW* ◦ *수량 : 3식(업무망 이중화, 모바일망 단일장비 기준)* ◦ *기본규격* - *Good Software 인증(사업 검수 완료 전 인증 획득 제품에 한함)* - *국가정보원 CC 인증 또는 검증필 암호화 알고리즘 적용* - *시간동기 방식(질의/응답, 이벤트 방식 불가)* - *다양한 인증매체(Mobile, SMS, E-mail, PC, Web 등) 지원* ◦ *요구기능* - *Android 및 iOS 지원* - *OTP 인증매체 발급/등록에 대한 보안성 제시*
산출정보	
관련요구사항	

※ 정보보호 상세요구사항 작성표 참조

나. 정보보호 준거성, 위험관리 방안 도출

(1) 정보보호 준거성 정의

○ 정보보호시스템 개발 사업에 적용받는 보안규제 및 기준/지침 등을 준수하여 정보보호 요구사항을 정의합니다.
- 법적 요구사항을 지속적으로 파악하여 최신성을 유지하고 준수여부를 지속적으로 검토
- 법/규정을 반영한 정보보호 정책의 실현 가능성을 확인
- 정보시스템 정보보호 정책서 및 지침서에 보안 관련 요구사항 반영여부 점검

○ 정보보호 정책 및 지침에 따라 해당 정보시스템에 적용해야 할 정보보호 요구사항을 도출합니다.

(2) 정보보호 위험관리 방안 정의

○ 정보시스템 구성요소별 정보보호 위협을 사전에 파악하고 정보시스템 구축 대상 별 정보보호 위협평가 계획을 수립합니다.
- 정보시스템 보안위협요소와 보안 등급 분류
- 정보시스템 구축과 관련된 신규 위험 및 위협을 목록화
- 정보시스템 구축 대상 별 정보보호 위협평가 계획에 자산(예: 서버 등), 중요정보(주요 데이터, 개인정보 등)에 대한 위협평가를 포함

○ 구축 대상 정보시스템에 대한 정보보호 위협 및 취약점을 식별하고 대응방안을 수립합니다.
- 정보시스템과 관련 있는 네트워크, 서버, 데이터베이스, 어플리케이션, PC등 시스템과 서비스의 기술적 보안 취약점을 식별하여 대응방안 수립

○ 정보시스템 개발 단계 전체 과정에 대한 정보보호 위험관리 전략(대응방안)을 수립합니다.
- 정보시스템 위험 관리전략을 정의
- 정보시스템 위험관리 전략을 인적·관리적, 기술적, 물리적 보안으로 구분

○ 정보시스템 위험관리 방안에 최근 1년 이내 발생한 정보보호 침해사고 및 취약점 항목을 반영합니다.
- 효과적인 정보시스템 위험관리 방안 수립을 위해 최근 1년 이내 발생한 주요 정보보안 사고 유형을 파악하고 위협 및 취약점 항목에 포함

다. 정보보호 요구사항 유형별 분석 및 도출

[표 2-10] 정보보호 요구사항 유형

유형분류	Code	요구사항 명	정보보호사업 고유
사업 공통 요구사항	CFI	프로젝트 기밀성 유지 요구사항	
	PMR	프로젝트 관리	
	PSR	프로젝트 지원	
	COR	제약사항	
	QUR	품질 요구사항	
사업 선택 요구사항	OFR	자산 관리 기능 요구사항	○
	PER	성능 요구사항	
	TER	테스트 요구사항	
	DAR	데이터 요구사항	
	INR	인터페이스 요구사항	
	CNR	제품 컨설팅 요구사항	○
정보보호 제품 요구사항	ECR	시스템 장비 구성 요구사항	
	SFR	보안 기능 요구사항	
정보보호 서비스 요구사항	TSC	정보 보안 컨설팅	○
	PSS	보안성지속 서비스	○
	SMS	보안관제	○
	SIM	SI 서비스 사업 요구사항	○
	PEI	물리보안 및 기타 정보보호서비스	○

(1) 사업 공통/선택 요구사항 분석 및 도출

○ 정보보호 사업을 수행함에 있어 공통적으로 적용해야 하는 프로젝트 기밀성 유지 요구사항과 일반적인 공공 정보화사업의 요구사항에 해당하는 프로젝트관리, 프로젝트 지원, 제약사항, 품질 요구사항을 기술합니다.

○ 정보보호 사업 유형에 따라 성능 요구사항, 테스트 요구사항, 데이터 요구사항, 인터페이스 요구사항을 선택하여 기술하며 정보보호 제품이나 서비스 사업 특성을 고려하여 자산관리 기능 요구사항, 제품 컨설팅 요구사항을 선택하여 기술할 수 있습니다.

(2) 정보보호제품 요구사항 분석 및 도출

○ 정보보호 제품은 하드웨어와 소프트웨어가 결합된 일체형 정보보호제품인 어플라이언스(Appliance) 장비를 도입, 설치하여 사용할 수 있는 시스템 장비 구성 요구사항과 소프트웨어 제품에 대한 보안 기능 요구사항을 기술합니다.

○ 시스템 장비 구성 요구사항과 보안 기능 요구사항은 보안 관리(Protection & Management), 침입 탐지(Detection & Monitor), 대응 및 복구(Response & Recovery)와 기타 물리 보안 제품으로 분류되며 제품별 정보보호 특성과 세부 사양을 기술합니다.

(3) 정보보호 서비스 요구사항 분석 및 도출

○ 정보보호 서비스 요구사항은 정보보호사업 유형에 따라 정보보안 컨설팅, 보안성 지속 서비스, 보안관제 등의 대표적인 정보보호 서비스에 대한 요구사항을 기술하며 정보보호시스템을 개발하는 SI 서비스 사업 요구사항과 물리 보안 및 기타 정보보호 서비스 요구사항을 선택하여 기술할 수 있습니다.

라. 요구사항 상세내역 작성 및 검토

(1) 요구사항 상세내역 작성

○ 사업의 요구사항을 지속적이고 효과적으로 관리하기 위해 표준화된 서식에 맞추어 요구사항 상세 내역을 작성합니다. 요구사항을 유일하게 식별할 수 있는 요구사항 분류, 요구사항 고유번호, 요구사항 명칭, 요구사항 상세설명, 산출정보, 관련 요구사항, 요구사항 출처 등의 항목을 포함합니다. 정보보호사업의 유형 및 특성에 따라 수정할 수 있습니다.

[표 2-11] 상세 요구사항 구성항목

작성항목	작성 여부	비고
요구사항 분류	필수 작성	
요구사항 고유번호	필수 작성	
요구사항 명칭	필수 작성	
요구사항 상세설명 (정의, 상세설명)	필수 작성	
산출정보	해당 시	
관련 요구사항	해당 시	
요구사항 출처	필수 작성	

(가) 요구사항 분류: 요구사항 분류항목 중 해당 항목을 선택하여 기술

(나) 요구사항 고유번호(ID): 제안요청서에 정의된 요구사항에 대해 계약, 사업수행, 사업 완료 및 검수 시까지 변경, 삭제, 수정 여부에 대한 관리를 위해 요구사항별 고유번호를 생성하며 요구사항 분류(또는 약어)와 일련번호를 조합하여 표현 가능

(다) 요구사항 명칭: 요구사항의 명칭을 명확하고 세분화하여 중복이 발생하지 않는 수준으로 작성

(라) 요구사항 상세설명: 사업의 목적을 달성하기 위해 어떻게 구현하거나 어떻게 수행해야 하는지에 대한 내용을 상세하게 작성
- 요구사항 정의 : 요구사항에 대한 개념을 간략하게 설명
- 요구사항 세부내용 : 각 요구사항에 대하여 발주자와 수주자가 모두 명확하게 이해할 수 있도록 상세하게 작성하며, 이해하기 쉽게 도표나 그림을 사용하여 표현도 가능

(마) 산출정보: 해당 요구사항의 수행을 통해 사업완료 후 어떠한 산출물이 제출되어야 하는지를 작성함. 다만, 요구사항에 따라 타 요구사항의 산출정보와 통합되어 별도의 산출물이 없을 수 있으며, 비기능적 요구사항의 경우 문서, 보고서, 화면의 형태로 산출될 수 있음

(바) 관련 요구사항: 동 요구사항과 직접적으로 연관되어 있는 여타 요구사항의 고유번호를 기입

(사) 요구사항 출처: 해당 요구사항이 도출된 출처(사업계획서, 담당자/부서, 근거 법령, 위험관리방안 등)를 기입하여 향후 요구사항 변경이나 수정, 삭제 필요 시 의사결정을 원활히 하고, 사업수행 시 상세 요구사항에 대한 설명이나 추가 정보 필요 시 활용하도록 함. (요구사항 변경·관리 용도로 사용하며, 제안요청서에는 명시하지 않음)

(2) 이해관계자별 요구사항 상세내역 검토 및 확정

○ 작성된 개개의 상세 요구사항 세부내용을 분류기준 별로 분류하여 요구사항 상세 내역 초안을 작성합니다. 이해관계자는 상세 내역에 요구사항이 누락 없이 반영되었는지, 구체적이고 상세한 수준으로 기술되어 있는지를 검토합니다. 사업담당자는 검토 의견을 취합하여 요구사항 상세 내역에 반영하고 최종 확정합니다. 이러한 과정은 사업의 범위 및 요구사항에 대한 공감대를 형성하고, 프로젝트 진행 과정에서 혼란을 최소화하여, 정해진 기간 내 목표 요구사항을 구현할 수 있도록 하는 데 그 목적이 있습니다.

마. 공공 정보화사업 추진 시 적용해야 하는 정보보호 규정

(1) 개인정보영향평가 실시

○ 일정규모 이상의 전자적으로 처리하는 개인정보파일을 구축, 운영 또는 변경하려는 공공기관은「개인정보 보호법」제33조 및 시행령 제35조에 근거하여 개인정보영향평가를 수행하여야 합니다. 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 그 위험요인의 분석과 개선 사항 도출을 위한 평가를 하고 그 결과를 행정안전부장관에게 제출하여야 합니다.

- (5만 명 조건) 5만 명 이상의 정보주체의 민감정보 또는 고유식별정보가 포함된 개인정보파일
- (50만 명 조건) 공공기관의 내부 혹은 외부의 다른 개인정보파일과 연계하려고 할 때, 연계결과로서 정보주체의 수가 50만 명 이상의 개인정보 파일
- (100만 명 조건) 100만 명 이상의 정보주체 수를 포함하고 있는 개인정보 파일
  ※ 현시점 기준으로 영향평가 대상은 아니나 가까운 시점(1년 이내)에 정보주체의 수가 기준을 초과할 것이 확실한 경우, 영향평가를 수행할 것을 권고
- (변경 시) 영 제35조에 근거하여 영향평가를 실시한 기관이 개인정보파일의 운용체계를 변경하는 경우, 변경된 부분에 대해서는 영향평가를 실시

(2) 소프트웨어개발보안 실시

○ 행정기관 등이 전자정부법 시행령 제71조(정보시스템감리의 대상) 제1항에 해당하는 정보화사업을 추진할 때에는 “소프트웨어 보안약점 기준”에 해당하는 소프트웨어 보안약점이 없도록 소프트웨어를 개발 또는 변경하여야 합니다. 정보화사업 감리를 수행하는 경우 감리법인으로 하여금 사업자가 소프트웨어 보안약점을 제거하였는지 진단하도록 하고 있습니다.

전자정부법 시행령 제71조(정보시스템감리의 대상) 제1항
- 정보시스템의 특성
  가. 대국민 서비스를 위한 행정업무 또는 민원업무 처리용으로 사용하는 경우
  나. 여러 중앙행정기관 등이 공동으로 구축하거나 사용하는 경우
- 정보시스템 구축사업으로서 사업비가 5억 원 이상인 경우

[행안부 고시] 행정기관 및 공공기관 정보시스템 구축·운영지침 제50조(소프트웨어개발보안 원칙) 정보화사업 추진 시 적용해야 할 소프트웨어 개발보안의 범위
- 신규 개발의 경우 : 설계단계 산출물 및 소스코드 전체
- 유지보수의 경우 : 유지보수로 인해 변경된 설계단계 산출물 및 소스코드 전체

제 3 절 제안요청서 작성

1. 제안요청서 작성 절차

○ 표준 프로세스 및 활동을 통하여 상세 요구사항을 도출한 후, 사전 준비 과정을 거쳐 제안요청서 본문을 작성합니다.

가. 사업 개요

사업의 추진배경, 필요성, 추진경과 등을 알기 쉬운 문장으로 일목요연하게 정리한다. 특히, 추진경과는 과거의 사업수행계획이나 결과를 쉽게 파악할 수 있도록 제시하여 제안업체가 이를 참조할 수 있도록 함으로써 제안서 작성을 용이하게 하는데 도움이 될 수 있습니다

(1) 추진 배경 및 필요성

(가) 기술 내용

○ 사업을 추진하게 된 배경 및 경위를 기술합니다.

○ 국가경쟁력 강화, 업무효율성 증대, 대민서비스 개선, 국민 삶의 질 향상 등 정보화사업 추진 목적과 함께 정보보호 사업을 추진하는 필요성을 기술합니다.

(나) 기술 방법

○ 정보화전략계획(ISP), 정보보호컨설팅, 개인정보영향평가, 취약점 진단 등 수행의 결과물, 사업계획서, 발주계획서 등을 참조하여 정보의 훼손 · 변조 · 유출 방지와 사이버범죄 대응 등 정보보호 사업이 추진되어야 할 배경과 필요성을 제시합니다.

○ 공공 정보화사업의 경우 정부정책 등 법제도의 변화에 따라 구축되는 경우도 많이 있으므로 이를 적절히 기술하여 사업 추진에 대한 이해를 명확하게 할 수 있도록 관련 법제도 등에 대해서도 기술합니다. 특히 정보보호 관련 법령, 지침의 제개정에 따라 정보시스템에 반영해야 할 정보보호 요건이 추가될 경우 이를 기술합니다.

(다) 작성 시 유의사항

○ 법제도의 변화 또는 기존 정보보호 장비의 노후화 등 사업 추진 필요성을 명확하게 기술합니다.

○ 사업이 단계별로 나누어져 있거나 장기적일 경우에는 단계별 및 연도별 추진 계획을 명시하여야 합니다.

○ 본 사업과 관련되는 분리발주사업 등 별도의 사업이 진행되고 있는 경우에는 이를 반드시 명시하도록 합니다.

작성 예시

□ 목 적

○ 정부 당국의 정책 변화, 본사의 이전 등 대내외 환경 변화와 날로 지능화·대형화되는 사이버위협에 능동적으로 대응하기 위하여,

○ 우리원의 정보보호 현황을 진단·분석하고 이에 따른 개선과제를 도출함으로써 전자거래제도 도입 등 제반 환경 변화에 최적화된 위협 대응 체계 마련을 위한 전략을 수립하고자 함

□ 추진배경

○ 지능정보사회 도래로 지능화되는 사이버 위협 대응 전략의 필요

– 지능정보기술 활용의 보편화로 사이버 침해 위협의 지속적인 증가 및 다양화

○ 정부의 지속적인 보안 강화 정책 추진에 부응

– “금융전산 보안 강화 종합대책” 발표 등 정책당국의 사이버공격에 의한 금융사고 피해예방 감독 강화(금융위, ‘13.7)

– 금융보안 강화를 위한 전담기구 금융보안원의 출범(금융위, ‘15.4.)

– 『개인정보보호법』주민번호 암호화 조치 강제화(행정안전부, ‘16.1.)

– 개인정보 유출 인터파크에 역대 최대 과징금 부과(방통위, ‘16.12.)

나. 서비스 내용

(1) 기술 내용

○ 사업 완료 후 제공될 정보보호 서비스 및 프로세스(업무처리 절차) 개선 내용에 대해 간략히 기술합니다.

- 서비스 이용 대상자를 구분하고 대상 그룹별로 정보보호 서비스 제공 내용을 제시
- 프로세스 개선 전과 후를 명확하게 구분하여 기술합니다.

(2) 기술 방법

○ 서비스 내용은 사업추진 결과로 제공되는 서비스의 개선내용을 기재하며, 정보보호시스템 개발사업 이외의 정보보호 컨설팅 사업이나 보안지속성 서비스 사업의 경우에는 생략할 수 있습니다.

작성 예시

□ 컴플라이언스 부문 점검 및 대책 수립

○ 개정된 규정(법규 포함) 적용 검토 및 조치사항 도출

- 전자금융감독규정, 국가정보보안지침 등

ㅇ 개인정보보호 관련 진단 사항 점검

- 개인정보보호법에 따른 기술적 보호조치 등에 대한 보안 진단

ㅇ 방화벽 정책 분석 및 최적화 수행

□ 기술적 위협에 대한 취약점 분석 및 대응방안 수립

ㅇ 시나리오 기반 모의 해킹 실시 및 대응 프로세스 점검

- OA 기기 등 사무기기를 통한 자료 유출 시나리오
- 랜섬웨어 등의 악성코드를 통한 2차 피해 발생 시나리오
- 최신 해킹 기법을 이용한 공개 홈페이지 공격 시나리오 등

ㅇ IT자산에 대한 기술적 취약점 분석·평가 수행

- IT자산(주요정보통신기반시설 포함)에 대한 기술적 점검 수행

다. 사업 범위

(1) 기술 내용

○ 본 사업에서 개발 또는 수행되어야 할 범위(정보보호시스템 개발사업의 경우, 응용 소프트웨어의 개발내용 및 범위)를 간략히 기술하고, 이와 관련된 소프트웨어, 하드웨어, 데이터베이스 및 네트워크 등 제반 시스템 구축내용을 간략히 기술합니다.

(2) 기술 방법

○ 연도별, 단계별, 분야별 사업범위를 명확하게 제시함으로써 제안사가 과업 내용과 목표시스템 등을 정확히 파악하고 적정 사업비를 제안할 수 있도록 기술합니다.

○ 연도별 사업범위는 제안서 작성의 기준이 되므로 당해 연도 사업범위에 대해서는 상세하고 명확하게 작성합니다.

(3) 작성 시 유의사항

○ 사업범위는 사업유형을 결정하게 되므로 주요 항목을 개괄적으로 빠짐없이 기술합니다.

작성 예시

□ 점검 대상

ㅇ 관리체계 부문 (법령, 규정, 컴플라이언스 등 포함)

ㅇ 물리적 자산 부문(시설, 건물, 소방 등)

ㅇ IT정보자산 부문(서버, DB, 네트워크 등)

구 분	장 비	모델명	수량(대)	비 고
주전산 센터 및 백업 센터	서버	Unix	71	정보처리 및 저장
		Windows	23	
	침입차단시스템	secui 등	35	보안시스템
	VPN	secui 등	10	
	침입방지시스템	스나이퍼 등	8	
	DDoS방어장비	Radware	2	
	라 우 터	Cisco	34	패킷, 라우팅
	스 위 치	Alteon	5	
합계			188	

라. 기대 효과

(1) 기술 내용

○ 정보보호 서비스 개발 및 제공으로 발생되는 프로세스 개선 및 정보보호 강화 효과 등 제반 기대효과를 제시하고, 정량적 효과와 정성적 효과로 구분하여 기술합니다.
○ 사업계획서의 성과지표 등을 참고하여 기술합니다.

(2) 기술 방법

○ 서비스 내용 및 사업범위에 대해 연도별, 단계별, 분야별 기대효과를 정성적인 효과와 정량적인 효과로 구분하고 산출근거를 제시함으로써 사업 추진의 당위성과 목적을 이해관계자들에게 명확하게 알리도록 기술합니다.

○ BPR/ISP를 추진하는 경우 동 사업의 정성적, 정량적 기대효과를 사전에 도출하도록 하여 정보보호시스템 구축사업 제안요청서 작성 시 이를 활용할 수 있습니다.

(3) 작성 시 유의사항

○ 현재의 서비스 및 업무 내용의 개선을 통해 기대되는 효과를 기술합니다.

○ 정성적 효과의 경우 대내외 서비스 측면, 기술적 측면 등을 도출하여 기술하며, 정량적 효과 측면에서는 관련 보고서나 ISP 결과 등을 참고하여 기술합니다.

작성 예시

❍ 사이버침해에 대한 실시간 모니터링 및 내부 대응능력 강화로 대규모 사이버공격으로부터 행정서비스의 연속성 유지
❍ 급증하는 보안 위협에 대한 사전예방과 침해사고 재발방지 대책 마련 등 사후조치를 위한 사이버안전센터 기능 강화
❍ 공공기관 및 정보보호 유관기관 간 정보공유를 통한 신속한 사이버위협 대응체계 확보
❍ 고도의 보안관제 능력을 갖춘 민간 전문업체를 통한 전문성 향상으로 사이버안전센터의 기술역량 제고 및 대외적 위상 강화
❍ 정보보안 교육 등을 통한 직원의 정보보안 수준제고

2. 업무 및 시스템 현황

본 사업과 관련된 업무, 정보화 현황 등을 기재한다.

가. 업무 현황

(1) 기술 내용

○ 정보보호 대상 전체 업무구성도(전체업무 개요를 도식화)를 작성합니다.
- 관련부처 · 조직 · 서비스 대상자 등을 기술, 본 사업의 정보교환 및 상호간 연계성을 도식화

○ 사업 내에 포함된 업무명, 업무개요 및 기능, 수행조직, 관련기관, 정보화 현황 등을 기술합니다.

○ 업무조직도 작성 : 업무와 관련된 수행조직은 조직도를 참조하여 도식화하고 각 조직별 역할을 기술합니다.

(2) 기술 방법

○ 관련 부처, 조직, 서비스 대상자를 기술하고, 전체적인 업무 구성도를 작성하여 제안사가 사업 및 서비스 현황, 관련되는 기관 등을 충분히 이해할 수 있도록 하여야 합니다.

○ 사업 내에 포함된 업무명, 업무 개요 및 기능, 수행조직, 관련 기관, 정보화 현황 등을 명시하고, 업무 및 기능 단위로 도식화하여 대상 사업을 이해하기 쉽도록 기술합니다.

○ 업무단위별 문제점을 상세하게 제시하여 제안사가 개선방안과 정보보호 시스템을 제안할 수 있도록 작성합니다.

(3) 작성 시 유의사항

○ 발주대상 사업과 관련된 업무로 한정하여 기술합니다. 특히, 관련된 기관이 있는 경우에는 해당 업무 내용도 상세히 기술하여야 합니다.

작성 예시

가. 나이스 교직원 업무포털 및 업무프로그램

❍ 교직원은 업무포털을 통해 나이스 업무프로그램에 접속하고 일반행정, 교무업무, 학교행정 등의 주요 업무를 처리

❍ 업무포털 주요기능

■ 나이스, 에듀파인, 업무관리시스템, 기타 시·도교육청 서비스 통합 접속(전자서명인증서 기반 단일 로그인 방식)
■ 나의 업무현황 조회(나이스 승인신청현황, 업무관리 결재/대기/공람 등)
■ 마이페이지, 업무바로가기, 학사일정 등을 통한 개별화된 업무환경 구축
■ 포틀릿을 통한 교육소식 및 교육정보서비스 연계, 지식 공유 등

❍ 나이스 업무프로그램은 일반행정, 교무업무, 학교행정, 대국민서비스 부문 총 37개 단위업무, 250개 세부업무로 구성

구분	설명	업무 수
일반행정	시·도교육청 및 교육지원청, 각급 학교 행정실의 주요 행정업무 처리	19개 단위업무, 96개 세부업무
교무업무	초, 중, 고, 특수학교, 학력인정평생교육시설, 재외한국학교, 영재학교의 교무 업무 처리	6개 단위업무, 87개 세부업무
학교행정	장학, 체육, 급식 등의 학교행정 업무 처리	7개 단위업무, 50개 세부업무

나. 나이스 대국민서비스

❍ 나이스 교무업무, 학교행정 업무 데이터를 기반으로 학생 및 학부모에게 교육정보 서비스를 제공
❍ 민원인에게 인터넷 제증명 발급 서비스를 위한 홈에듀 민원서비스 제공
❍ 교원 임용고시 및 지방공무원 공채, 검정고시 응시생 서류 접수를 위한 교원 및 공무원 온라인 채용, 검정고시 온라인 접수 서비스 제공

나. 정보시스템 현황

(1) 기술 내용

○ 최종사용자, 통신망, 주전산기, 소프트웨어, DB로 구성된 전체의 시스템을 도식화 (통신회선 속도 명시)하여 현행 시스템 구성도를 작성합니다.

○ 주전산기의 CPU종류, CPU수량, 메모리량, 디스크 보유량, 디스크 여유량, 백업장치, 운용업무, 본 사업에의 활용가능성을 기술합니다.

○ 현행 시스템의 하드웨어 구성도를 작성합니다.

○ 현행 시스템의 소프트웨어 구성도를 작성합니다.

○ 현행 시스템의 네트워크 구성도를 작성합니다.

○ 업무와 관련하여 구축된 DB관련 DBMS명 및 논리적 DB내용, 구축자료 건수, 암호화 대상 등을 제공하는 현행시스템 DB구축현황을 작성합니다.

○ 상기 언급하지 않은 자원 중 본 사업에서 활용될 장비의 품명, 주요기능, 시스템 개발/운영/유지관리 연혁, 특징 및 용도 등을 기술합니다.

(2) 기술 방법

○ 관련 정보화 현황은 제안서 작성에 필요한 기초 정보로서 효과적인 제안내용을 제출받기 위해서는 사업추진 관련 정보화 현황을 제공합니다.

○ 특히, 하드웨어, 소프트웨어 등에 대한 세부 기능별 활용 현황을 명시하여 새로 구축하고자 하는 정보보호 시스템과의 연계성·복잡도 등을 정확히 측정하여 제안사가 사업비 등을 적정하게 산정할 수 있도록 합니다.

○ 관련기관 간 연계가 있는 경우 모든 기관의 정보시스템 구축현황, DB 및 정보 연계현황 등을 상세하게 명시하여야 합니다.
※ 단, 제안요청서에는 정보보호 측면에서 해당 항목을 생략하는 것으로 표시하고 제안사 요청 시 현장에서 열람할 수 있도록 조치 가능

(3) 작성 시 유의사항

○ 현황 작성 시, 다음의 정보보안 관련 사항은 제안요청서 상에 포함되지 않도록 유의하고, 제안 작업 시 필요한 경우에는 방문 열람하도록 조치합니다.

- 정보시스템의 내·외부 IP 주소 현황
- 정보시스템의 제조사, 제품버전 등 도입현황 및 구성도
- 정보시스템의 환경파일 등 구성 정보
- 사용자 계정 및 패스워드 등 시스템 접근권한 정보
- 정보시스템 취약점 분석 결과물
- 방화벽·침입방지시스템(IPS) 등 정보보호제품, 라우터·스위치 등 네트워크 장비 도입현황 및 설정 정보
- 「공공기관의 정보공개에 관한 법률」제9조 제1항 단서에서 정한 비공개 대상
- 「개인정보 보호법」제2조제1호에 따른 개인정보
- 국정원「보안업무규정」제4조의 비밀, 동 시행규칙 제7조 제3항의 대외비
- 그 밖에 행정기관 등의 장이 공개가 불가하다고 판단한 자료

작성 예시

「국가정보보안 기본지침」에 의거, 사업 참여와 관련하여 열람을 신청하는 경우에 한해 방문 시 열람(수요기관에 요청)

3. 사업 추진방안

사업 추진방안으로 발주기관의 목표, 비전을 제시하고, 이를 위한 분야별 추진전략 및 방향을 기술하며, 이에 필요한 조직 및 역할을 기재하여 단계별 추진 일정, 추진방안을 작성하도록 합니다.
- 본 사업의 목표와 필수적인 전략·방향
- 본 사업 추진을 위해 필요한 조직 및 역할
- 본 사업 추진의 주요 일정(주/월 단위)
- 본 사업의 주요 추진방안을 제시, 긴급발주 여부, 기술 대 가격 비율의 조정 여부, 분리발주 여부, 대기업 참여제한 여부 등

가. 추진 목표

(1) 기술 내용

○ 조직목표 등 상위 목표와 정보보호 사업의 목표를 명확히 제시하고 정보보호 사업으로 상위 목표의 어떤 부분을 어떻게 달성할 것인지 연관관계를 명확히 기술합니다.

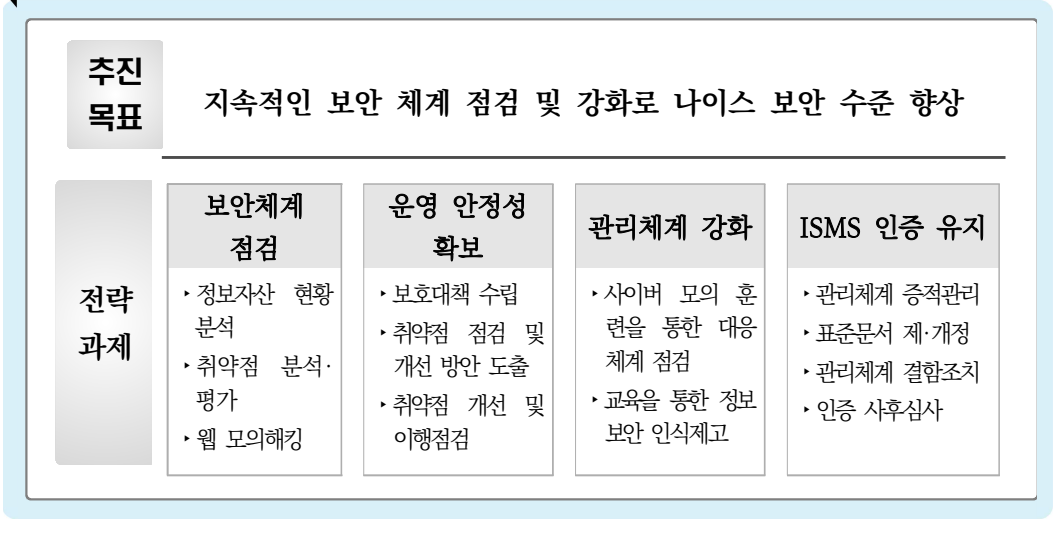
○ 정보보호 사업을 통해 추구하는 목표를 장·단기적으로 구분하여 기술합니다.
- 장기목표는 발주기관의 기본계획 목표와 일관성을 유지하도록 기술
- 단기목표는 최대한 계량화하여 구체적으로 기술

(2) 기술 방법

○ 발주기관은 명확한 비전, 최종목표, 단계별 추진목표를 명확하게 제시하여 제안사들이 목표 시스템을 체계적으로 구성하도록 합니다.

○ 다만, 너무 많은 목표나 정성적 위주의 추진목표 설정은 제안사에게 혼란을 줄 수 있으며 사업 추진에 대한 비전, 최종 목표 및 단계별 추진목표를 당해 사업관련 각종 기본계획, 시행계획, 발주계획서 등을 토대로 제시합니다.

작성 예시



나. 추진 전략

(1) 기술 내용

○ 본 사업의 목표달성을 위해 필수적인 전략과 방향을 기술합니다.
- 기술적 측면, 관리적 측면, 정책적 측면, 표준화 측면, 법·제도적 측면 등에서 구체적인 추진방향을 기술

○ BPR/ISP 등 선행사업 수행전략, 신기술 적용 등 정보기술 활용전략, 사업관리 전략, 표준화전략, 개발시스템의 확산전략, 관련기관 간 협조 등을 기술합니다.

(2) 기술 방법

○ 정보보호 전략 방향과 이해관계자의 기대사항을 고려하여 정보보호 사업을 통해 획득하고자 하는 목표 및 추진방향을 정의합니다.

○ 사업추진 시 목표를 달성하기 위한 중점 전략을 공유하고 제안사가 이를 충실히 이행할 수 있도록 추진전략을 설정합니다.

작성 예시

❍ 통합 보안 관제를 위한 원격보안관제 서비스 제공

- 네트워크 보안장비에 대한 24시간×365일 실시간 보안관제

- 사이버 침해 대응 예·경보 및 즉각적인 피해확산 대응 활동
- 사이버 침해사고 발생 시 원인분석, 재발방지 대책 등 지원
- 보안로그 분석 및 이슈 사항을 정리하여 관제보고서 제공(월간)

❍ 통합보안관제시스템 운영·유지관리 지원

- 종합지원시스템의 통합보안관제시스템 운영 및 관제 지원
- 보안장비 운영 업무 수행 프로세스 구축
- 사이버 침해사고 및 대응에 대한 기술동향 제공
- 최신 보안관련 이슈·해킹에 대한 정보 조사 및 보안권고
- 사이버 침해 대응 훈련(을지연습, 모의 사이버테러 대응훈련) 지원

다. 추진 체계

(1) 기술 내용

○ 사업추진을 위해 필요한 조직과 역할을 기술합니다.

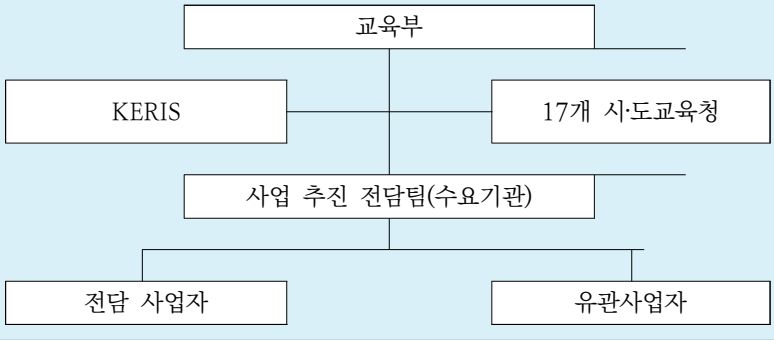
- 사업수행에 필요한 기관(발주기관, 사업자 및 관련기관 등)을 주관기관을 중심으로 도식화하고, 담당업무 및 기능을 상세히 기술합니다.

(2) 기술 방법

○ 대상 사업과 관련하여 참여주체별 역할과 기능을 상세히 명시하여 시스템 통합, 정보보호시스템 개발 등에서 제안사가 해야 할 일을 제안하도록 합니다.

○ 사업과 관련한 주요 이해관계자에 대한 정보를 제시하여 사업을 원활하게 수행하기 위한 관리방안이 제안될 수 있도록 합니다.

작성 예시



구분	구성	주요역할
주관부처	교육부 (교육정보화과)	- 관계 법령 해석 및 지침 제·개정, 유관 부처 협의·조정 - 주요정보통신기반시설(나이스) 운영 관련 정책 방향 설정 및 추진 - 교육부 및 시·도교육청 관련 업무 협의 및 조정 - 관련 예산 확보 및 지원 등
발주기관	한국교육학술정보원 (인프라운영부)	- 사업 계획 수립 및 사업 수행 총괄 - 통합 조달 발주 및 계약 체결 지원 - 사업 현황 및 관리 등 관리·감독 - 기타 사업 추진에 필요한 정책 수립·지원 등
사업 추진 전담팀 (수요기관)	17개 시·도교육청, 한국교육학술정보원	- 기관별 예산 계획 수립 및 집행(계약, 검수 등) - 기관별 업무 협의 및 사업 관리(사업 추진 전담팀 운영) - 나이스 보안 취약점 분석·평가 사업 수행 - 정보보호관리체계 유지 및 관리 등
전담사업자	본 사업 수행사	- 취약점 분석·평가 세부 과업 수행 - 정보보호관리체계 세부 과업 수행 등
유관사업자	응용SW 유지보수 및 물적기반 유지관리 사업자	- 응용소프트웨어 소스진단 및 모의해킹 관련 업무지원 및 진단 결과에 따른 취약점 제거 지원 - 기술적 분야 취약점 영향도 분석 및 개선 지원

라. 추진 일정

(1) 기술 내용

○ 본 사업추진의 주요 일정을 월별로 제시합니다.

- 사업의 총 수행기간, 계약기간, 추진단계, 일정별 주요 이벤트(착수 및 종료 보고회, 워크숍, 법·제도 개정, 서비스 개통일 등)을 표시

○ PMO 도입 여부, 각 단계별 감리 실시 여부에 따라 관련 일정을 포함하여 기술합니다.

(2) 기술 방법

○ 사업추진 일정은 사업기간 내에 주요 시스템에 대한 세부일정을 기능단위별로 명확히 기술합니다.

○ 제안사가 전체적인 사업추진 일정을 제안하고, 각 세부 공정별 과업추진 및 인력투입계획 등을 수립하여 제안할 수 있도록 세부 일정을 기술합니다.

(3) 작성 시 유의사항

○ 사업 전 기간 동안에 수행될 주요 마일스톤과 이벤트를 서브시스템 수준까지 상세하게 정의하여 제시하여야 합니다.

- 특히 시범운영, 서비스 개시, 안정화 기간 등을 구체적으로 제시하여 사업자가 사업 추진 일정을 명확하게 제시할 수 있도록 하여야 합니다.

작성 예시

추진업무	M	M+1	M+2	M+3	M+4	M+5	M+6	M+7	M+8
.현황 분석 및 세부 수행계획 수립									
.담당자 인터뷰, 정밀진단 계획 수립									
.정보시스템 취약점 등 점검 .개인정보 처리실태 점검 ※개인정보 분야 점검 4개월									
.교육 및 지도 점검									
.정보보안 관리실태 점검									
.종합 개선대책 수립									
.사업수행 결과(산출물) 제출 및 보완									

※ 상기 추진일정을 참고하여 용역사에서 구체적인 추진일정을 제시하여야 함.

라. 추진 방안

(1) 기술 내용

○ 본 사업추진 방안에 대한 내용을 간략히 제시합니다.
- 사업의 긴급발주 여부, 기술/가격점수 비율, 소프트웨어분리발주 여부, 대기업참여제한 여부 등 법제도적인 근거를 포함하여 기술

(2) 기술 방법

○ 긴급발주 여부, 기술/가격점수 비율, 소프트웨어 분리발주 내용, 사업예산에 따른 대기업 참여 여부 등 사업추진 내용을 확인하여 기술합니다.

○ 제안요청서 추진방안은 목표시스템 구축에 필요한 최신 근거 법령을 명시하고 제안사가 제안할 수 있도록 기술하여야 합니다.

(3) 작성 시 유의사항

○ 추진방안은 발주계획 단계에서 사전검토하고, 관련사항 (법적근거 포함)을 제안사가 사전에 확인할 수 있어야 합니다.

작성 예시

가. 추진방법: 발주기관이 통합 발주(조달청 구매요청)
  ❍ 발주기관: 한국교육학술정보원
  ❍ 수요기관: 17개 시·도교육청(정보원), 한국교육학술정보원
나. 계약 및 검수 방법: 수요기관별로 선정된 사업자와 개별 계약 후 검수

4. 제안 요청내용

기술제안서의 핵심부분으로 제안요청내용을 명확하게 제시하여야 합니다.
사업유형별로 요구사항을 명확하고 상세하게 정의함으로써, 사업자가 본 사업에서 수행해야 하는 과업내용을 명확하게 인지하고 제안하여 사업수행 시 과업내용과 관련한 이슈가 발생하지 않도록 하여야 합니다.

가. 제안요청 개요

(1) 기술 내용

○ 본 사업의 주요 핵심내용을 간략히 기술합니다.
- 주요 개발 업무 내용 등 사업자가 수행하여야 하는 핵심 내용을 요약해서 제시합니다.

(2) 기술 방법

○ 발주기관은 당해 사업의 전체적인 측면을 요약 정리하고, 사업기간, 사업범위 등을 개략적으로 기술합니다.

(3) 작성 시 유의사항

○ 사업에 대한 개괄적 범위에 대한 이해가 가능하도록 핵심 내용을 정의합니다.

작성 예시

❍ 사업명 : 공공기관 보안관제 종합시스템 구축
❍ 사업기간 : 계약일로부터 ~ 2018.12.31
❍ 사업금액 : 0,000백만 원(부가세 포함)

작성 예시

1. 일반 사항
o 제안사는 본 사업의 목표, 범위, 요건 등의 제반사항을 충분히 인지한 후 제안하여야 함
o 제안서에는 사업계획과 제안요청 제반사항에 대해 제안사의 정보보호 수준강화를 위한 사업 추진전략, 추진계획 등이 구체적이고 명확하게 제안하여야 함
o 본 사업에서 요구하는 세부 제안사항에 대한 구체적이고 체계적인 수행방안을 기술하고 제안사의 역할을 명확하게 제안하여야 함

나. 용어의 정의

(1) 기술 내용

○ 본 사업 또는 제안요청서에서 사용되는 용어를 기재합니다.

(2) 기술 방법

○ 제안요청서에 기재된 용어 중 설명이 필요한 용어를 정리하여 요구사항의 명확화와 제안요청사항의 이해를 돕도록 기술합니다.

○ 발주기관에서 사용하는 관련용어에 대하여 구체적이고 명확한 정의를 통해 제안사가 혼동하지 않도록 합니다.

○ 제안요청서에 기재된 용어가 일반적인 정보보호 관련 용어일 경우에는 생략이 가능합니다.

작성 예시

❍ 소프트웨어 개발보안: 안전한 소프트웨어 개발을 위해 소스코드 등에 존재 할 수 있는 잠재적인 보안취약점을 제거하고, 보안을 고려하여 기능을 설계 및 구현하는 등 소프트웨어 개발보안과정에서 일련의 보안활동
❍ 보안취약점: 해킹 등 실제 보안 사고에 이용되는 소프트웨어 보안약점
❍ 소프트웨어 보안약점: 소프트웨어 결함, 오류 등으로 해킹 등 사이버공격을 유발할 가능성이 있는 잠재적인 보안취약점을 말함
❍ 표준연동규격: 이기종 보안장비간의 데이터 수집 표준화를 위하여 전송 방법, 전송항목 등을 지정하는 것
❍ 원본데이터: 관제 대상기관 보안장비에서 탐지되어 표준연동규격에 의해 ECSC로 수집된 데이터
❍ 위협정보: 이기종 원본데이터를 분석 시스템 정책 기반으로 정규화한 데이터
❍ 위협경보: 위협정보를 인텔리전스 기반 관제정책에 의해 위험지수로 수치화한 데이터
❍ 위험지수: 국내·외 다양한 인텔리전스 DB 및 자체적으로 분석한 다양한 보안정보를 토대로 하여 각각의 수집정보 및 데이터 필드의 위험성을 수치화
❍ 관제정책: 인텔리전스 DB 기반의 위협정보 위험지수 산정 기준
❍ 위험도: 위험지수의 시각화를 위하여 다양한 유형별로 위험지수를 분류하여 등급화
❍ 침해사고: 다양한 위협경보를 관제요원이 분석하여 실제 위험이 발생한 데이터
❍ 인텔리전스 분석: 국내·외 다양한 보안정보(IP, URL, MD5등) 및 기존 침해사고처리 이력 등을 인텔리전스 DB로 구축하여 이를 관제대상기관에서 수집된 원본데이터, 위협정보, 위협경보 와 데이터 필드별로 연관 분석하는 방법
❍ 시나리오 분석: 내·외부에서의 보안사고 발생 시 발생 가능한 시나리오를 기반으로 하여 다양한 데이터 보안정보(IP, URL, 탐지규칙명 등)를 상호 연관 분석하는 분석 기법
❍ 통계 분석: 보안사고 시 기존에 발생한 원본데이터, 위협정보, 위협경보를 통계적인 기법(분포도, 시간당 임계치 등)을 이용하여 분석하는 기법
❍ 분석 정책: 관제대상기관으로부터 수집, 분석된 원본데이터, 위협정보, 위협경보를 교육부 사이버안전센터 관제인원들이 자체적으로 분석하기 위한 정책

다. 목표시스템 개념도

(1) 기술 내용

○ 목표시스템을 중심으로 서비스 이용자, 주요 서비스 내역 등을 기술합니다.

(2) 기술 방법

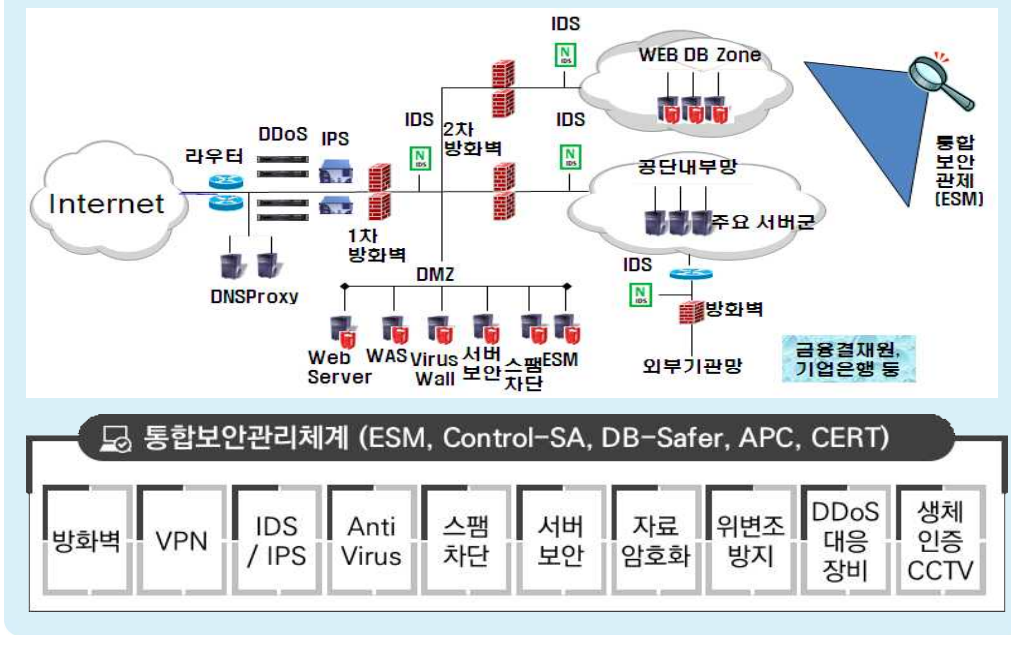
○ 정보보호시스템 개발사업, 보안지속성유지 사업 등의 경우에는 목표시스템 개념도를 제시하여 업무 프로세스 및 세부 개발 내용 등을 이해할 수 있도록 기술하고, 정보보호 컨설팅 유형의 사업 등에서는 생략 가능합니다.

(3) 작성 시 유의사항

○ 연차 사업인 경우 목표시스템 개념도에서 해당연도 사업 추진 부문만 명확하게 식별될 수 있도록 기술합니다.

○ 네트워크 구성도나 시스템 구성도 등 보안상 공개하기 어려운 정보에 대해서는 제안사가 방문하여 열람하도록 조치합니다.

작성 예시



라. 상세 요구사항

「정보보호산업진흥법」 제7조에 따라, 발주기관에서는 요구사항을 상세히 기술하여야 합니다.

(1) 기술 내용

○ 요구사항 총괄표, 목록표를 작성하여 제안요청의 전체 내용을 확인할 수 있도록 기술합니다.

○ 요구사항 유형별로 「요구사항 내용 작성표」를 작성합니다.

(2) 기술 방법

○ 사업에서 수행하여야 하는 요구사항을 상세하게 기술하는 부분입니다.

○ 유형별 요구사항을 집계하고 요구사항 총괄표를 작성하여 전체 요구사항의 유형 및 물량을 확인함으로써 구체적인 사업의 범위를 이해할 수 있도록 합니다.

(3) 작성 시 유의사항

○ 요구사항 유형은 사업특성 및 정보보호사업 유형에 따라 다르며 사업내용을 파악하여 정확하게 도출하여야 합니다.

작성 예시

요청사항 구분	ID부여규칙	요구사항수
시스템장비구성 요구사항 (ECR)	ECR-OOO	7
기능 요구사항 (SFR)	SFR-OOO	1
성능 요구사항 (PER)	PER-OOO	1
보안 요구사항 (SER)	SER-OOO	4
품질 요구사항 (QUR)	QUR-OOO	1
테스트 요구사항 (TER)	TER-OOO	2
사업관리 요구사항 (PMR)	PMR-OOO	7
사업지원 요구사항 (PSR)	PSR-OOO	3
제약 요구사항 (COR)	COR-OOO	1
합 계		**27**

※ 정보보호 요구사항 분류체계에 따른 기존 발주 사례는 없음

○ 다음으로는 요구사항 목록표를 작성하여 발주하고자 하는 정보보호사업 요구사항의 개요를 파악할 수 있도록 합니다.

작성 예시

요구사항 유형	요구사항 번호	요구사항 명
시스템장비구성 요구사항	ECR-001	시스템 구성 공통사항
	ECR-002	L4 스위치 도입
	ECR-003	DNS 전용장비 도입
	ECR-004	유해사이트 차단 솔루션 도입
	ECR-005	저장자료 완전삭제 소프트웨어 도입
	ECR-006	네트워크 접근제어(NAC) 도입
	ECR-007	스팸메일 차단 솔루션 도입
보안 기능 요구사항	SFR-001	최적화된 이중화 구성
성능 요구사항	PER-001	성능 요구사항 일반
보안 요구사항	SER-001	보안 공통사항
	SER-002	사업수행장비 보안
	SER-003	보안 교육 및 취약성 점검
	SER-004	기타 보안사항
품질 요구사항	QUR-001	품질 요구사항
테스트 요구사항	TER-001	적용 및 테스트 일자
	TER-002	승인(인수) 검사 및 성능 테스트
사업관리 요구사항	PMR-001	사업수행 조직 및 수행환경 구성
	PMR-002	일정 및 진척관리
	PMR-003	투입인력
	PMR-004	컨소시엄 및 하도급
	PMR-005	검수
	PMR-006	보고 및 산출물 관리
	PMR-007	사업수행 일반
사업지원 요구사항	PSR-001	하자보수 요구사항
	PSR-002	교육 및 기술전수
	PSR-003	매뉴얼 제공 및 기술이전
제약 요구사항	COR-001	제약 사항 일반

※ 정보보호 요구사항 분류체계에 따른 기존 발주 사례는 없음

○ 요구사항 목록표의 각 요구사항은 본 실무가이드의 요구사항별로 「요구사항 내용 작성표」를 작성합니다.

(4) 요구사항 내용 작성표

○ 소프트웨어사업 상세 요구사항 세부내용 작성표[서식]를 준용하여 일관성있게 작성합니다.

요구사항 분류	
요구사항 고유번호	(예시:기능요구사항-00X)
요구사항 명칭	

요구사항 상세 설명	정의	
	세부 내용	
산출 정보		
관련 요구사항		
요구사항 출처		

○ 상세 요구사항별 세부내용 작성기준

작성 항목	설 명		비 고
요구사항 분류	• 정보보호 제품 요구사항, 정보보호 서비스 요구사항, 공통/선택 요구사항 등 요구사항 분류항목 중 해당 항목을 선택하여 기술		필수 작성
요구사항 고유번호	• 제안요청서에 정의된 요구사항에 대해 계약, 사업수행, 사업완료 및 검수 시까지 변경, 삭제, 수정 여부에 대한 관리를 위해 요구사항별 고유번호를 생성 • 요구사항 분류(또는 약어)와 일련번호를 조합하여 표현가능		필수 작성
요구사항 명칭	• 요구사항의 명칭을 명확하고 세분화되어 중복이 발생하지 않는 수준으로 작성함 • 단, 정보보호시스템 기능 요구사항은 상위기능과 하위기능을 조합하여 계층화 될 수 있도록 기술		필수 작성
요구사항 상세설명	• 사업의 목적을 이루기 위해 기능을 어떻게 구현하거나 요구사항을 어떻게 수행해야 하는지에 대한 내용을 상세하기 작성함		
	정의	• 요구사항에 대한 개념을 간략하게 설명	필수 작성
	세부내용	• 각 요구사항에 대하여 발주자와 수주자가 모두 명확하게 이해할 수 있도록 이해하기 쉽게 상세하게 작성하며, 이해성을 높이기 위하여 도표나 그림을 사용하여 표현도 가능 • 단, 정보보호시스템 기능 요구사항의 경우 기능의 누락이나 중복이 없도록 전체시스템을 계층적으로 분류하고 기능구조를 도출하여, 세부기능별로 작성하여 사업비 산정이 가능 하도록 함	필수 작성
산출정보	• 해당 요구사항의 수행을 통해 사업완료 후 어떠한 산출물이 제출되어야 하는지를 작성함 • 단, 요구사항에 따라 타 요구사항의 산출정보와 통합되어 별도의 산출물 없을 수 있으며, 비기능적 요구사항의 경우 문서, 보고서, 화면의 형태로 산출될 수도 있음		해당 시
관련 요구사항	• 동 요구사항과 직접적으로 연관되어 있는 여타 요구사항의 고유번호를 기입 • 단, 정보보호시스템 기능 요구사항의 경우 기능 수행을 위한 관련 데이터 요구사항과 연계관리가 요구됨		해당 시

작성 예시

요구사항 분류		시스템장비구성 요구사항
요구사항 고유번호		ECR-005
요구사항 명칭		저장자료 완전삭제 소프트웨어 도입
요구사항 상세설명	세부 내용	ㅇ장비 수량: 1식 ㅇ장비 기능: 저장자료 완전삭제 ㅇ장비 성능 및 특징 - HDD에 저장된 데이터를 영구적으로 복구할 수 없도록 완전 삭제하여야 함 - 저장자료 완전삭제를 위한 CD 및 USB는 각각 최소 50개 이상 제공하여야 함 - 완전 삭제된 HDD는 재사용 가능하여야 함 - 작업 시작 후 매체(CD 또는 USB)를 제거하여 바로 연속 작업 가능 기능 제공 - 하드디스크의 고유 시리얼 번호, 사용자, 관리번호 등 보고서 출력 기능 제공 - 기존 저장자료 완전삭제 제품의 버전 업그레이드

(5) 제안요청서 표준 템플릿 활용

○ 본 가이드는 제안요청서 표준 템플릿을 제공하며, 사업유형별로 요구되는 요구사항에 대해 필수인지 여부를 확인하고 세부내용을 작성합니다.

○ 요구사항이 대량인 경우나 부가 정보가 많을 경우에는 각각의 요구사항을 요구사항 내용 작성표 형식으로 작성하기 어려울 수 있습니다. 따라서 상세 요구사항과 별도로 해당 내역을 작성하고 이를 참조하는 방식으로 작성할 수 있습니다. (예, 유관기관 연계를 위한 송수신 정보 목록과 연계 방법, 개발주체 등)

4-1. 정보보호 제품 요구사항

가. 기술 내용

○ 정보보호시스템 구축에 필요한 정보보호 전용 또는 범용 하드웨어, 소프트웨어, 네트워크 등의 도입 장비 내역, 시스템 장비 구성과 보안기능에 대한 요구사항을 기술합니다.

○ 정보보호시스템의 하드웨어, 소프트웨어 및 네트워크 등의 구성도는 [참고사항]으로 별도 제시할 수 있습니다.

○ 정보보호시스템 구성을 위해 필요한 도입대상 하드웨어, 소프트웨어, 네트워크 등의 내역(품목, 규격, 수량, 용도 등), 필수 요구사항(기능요건) 및 구성요건을 제시합니다.
※ 정보보호제품 도입요건에 따른 기준을 명시합니다.
※ 본 사업에서 도입되는 장비는 통합발주, 소프트웨어분리발주, 위임발주(국가정보자원관리원)로 구분하여 기술합니다.
※ 소프트웨어 분리발주 대상 소프트웨어인 경우 이를 명시하고, 소프트웨어 분리 발주대상임에도 분리발주하지 않을 경우에는 반드시 그 사유를 제시합니다.

○ CCTV, 생체인증 등 물리적 보안을 위한 제품 도입, 설치에 대한 요건을 제시합니다.

나. 기술 방법

○ 품목 : H/W 및 N/W, S/W 등 장비의 종류를 명시하여야 합니다. 예를 들어 서버인 경우 서버 종류(DB서버, WEB서버, WAS 서버) 및 시스템 아키텍처를 기술합니다.

○ 수량 : 서버의 경우에는 정보시스템 하드웨어 규모산정 지침을 참고하여 도출된 H/W 및 N/W의 규모와 수량을 기술합니다. S/W는 설치되는 HW와 사용자 권한에 따라 라이선스 수량을 책정합니다.
- TTAK.KO-10.0292_R1 정보시스템 하드웨어 규모산정 지침 (2017.6.28.)
- TTAK.KO-01.0103_R1 네트워크 구축을 위한 장비 규모산정 지침 (2017.6.28)

○ 성능 및 특징 : H/W의 경우, CPU 규모, 메모리 규모, 디스크 규모를 제시하며, 이를 산정하기 위해 정보시스템 하드웨어 규모산정 가이드라인 및 e-Sizing 웹사이트를 이용하여 정의합니다. N/W의 경우, 슬롯수, 동시세션 처리수, Backplane, Throughput 등 필요한 성능 요건을 기술합니다. 소프트웨어 경우, 제공받아야 할 기능에 대한 성능 요건을 제시합니다.

○ 기능 : 시스템 용도 및 서비스 형태를 기술합니다. S/W인 경우, 제공해야 하는 정보보호 기능을 기술하며, 도출된 기능 요구사항을 지원하는 S/W라면 기능 요약과 함께 기능 요구사항 ID를 기입합니다.

○ 그 외 시스템 OS 유형, 보안 등 목표시스템 요구사항을 만족시키기 위해 장비에서 제시해야 하는 사항을 기술합니다.
- 소프트웨어 경우, 운영환경, CC인증, GS인증 제품, 성능 요건, 보안정책 등

○ 설치 요건 : 도입되는 장비 설치에 대한 시간, 자원, 중복된 시스템, 장애 처리 등에 대한 요구사항이나 제약사항을 명시합니다.
- 시간 제약사항 : 장비 도입 시기 및 설치 허용 시간 등 장비 도입 및 설치 일정에 영향을 주는 제약사항을 명시
- 자원 제약사항 : 장비 설치 시, 데이터베이스 관리자, 사용자 등 장비 설치를 도와주고 관리하는 내부 인력에 대한 제약사항이 있다면 이를 명시
- 중복된 시스템에 대한 제약사항 : 도입된 장비와 동일한 기능을 수행하는 장비가 있다면 이를 유지할 것인지, 폐기할 것인지 등 중복 시스템처리 및 역할, 책임에 대해 명시
- 장애 처리 : 도입된 장비 설치로 인해 장애 발생 시, 이에 대한 처리 시간, 책임 등의 요구사항과 제약사항을 명시

○ 국가 · 공공기관 정보보호제품 도입기준 및 절차(국가정보원)를 준수해야 합니다.
- CC인증 대상인 '중요' 정보보호제품은 CC인증필 제품 도입을 원칙으로 함
- 국내용 CC인증제품·국가용 암호제품·보안적합성 검증필 제품 등이 아닌 정보보호제품 도입은 제안서 접수시점까지 국내용 CC인증을 획득하거나 보안적합성 검증을 필한 제품에 한함
- 보안적합성 검증 생략이 가능한 경우, 관련기관의 증빙 문서 첨부
  ※ 정보보호제품 도입 시 정보보호제품 도입요건에 따른 기준 명시

[표 2-12] CC인증 필수 제품유형

제품유형	용도
침입차단시스템	네트워크 유입 및 유출 트래픽 통제
침입방지시스템	네트워크 유해 트래픽 침입탐지 및 자동차단 (침입탐지시스템포함)
통합보안관리 제품	복수의 관리대상 시스템 중앙통제, 보안 이벤트통합 모니터링 및 분석
웹 응용프로그램 침입차단 제품	웹기반 유해 트래픽 침입탐지 및 자동차단
DDoS 대응장비	DDoS 공격 탐지 및 자동차단
가상사설망 제품	IPSec 또는 SSL방식 가상 사설망

제품유형	용도
서버접근통제 제품	서버 접근권한 통제 및 주요 파일 보안 설정
DB 접근통제 제품	DB 접근통제 및 데이터 유출방지
네트워크접근통제 제품	보안프로그램 설치 PC만 네트워크 접속 허용
인터넷전화 보안 제품	인터넷전화 관련 유해 트래픽 탐지 및 침입차단
무선침입방지시스템	무선랜 환경에서 보안위협 침입탐지 및 침입차단
무선랜인증 제품	인증된 사용자만 무선랜 접속을 허용
스팸메일 차단시스템	스팸메일 유입 탐지 및 차단
네트워크 자료유출방지 제품	네트워크 간 전송되는 트래픽을 통제하여 중요 데이터의 외부유출 차단
호스트 자료유출방지 제품	호스트에 설치되어 매체제어 등을 통해 중요데이터의 외부유출차단 (매체제어 제품 포함)
안티바이러스 제품	PC에 존재하는 악성코드 탐지 및 제거
패치관리시스템	중앙 서버에서 다수 PC에 대한 보안패치 자동 수행
소프트웨어기반 보안USB	USB 메모리 접근통제 및 분실 시 자동 삭제
가상화 제품	PC 또는 서버에서 실제 영역과 가상 영역에 대한 엄격한 영역분리 또는 영역분리 지원
망간 자료전송 제품	보안수준이 서로 다른 영역 간 데이터 및 정보흐름 통제
소스코드 보안약점 분석도구	소프트웨어 소스코드 분석 및 보안약점 식별
스마트폰 보안관리 제품	업무용 관리 대상 스마트폰 중앙통제 및 보안관리

- 암호 모듈은 국가 공공기관 정보통신망에서 소통되는 자료 중에서 비밀로 분류되지 않은 중요 정보의 보호를 위해 사용되며 암호모듈의 안정성과 구현 적합성을 검증받은 암호모듈을 사용하도록 하고 있습니다.
- CC인증을 획득한 DB암호화, 통합인증(SSO), 문서암호화(DRM 등) 제품은 국가 공공기관에 도입할 수 있습니다.

[표 2-13] 암호화가 주 기능인 정보보호시스템

제품군	CC인증	검증필 암호모듈 탑재
▪ DB 암호화 ▪ 통합인증(SSO) ▪ 문서 암호화(DRM 등)	가능 (2017.8.18.부)	필수
▪ 메일 암호화 ▪ 구간 암호화 ▪ 디스크 파일 암호화 ▪ 하드웨어 보안 토큰 ▪ 기타 암호화	해당사항 없음	

다. 제안요청서 표준 템플릿 활용

○ 본 가이드에서 제공하는 정보보호 제품 - 시스템 장비 구성 요구기능과 보안 요구기능은 다음의 표와 같습니다.

[표 2=14] 정보보호 제품 요구사항 목록

Level 1	Level 2		Level 3	
ECR 시스템 장비 구성 요구기능	P/M	보안 관리(Protection & Management) 장비 구성	ACM	접근통제
			PAM	암호/인증관리
			DCS	데이터·콘텐츠 보안
			NWS	네트워크 보안
			MOS	모바일 보안
			BIO	바이오인식
			SSM	보안운영
	D/M	침입 탐지(Detection & Monitor) 장비 구성	PDS	침입방지 및 탐지
			MON	모니터링
	R/R	대응 및 복구(Response & Recovery) 장비 구성	IVM	침해관리
			RNB	복구 및 백업
	EEC	기타 장비 구성	IMR	영상 기록
			IRP	영상 기록 보호
SFR 보안기능 요구기능	P/M	보안 관리(Protection & Management) 기능	ACM	접근통제
			PAM	암호/인증관리
			DCS	데이터·콘텐츠 보안
			NWS	네트워크 보안
			MOS	모바일 보안
			BIO	바이오인식
			SSM	보안운영
	D/M	침입 탐지(Detection & Monitor) 기능	PDS	침입방지 및 탐지
			MON	모니터링
	IAM	침해관리(infringement accident management) 기능	IAR	침해 대응
			RNB	복구 및 백업 (Recovery & backup)
	ESF	기타 기능 구성	IMR	영상 기록
			IRP	영상 기록 보호

라. 작성 시 유의사항

○ 제안사가 하드웨어 또는 상용소프트웨어를 직접 제조하는 자가 아닐 경우, 제안사와 제조사 간 기술 또는 판매와 관련된 관계임을 입증할 수 있는 증명을 제안서에 포함하여야 합니다.

○ 공개소프트웨어 도입을 저해하는 비표준적인 특정기술 조건을 명시할 수 없으며, 특정 스펙을 명시하지 않아야 합니다.

작성 예시

요구사항 분류		시스템장비구성 요구사항
요구사항 고유번호		ECR-007
요구사항 명칭		스팸메일 차단 솔루션 도입
요구사항 상세설명	세부내용	ㅇ장비 수량: 1대 ㅇ장비 기능: 스팸메일 차단 ㅇ장비 성능 및 특징 - CPU: 6Core 이상 - Mem: 16GB 이상 - HDD: 2TB 이상 - 10/100/1000 BASE-TX 2포트 또는 1G BASE-SX 2포트 이상 - 국가정보원 CC 인증 제품(스팸메일차단 유형, 보안등급 EAL2 이상) - 메일서버 관리, 스팸메일관리, 감사로그관리, 통계 지원 - 메일서버로 수신되는 스팸메일 차단, 스팸메일서버에 일정기간 보관 기능 - 연/월/주/일 별로 스팸 및 메일 현황 통계 제공 - 도메인, 사용자, IP, 첨부파일, 확장자 등 검색 지원 - 기존 웹메일과 연동하여 개인별 스팸메일 차단/등록 - 불법적인 메일 릴레이 차단 기능 - 스팸메일엔진, 바이러스엔진, 필터엔진 등 자동업데이트 기능 - Dual Stack (IPv6) 지원 - 1,000 user 이상 라이선스 제공 - 접속 비밀번호 실패 횟수 설정 - 관리자 접속 IP 또는 MAC 제한 - 일정시간 후 자동 로그아웃 기능 - 기존 웹메일 사용자 정보 항목(연락처 등) 추가 및 관리 - 웹메일의 로그인 2단계 인증 변경 구현 및 지원 - 2단계 인증에 따른 기관메일 담당자 지정관리

4-2. 정보보호 서비스 요구사항

가. 기술 내용

○ 정보 자산을 보호하기 위하여 전반적인 정보보호 컨설팅과 마스터플랜 수립, 취약점 진단, 모의해킹, 개인정보영향평가 등을 통하여 정보보호시스템 구축 요건을 도출하기 위한 요구사항을 기술합니다.

○ 정보보호시스템에 대한 운영 및 보안관제를 위한 운영 대상 장비, 소프트웨어, 정보자산과 운영/관제 인력 근무조건 등의 요구사항을 기술합니다.

○ 정보보호 소프트웨어에 대한 일반 상용소프트웨어의 유지관리 요구사항 이외에 보안지속성 서비스를 위한 별도의 요구사항을 기술합니다.

○ 물리적인 침입탐지 및 비상 출동, 보안 교육 등의 요구사항을 기술합니다.

나. 기술 방법

○ 정보보호 컨설팅은 모든 정보 기술(IT) 자산과 조직에 일어날 수 있는 위험을 분석하고 이에 대한 대책을 수립함으로써 관리자와 조직이 그 대책을 실현할 수 있도록 지원하는 자문 서비스로서 다음과 같이 컨설팅 목적과 유형에 따라 구분하여 요구사항을 기술합니다.
- 정보보호 마스터플랜 수립
- 정보보호관리체계, 개인정보보호관리체계 인증 컨설팅
- 보안 취약점 진단 및 모의해킹
- 개인정보영향평가
- 정보보호 일반, 종합 컨설팅

○ 보안 관제는 원격관제와 파견관제로 구분할 수 있으며 24시간 근무 특성과 보안관제 서비스 유형 (기본 서비스, 분석 서비스, 진단서비스, 운영 서비스, 기획 서비스, 개발 서비스 등)을 구분하여 요구사항을 기술합니다.

○ 보안성 지속 서비스는 정보보호제품을 활용하여 정보의 훼손, 변조, 유출 등을 방지하기 위해 지속적으로 요구되는 기술 기반의 서비스로서 보안 업데이트, 보안정책관리, 위험/사고 분석, 보안성 인증효력 유지, 보안기술 자문 등의 세부 요구사항을 기술합니다.
- 보안성 지속 서비스는 안티바이러스(백신), 스팸차단 솔루션 등과 같이 라이선스 형태로도 계약 가능
- 사고 시 긴급 대응 등 특정 요구에 따라 추가 서비스 비용 발생

○ 정보자산 보호를 위하여 구축하는 정보보호시스템의 보안 기능 요구기능을 기술합니다.
- 인증 및 권한 보안 요구사항 : 목표 시스템 사용자 인증 및 계정 정보보호, 패스워드 암호화, 그리고 목표시스템의 기능 및 정보에 대한 접근 권한 요건을 기술
- UI 보안 요구사항 : 목표시스템의 화면에 권한이나 인증절차 없이 나타내는 개인정보, 소스코드에 개인정보가 노출되지 않도록 보안 요건 기술
- 데이터 보안 요구사항 : 목표시스템 및 테스트 DB에 보안이 필요한 필드 암·복호화, 데이터 접속 권한 등 데이터를 보호하기 위한 요구사항 기술
- 네트워크 보안 요구사항 : 네트워크 접근 통제, 네트워크 장비의 취약성 및 구성설정에 대한 보안 요구사항 등 통신을 위해 사용하는 장비 및 접근과 관련하여 요구사항을 기술
- 인터페이스 보안 요구사항 : 외부 정보시스템과 데이터를 송·수신할 때 데이터 암호화 및 로깅 등 보안에 대한 요건을 기술

○ 정보보호 컨설팅 및 보안관제, 정보보호시스템 구축 등에 적용되어야 하는 정보보안 및 개인정보보호 대책을 제시합니다.
- 정보보호 컨설팅 요구사항은 취약점 분석 평가, 정보보호관리체계(ISMS), 개인정보보호(PIMS, PIA), 기본·종합 컨설팅, 개발보안 컨설팅 등에 대한 세부 수행업무를 기술
- 보안관제는 원격관제, 파견관제, 하이브리드관제(원격+파견) 서비스 등의 기본 서비스와 보안관제 부가서비스(기획, 진단, 분석, 운영, 개별 서비스), 모의훈련 서비스(침해사고, DDoS, 악성메일(파일) 유입/전파 대응 등) 등을 선택적으로 기술
- 개인정보 보호법 제33조 및 동법 시행령 제35조에 따른 개인정보 영향평가 대상 여부 검토 (민감정보, 고유식별정보 등)
  ※ (개인정보영향평가 사이트 : www.pia.go.kr)
- 개인정보영향평가 기관이 '개인정보 영향평가 수행안내서', '개인정보 위험도 분석기준 및 해설서' 근간으로 평가한 개인정보영향평가 결과에 대해서는 주사업자가 개발 시 반영하도록 명시
- 개인정보 취급 시 준수해야 하는 공통법규(법률, 지침, 매뉴얼, 고시 등)와 사업의 특성에 따라 적용되는 관련법 등을 파악하여 적용대상 개인정보 관련 대책을 기술
  ※ '상용 정보보호시스템 보안성 검토지침(국가정보원)' 준수 여부 제시

○ 정보시스템 및 정보보호시스템 구축 시 소프트웨어 개발보안 (시큐어 코딩)관련 가이드를 준수하여 구축하도록 요구합니다.
- '행정기관 및 공공기관 정보시스템 구축·운영 지침(행정안전부)' 제50조(소프트웨어 개발보안 원칙)과 제53조(보안약점 진단절차)에 따라 소프트웨어 개발 보안을 적용하고 〈별표 3〉 소프트웨어 보안약점 기준을 사업자에게 준수 요구
- 정보시스템 감리를 실시할 경우 사업자가 보안약점을 제거하였는지 진단 요구

※ 개발 시 '소프트웨어 개발보안 가이드', 점검 시 '소프트웨어 보안약점 진단가이드'

- 소프트웨어 개발보안 가이드'에 따른 소스코드 보안성 확보를 위해 착수 단계 에서 표준 코딩스타일 정의 및 적절한 개발절차·개발방법론, 교육 계획 등을 제시토록 요구
- 소스코드 보안취약성을 자체 진단하고 제거하기 위한 방안 제시 요구 (진단도구, 진단 전문인력 활용, 진단환경, 진단회수, 진단·조치방안 등)

○ 보안 요구사항은 정보 자산의 기밀성과 무결성을 확보하기 위해 목표 시스템의 데이터 및 기능, 운영 접근을 통제하기 위한 요구사항을 기술합니다.

○ 목표시스템 또는 목표시스템의 사용, 목표시스템이 사용하거나 생성하는 데이터 보호에 영향을 미치는 보안(인증, 접근 통제 등), 무결성, 개인정보 보호에 대한 요건이나 제약사항을 기술합니다.

○ 프로젝트 결과 산출물(시스템)에 반영되는 보안사항에 한정하여 보안요구사항을 정의합니다. 즉, 사업수행과 관련하여 요구되는 보안사항은 보안요구 사항이 아닌 프로젝트 관리 요구사항 유형으로 보아야 합니다.

다. 제안요청서 표준 템플릿 활용

○ 본 가이드에서 제공하는 정보보호 서비스 요구사항은 정보보안 컨설팅, 보안성 지속 서비스, 보안관제, SI 서비스사업 요구사항, 물리보안 및 기타 정보보호 서비스 등으로 구분하고 있습니다.

[표 2-15] 정보보호 서비스 요구사항 목록

Level 1		Level 2	
TSC	정보 보안 컨설팅	GSC	보안 컨설팅 공통 일반 요구사항
		ISMS	정보보호관리체계 인증 요구사항
		PIM	개인정보보호 관리 체계 구축 요구사항
		PIA	개인정보 영향평가 요구사항(추가)
		ISMP	정보보호마스터플랜수립
		EDC	교육 체계 및 컨텐츠 개발 요구사항
		PTR	모의 해킹 요구사항
		VSR	보안 취약점 진단 요구사항
		SCG	솔루션 컨설팅 요구사항
		AMR	접근 관리 요구사항
		AUT	정보 감사
PSS	보안성지속 서비스	(ZZZ)	보안시스템 운영 및 유지관리 요구사항

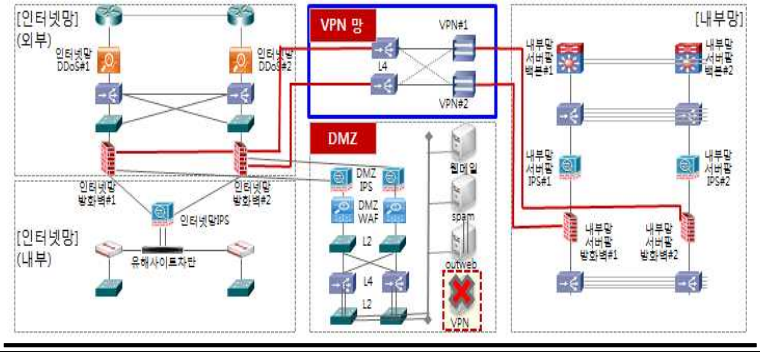
Level 1		Level 2	
		OMT	시스템 운영 및 유지 관리 대상
		HLD	시스템 유지 관리 서비스 데스크운영
SMS	보안관제	BCS	원격·파견관제 서비스 요구사항
		SOS	보안관제 부가서비스
SIM	SI 서비스 사업 요구사항	HRM	조직 및 인력관리
		SAA	시스템 분석·설계
		INS	시스템 장비 설치
		SYT	시스템 테스트
		PRI	시스템 유지 관리를 위한 예방 점검 및 보안 관리
PEI	물리보안 및 기타 정보보호 서비스	VMS	영상보안
		SPS	출동보안
		EDM	정보보안 및 개인정보보호 교육
		ICS	기타 서비스

라. 작성 시 유의사항

○ 정보보호 서비스 요구사항은 정보보호 수행 활동과 관련된 상세 요구사항을 작성하는 것으로 수행 결과물과 완료 조건을 파악할 수 있도록 작성합니다. 또한 해당 요구사항을 수행함에 있어서 적용되어야 하는 법령, 지침 등에 대해서도 기재하여 정보보호 서비스의 결과가 관계 법령을 준수하여 수행될 수 있도록 해야 합니다.

작성 예시

요구사항 고유번호		SFR-001
요구사항 명칭		VPN망 분리 구성
요구사항 분류		기능 요구사항
요구사항 상세 설명	**세부 내용**	ㅇ 공사의 업무환경에 최적화된 VPN망 분리 구성 방안 제시 및 적용 ㅇ 국가정보원 및 금융위원회 가이드라인 등 관련 법규 및 지침 준수 ㅇ 공사가 보유중인 VPN 장비(현재 운영 장비를 교체하기 위해 보유중인 장비)를 사용하여 독립된 영역으로 VPN망 구성 ※ 제안사 타 신규 VPN 장비 제안 가능 - 현 운영중인 장비의 설정 정보 등을 신규 장비로 이관 작업 필요 ㅇ 원격지 사용자와 내부 정보시스템의 통신을 안전하게 사용할 수 있도록 사용자와 SSL간 통신 패킷은 암호화 하여야 함 ㅇ 원격지 사용자의 접속 권한을 접속 서버 및 시간/요일/기간별 설정이 가능하여야 함 ㅇ 현 운영중인 장비에서 구현되는 모든 기본 기능 및 커스터마이징 기

		능(2-factor 인증, 사용자 로그인 실패 허용 횟수 5회 지정, 키보드보안, SMS 서버 연동 등)이 교체 장비에서 정상 운영되도록 구현 ㅇ 휴면계정 자동 차단 기능, 관리자페이지 접근 단말기 지정(IP/MAC) 등 보안강화를 위한 추가적인 기능 제공 ㅇ 신규 VPN 사용을 위한 인증서 발급 등 사용자 지원(유선 또는 원격 지원) **TO-BE(안)** 

※ 기존 제안요청서 사례는 정보보호 요구사항을 기능 요구사항으로 분류하여 작성된 사례임

○ 정보보호사업과 관련하여 요구사항 중 프로젝트 기밀성 요구사항은 프로젝트관리 요구사항의 유형으로 분류하였습니다. 이는 검사대상이 아닐 뿐만 아니라 사업이행과 관련한 항목으로서 실제 시스템에 구현되는 요건이 아닙니다.

5. 제안서 작성요령

제안서의 효력과 작성요령, 목차, 각 목차별 세부 작성 지침을 제시하여 제안사별 동일한 목차에 따라 작성하게 함으로써, 제안내용에 대한 비교 및 평가가 쉽도록 하고 제안요청내용을 충족하였는지 확인될 수 있도록 합니다.

가. 제안서의 효력

(1) 기술 내용

○ 제출된 제안서의 내용은 변경할 수 없으며, 계약체결 시 계약조건의 일부로 간주함을 기술합니다.

(2) 기술 방법

○ 제안서가 계약에 미치는 영향과 입찰 시 제출해야할 제안서와 관련서류에 대해 기술합니다.

작성 예시

❍ 제안요청서 및 제안서의 내용은 선정된 후 계약서에 명시되지 않더라도 계약서와 동일한 효력을 가진다.(단, 계약서에 명시한 경우에는 계약서 사항이 우선한다.)
❍ 공단은 필요 시 제안사에 대하여 추가 제안 또는 추가 자료를 요청할 수 있으며, 이에 따라 제출된 자료는 제안서와 동일한 효력을 가진다.
❍ 추가자료 요청 시 제안업체는 이에 성실히 임해야 하며 미제출시의 불이익은 제안업체가 책임을 진다.(제안서 검토 후 추후 통보)
❍ 이 제안과 관련하여 용어 또는 해석상의 견해차이 있을 경우 상호 협의하며, 의가 발생할 때에는 공단의 의견이 우선한다.
❍ 요구사항(규격)에 명시되지 않았으나, 본 사업 관련 요구사항을 충족시키는데 필수적인 부품(소프트웨어 솔루션 및 기능 포함)은 추가 비용 없이 반드시 제공되어야 한다.

나. 제안서 작성 지침 및 유의사항

(1) 기술 내용

○ 제안서 작성 시 준수해야할 규격(분량, 서식, 제출부수 등)을 제시(권고)하여 제안평가 시 효율적인 검토가 가능하도록 합니다.

(2) 기술 방법

○ 제안요청서에 포함되어야 할 제안서 규격에는 다음과 같은 정보가 포함될 수 있으나, 각 내용에 대해 강제하는 부분을 권고로 명시합니다.
- 제안서의 분량(페이지 수) : 사업규모 등을 고려하여 적정한 페이지 분량 제시
- 용지의 색깔 및 크기, 방향, 줄 간격, Font, 글자크기, 문단번호 양식 등
- 제출 서류의 원본, 사본의 여부와 제출부수, 제출서류와 관련된 제약사항 등

○ 제안서의 규격을 권고하고, 제안서에 포함되는 서류 중 서식이 있는 경우는 [별지서식]으로 포함하여 제안요청서에 안내합니다.

○ 제안서 평가 시 효율적인 검토를 위하여 제안서의 양식 및 규격이 통일되도록 기관의 정해진 제안서의 규격과 별지 서식을 제공합니다.

(3) 작성 시 유의사항

○ 제안서 작성지침 및 유의사항에 대해서 강제적 사항이 아닌 “권고사항” 및 “가급적” 용어를 사용하여 기술함으로써, 제안서 제출 시 매수 규격 등이 부적합할 경우 문제 발생 소지를 예방합니다.

작성 예시

❍ 제안서는 제시된 ‘별첨3. 제안 목차’ 순서대로 제안요구사항을 최대한 갖추어야 하며, 꼭 필요한 사항 위주로 간단명료하게 작성하여야 한다.
❍ 제안서는 목차에 의거하여 색인표를 부착하여야 한다.
❍ 제안개요에는 제안목적 및 범위를 명확하게 기술하고 타 제안업체에 비하여 차별적으로 비교우위에 있는 모든 사항들을 기술하여야 한다.
❍ 제안내용의 근거자료 및 참고자료 등을 따로 붙여야 한다.
❍ 제안서의 내용은 명확한 용어를 사용하여 표현하여야 하며, 계량화가 가능한 것은 계량화하여야 한다.
- 사용가능하다, 할 수 있다, 고려하고 있다 등과 같이 모호한 표현은 평가 시 불가능한 것으로 간주한다. 단, 발주기관의 요구에 의하여 입증자료를 제출받아 가능할 것으로 판단될 시에는 제안한 것으로 평가한다.

❍ 제안서는 A4 횡 방향작성을 원칙으로 하며, 부득이한 경우 A4 종 또는 기타 용지를 일부 사용할 수 있으며 책자로 제작 하여야 한다.
※ 온라인 평가의 경우에는 제안서 인쇄를 생략할 수 있음
❍ 핵심 투입인력에 대해서는 정보보호 제품, 정보보호 서비스 관련 전문인력을 지정하여 핵심인력 투입계획을 제출하여야 한다.
※ 핵심참여 인력별 참여 프로젝트, 경력(기간), 유사사업 참여실적을 기술
보안 전문인력에 대해서는 보안 관련 교육 이력 기술
❍ 제안서는 원본과 요약본으로 작성하며 제안서는 150장 내외, 기술평가항목별 제안 요약서 30장 이내로 작성하여야 한다.

다. 제안서 목차

(1) 기술 내용

○ 제안서를 작성하기 위한 목차를 제시합니다.

(2) 기술 방법

○ 제안사별로 목차를 통일하여 비교 검증 평가가 용이하게 하고 요구사항을 충족하였는지 확인하기 위하여 제안서 목차를 기술합니다.

○ 제안서의 목차는 사업유형을 고려하여 조정이 가능합니다.

(3) 작성 시 유의사항

○ 제안서의 목차는 사업유형별로 수정하여 사용할 수 있으며, 기술평가항목 및 제안요청사항과 일관성을 유지하도록 합니다.

작성 예시

작성항목	세부목차
Ⅰ. 제안개요	1. 목적 및 배경 2. 수행범위 3. 사업추진 전략 및 목표 4. 제안의 특징 및 장점 5. 기대효과
Ⅱ. 제안업체 일반	1. 일반현황 2. 재무현황 3. 조직 및 인력 4. 주요사업 내용 5. 유사분야 주요사업 실적
Ⅲ. 사업 수행방안	1. 제안범위 2. 보안관제 운영 방안 3. 침해사고 분석 및 대응방안 4. 정보보안컨설팅 수행 방안 5. 보고 및 산출물 방안 6. 예방활동 방안
Ⅳ. 사업관리부문	1. 수행 조직 및 업무분장 2. 사업관리 방안 3. 품질보증 및 사업관리 방안 4. 보안관리 5. 투입인력 및 이력사항

※ 제시된 제안목차를 기준으로 하고, 목차에 제시되지 않은 제안내용 및 제안서평가 관련 내용은 목차를 추가하거나 적절한 장절에 작성

6. 제안안내 사항

사업자 선정방식 및 입찰참가자격, 제안서 제출일정, 평가방법 등을 기술하여 제안사에게 입찰절차 및 방법을 제시하고 제안사가 최종 사업자로 선정될 때 까지 수행하여야 하는 내용을 기술합니다.

가. 입찰 방식

(1) 사업자 선정방식

(가)기술 내용

○ 사업자 선정방식의 기본 원칙을 작성합니다.

(나) 기술 방법

○ 국가(지방)계약법 시행령에 따라 지식기반사업(정보과학기술 등 집약도가 높은 지식을 이용한 사업)은 '공개경쟁 입찰방식과 협상에 의한 계약체결'을 우선적으로 적용함을 기재합니다.

작성 예시

❍ 중소기업자간 제한경쟁입찰/협상에 의한 방법/총액/직찰
※ "국가를 당사자로 하는 계약에 관한 법률 시행령 제43조", "소프트웨어산업 진흥법 제20조 제1항", "협상에 의한 계약체결기준(기획재정부계약예규 제114호)"

❍ 기술평가 90%, 가격평가 10%로 하고, 제안서 평가결과 기술능력평가 점수가 기술평가분야 배점한도(100점)의 85%(85점) 이상인 업체를 협상적격자로 선정하며, 기술·가격평가 합산점수 고득점 순위로 우선 협상대상자 순위를 준다.
- 협상대상자의 종합평점이 동일한 경우 기술평가 점수가 높은 업체에게 우선순위를 준다.
- 기술평가 점수에서도 동일한 경우에는 기술평가의 세부평가 항목 중 배점이 큰 항목에서 높은 점수를 얻은 업체를 선 순위자로 선정한다.

관련근거

♣ 국가를 당사자로 하는 계약에 관한 법률 시행령 제43조의 2(지식기반사업의 계약방법)
♣ 지방자치단체를 당사자로 하는 계약에 관한 법률 시행령 제44조(지식기반사업 등의 계약방법)

나. 입찰 참가자격 기준

(1) 경쟁입찰 참가자격 제시

(가) 기술 내용

○ 사업 성격에 따른 IT분야의 입찰 참가자격을 명시합니다.

(나) 기술 방법

○ 「등록된 종목·품목」에 한하여 교부받은 경쟁입찰 참가자격 등록증에 의하여 자격을 증명하도록 해당 자격을 명시합니다.

○ 정보보호사업인 경우 사업 유형에 따라 특정 분야 전문업체로 지정된 사업자이어야 함을 명시합니다.
- 정보보호 전문서비스 기업 (정보보호산업진흥법 제23조) : 주요정보통신기반시설의 취약점 분석 · 평가업무, 보호대책 수립업무 등
- 보안관제 전문업체 (국가사이버안전관리규정 제10조의2) : 보안관제센터 운영
- 개인정보영향평가 기관 (개인정보보호법 시행령 제37조) : 개인정보영향평가
- 정보보호준비도평가 기관 (정보보호산업진흥법 제12조) : 정보통신서비스 제공자의 정보보호 준비도 평가

○ 소프트웨어사업인 경우 소프트웨어 사업자 신고요령 제6조에 해당하는 신고분야를 명시합니다.
※ (종목) 1.컴퓨터관련 서비스사업, 2.패키지소프트웨어 개발·공급사업 3. 디지털콘텐츠 개발서비스 사업, 4.데이터베이스 제작 및 검색서비스사업 자로 등록한 자 이어야 함을 명시합니다.

작성 예시

① "국가를당사자로하는계약에관한법률"시행령 제12조(경쟁입찰의 참가자격) 및 시행규칙 제14조(입찰참가자격요건의 증명)의에 의한 유자격자로 기간 내 조달청전자입찰 이용자등록을 마친 자
② "국가를 당사자로 하는 계약에 관한 법률" 제27조 1항의 부정당업체로 지정되지 않은 자
③ "국가를 당사자로 하는 계약에 관한 법률" 시행령 제43조 6항에 따른 제안요청 사업설명회에 참석한 자
③ "①~③"의 입찰참가자격을 모두 충족하고, 아래와 같이 분담이행 방식의 공동수급체로 구성하여, ❶대표자의 분담율이 87%, ❷부사업자의 분담율을 13%로 구성한다. 단, 대표사업자는 2인 이하의 공동 수급체(공동이행방식)로 참여 가능
❶ 공동수급체 대표자 자격 … DB 암호화 분야
- 소프트웨어산업진흥법 제24조 및 동법시행령 제17조에 의하여 소프트웨어사업(컴퓨터

관련 서비스사업)의 신고를 필한 자로서 최근년도 결산신고가 완료된 사업자
※「소프트웨어산업 진흥법」에 따라 최근년도 결산신고된 SW사업자 신고확인서 제출 필수
- 소프트웨어산업 진흥법 제24조의2(중소소프트웨어사업자의 사업참여 지원) 및 대기업인 소프트웨어 사업자가 참여할 수 있는 사업금액의 하한(과학기술정보통신부 고시)에 따른 개별사업 예산 기준으로 중소기업자간 제한경쟁 실시
※ 단, 소프트웨어산업 진흥법 제24조의2제3항에 따라 상호출자제한기업집단에 속하는 회사는 사업금액과 관계없이 참여 불가
※ 상호출자제한집단에 속한 회사를 포함하여 대기업이 하수급인이 되는 도급계약 금지(대기업 하도급 금지) 다만 ①대기업에서 제조한 제품으로 국내에 총괄판매사가 없는 경우, ②과학기술정보통신부 장관이 지정한 정보보호 전문서비스 기업의 보안취약점 점검에 한하여 해당 대기업은 하도급 참여가능
- 도입 제품의 설치 공급이 가능한 업체로써 제조(공급)업체의 "정품공급인증 및 기술지원 협약서"를 체결 제출 가능한 업체

2 공동수급체 부사업자 … 정보보호 컨설팅 분야
- "정보보호산업의 진흥에 관한 법률" 제23조에 의거 과학기술정보통신부장관이 지정한 정보보호 전문서비스 기업

* 다만, 단일사업자가 1,2의 조건을 모두 충족하는 경우 단독입찰가능

※ 입찰마감일 기준으로 입찰참가자격 요건을 판단하며, 우선협상대상자가 된 경우 계약체결일까지 입찰참가자격을 유지하여야 함.

관련근거

♣국가를당사자로하는계약에관한법률시행령제12조(경쟁입찰의참가자격)
♣지방자치단체를당사자로하는계약에관한법률시행령제13조(입찰의참가자격)
♣정보보호산업 진흥에 관한 법률 제12조, 제23조
♣국가사이버안전관리규정 제10조의2
♣개인정보보호법 시행령 제37조
♣소프트웨어산업진흥법제24조 및 소프트웨어사업자신고요령

(다) 사업유형별 입찰참가 자격기준

[표 2-16] 정보보호사업 유형별 입찰 참가자격 제한

구분	정보보호 사업 유형		입찰참가 자격
정보보호제품	정보보호 제품 도입 · 구축 사업		
	물리보안 제품 도입 · 설치 사업		
정보보호서비스	정보보안 컨설팅 사업	취약점 분석평가	정보보호 전문 서비스 기업
		정보보호관리체계	
		개인정보보호	
		개인정보영향평가	개인정보 영향평가기관
		기본 · 종합 컨설팅	
		개발보안컨설팅	
	보안성지속서비스 사업		

구분	정보보호 사업 유형	입찰참가 자격
	보안관제 사업	보안관제 전문기업
	정보보호시스템 개발 사업	
	물리보안 서비스 사업	

(2) 대기업 참여제한 명시

(가) 기술 내용

○ 사업금액에 따라 대상기준(매출액 등)으로 대기업인 소프트웨어사업자의 참여를 제한함을 명시하여야 합니다.

○ 상호출자제한기업집단 소속기업*의 참여 제한사항을 명시합니다.
※ 공정거래위원회 공고(상호출자제한 기업집단 등의 소속회사 변동현황)에 따름

(나) 기술 방법

○ 사업금액(추정가격 + VAT, 40억·80억 이상) 기준에 따라 대기업인 소프트웨어 사업자의 참여를 제한함을 명시합니다.
※ 대기업인 소프트웨어사업자의 참여가능 사업금액의 하한

대상 업체	사업금액의 하한
매출액 8천억원 이상인 대기업	80억원 이상
매출액 8천억원 미만인 대기업	40억원 이상
중소기업이 산업발전법 제10조의2 제1항의 '중견기업' ※	20억원 이상

.

※ 중소기업이 대기업이 된지 5년 이내의 기업, 상호출자제한기업집단에 속하지 않는 중견기업 (증빙서류 : 한국소프트웨어산업협회 소프트웨어 신고확인서)
※ 상호출자제한기업집단 소속기업은 사업금액에 관계없이 원칙적으로 공공소프트웨어 사업에 참여제한 (소프트웨어산업진흥법 제24조의2 제3항)

○ 해당사업이「대기업의 공공소프트웨어 사업자 참여제한 예외사업 (과학기술정보통신부)」인 경우 관련내용을 기술합니다.

○ 소프트웨어사업 운영과 유지관리를 묶어 발주한 사업인 경우 대기업 참여제한 예외사업으로 인정되지 않음을 유의하여야 합니다.

○ 중소기업이「산업발전법」제10조의2 제1항의 '중견기업'에 해당하는 대기업이 된 경우 그 사유가 발생한 날로부터 5년이 경과되지 않을 시에는 사업금액의 하한을 20억원 이상으로 합니다.

작성 예시

o 「소프트웨어산업진흥법」제24조의2 및 「대기업인 소프트웨어 사업자가 참여할 수 있는 사업금액의 하한」(과학기술정보통신부 고시)을 준수하여야 하고, 이에 따라 추정가격 20억원 미만의 사업인 경우 중소기업자만이 입찰참가 가능

〈대기업인 소프트웨어사업자의 참여가능 사업금액의 하한〉

대상업체	사업금액의 하한
매출액 8천억원 이상인 대기업	80억원 이상
매출액 8천억원 미만인 대기업	40억원 이상

관련근거

♣소프트웨어산업진흥법 제24조의2 제3항 (중소 소프트웨어 사업자의 사업참여 지원)

♣대기업인 소프트웨어 사업자가 참여할 수 있는 사업 금액의 하한

♣상호출자 제한 기업집단 소속 회사의 중요사항 공시에 관한 규정

(3) 부정당업자의 입찰참가자격 제한

(가) 기술 내용

○ 국가 및 지방자치단체를 당사자로 하는 계약에 관한 법률에 따라 부정당업자의 입찰참가자격 제한사항을 기술합니다.

(나) 기술 방법

○ 「공정한 집행 또는 계약의 적정한 이행을 해칠 염려가 있거나 그 밖에 입찰에 참가시키는 것이 부적합하다고 인정되는 계약상대자 또는 입찰자(계약상대자 또는 입찰자의 대리인·지배인, 그 밖의 사용인 포함. 이하 '부정당업자'라 함)는 입찰참가자격이 제한됨을 기술합니다.

작성 예시

o 공사 자산관리 및 계약세칙 제39조(부정당업자의 입찰참가자격 제한)에 의한 계약당사자 또는 입찰자는 일정기간 동안의 입찰참가자격 제한조치를 받게 되며, 정부, 지방자치단체, 정부투자기관 또는 금융기관에서 부정당업자로 제재중인 자도 동일함

관련근거

♣ 국가를 당사자로하는 계약에 관한 법률 제27조 및 시행령 제 76조 (부정당업자의 입찰참가자격 제한)
♣ 지방자치단체를 당사자로하는 계약에 관한 법률 제31조 및 시행령 제 92조 (부정당업자의 입찰참가자격 제한)

(4) 공동수급 허용 및 제한

(가) 기술 내용

○ 정보보보 사업에 대한 공동계약 허용여부를 명시합니다.

(나) 기술 방법

○ 공동계약이 부적절한 경우 이외에는 가능한 공동계약 허용함을 기술합니다.
- 불허 시에는 사유를 제안요청서 상에 명시합니다.

○ 매출액 8천억원 이상인 대기업간 공동수급은 제한함을 명시해야 합니다.
- 대기업 참여대상 사업에 대하여 매출액 8천억 이상인 대기업간 공동수급은 제한한다는 내용을 명시

○ 공동수급체 구성
- 2인 이상 5인 이하(발주기관과 협의하여 조정 가능)
- 최소지분율(단, 분담이행은 제외) : 국가는 10% 이상, 지방은 5% 이상
- 하도급 비율이 10% 이상인 경우 공동 수급으로 제안할 것을 권고

작성 예시

o 공동수급체(공동이행방식)를 구성하여 참여할 수 있으며, 공동수급체 구성은 기획재정부 계약예규 “공동계약운영요령”에 따라야 함
※ 공동도급의 경우 계약예규 “공동계약운용요령” 제9조에 의거 공동수급체는 5개 이내이고, 최소지분율은 10% 이상 이어야 함

관련근거

♣ 국가를 당사자로 하는 계약에 관한 법률 제25조(공동계약)
♣ 공동계약운용요령 제9조(공동수급체의 구성)
♣ 지방자치단체를 당사자로 하는 계약에 관한 법률 제29조(공동계약)
♣ 지방자치단체 공동계약 운용요령 제2절(공동수급체의 구성 및 적용범위)

(5) 중소기업간 경쟁제도

(가) 기술 내용

○ 중소기업자 간 경쟁제품인 경우 사업 분야에 해당하는 직접생산증명서를 제출해야함을 명시합니다.

(나) 기술 방법

○ 중소기업제품 구매촉진 및 판로지원에 관한 법률 제9조에 따라 중소기업자간 경쟁의 방법으로 제품조달계약을 체결 시 주요 생산증명서 분야를 기술합니다.

- 전산업무(소프트웨어개발) : 정보시스템개발서비스, 패키지소프트웨어 개발 및 도입서비스, 소프트웨어유지 및 지원서비스, 정보시스템유지관리서비스, 운영 위탁서비스, 인터넷지원개발서비스, 정보인프라구축서비스 (7개 세부품목)
- 자료처리업무 : 데이터처리서비스

※ 추정가격이 1억원 이상(2억3천만 미만)으로서「국가를 당사자로 하는 계약에 관한 법률」제4조제1항에 따라 기획재정부장관이 고시하는 금액 미만인 물품 또는 용역을 조달하려는 경우에는 중소기업자 간 제한경쟁입찰에 따라 조달 계약을 체결함

※ 국가를 당사자로 하는 계약에 관한법률 제4조제1항의 규정에 의한 장관이 정하여 고시하는 금액(기획재정부)을 확인해야함

작성 예시

ㅇ 중소기업제품 구매촉진 및 판로지원에 관한 법률 제9조 및 동법 시행규칙 제5조에 의거, 직접생산확인증명서[전산업무(소프트웨어개발)-정보시스템 개발서비스]를 입찰마감일 전일까지 발급하여 소지한 업체

관련근거

♣ 중소기업제품 구매촉진 및 판로지원에 관한 법률 시행령 제2조의2(중소기업자와의 우선조달계약)
♣ 국가를 당사자로 하는 계약에 관한 법률 제4조제1항의 규정에 의한 장관이 정하여 고시하는 금액
♣ 중소기업제품 구매촉진 및 판로지원에 관한 법률 제9조(직접생산의 확인 등)

나. 제안서 평가방법

(1) 기술 내용

○ 제안서를 공정하고 객관적으로 평가하기 위한 기준을 제시합니다.
- 사업자 선정 시 우수한 역량과 인력, 사업을 성공적으로 수행하기 위한 제안 내용을 제안한 업체가 선정될 수 있도록 세부 평가방법을 제시
- 제안서 제출에 관한 사항, 평가기준 및 평가방법, 기술평가 진행세부사항, 평가결과 공개, 협상적격자 선정방식 등

(2) 기술 방법

(가) 제안서 제출에 관한 사항

○ 사업예산별 평가위원 수에 맞는 제안서 제출부수, 제안요약서·발표자료, 전자파일(CD, USB) 등 제출여부를 기술합니다.
- 정보보호사업의 경우에는 평가위원장을 포함하여 10인 이내의 위원으로 구성
- 공공 정보화사업의 경우에는 사업 예산규모에 따라 제안서 평가위원의 수를 선택하여 구성

※ 사업예산액별 제안서 평가위원 수

사업 예산액	1억원 미만	1억원 이상~ 50억원 미만	50억원 이상
위원수	8명 이하	8명 이상	9명 이상

(나) 평가기준 및 평가방법

○ 정보보호 사업은 2단계 경쟁 입찰, 최저가입찰(적격심사), 협상에 의한 계약체결. 품질 등에 의한 낙찰자 결정 등을 선택하여 적용할 수 있습니다.

관련근거

♣ 「국가를 당사자로 하는 계약에 관한 법률 시행령」(이하 "국가계약령"이라 한다) 제18조 및 「지방자치단체를 당사자로 하는 계약에 관한 법률 시행령」(이하 "지방계약령"이라 한다) 제18조에 따른 규격 또는 기술입찰서 심사
♣ 국가계약령 제42조 및 지방계약령 제42조에 따른 계약이행능력 심사
♣ 국가계약령 제43조 및 제43조의2, 지방계약령 제43조 및 제44조에 따른 제안서의 평가
♣ 국가계약령 제44조 및 지방계약령 제45조에 따른 품질 등의 심사

○ 공공 정보화사업은 지식기반사업으로 분류하여 협상에 의한 계약체결 방식을 우선 적용하도록 하고 있습니다.

○ 정량적(객관적)·정성적(주관적) 평가 주체, 기술·가격평가에 관한 방법· 평가기준·비율을 기술합니다.

※ 기술평가는 조달청 평가대행 요청 시 정량적 평가부분은 발주기관이 수행하여 결과를 조달청에 통보하도록 합니다.

(다) 기술평가진행 세부사항

○ 제안서 평가 시 기술능력과 입찰가격을 종합적으로 평가하며, 이때 기술 능력 평가의 비율은 90%로 정합니다. 다만 하드웨어 비중이 50% 이상인 경우, 1억 미만 개발사업 등은 기술능력평가 배점한도를 80%이상으로 할 수 있습니다.

- 적용대상 : 소프트웨어사업의 계약 시 협상에 의한 계약체결방식을 적용한 사업
- 행정기관 및 공공기관 정보시스템 구축·운영 지침 (행정안전부) 제18조

(라) 평가결과 공개

○ 계약집행자는 제안서 평가 종료 후 3일 이내에 국가종합전자조달시스템을 이용하여 평가위원별 점수를 공개하되, 평가위원 실명은 비공개로 합니다.

○ 국가계약법 적용기관 : 기술능력평가분야 배점한도의 85% 이상인 자, 예정가격 초과 여부와 무관

○ 지방계약법 적용기관 : 기술능력평가분야 배점한도의 85% 이상인 자, 예정가격 초과자 제외

(마) 협상적격자 선정방식

○ 적용대상 : 협상에 의한 계약체결방식을 적용한 사업

- 국가계약법 적용기관 : 기술능력평가분야 배점한도의 85% 이상인 자, 예정가격 초과 여부와 무관
- 지방계약법 적용기관 : 기술능력평가분야 배점한도의 85% 이상인 자, 예정가격 초과자 제외

(3) 작성 시 유의사항

○ 지방계약법이 적용되는 경우 정량적 평가에 제안사 지역에 따른 배점항목은 포함할 수 없습니다.

※ 정량적 평가분야(계량화) 평가항목의 배점한도는 20점이며, 평가항목은 수행경험, 경영상태, 기술인력 보유상태, 신인도 등을 대상으로 평가합니다.

○ 공동계약인 경우 실적·기술능력·경영상태·신인도 평가 방법은 다음과 같습니다.

- 실적 : 공동수급체 구성원별로 각각의 실적에 지분율을 곱하여 산정한 후 이를 합산하여 산정

※ 10억 만점 : A(15억)×80% + B(5억)×20% = 12억 + 4억 = 16억 ☞ 평가점수 산출

※ 분담이행일 경우는 각각의 이행실적 평가점수에 분담비율을 곱한 후 합산하여 산정

- 기술능력·경영상태·신인도 : 공동수급체를 구성원별로 각각 산출한 점수에 출자비율 또는 분담비율을 곱하여 합산, 감점 시 해당 감점점수에 해당업체 출자비율 또는 분담비율을 곱한 점수를 감점합니다.

※【조달청 일반용역 적격심사 세부기준 (조달청)】

○ 실적에 대한 평가는 당해 사업예산 범위를 초과하지 못합니다.

○ 실적 인정 범위는 공공기관 및 민간실적까지 인정해야 하며, 특정 기관 또는 특정 지역의 실적만 인정할 수 없습니다.

작성 예시

❍ 제안서 평가 원칙

- 접수된 제안서에 대한 기술(규격)평가는 제안서 평가위원회 별도 계획에 의거 실시되며, 이에 대하여 제안사는 이의를 제기할 수 없다.
- 제출된 제안서를 기초로 제안서 평가기준에 명시된 부문별 제반 평가 요소에 대해 제안요청서의 요구한 요건, 수량 및 조건 등의 적합 여부를 평가한다.
- 제안 평가회에 참여하지 않은 업체는 본 사업에 참여할 의사가 없는 것으로 간주하여 기술평가에서 제외한다.
- 참가자격 등 각종 증빙서류를 허위로 기재하거나 입찰기한 내 제출하지 못하는 경우에는 계약 무효가 될 수 있다.
- 제안내용 중 “가능하다”, “동의한다”, “고려한다” 등의 표현은 불가능한 것으로 평가한다. 단, 공단의 요구에 의하여 입증자료를 제출받아 가능할 것으로 판단될 시는 제안한 것으

로 평가한다.

❍ 기술평가 방법

- 각 항목별 평가배점과 방법은 “기술성평가 기준”에 의한다.
- 각 평가위원의 평가점수 중 최고점수와 최저점수를 제외한 나머지 점수를 산술평균한 점수를 90점 만점으로 환산하며, 기술능력평가 분야 배점한도의 85% 이상인 자를 협상적격자로 선정

❍ 가격평가 방법

- “기획재정부 계약 예규 7. 협상에 의한 계약체결 기준” 및 “행정안전부 고시, 행정기관 및 공공기관 정보시스템 구축·운영 지침”에 의한 가격 평가(10점)

❍ 우선협상대상자 선정 및 계약 체결

- 협상대상자 중 기술평가점수와 가격평가점수를 합한 점수가 고득점인 순위로 우선협상대상 순위 부여
- 협상대상자의 종합평점이 동일한 경우 기술평가점수가 높은 업체에게 우선순위를 부여
- 기술평가점수에서도 동일한 경우에는 기술평가의 세부평가 항목 중 배점이 큰 항목에서 높은 점수를 얻은 업체를 선 순위자로 선정

관련근거

♣ 협상에 의한 계약 제안서평가 세부기준 제6조(평가기관 및 평가방법 등의 공개), 제9조(제안서의 평가항목 및 배점한도), 제16조(제안서 평가결과 공개)
♣ 협상에 의한 계약체결기준 제7조(제안서의 평가), 제8조(협상적격자 및 협상순위의 선정)
♣ 행정기관 및 공공기관 정보시스템 구축 · 운영 지침 제18조(평가배점)
♣ 협상에 의한 계약 제안서평가 세부기준

다. 기술성 평가기준

(1) 기술 내용

○ 기술성 평가기준은 협상에 의한 계약체결 기준 등을 준용하여 평가항목 및 배점을 조정(30점내)하여 기준을 제시합니다.

(2) 기술 방법

○ 정보보호사업은 정보보호 제품/서비스 사업의 특성에 따라 평가항목과 배점을 조정하여 적용합니다.

- 정보보호 서비스 사업유형의 경우에는 [별표 1] 기술제안서 평가항목 및 배점한도를 적용하고 기술 및 기능, 성능 및 품질 등의 평가부문/평가항목을 정보보호 서비스 요구사항으로 대체하여 제시합니다.

- 정보보호 서비스 사업의 세부 요구사항에 명시되지 않은 요구사항에 대해서는 평가 항목에서 제외합니다.
- 정보보호사업 수행 사업자가 다음 각 호의 어느 하나에 해당하는 경우에는 총 배점한도 이외에 2점이내의 가점을 부여 가능합니다.
  · ISMS, PIMS, ISO27001 인증기업, 정보보호 준비도 평가 우수등급(AA등급 이상)기업, '우수 정보보호기업'으로 지정된 기업
  · 정보보호산업진흥법 제13조 제2항에 따라 「정보보호공시」를 이행한 기업

[표 2-17] 정보보호사업 기술성 평가기준(안) - 정보보호사업 공통

평가부문	평가항목	배점
전략 및 방법론	사업 이해도	
	추진전략	
	적용기술	
	표준 프레임워크 적용	
	방법론	
	정보보호 전문성	가점
기술 및 기능	시스템 장비 구성 요구사항	
	보안 기능 요구사항	
	정보보안 컨설팅 요구사항	
	보안성 지속 서비스 요구사항	
	보안관제 요구사항	
	정보보호시스템 개발 요구사항	
	물리보안 및 기타 정보보호 서비스 요구사항	
	제약 사항	
성능 및 품질	자산관리 기능 요구사항	
	품질 요구사항	
	성능 요구사항	
	테스트 요구사항	
	데이터 요구사항	
	인터페이스 요구사항	
	제품컨설팅 요구사항	
프로젝트 관리	관리 방법론	
	일정계획	
	개발 장비	
프로젝트 지원	품질보증	
	교육훈련 및 기술이전	
	유지관리	
	하자보수 계획	
	프로젝트 기밀성 유지	
	문제상황 대응	
상생협력 및 하도급계약 적정성	상생협력	
	하도급계약 적정성	
합 계		100

- 정보보호시스템 구축 사업에 대한 기술평가표를 작성함에 있어서는 사업 유형별 요구사항 매핑표를 참조하고 사업 내용을 검토하여 해당 사업에 적용되지 않은 요구사항을 평가항목에서 제외할 수 있습니다.
- 정보보호제품 사업유형의 경우에는 [별표 2] [별표 2] 상용소프트웨어 평가항목 및 배점한도를 적용하고 평가부문/평가항목을 정보보호제품 요구사항으로 대체하여 제시합니다.

[표 2-18] 정보보호사업 기술성 평가기준(안) - 정보보호제품

평가부문	평가항목	배점
보안 기능성	보안 기능구현 완전성	
	보안 기능구현 정확성	
	상호 운용성	
	암호모듈 검증	
	국정원 CC인증 규격 준수	
사용성	기능학습 용이성	
	입출력 데이터 이해도	
	사용자 인터페이스 조정가능성	
	사용자 인터페이스 일관성	
	진행상태 파악 용이성	
	운영절차 조정 가능성	
이식성	운영환경 적합성	
	설치제거 용이성	
	하위호환성	
효율성	반응시간	
	자원사용률	
	처리율	
유지 관리성	문제진단/해결 지원	
	환경설정변경 가능성	
	업데이트 용이성	
	보안성 지속 서비스	
	백업/복구 용이성	
신뢰성	운용 안정성	
	장애복구 용이성	
	서비스 지속성	
	데이터 회복성	
공급업체 지원	유지관리 지원	
	하자보수 계획	
	교육훈련 지원	
	제품 신뢰도	
	직접생산여부	

- 정보보호시스템의 경우 정보보호산업진흥법 제17조 및 동법 시행령 제 10조에 따라 지정된 성능평가기관의 성능평가 결과서 및 기타 벤치마크테스트(BMT) 등 객관적인 인증결과를 평가에 우선 반영하거나, 평가 미실시 가능합니다.

○ 조달 요청 시 제안 평가항목, 배점한도의 조정을 요청할 수 있으나, 각 평가부문의 배점한도는 30점을 초과할 수 없으며, 공정하게 평가기준을 기술합니다.
※ 지방계약법 정량평가 항목의 배점 한도는 정량평가 전체 배점의 30%를 초과할 수 없음.

○ 사업유형별로 요구사항 유형이 다르고, 그에 따라 제안서 목차가 결정되며, 평가 부문이 결정되므로 이를 고려하여 평가기준을 작성합니다.

(3) 작성 시 유의사항

○ 정량적 기술평가는 발주기관에서 직접수행 하여야 하며, 다음과 같은 평가 항목 및 배점을 확인해야 합니다.

구분	평가 항목	배점 한도
정량적 평가분야 (계량화)	수행경험(실적), 경영상태 기술인력 보유상태, 신인도 등	
정성적 평가분야	기술·지식, 사업수행계획, 상생협력, 지원기술 등	

작성 예시

평가부문	평가항목	평 가 요 소	배점
제안개요 및 제안사항 (20점)	사업이해도	○ 제안의 배경 및 목적, 제안범위 및 추진전략 ○ 제안의 특징 및 장점, 기대효과 ○ 현행 보안관제 업무 이해도	10
	제안서 작성의 충실도	○ 사업수행을 위한 핵심 업무 분석의 적정성 ○ 제안요청서와의 적합성 및 작성방법 준수여부	10
사업수행 부문 (30점)	보안관제 수행방안	○ 보안관제 위탁운영 업무 수행방안의 적정성 ○ 사이버 침해대응 방안의 적정성 ○ 취약점 점검 및 모의 훈련 실시 방안의 적정성 ○ 정보시스템 모니터링 방안의 적정성 ○ 홈페이지 위변조 모니터링 방안의 적정성	10
	주요정보통신 기반시설 보안취약점 분석 평가	○ 주요기반시설 보안취약점 진단 평가 방안 ○ 주요기반시설 보호대책 수립 방안 ○ 기반시설 점검 후, 이행점검의 적절성 ○ 각 기반시설 운영담당자 보안교육 방안 ○ 기반시설 취약점 제거를 위한 기술지원 방안	10
	네트워크 및 정보보호시스템 보안강화	○ 네트워크 장비 보안설정 및 강화 방안 ○ 네트워크 장애 발생시 대응 조치방안 제시 ○ 정보보호시스템 운영관리 방안 제시	10

관련근거

♣ 지방자치단체 입찰 시 낙찰자 결정기준
♣ 협상에 의한 계약 제안서평가 세부기준

라. 제출 서류

(1) 기술 내용

○ 입찰에 참여하는 제안사가 제출하여야 하는 각종 서류를 기재합니다.

(2) 기술 방법

○ 입찰에 참여하는 제안업체는 요청되는 각종 서류를 제출하여야 합니다. 통상적으로는 공고문에 게시되므로 공고서에 따르는 것으로 기술합니다.

(3) 작성 시 유의사항

○ 보통 공고문에도 제시되므로 필요시 공고문에 상세하게 제시할 수 없는 내용에 대한 세부 규격을 명시합니다.

작성 예시

❍ 기술제안서 및 구비서류 : 공고서에 의함
❍ 가격입찰 부문 : 공고서에 의함(별봉 제출)
- 제안금액은 별도 양식에 의거 본 사업에 따른 비용을 구체적으로 제시하여야 한다.
- 제안금액은 항목별로 구분하여 제시하여야 한다.
- 제안금액에는 시스템 유지관리에 필요한 각 항목별 세부비용을 구분하여 제안토록 하고 금액에 대한 산출근거 및 기준을 부가가치세를 포함하여 구체적으로 제시하여야 한다.

마. 제안서 제출일정 및 방법

(1) 기술 내용

○ 제안서의 제출일정과 제출방법에 대해 기술합니다.

(2) 기술 방법

○ 입찰공고문에 제안서 제출일정 및 방법에 대해 기재되어 있기 때문에 제안요청서에는 공고문을 참조하도록 기재합니다.

(3) 작성 시 유의사항

○ 제출시간과 장소를 명확하게 제시하여 입찰참가 인정여부에 대한 논란이 발생되지 않도록 합니다.

작성 예시

❍ 제안서 제출기한 및 제출처 : 공고서에 의함
❍ 제출 방법
- 제안서는 등록서류를 갖추어 공문으로 직접 제출하며 우편접수는 인정하지 않는다.
- 제출기한 내 미제출시 제안의사가 없는 것으로 처리하며 제출된 제반 자료는 반환하지 않는다.
- 질문사항 등은 문서 또는 FAX에 의해 제출하고 전화 등의 문의는 법적 효력을 갖지 못한다.(질문사항은 제출마감일 3일전까지 가능)

※ 제안서를 포함하여 본 제안과 관련되어 제출된 모든 문서는 반환 및 공개하지 않으며, 본 제안과 관련된 일체의 소요비용은 입찰참가자의 부담으로 한다.

※ 총 사업예산이 20억 미만으로 제안서 보상을 하지 않음
(과학기술정보통신부 고시 "소프트웨어사업의 제안서 보상기준 등에 관한 운영규정" 제2조 제안서 보상 대상 사업)

관련근거

♣ 행정기관 및 공공기관 정보시스템 구축·운영 지침 제29조(제안서 등의 제출)

바. 제안요청 설명회

(1) 기술 내용

○ 발주 대상 사업에 대한 사업내용을 잠재적인 참여업체에게 설명하기 위한 사항을 기술합니다.

(2) 기술 방법

○ 제안요청서 설명회 실시여부와 실시할 경우 그 장소·일시 및 참가의무여부에 관한 사항을 기재합니다.

○ 협상에 의한 계약방식에서 동 설명회를 실시하지 않을 경우 담당자 연락처 (유·무선 전화, 이메일, 연락 가능한 시간 등)를 반드시 기술합니다.

(3) 작성 시 유의사항

○ 제안요청 설명회의 참석 여부가 입찰참가자격 요건일 경우 제안요청서에 명확하게 기재하여야 합니다.
○ 제안요청 설명회를 실시하지 않을 경우에도 실시하지 않음을 기술합니다.

작성 예시

1) 제안요청 설명회 : 제안요청서로 갈음함
2) 제안 발표
   ❍ 일시 및 장소 : 제안서 접수 후 별도 통보
3) 문의처

관련근거

♣ 행정기관 및 공공기관 정보시스템 구축·운영 지침 제28조(제안요청 설명회 개최)

사. 제안설명회 개최

(1) 기술 내용

○ 제안설명회(기술평가) 개최 내용 및 유의사항을 기술합니다.

(2) 기술 방법

○ 정보시스템 구축운영지침에 반드시 실무책임자(PM)이 발표하도록 규정되어 있으므로, 제안설명회를 실시하는 경우에는 PM이 발표하도록 기재하여야 합니다.

○ 제안설명회의 일자, 발표순서 등의 내용은 공고문에 기술하고, 평가기관, 유의사항 등은 제안요청서에 기술합니다.

(3) 작성 시 유의사항

○ 제안설명회를 개최하는 경우 제안 설명은 제안사(주사업자)의 PM이 직접 발표하여야 하며, PM이 발표하지 않을 경우 발표 없이 제안서에 대한 서면 평가로만 진행합니다. 발표내용이 제안서와 상이한 사항이 있는 경우 이를 별도로 명기하여야 합니다.

작성 예시

❍ 제안서 내용의 검토를 위해 추후 발주기관이 지정하는 장소에서 제안서와 관련된 설명회를 실시할 수 있다.

❍ 제안 발표는 제안사의 사업수행 PM이 직접 설명하여야 하며 제안업체, 설명방법 및 일정은 공고서를 참조한다.

❍ 발주기관은 제안평가일에 제안발표자가 제안사의 PM임을 입증토록 요청할 수 있으며, 제안사는 이에 응해야 한다.

❍ 제안 발표 시간은 한 업체당 발표 20분, 질의응답 20분을 기준으로 하고 제안평가회 참석 인원은 각 제안사당 5명 이내로 하며 제안 발표에 필요한 장비 등은 제안업체에서 직접 설치 사용할 수 있으며, 제안발표 자료는 별도로 작성하여 제안발표일에 제출할 수 있다.

❍ 제안업체는 전담사업자 선정과 관련한 제안평가회에서 논의·답변 및 제안한 내용에 대해서도 제안서와 동일한 법적인 효력을 가지며, 제안평가회 불참 시 이로 인하여 제안서 평가에서 발생할 수 있는 불이익을 감수해야 한다.

관련근거

♣ 행정기관 및 공공기관 정보시스템 구축·운영 지침 제20조(제안서 발표)

아. 입찰 시 유의사항

(1) 기술 내용

○ 당해 사업의 입찰에 참여하는 업체가 입찰 및 계약추진과정, 사업을 추진하면서 유의해야 할 사항에 대해 기술합니다.

(2) 기술 방법

○ 입찰에 참여하는 제안업체가 입찰(계약) 추진과정에서 반드시 확인할 수 있도록 관련 유의사항을 기술합니다.

(3) 작성 시 유의사항

○ 입찰시 최신의 법제도 및 관련근거를 확인하여 기술하되 불필요한 내용은 제외합니다.

작성 예시

1) 제출된 제안서는 일체 반환하지 않으며, 본 제안과 관련된 일체의 소요 비용은 입찰 참가자의 부담으로 하며, 제안서 보상비는 지급하지 않는다.
2) 제출된 제안서에 기재된 내용은 사실과 일치하여야 하며, 발주기관이 요구하지 않는 한 수정, 추가 또는 대체할 수 없다.
3) 발주기관은 제안서 평가 이전에 사전 열람을 실시할 수 있으며, 공정하고 명확한 평가를 위하여 객관적이고 정량적 자료를 종합하여 평가위원에게 제시할 수 있다.
4) 제안내용에 대한 확인을 위하여 추가 자료요청 또는 현지 실사를 할 수 있으며, 입찰 참가자는 이에 응하여야 한다.
5) 발주기관은 제안서의 내용이 사실과 다른 경우 해당 제안사를 협상대상에서 제외할 수 있다.
6) 공동수급 구성원을 변경할 수 없다.
7) 제안서 기재된 인력은 자사인력(공동수급구성원)으로 구성하여야 한다.
   ❍ 채용예정인력인 경우에는 별도로 이를 명기하고, 계약체결 전까지 채용을 완료하여야 한다.
   ❍ 적법한 파견근로자는 자사인력으로 간주하나, 원 소속사를 반드시 명기하여야 한다.
   ❍ 공동수급구성원 소속 외의 인력은 하도급으로 간주하며, 주관기관의 승인을 얻지 못할 경우에는 공동수급구성원의 자사인력으로 대체하여야 한다.
   ※ 단, H/W 및 상용S/W, 패키지 등의 서비스 지원인력, 외부 자문인력 등은 제안서에 명기하지 말 것 (참여인력에서 제외)
8) 본 사업의 수행에 필요한 모든 비용은 가격입찰금액에 포함하여야 한다.
9) 제안요청서 및 입찰공고 등에 포함되지 않은 사항은 "국가를 당사자로 하는 계약에 관한 법률", "협상에 의한 계약 체결 기준", "공동계약 운용요령" 등 국가계약관련 법령을 준용한다.

관련근거

♣ 국가를 당사자로 하는 계약에 관한 법률
♣ 협상에 의한 계약 체결 기준
♣ 공동계약 운용요령

차. 붙임 서식

(1) 기술 내용

- 붙임서식1호 : 일반현황 및 연혁
- 붙임서식2호 : 자본금 및 매출액(최근 3년간)
- 붙임서식3호 : 핵심 참여인력 이력사항
- 붙임서식4호 : 기술적용계획표

- 붙임서식5호 : 하도급 대금지급 비율 명세서
- 붙임서식6호 : 정보보호사업 하도급 계약승인 신청서

(2) 기술 방법

○ 제안서 작성 및 서류제출 시 업체의 서류준비를 최소화하도록 권장합니다. 각 기관에서 개별적으로 양식을 정의하여 발주하고 있으나, 서류의 양식도 표준화되어 있으므로, 제시된 양식의 사용을 권장합니다.

(3) 작성 시 유의사항

○ [붙임서식]은 가능한 표준화 서식을 활용하여 제안업체의 부담을 줄여줄 필요가 있습니다.

○ 특히, 사업실적증명서의 경우 사업발주기관에 직접 방문하여 발급받아야 하는데, 사업수행 당시의 담당자가 인사이동이 되어 부재한 경우에는 사업내용 확인 등에 따라 절차 및 기간이 많이 소요되므로 업체의 불편이 있으므로 가능한 제시된 표준양식을 사용하여 제안업체의 부담을 줄여줄 필요가 있습니다.

7. 기타 사항

위에서 기술하지 않은 사업 추진을 위해 필요한 기타 사항들을 제시함
- 분리발주, 특허권 및 저작권 보호, 작업장소 상호협의 결정, 하자담보 등

가. 소프트웨어 분리발주 제도 준수

(1) 기술 내용

○ 5억 원 이상 사업에서 5천만 원 이상 소프트웨어 구매의 경우, 분리해서 발주해야 하며 관련 내용을 명시합니다.

(2) 기술 방법

○ 분리발주 대상 소프트웨어를 확인하고 기술합니다.
※ 품질인증(GS인증) 제품, 행정업무용 소프트웨어 선정 제품, 정보보호시스템 인증(CC인증) 제품, 국가정보원 검증 또는 지정 제품, 신제품인증(NEP) 제품, 신기술인증(NET) 제품

※ 분리발주 대상 소프트웨어가 나라장터 종합쇼핑몰에 등록된 경우「조달사업에 관한 법률」 제5조의2 및 같은 법 시행령 제9조의3에 따라 쇼핑몰 제품을 우선 구매하여야 한다.

○ 분리발주 하지 아니하는 경우 그 사유를 제안요청서 및 공고문에 명시합니다.

작성 예시

○ **도입 SW 내역**

품명	규격	수량
DB 암호화 SW	• DB 암호화 SW 및 라이센스 - 34개 업무 시스템	496 Core
Oracle 업그레이드	• Oracle DBMS 11g 업그레이드 - 16개 업무 시스템	121 Core

※ 분리발주 대상 S/W 품목별 제외사유서 [별첨1] 참조

관련근거

♣ 소프트웨어산업진흥법 제20조(국가기관 등의 소프트웨어사업 계약)
제84조(소프트웨어사업에 대한 소프트웨어의 관급)
♣ 분리발주 대상 소프트웨어

나. 하자담보 책임기간 1년 이내 명시

(1) 기술 내용

○ 계약목적물의 하자에 대한 보수책임을 1년 이내의 범위로 명시합니다.

(2) 기술 방법

○ 하자담보 책임기간을 1년 이내로 명시합니다.
- 사업의 완성을 확인한 후 1년간을 계약목적물의 하자담보 기간으로 명시함. (별도의 관련 법률에서 따로 정하고 있는 경우는 제외)
※ 유지관리, 운영위탁, 컨설팅, 전산감리 사업은 해당 없음

○ 유상 유지보수 또는 재개발에 대해서는 계약목적물을 인수한 직후부터 계약을 체결하여 시행하여야 함 (용역계약일반조건 제58조제4항)

작성 예시

- o 제안하는 장비, 네트워크 및 소프트웨어에 대해 분야별 충분한 하자보수 지원 방안이 분야별로 구분되어 구체적으로 제시되어야 하며, 다음의 사항을 포함하여 기술해야 함
  - 분야별 무상 하자보수 기간
  - 하자보수조직 지원범위, 지원방법, 인원
- o 하자보수 기간 동안 OS 및 보안SW의 신규 버전 Upgrade 시 무상 또는 유상 여부를 제시해야 함
- o 제안사는 사업을 종료한 날(사업에 대한 시험 및 검사를 수행하여 최종산출물을 인도한 날을 말한다)부터 1년 이내의 범위에서 발생한 하자에 대하여 담보책임이 있음
  * 용역계약일반조건(기획재정부계약예규) 제58조 (하자보수 등)을 따른다.
- o 제안사는 하자보수 기간 중 H/W 장비의 불량(소모품 포함) 및 설치상의 오류 등으로 인한 시스템의 결함 등의 하자에 대한 보수를 요청 받았을 경우 가능한 빠른 시간 안에 해당 부품을 무상으로 수리하거나 동일 신품으로 교환하여야 함
- o 공급되는 장비 및 부품, S/W의 생산 중단 시는 최소 3개월 전에 서면으로 통보하고 관련 장비의 예비부품을 사전확보 및 대체품으로 지속운용을 위한 대책을 강구 지원하여야 함
- o 하자보수 지원은 공단 근무시간을 기준으로 하되, 장애 등 긴급한 조치가 필요한 경우 근무시간 및 휴일에 관계없이 지원하여야 함
- o 제안사는 하자보수 기간 중 도입된 제품에 보안취약점이 발견되거나, 발주기관이 보안취약점 진단을 요청할 경우 취약점 제거를 위해 적극 지원하여야 함

관련근거

- ♣ 소프트웨어산업진흥법 제20조의4(소프트웨어사업의 하자담보책임)
- ♣ 용역계약 일반조건 제58조(하자보수 등)

다. 작업장소 상호 협의 결정

(1) 기술 내용

○ 사업수행에 필요한 작업장소를 상호 협의하여 정함을 기술합니다.

(2) 기술 방법

○ 소프트웨어사업 수행을 위해 필요한 장소 및 설비, 기타 작업환경을 발주기관과 계약당사자가 상호 협의하여 결정합니다.

○ 제안요청서 작성 시 작업장소 등의 상호협의 결정을 명시하고, 발주기관이 제공 하는 경우 작업장소 등에 관한 비용에 대해 사업예산 또는 예정가격에 계상 여부를 명시합니다.

(3) 작성 시 유의사항

○ 향후 기술협상 등의 과정에서 상호 협의하여 발주기관 사업장에 작업장소를 마련하여 제공하는 경우 작업장소 이외에도 설비, 기타 작업환경에 대한 제공여부 및 비용부문에 대해서도 명확하게 협의하여야 합니다.

※ 정보보호시스템 운영과 같이 정보시스템의 위치에 따라 작업장소 등이 결정되는 사업의 경우 포함

○ 국가기관 등이 작업장소 등에 관한 비용을 명시하지 않을 경우 관련 지침에 따라 국가기관 등이 무상으로 제공하는 것으로 간주하게 되므로 반드시 명시하는 것이 향후 협상이나 사업 이행과정에서 불필요한 분쟁을 예방할 수 있습니다.

작성 예시

ㅇ 본 사업 수행 장소는 공단에서 제공한 공간을 상호 협의하여 사용하도록 함
ㅇ 본 사업을 위하여 필요한 사무기기, 집기, 비품 등의 모든 제반비용은 제안사 부담으로 함

관련근거

♣ 용역계약 일반조건 제52조(작업장소 등)
♣ 행정기관 및 공공기관 정보시스템 구축운영지침 제41조(작업장소 등)

라. 계약목적물의 지재권 귀속

(1) 기술 내용

○ 계약목적물의 지식재산권 귀속주체에 대한 사항을 명시합니다.

(2) 기술 방법

○ 당해 계약으로 지식재산권이 발생할 경우 계약당사자 간 공동소유를 원칙으로 합니다.
- 적용대상 : 계약목적물의 지식재산권이 발생하는 소프트웨어사업
- 예외사항 : 개발의 기여도 및 계약목적물의 특수성(국가안전보장, 국방, 외교 관계 등)을 고려하여 계약당사자간 협의를 통해 공동소유와 달리 정할 수 있음

※ 발주기관 귀속 시 정당한 귀속사유 명시 혹은 계약당사자에게 지식재산권 부여

(3) 작성 시 유의사항

○ 입찰공고 시 계약목적물의 지식재산권은 계약당사자간 공동 소유로 한다고 명시하고 사업관리 시 준수해야 합니다.

작성 예시

❑ 본 사업의 수행 결과물(계약목적물)에 대한 지식재산권은 발주기관과 계약상대자가 공동으로 소유하며, 별도의 정함이 없는 한 지분은 균등한 것으로
- ㅇ 다만, 구축·개발의 기여도 및 계약목적물의 특수성(보안, 영업비밀 등)을 고려하여 계약당사자간 협의를 통해 지식재산권 귀속주체 등에 대해 공동소유와 달리 정할 수 있음
- ㅇ 또한, 지식재산권의 타용도 및 상업적 활용 시 반드시 공사와 협의를 해야 함

관련근거

♣ 용역계약 일반조건 제56조(계약목적물의 지식재산권 귀속 등)

♣ 행정기관 및 공공기관 정보시스템 구축운영지침 제60조(계약목적물의 지식재산권 귀속 및 기술자료 임치)

마. 하도급계약 사전 승인제

(1) 기술 내용

○ 하도급계약 적정성 평가를 통한 하도급 계약 적정성 판단기준을 기술합니다.

(2) 기술 방법

○ (원)도급자와 (재)하도급자간에 계약을 체결하기 전에 발주기관으로부터 하도급자의 사업수행능력과 계약방식 등의 적정성 평가를 통해 사전 승인을 받아야 하고, 하도급 계약 적정성 판단기준 등을 제안요청서 상에 명시하여야 합니다.

※ 다음의 경우 하도급 계약 승인 대상에서 제외할 수 있다.
- 단순 물품(하드웨어를 포함한다)의 구매·설치 용역·유지관리
- 단순 조사업무 또는 외부자문
- 나라장터 종합쇼핑몰에 등록되어 가격 정보가 공개 된 상용소프트웨어의 구매·설치 용역·유지관리(별도의 커스터마이징 비용이 소요되는 경우는 제외)

○ 하도급을 허용하지 않는 사업은 제안요청서에 불가 사유를 명시합니다.

작성 예시

o 본 사업의 하도급의 경우 「정보보호산업 진흥법」 제8조 및 「정보보호시스템 구축사업의 하도급 승인 및 관리 지침」(과학기술정보통신부고시)에 따라 하도급 계약 전에 사전승인을 받아야 함
o 하도급 대금에 대한 기준은 직접인건비의 경우 한국소프트웨어산업협회장이 공표한 노임단가의 100%, 제경비와 기술료의 합은 직접인건비의 20% 이상으로 적용하여야 함
o 원도급자가 지급하는 하도급 대금을 서식으로 제안서에 포함하여 제출하여야 함
o 입찰 및 계약체결 시 「정보보호시스템 구축사업의 하도급 승인 및 관리 지침」(과학기술정보통신부고시)의 별지 제1호 서식의 하도급 적정성 판단 자기평가표를 제출하여야 함
o 「정보보호산업진흥법」, 동법 시행령, 동법 시행규칙 및 「정보보호시스템 구축사업의 하도급 승인 및 관리 지침」(과학기술정보통신부고시)에 따라 적정성 여부를 판단하며, 평가점수가 85점 이상인 경우에 한하여 하도급계약을 승인함
  · 다만, 85점 이상인 경우라 하더라도 하도급 계약의 세부 조건 등으로 인하여 사업의 원활한 수행이 불가능하다고 인정되는 경우 그 사유를 기재하여 하도급 승인 거절을 통보할 수 있음

관련근거

♣ 정보보호산업진흥법 제8조(하도급의 승인)
♣ 정보보호산업진흥법 시행규칙 제2조(하도급의 승인절차 등)
♣ 정보보호시스템 구축사업 하도급계약의 적정성 판단기준 제3조(적정성 판단기준 등의 사전공개), 제4조(승인 대상의 제외), 제7조(적정성 판단 등)

바. 누출금지정보의 명시

(1) 기술 내용

○ 정보시스템의 구축 및 유지관리 계약의 이행과정에서 누출될 경우 국가에 피해가 발생할 것으로 판단되는 정보를 지정하여 명시합니다.

(2) 기술 방법

○ 제안사가 제안서 작성 및 입찰 시, 열람 혹은 알게 될 기관 정보 중 사업 수행 중 누출될 경우 국가에 피해가 발생할 가능성이 있는 정보를 명시합니다.

○ 누출금지 정보로 명시한 정보에 대하여 제안사 및 사업자가 누출할 경우 부정당업자로 제재됨을 기술합니다.
※ 본 사업이 누출금지정보와 관련이 없을 경우 생략할 수 있습니다.

작성 예시

국가를 당사자로 하는 계약에 관한 법률 시행령 제76조(부정당업자의입찰참가자격제한)제1항 18호에 따라 사업 수행자는 사업수행과정에서 알게 된 정보 중 아래에 해당하는 정보를 무단으로 유출하는 경우 국가를 당사자로 하는 계약에 관한 법률 시행규칙 별표2제20호 부정당업자의 입찰참가자격 제한기준을 따라 입찰참가자격을 제한 함

① 기관 소유 전산시스템의 내·외부 IP주소 현황
② 세부 전산시스템 구성현황 및 전산망구성도
③ 사용자계정 및 패스워드 등 시스템 접근권한 정보
④ 전산시스템 취약점분석 결과물
⑤ 용역사업 결과물 및 프로그램 소스코드
⑥ 국가용 보안시스템 및 정보보호시스템 도입현황
⑦ 방화벽·IPS 등 정보보호제품 및 라우터·스위치 등 네트웍장비 설정 정보
⑧ '개인정보 보호법'의 개인정보
⑨ '보안업무규정' 제4조의 비밀, 同 시행규칙 제7조3항의 대외비
⑩ 기타 각 기관이 공개가 불가하다고 판단한 자료

관련근거

♣ 국가를 당사자로 하는 계약에 관한 법률 시행령 제76조(부정당업자의 입찰참가 자격 제한) 및 시행규칙 별표2 제20호
♣ 지방자치단체를 당사자로 하는 계약에 관한 법률 시행령 제92조(부정당업자의 입찰참가자격 제한) 및 시행규칙 별표2 제21호

제 4 절 제안요청서 검토

1. 제안요청 사항 검토

○ 템플릿의 양식 및 본 가이드의 지침에 따라 제안요청서 작성을 완료한 후, 사업 발주 전 제안요청의 준수 항목에 대해 검토합니다.

[표 2-19] 제안요청 준수 항목

(X:미준수, ●:준수)

구분	관련근거	항목	준수 여부
계약 상대자의 이익제한금지	- 국가를 당사자로하는 계약에 관한 법률 시행령 제4조 (계약의 원칙) - 지방자치단체를 당사자로 하는 계약에 관한 법률 제6조 (계약의 원칙) - 용역계약일반조건 제4조 (계약문서)	예산 대비 무리한 과업 요구 금지	
		과업과 무관한 요구 금지	
		그 외 불공정한 요구 금지	
정보보호서비스의 적정대가 지급	- 정보보호산업법 제10조제1항 (정보보호제품 및 정보보호서비스의 대가) 및 시행령 제5조 - SW사업 대가산정 가이드	정보보호제품 및 정보보호서비스의 품질보장을 위하여 적정 수준의 대가 지급	
물품공급 및 기술지원 협약	- 정부 입찰·계약 집행기준 제5조의2 (신기술 또는 특허 공법이 요구되는 공사 적용기준)	특수한 성능·품질 등의 납품능력이 요구되는 물품에 대한 사전 협약내용을 명시	
특정 규격 등 명시 금지	- 정부입찰·계약 집행기준 제5조 (제한기준) - 지방자치단체 입찰 및 계약 집행기준 (나. 입찰 및 계약 시 금지해야 할 사항)	설계서·규격서 등에 부당하게 특정 규격·모델·상표 등 명시 금지	
하자담보 책임 범위 외 요청 금지	- 정보보호산업법 제9조 (정보보호시스템의 하자담보 책임) - 용역계약일반조건 제58조 (하자보수 등)	법률이 정하는 하자 담보 책임 외의 요청 금지	
표준계약서 사용	- 정보보호산업법 10조제3항 (정보보호제품 및 정보보호서비스의 대가) - 약관법 제17조(불공정약관조항의 사용금지)	불공정한 조항 사용 금지	
요구사항 명확화	- 정보보호시스템 구축에 관한 세부 기준 제4조 (발주준비)	정보보호사업 공통 요구사항	
		정보보호사업 선택 요구사항	
		정보보호 제품 요구사항	
		정보보호 서비스 요구사항	

2. 제안안내 사항 검토

○ 템플릿의 양식 및 본 가이드의 지침에 따라 제안요청서 작성을 완료한 후, 사업 발주 전 제안안내 사항의 법 제도 항목에 대해 검토합니다.

[표 2-20] 제안안내 검토 항목

(X:반영안함, ●:필수반영)

분야	항목	관련 근거	반영 여부
가. 입찰방식			
(1) 사업자 선정 방식	① 협상에 의한 계약 체결 우선적용	- 국가계약법 제10조2항 (경쟁입찰에서의 낙찰자 결정) - 국가계약법 시행령 제43조(협상에 의한 계약체결) 및 제43조의2 (지식 기반 사업의 계약방법)	
(2) 입찰 참가 자격	① 경쟁 입찰 참가자격		
	- 사업유형별 면허 등 자격	- 소프트웨어산업진흥법 제24조 - 정보통신공사업법 제14조	
	- 보안관제사업 입찰참가자격 보안관제 전문업체로 한정	- 국가정보보안기본지침 제127조 (보안관제 용역업체 선정 및 관리) - 국가사이버안전관리규정 제10조의2 (보안관제센터의 설치·운영)	
	- 정보보호컨설팅사업 입찰참가자격 정보보호 전문서비스 기업으로 한정	- 정보보호산업법 제23조 (정보보호 전문서비스 기업의 지정·관리) - 정보통신기반 보호법 제9조 (취약점의 분석·평가)	
	② 상호출자제한기업 및 대기업 참여제한		
	- 상호출자제한기업 집단 참여제한	- 소프트웨어산업진흥법 제24조의2 (중소 소프트웨어사업자의 사업 참여 지원) - 사업금액에 관계없이 참여를 제한	
	- 대기업간 컨소시엄 금지	- 소프트웨어사업 관리감독에 관한 일반기준 제4조 (발주준비) - 매출 8천억원 이상 대기업간 공동수급 금지	
	- 사업규모별 대기업 참가제한	- 대기업인 소프트웨어 사업자가 참여할 수 있는 사업금액의 하한	
	③ 부정당업자 참여제한		
	- 부정당 제재기간에 해당되지 않은 업체	- 국가계약법 시행령 제76조 (부정당업자의 입찰참가자격)	
	④ 공동수급 허용 및 제한		
	- 공동수급 허용 및 제한	- 국가계약법 제25조 및 시행령 제72조 및 제72조의2 (지식기반사업의 공동계약) - 공동계약운용요령 제9조 (공동수급체의 구성) - '소프트웨어사업 관리감독에 관한 일반기준 제4조 (발주준비)	
	⑤ 중소기업 우선조달 제도		
	- 중소기업자와의 우선	- 중소기업제품 구매촉진 및 판로 지원에 관한	

분야	항목	관련 근거	반영 여부
	조달 계약제도	법률 시행령 제2조의 2 (중소기업자와의 우선조달계약)	
	⑥ 제안요청 설명회 참석 여부		
	- 제안요청 설명회 참석 여부	- 행정기관 및 공공기관 정보시스템 구축 운영 지침 제28조 (제안요청 설명회 개최)	
나. 제안서 평가방법			
① 제안서 평가 일반사항		- 협상에 의한 계약 제안서평가 세부 기준	
② 협상적격자 선정 방식		- 협상에 의한 계약체결기준 제8조 (협상적격자 및 협상순위의 선정)	
다. 기술성 평가기준			
① 정보보호시스템의 사업자 선정을 위한 기술평가 기준 적용		- 정보보호산업법 제7조제2항 (공공기관등의 정보보호시스템 구축등 계약)	
② 기술 위주 평가 (기술능력 평가비중 90% 명시)		- 행정기관 및 공공기관 정보시스템 구축운영지침 제18조 (평가배점)	
③ 기술 평가 항목 배점	- 제안서 기술성 평가기준	- 소프트웨어 기술성 평가기준 - 행정기관 및 공공기관 정보시스템 구축운영지침 제21조 (제안서 기술 평가 기준)	
	- 상생협력 평가항목 평가 방법		
	- 상대평가 항목지정		
④ 평가의 공정성		(협상계약에서 실적제한 금지)	
라. 제출서류			
마. 제안서 제출일정 및 방법		- 행정기관 및 공공기관 정보시스템 구축운영지침 제29조 (제안서 등의 제출)	
바. 제안요청 설명회		- 행정기관 및 공공기관 정보시스템 구축운영지침 제28조 (제안서요청 설명회 개최)	
사. 제안설명회 개최		- 행정기관 및 공공기관 정보시스템 구축운영지침 제20조 (제안서 발표)	
아. 입찰 시 유의사항		- 용역계약일반조건 - 협상에 의한 계약 체결기준	
자. 제안서 보상 **- 제안서 보상 명시**		- 소프트웨어산업진흥법 제21조 - 소프트웨어사업 관리감독에 관한 일반기준 제5조 (제안요청서 준비)	
차. 기타 사항	① 정보보호제품 분리발주	- 소프트웨어산업진흥법 제20조제2항 (국가기관등의 소프트웨어사업 계약) 및 과학기술정보통신부 고시 분리발주 대상 소프트웨어 제2조 (분리발주 대상 사업), 제3조 (분리발주 대상 소프트웨어)	
	② 하자담보 책임기간	- 정보보호산업법 제9조 (정보보호시스템의 하자담보책임) - 용역계약일반조건 제58조 (하자보수 등)	
	③ 작업장소 상호 협의 결정	- 용역계약일반조건 제52조 (작업장소 등)	
	④ 계약 목적물의 지식재산권 귀속	- 용역계약일반조건 제56조 (계약목적물의 지식재산권 귀속 등)	
	⑤ 하도급 계약 사전	- 정보보호산업법 제8조 (사업 하도급의 승인) 및	

분야	항목	관련 근거	반영 여부
	승인제	시행규칙 제2조 (하도급의 승인절차 등) - 정보보호시스템 구축 사업의 하도급 승인 및 관리 지침 제6조 (승인신청)	
	⑥ 하도급대금 지급 확인	- 용역계약일반조건 제27조 (하도급대금 지급 확인)	
	⑦ 제안요청서 보안 사항 (제안요청서상의 보안사항은 기술하지 않음)	- 행정기관 및 공공기관 정보시스템 구축운영지침 제17조 (제안요청서 보안사항 등)	
	⑧ 누출금지 정보의 명시 (정보시스템 구축 및 유지관리계약의 이행과정에서 정보 누출금지)	- 국가를 당사자로 하는 계약에 관한 법률 시행령 제76조 (부정당업자의 입찰참가자격 제한) 및 시행규칙 별표2 제20호 - 지방자치단체를 당사자로 하는 계약에 관한 법률 시행령 제92조 (부정당업자의 입찰참가자격 제한) 및 시행규칙 별표2 제21호	
	⑨ 기술 적용 계획 준수	- 행정기관 및 공공기관 정보시스템 구축운영지침 제7조 (기술적용계획 수립 및 상호운용성 등 기술평가)	
	⑩ 소프트웨어 개발보안 적용 명시	- 행정기관 및 공공기관 정보시스템 구축·운영 지침 제16조(제안요청서 작성)	

제3장
사업자 선정 및 계약

제 3 장 사업자 선정 및 계약

제 1 절 사업 발주계획 수립

○ 사업 발주계획 수립 및 발주단계에서는 사업 발주에 앞서 사업 전체에 대한 추진 범위 및 기간을 확정함과 동시에, 필요한 예산에 대한 조정 및 확보작업을 수행합니다. 또한 본 단계에서는 사업추진을 위해 구성되어야 하는 조직 및 역할에 대해서 정의합니다.

○ '정보보호산업진흥법', '국가를 당사자로 하는 계약에 관한 법률 시행규칙', '지방자치단체를 당사자로 하는 계약에 관한 법률 시행규칙' 및 '분리발주 대상 소프트웨어(과기정통부 고시)'에서 기술하고 있는 소프트웨어 분리발주와 관련하여 상용 소프트웨어의 분리발주 가능성을 분석하고, 보안소프트웨어 분리발주 적용 여부를 파악하는 작업이 필요합니다. 상기 언급된 내용들은 단계4에서 작성한 요구사항 상세내역과 함께 제안요청서를 작성하기 위한 기본 자료가 됩니다. 이를 통해 제안요청서를 작성하며, 사업자를 선정하기 위한 평가 요소를 선정합니다.

1. 사업 발주계획 수립

가. 사업추진 범위 및 기간 확정

○ 해당사업의 추진 범위를 확정하여 과업이 수행됩니다. 사업 범위 및 방향성 수립 단계에서 정의한 추진 범위가 요구사항 분석을 통해 변동이 있는지 파악합니다. 초기 수립된 범위에서 벗어나는 요구사항에 대해 범위에서 제외할지 수용할지에 대하여 이해관계자와 함께 협의하여 사업 범위를 최종 확정합니다. 연도별/단계별 사업의 경우, 당해 연도 사업범위를 구분하여 명시합니다.

○ 사업 일정 및 기간의 확정을 위해 정보보호시스템 구축사업의 총 수행기간, 일정별 주요 이벤트(사업 발주, 선정 및 평가, 착수, 서비스 개통일 등)를 월별 또는 업무별로 수립합니다. 정보보호시스템 구축 사업이 다수의 세부 과제로 구성된 경우, 각 과제의 완료 시점에 대해 통합 또는 단계별 추진 등을 포함한 일정 계획을 수립합니다.

나. 사업 예산 조정 및 예산 확정

○ 요구사항 상세 내역을 토대로 정보보호시스템 구축사업 예산을 산정합니다. 예산은 한국소프트웨어산업협회의 "소프트웨어 사업대가 산정 가이드"를 참고하며, 예산을 토대로 예산 산출 내역을 작성, 검토 후 확정합니다. 정보보호시스템 구축사업 예산은 크게 용역비와 장비 구입비, 기타 개발에 소요되는 비용으로 구성됩니다.

- 용역비 : 소프트웨어개발비, 시스템 운용환경 구축비, DB 구축비를 포함합니다.
- 장비 구입비 : 소프트웨어 구매, 하드웨어 구매, 그리고 기타 필요장비 구매비용을 포함합니다.

○ 정보보호 소프트웨어에 대해서는 보안성지속 서비스 대가를 적용하여 상용소프트웨어와 구분하여 산정합니다.

○ 소프트웨어사업 대가산정 가이드(2017년 개정판)에는 정보보호사업대가 산정가이드가 통합되어 있으며 정보보호 관련 3개 사업 유형에 대한 대가산정 방식이 제시되어 있습니다.

○ 정보보호 제품에 대하여 일반 상용소프트웨어의 유지관리 업무와 별도로 보안성 지속 서비스를 요구하는 경우에는 이를 사업비 산정에 반영하여야 합니다.

[표 3-1] 보안성 지속 서비스와 유지관리 항목 비교

<table>
<tr><th colspan="2">구분</th><th colspan="2">서비스</th></tr>
<tr><td colspan="2" rowspan="5">보안성지속
서비스</td><td colspan="2">보안업데이트</td></tr>
<tr><td colspan="2">보안정책관리</td></tr>
<tr><td colspan="2">위협/사고분석</td></tr>
<tr><td colspan="2">보안성 인증효력 유지</td></tr>
<tr><td colspan="2">보안기술자문</td></tr>
<tr><td rowspan="8">유지관리</td><td rowspan="3">제품
관련</td><td rowspan="2">제품 수정 및 보완</td><td>패치 서비스</td></tr>
<tr><td>업데이트</td></tr>
<tr><td>기능 향상</td><td>업그레이드</td></tr>
<tr><td rowspan="4">기술
지원</td><td colspan="2">일상지원</td></tr>
<tr><td colspan="2">(긴급)장애처리</td></tr>
<tr><td colspan="2">예방/예측지원</td></tr>
<tr><td colspan="2">고객 맞춤지원</td></tr>
<tr><td rowspan="2">교육</td><td colspan="2">운영자 교육</td></tr>
<tr><td colspan="2">사용자 교육</td></tr>
</table>

○ 보안성 지속 서비스는 정보보호 제품의 유지관리에만 적용되는 대가 산정 기준으로 사업비 산정 시 이를 적용할 필요가 있습니다.

보안성 지속 서비스 대가 = 제품공급가 * 비율

- 제품공급가에 일정 비율(예 10% 이상)을 적용하여 보안성 지속 서비스 대가를 별도로 산정
- 보안성 지속 서비스 제공 기업은 안티바이러스(백신), 스팸차단 솔루션 등과 같이 라이센스 형태로도 계약 가능

- 사고 시 긴급 대응 등 고객의 특정 요구에 따라 추가로 제공되는 서비스의 경우, 서비스 투여시간 및 인건비 등에 따라 별도로 책정 가능
- 보안성 지속 서비스 계약 예시 : 1차년도부터 정보보호 제품 도입 및 구축비(공급가)와 별도로 일정비율(예 10% 이상)을 보안성 지속 서비스 대가로 산정하여 계약

[표 3-2] 보안성 지속 서비스 항목

서비스 항목	서비스 내용
보안업데이트	패턴 업데이트(룰패턴 및 시그니쳐), IT환경변화(신규 OS/시스템 및 단말/표준 등)에 대한 패치
보안정책관리	사용자 환경에 따른 보안정책 수립/변경
위협/사고분석	침해사고대응(사전/사후), 제품군별 위협분석보고서 등
보안성 인증효력 유지	CC인증, 보안적합성 검증, KCMVP 등 각종 보안성 인증 유지
보안기술자문	모의훈련대응, 정보보호 교육, 원격문의 대응, 보안감사 지원 등

○ 보안 업데이트 : 대부분의 보안시스템은 지속적으로 발견되는 공격기법을 시그니쳐로 변환하여 공격패턴 비교방식의 메커니즘을 사용하므로 보안 시그니쳐 업데이트를 지속적으로 관리함으로써 보안성을 향상시킬 수 있습니다. 또한, 신규 OS나 시스템 및 단말, 신규 표준이나 프로토콜 반영 등 IT환경변화에 대한 패치도 보안 업데이트에 포함되는 사항입니다.

- 제품의 특성과 공급업체의 관리기준에 따라, 정기 또는 수시로 시그니쳐 업데이트 시기를 결정할 수 있으며, 업데이트 방식은 온라인 또는 USB를 이용한 방식, 혼합 선택방식 등을 제공합니다.

○ 보안정책관리 : 보안정책 변경관리는 일반적으로 보안강화 또는 완화 등과 같이 보안 룰셋의 변경관리 업무와 납품된 보안시스템 자체에 대한 정책 변경관리가 있습니다. 보안정책 변경은 기업이나 기관의 변경사항이 발생하거나 보호해야 할 정보시스템에 변화가 있을 경우에 발생합니다.

- 웹방화벽의 경우 보호할 웹 어플리케이션의 소스 또는 구조가 변경되었을 경우 보안정책의 변경이 필요하게 됩니다.

○ 위협/사고분석 : 해킹이나 악성코드, 최신 정보보안 기술에 대한 정보를 제공하는 것으로, 제공시기에 따라 정기적인 정보제공과 수시 정보제공 형태로 나눠집니다. 수시 정보제공 형태는 침해사고 발생 시 그 원인과 대응방안 등을 제공하는 것이 일반적이며, 침해사고 대응 보고서, 침해사고 분석 보고서 제공 등도 해당됩니다. 이 서비스를 통해 대내외 서비스의 위협요소들에 대한 잠재적 취약점 분석과 침투경로에 대한 점검, 고객의 정보시스템을 가장 안전하게 보호할 수 있는 최적의 해결 방안 및 대응 방안을 제시할 수 있습니다.

○ 보안성 인증효력 유지 : IT 정보보호 제품 보안성 평가/인증 정책에 따라 정보보호 제품에 특화된 인증이 필수요건으로 적용되는데, 해당하는 인증에는 국제공통평가기준(CC:Common Criteria) 인증, 보안적합성 검증, 암호검증 등이 포함됩니다. 이는 정보보호 제품 최초 개발단계부터 폐기시까지 전 주기에 걸쳐 지속적으로 관리되어야 하는 부분입니다.

○ 보안기술 자문 : 발주기관의 침해사고 모의훈련대응, 정보보호 교육(제품관련 교육 外) 지원, 원격문의 대응, 보안감사 지원 등 발주기관이 긴급한 문제 해결을 요청한 경우, 온라인과 전화를 이용하거나 전문 인력의 방문지원 등을 통해 문제를 해결하는 서비스를 말합니다.(제품에 대한 일반적 지원 사항은 해당되지 않음)

※ 보안컨설팅 사업비는 투입공수(MM) 방식으로 대가를 산정하며 컨설턴트 등급별 공수에 컨설턴트 평균 임금을 적용하고 제경비, 기술료 등을 추가하여 산정합니다.

※ 보안관제 서비스 사업비는 관제 서비스 유형별 투입인력의 기술자 등급, 소요공수를 적용하여 인건비를 계산하고 제경비, 기술료를 추가하여 산정합니다.

직접인건비 = 순환근무조{(평균임금 합계 ÷ 인원) × 연간 근무시간 × 최소 상시근무 인원)} + 관리자(PM) 및 추가 인력(평균임금 × 연간 근무시간)

다. 사업수행 조직 및 역할 확정

○ 기존의 사업수행 내부조직에 관련부서(기타 이해관계부서) 담당자를 포함하여 사업수행 조직을 보완하고 조직/인력별 역할을 확정합니다. 사업수행 조직은 사업의 준비 단계에서부터 수행, 향후 관리 및 운영 단계까지의 전 과정에 참여할 수 있는 전담조직으로 구성하며, 구성원은 관련 업무에 대한 이해도가 높거나 경험을 보유한 인력으로 구성합니다.

○ 사업추진 활동에 연관된 이해관계자들은 포괄적인 개념으로 추진조직과 같은 형태를 가지고 있습니다. 사업 추진 전 이해관계자의 구성과 각 주체별 역할 및 기능 정의가 이루어져야 사업의 총괄책임 주체가 통합 적인 관점에서 사업의 특정 부분에 대한 수행 여부 확인, 사업수행을 위한 사전 자료 요청, 이슈가 발생 한 부서에 대해 인력·산출물 조정 등의 점검을 할 수 있습니다.

라. 사업 연관성 파악 및 발주일정 계획 수립

○ 사업 연관성 파악은 발주일정 계획 수립에 있어서 중요한 고려 요인이 됩니다. 다년간 수행되고 있는 사업 이거나 본 사업수행의 결과가 현재 진행 중이거나 발주예정인 타사업의 결과와 깊은 연관이 있을 경우, 본 사업의 발주일정 계획 수립에 반드시 반영되어야 합니다.

마. 분리발주 및 벤치마크테스트(BMT)

○ '소프트웨어산업 진흥법 제20조 제2항', '국가를 당사자로 하는 계약에 관한 법률 시행규칙 제87조', '지방자치단체를 당사자로 하는 계약에 관한 법률 시행규칙 제84조' 및 '분리발주 대상 소프트웨어(과기정통부 고시)'에 의거하면 공공 소프트웨어사업은 분리발주 대상 소프트웨어에 대한 분리발주를 의무적으로 적용해야 합니다. 다만, 분리발주로 인하여 현저한 비용 상승이 초래되거나, 정보시스템과 통합이 불가능 하거나, 사업기간 내에 완성될 수 없을 정도로 현저한 지연이 우려되는 경우에는 해당 소프트웨어를 분리발주 대상에서 제외할 수 있으며, 그 사유를 발주계획서 및 입찰공고문에 명시하도록 규정하고 있습니다. 이에 따라 요구사항 상세내역을 토대로 이를 제공하는 상용소프트웨어 제품이 존재하는지 조사하고, 분리발주 대상 소프트웨어 여부를 검토합니다. 분리발주 대상 소프트웨어가 선정되면, 해당 상용소프트웨어 제품의 커스터마이징 범위를 분석하여 예산 수립 및 제안요청서 작성 시 참고하도록 합니다.

※ 소프트웨어 분리발주 관련 상세사항은 '소프트웨어사업 분리발주 매뉴얼' 참조

○ 발주기관은 경쟁입찰로 분리발주 대상 소프트웨어를 구매하려는 경우 BMT를 직접 실시하거나 시험기관에 의뢰하고, 그 결과를 기술성 평가에 반영할 수 있습니다. (전부 또는 일부)

○ 정보보호 제품 성능평가는 과학기술정보통신부장관이 지정한 KISA 등의 성능평가기관에 성능평가 신청 제품, 제품설명서, 사용자 취급설명서 등을 제출하여 평가를 의뢰하고 성능평가 종료 후 기술심의위원회 심의 · 의결된 정보보호제품 성능평가결과서를 제공받게 됩니다.

관련근거

정보보호산업진흥법 시행령

제10조(성능평가의 방법 및 성능평가기관의 지정) ① 법 제17조제1항에 따른 정보보호제품에 관한 성능평가(이하 "성능평가"라 한다)에는 다음 각 호의 사항에 대한 평가가 포함되어야 한다.

1. 정보보호제품 보안기능 처리 성능
2. 정보보호제품의 보안기능 외의 정보보호 관련 주요기능 구현 여부
3. 정보보호제품 운영 시 정보보호 기능 외의 일반기능 처리 성능
4. 정보보호제품의 시간 및 자원 관련 효율성

정보보호제품 성능평가 운영지침 (과학기술정보통신부 고시)

2. 사업자 선정 기준 및 절차 수립

가. 사업자 선정 기준 및 절차 수립

○ 정보보호시스템의 요구사항 분석과 사업의 특성 및 목적, 내용 등을 고려하여 정보보호사업의 상세 요구사항에 따라 평가항목을 선별하고 세부 평가항목별 배점을 조정합니다.

※ 사업자 선정을 위한 제안서 기술평가 기준 및 절차수립 관련 상세사항은 '소프트웨어 기술성 평가기준 적용가이드' 참조

[표 3-3] 정보보호사업 기술성평가 기준에 따른 평가항목

구분	평가기준	평가 항목
전략 및 방법론	사업의 대한 이해도와 사업추진을 위한 전략이나 기술 또는 사업수행방안을 구체적으로 제시하였는지, 실제 적용 사례와 경험을 활용하여 효율적인 방법을 제안하였는지를 평가합니다.	사업이해도
		추진전략
		적용기술
		표준프레임 워크적용
		방법론
		기업평가
		가점사항
프로젝트 기밀성 유지요구사항	정보 자산의 기밀성과 무결성을 확보하기 위해 목표 시스템의 데이터 및 기능, 운영 접근을 통제하기 위한 요구사항 내용이 충분히 기술되었는지 평가합니다.	관리적 보안 준수사항
		물리적 보안 준수사항
		기술 보안 준수사항
		법률 및 인증 준수사항
프로젝트 관리 요구사항	프로젝트의 원활한 수행을 위한 관리 방법 및 추진 단계별 수행방안에 대한 요구사항을 반영하기 위한 내용이 기술되었는지 평가합니다.	인력 관리
		공동 수급 및 하도급 협력 방안
		사업 일정 및 요구사항 관리
		위험 관리 사항
		산출물 관리 사항 및 품질 관리 사항
		유사사업 수행경험
프로젝트 지원 요구사항	프로젝트의 원활한 수행을 위해 필요한 지원 사항 및 방안에 대한 요구사항을 반영하기 위한 내용이 기술되었는지 평가합니다.	하자 보수 및 문제상황대응
		교육 훈련
제약사항	기능 및 품질 등 요구사항 구현 시 관련 제약사항과 대응방안을 구체적으로 기술되어 있는지를 평가합니다.	수행 업체 제한 및 하도급 제한
		지적 재산권 제한
		데이터 제약사항
		시스템 개발 제한
		설계 및 구현 제약사항
		업무 제약사항
품질 요구사항	분석·설계 등 각 단계별 품질 요구사항의 점검 및 검토 방안을 구체적으로 제시하였는지를 평가합니다.	신뢰성
		사용성
		상호 운용성 유지관리 방안
		효율성
		기능성
자산관리기능 요구사항	방법론 및 분석 도구를 통하여 구체적인 내용으로 분석되고 구현 방안이 구체적인 기술, 제안한	정보 자산 관리 기능

구분	평가기준	평가 항목
	방안 및 기술의 적용방안을 제시하였는지 평가한다.	소프트웨어 자산 관리기능
성능 요구사항	구현하고자 하는 기능을 통해 요구 성능이 충족되도록 방법론 및 분석 도구, 구현 및 테스트 방안을 구체적으로 제시하였는지 평가한다.	처리 속도/시간 성능/처리량 요구사항
		자원 사용량 요구사항
테스트 요구사항	구현하고자 하는 시스템을 검증하기 위한 테스트 환경, 방법, 절차 등 충분히 제시하였는지 평가한다.	성능 및 단위 테스트
		시스템 테스트
데이터 요구사항	데이터 전환 계획 및 검증 방법, 에러 데이터 처리 방법에 대해 구체적인 내용을 제시하였는지를 평가한다.	데이터 수집 및 입력 요구사항
인터페이스 요구사항	시스템 인터페이스 : 타 시스템과의 연계 방안들에 대한 장·단점의 분석을 통한 적합한 방안 도출 방안과 구현 경험이 있는 인터페이스 담당자 투입 사항의 내용이 구체적으로 기술되어 있는지를 평가한다. 사용자 인터페이스 : 사용자 편의성을 고려한 분석 및 설계, 구현 방안과 검토 계획과 구현 경험이 있는 사용자 인터페이스 담당자 투입 여부의 내용이 구체적으로 기술되어있는지를 평가한다.	사용자 인터페이스 요구사항
		시스템 인터페이스 요구사항
제품 컨설팅 요구사항	업무 효율성과 생산성을 높이기 위한 정보보호시스템 구매, 구축, 업무 프로세스 개선 방안 등의 도출을 위한 요구사항 이행 내용이 충분히 기술하고 있는지를 평가합니다.	환경분석
		현황분석
		개선 과제 도출
시스템 장비구성 요구사항	목표사업 수행을 위해 필요한 하드웨어, 소프트웨어, 네트워크 등의 도입 장비 내역 등 시스템 장비 구성에 대한 요구사항 이행 내용이 구체적으로 기술되었는지 평가한다.	보안관리 장비구성
		침입탐지 장비구성
		대응 및 복구 장비구성
		기타 장비 구성
보안기능 요구사항	사업에서 요구하는 보안 기능 방법론 및 분석 도구를 통하여 구체적인 내용으로 분석되고 구현 방안이 구체적인 기술, 제안한 방안 및 기술의 적용방안을 제시하였는지 평가한다.	보안관리 기능
		침입탐지 기능
		침해관리 기능
		기타 기능 구성
정보보호 서비스사업 요구사항	정보보호서비스 사업의 운영을 위한 장비구축·조직 및 인력·시스템유지관리와 관한 구체적인 내용을 확인하고 적절한 방안을 제시하였는지 평가합니다.	정보보안 컨설팅
		보안성 지속서비스
		보안관제
		SI서비스
		물리보안 및 기타서비스

○ 정보보호사업 평가항목 설계 시에는 발주사업의 유형 및 특성에 맞게 평가부문·평가항목 등을 가·감 조정하여 평가부문과 평가항목을 순차적으로 설계합니다. 이때, 평가항목 설계 시 평가항목을 계량/비계량 평가가능 항목으로 구분하여 설계합니다.

○ 정보보호사업의 경우에도 공공 SW정보화사업으로서 적용해야 하는 요구사항은 공통 요구사항과 선택 요구사항으로 구분하고 있으며 선택 요구사항은 정보보호사업 유형에 따라 선택하여 평가항목을 구성합니다.

[표 3-4] 사업유형별 공통/선택 요구사항 매핑표

요구사항 유형		정보보호제품		정보보호서비스				
		정보보호제품도입및구축	물리보안제품도입및구축	보안컨설팅	보안성지속서비스	보안관제	정보보호시스템개발	물리보안서비스
공통 요구사항	프로젝트 기밀성 유지 요구사항	●	●	●	●	●	●	●
	프로젝트 관리	●	●	●	●	●	●	●
	프로젝트 지원	●	●	●	●	●	●	●
	제약사항	●	●	●	●	●	●	●
	품질 요구사항	●	●	●	●	●	●	●
선택 요구사항	자산관리 기능 요구사항	●	●				●	○
	성능 요구사항	●	○				●	○
	테스트 요구사항	●	○				●	○
	데이터 요구사항	●	○				●	○
	인터페이스 요구사항	●	○				●	○
	제품 컨설팅 요구사항	●	●				●	○

○ 정보보호사업의 사업유형 구분에 따라 정보보호사업의 특성이 반영된 각 사업별 요구사항(필수 또는 선택)을 정의하고 정의된 요구사항에 맞는 평가항목을 선택하여 기술평가표를 도출합니다.

[표 3-5] 사업유형별 정보보호 요구사항 매핑표

요구사항 유형			정보보호제품		정보보호서비스				
			정보보호제품도입및구축	물리보안제품도입및구축	보안컨설팅	보안성지속서비스	보안관제	정보보호시스템개발	물리보안서비스
제품 선택 요구사항	시스템 장비 구성	보안관리 장비구성	●						
		침입탐지 장비구성	●						
		대응 및 복구 장비구성	●						
		기타 장비 구성		●					
	보안 기능	보안관리 기능	●						
		침입탐지 기능	●						
		침해관리 기능	●						
		기타 기능 구성		●					
서비스 선택 요구사항	정보 보안 컨설팅	보안컨설팅 공통 일반			●	○	○	○	○
		정보보호관리체계 인증			●				
		개인정보보호관리체계 구축			●				
		개인정보영향평가			●				
		정보보호 마스터 플랜 수립			●				
		교육체계 및 콘텐츠 개발			●				
		모의해킹			●				
		보안취약점 진단			●				
	보안성 지속 서비스				○	●	○	○	○
	보안 관제	원격 파견관제 서비스			○	○	●	○	○
		보안관제 부가서비스			○	○	●	○	○
	SI 서비스 사업 요구사항				○	○	○	●	○
	물리보안 및 기타 정보보호서비스				○	○	○	○	●

○ 다만 발주기관의 세부 요구사항에 따라 구분하여 배점하는 형태로 변경된 기술평가표는 평가 항목이 세분화되고 늘어나게 되어 실제 사업발주 시 변화된 평가표에 따라 사업자를 선정하는 데 다소 적응기간이 필요할 수 있습니다.

○ 정보보호사업 유형과 상세 요구사항에 따라 평가항목을 설계한 이후에는 각 항목별 중요도를 고려하여 가중치를 부여합니다.

[표 3-6] 정보보호사업 기술평가표

구분	평가항목	세부요구사항별 평가 항목	배점	
전략 및 방법론	사업이해도	사업의 목표 및 특성, 주변 환경 분석과 업무내용의 연관 관계를 잘 이해하고 있는가?		
		제안범위 및 제안요청서와의 부합성이 적합한가?		
		제안 내용 중 해당기업의 특징 및 장점을 잘 기술하고 있는가?		
	추진전략	사업 목표를 달성하기 위한 업무수행 방법과 업무수행 시 위험요소를 고려하여 창의적이고 현실적인 전략을 제시하였는가?		
	적용기술	사업에서 적용하고자 하는 기술이 향후 확정성을 고려하여 현실적으로 실현 가능하게 제시되어 있는가?		
	표준프레임 워크적용	정보보호시스템을 개발하고 유지관리 할 수 있도록 표준프레임워크를 적절하게 사용하고 있는가?		
	방법론	사업에 적정한 방법론을 제안하고 실제 적용사례와 경험을 바탕으로 효율적인 단계별 활동 내용을 구성하여 산출물 도출에 대한 적정성을 유지하고 있는가?		
	기업평가	기업안정성(신용평가 등급·재무상태)에 문제가 없고 유사사업수행경험 및 기술(특허, 인력 등) 등의 보유 사항이 있는가?		
	가점사항	제안사의 사업자 선정과 관련된 가점사항(ISMS인증, 정보보호공시 등)이 있는가?		
프로젝트 기밀성 유지 요구사항	관리적 보안 준수사항	수행 업체에서 요구하는 보안 일반 준수 사항을 충분히 반영하는가?		
		참여 인력(경력, 자격, 기술, 신원 등)이 보안 사업에 적합한가?		
		사업 종료 시 보안 사항을 충분히 준수할 수 있는가?		
		보안 요구사항 미준수 시 불이익 발생할 경우를 대비한 계획이 가능성이 있는가?		
		백업 및 IT 재해 복구 대책 수립 계획에 대한 충분한 기술이 되어 있는가?		
	물리적 보안	외부자 출입에 대한 대책을 충분히 제안하며 사무실 및 매체 장비 반		

구분	평가항목	세부요구사항별 평가 항목	배점
	준수사항	출·입과 장비 및 자료 보안 준수를 위한 내용이 충분히 기술되어 있는가를 평가한다.	
	기술 보안 준수사항	데이터, 시스템, 네트워크, PC 및 모바일 보안을 위한 자체적인 노력이 적합하게 기술되어 있는가를 평가한다.	
	법률 및 인증 준수사항	법적 제약 일반 사항에 대한 충분한 이해를 하고 있는가?	
		정보보호 관련 특별법과 표준 인증 준수사항에 대한 적합성을 갖추었는가?	
프로젝트 관리 요구사항	인력 관리	조직 및 인력 관리를 위한 방법이 타당한가?	
		투입 인력 자격 조건이 보안 사업에 적합한가?	
		제안 및 수행 PM 지정이 사업에서 요구하는 사항을 충분히 반영하는가?	
		지원 및 자문 조직 구성이 사업 내용에 적합하게 배정되어 기술되어 있는가?	
	공동 수급 및 하도급 협력 방안	공동 수급 형태 제안 및 하도급 관리 방안이 충분히 기술되어 있는가?	
	사업 일정 및 요구사항 관리	사업 일정 계획 관리와 요구사항 변동사항 관리에 대한 내용이 타당하게 기술되어 있는가를 평가한다.	
	위험 관리 사항	위험 관리 방안과 보고 체계, 비상 상황 발생에 대한 대책 제시에 대한 내용이 기술되어 있는가를 평가한다.	
	산출물 관리 사항 및 품질 관리 사항	산출물 관리 방안을 적절하게 제안하고 품질 보증 활동을 위한 노력과 전문가 검토 의견 수렴에 대한 방법이 기술되어 있는가를 평가한다.	
	유사사업 수행경험	최근 3년 이내 유사분야 사업수행경험 및 기술(특허, 인력 등)보유 사항이 있는가?	
프로젝트 지원 요구사항	하자 보수 및 문제상황대응	하자, 유지 보수 계획 및 문제 상황 발생 시 책임의 한계 명시되어 있는가?	
	교육 훈련	공급자가 실제 보안 시스템 운영 및 관리자를 위해 제공 및 지원하는 각종 교육 훈련을 위한 사항이 충분히 반영되었는가?	
제약 사항	수행 업체 제한 및 하도급 제한	수행 업체 및 수행 인력 제한 및 하도급 제한에 대한 요구사항 내용을 충분히 기술하였는가?	
	지적 재산권 제한	지적 재산권 귀속 명시에 대한 내용을 기술하고 있는가?	

구분	평가항목	세부요구사항별 평가 항목	배점
	데이터 제약사항	데이터 수집 및 관리·사용, 접근 제약 사항을 위한 방법을 충분히 기술하였는가?	
	시스템 개발 제한	표준 프레임워크 적용 및 개발언어 명시에 대한 내용이 충분히 기술되어 있는가?	
	설계 및 구현 제약사항	기존 시스템과의 호환성에 대한 내용이 구체적으로 기술되어 있는가?	
	업무 제약사항	감리 대응과 규정 변경에 따른 시스템 구현 유연성, PMO대응 등 업무상 나타날 수 있는 제약사항에 대한 내용의 방법이 기술되어있는가?	
품질 요구 사항	신뢰성	가용성의 보장 부분과 기능 구현의 정확성, 장애대응을 위한 백업 절차 제시에 대한 구체적인 방법을 기술했는가?	
	사용성	프로그램 학습성과 용이한 인터페이스를 제공한 방안에 대한 내용이 요구사항에 적합하게 기술되어 있는가?	
	상호 운용성 유지관리 방안	데이터 교환 방안 등의 상호 운용성에 대한 방법이 요구사항에 적합하게 기술되어 있는가?	
	효율성	시간 반응성 및 자원 효율성에 대한 방법이 요구사항에 적합하게 기술되어 있는가?	
	기능성	적합성과 보안성에 대한 방법이 요구사항에 적합하게 기술되어 있는가?	
자산 관리 기능 요구 사항	정보 자산 관리 기능	기업 정보 자원 생애 주기 관리에 대한 내용이 충분히 기술되어 있는가?	
		정보 시스템 현황 및 내역 관리에 대한 내용이 충분히 기술되어 있는가?	
		보안 제품 현황 및 내역 관리에 대한 내용이 충분히 기술되어 있는가?	
	소프트웨어 자산 관리기능	보안 솔루션 및 필수 소프트웨어 배포/설치의 이행이 이루어지는가?	
		불법 소프트웨어 설치 실시간 차단의 이행이 이루어지는가?	
성능 요구 사항	처리 속도/ 시간 성능/ 처리량 요구사항	응답 시간에 대한 요구사항을 이행하기 위한 내용이 충분히 기술되었는가?	
		동시 접속자 수에 대한 요구사항을 이행하기 위한 내용이 충분히 기술되었는가?	
		동시 처리 능력에 대한 요구사항을 이행하기 위한 내용이 충분히 기술되었는가?	
	자원 사용량 요구사항	CPU 사용율에 대한 요구사항을 이행하기 위한 내용이 충분히 기술되었는가?	
		메모리 사용율에 대한 요구사항을 이행하기 위한 내용이 충분히 기술되었는가?	
테스트 요구 사항	성능 및 단위 테스트	장비 성능 테스트를 위한 환경 이해, 방법론, 절차가 충분히 기술되어 있는가?	

구분	평가항목	세부요구사항별 평가 항목	배점
		단위 테스트를 위한 환경 이해, 방법론, 절차가 충분히 기술되어있는가?	
	시스템 테스트	성능 테스트를 위한 환경 이해, 방법론, 절차가 충분히 기술되어있는가?	
		부하테스트를 위한 환경 이해, 방법론, 절차가 충분히 기술되어있는가?	
		시험 개발 테스트를 위한 환경 이해, 방법론, 절차가 충분히 기술되어 있는가?	
		장애 복구 및 백업 복구 테스트를 위한 환경 이해, 방법론, 절차가 충분히 기술되어있는가?	
데이터 요구 사항	데이터 수집 및 입력 요구 사항	데이터 분석 요구사항을 이행하기 위한 계획 및 검증방법이 구체적으로 기술되어있는가?	
		데이터 수집 요구사항을 이행하기 위한 계획 및 검증방법이 구체적으로 기술되어있는가?	
인터페이스 요구 사항	사용자 인터페이스 요구사항	사용 단말을 고려한 화면 사이즈에 대한 해결 방법에 대한 내용이 기술되어 있는가?	
	시스템 인터페이스 요구사항	시스템 인터페이스 일반 사항을 이행하기 위한 내용이 충분히 기술되어있는가?	
		연계 모듈 제공을 위한 내용이 충분히 기술되어있는가?	
		표준 연계 모듈을 사용하는가?	
		시스템 정보 연계 방안에 대한 계획 및 방법론이 기술되어있는가?	
제품 컨설팅 요구 사항	환경분석	업무 환경 분석을 위한 내용이 충분히 기술되어있는가?	
		정보 기술 환경 분석을 위한 내용이 충분히 기술되어있는가?	
	현황분석	IT 인프라 분석을 위한 내용이 충분히 기술되어있는가?	
	개선 과제 도출	개선 과제 도출을 위한 방법론이 타당하게 기술되어있는가?	
시스템 장비 구성 요구 사항	보안관리 장비구성	보안관리를 위한 시스템 장비 구성내용이 충분히 기술되었는가?	
	침입탐지 장비구성	침입방지 및 탐지에 대한 사항은 충분히 기술되어있는가?	
	대응 및 복구 장비구성	복구 및 백업에 대한 대책과 관련 장비 구성 내용이 충분히 기술되어 있는가?	
	기타 장비 구성	기타 보안을 위한 장비 구성 내용이 충분한가?	
보안 기능	보안관리 기능	보안관리를 위한 기능 구성내용이 충분히 기술되었는가?	
	침입탐지 기능	침입방지 및 탐지에 대한 기능 사항은 충분히 기술되어있는가?	

구분	평가항목	세부요구사항별 평가 항목	배점
요구사항	침해관리 기능	침해관리를 위한 여러 가지 사항들이 충분히 기술되어 있는가?	
	기타 기능 구성	기타 보안을 위한 기능 구성 내용이 충분한가?	
정보보호 서비스 사업 요구사항	정보보안 컨설팅	보안컨설팅 일반사항(관리체계진단, 현황분석, 법조항 분석, 대책수립 등)에 대한 분석 및 적용은 충분한가?	
		정보보안 인증체계 요구사항을 이행하기 위한 내용이 충분히 기술되어 있는가?	
		솔루션 컨설팅 요구사항에 대한 내용이 충분히 기술되어 있는가?	
		접근 관리 요구사항을 이행하기 위한 내용이 충분히 기술되어 있는가?	
		정보보안 관련 감사나 실태점검 등 감사 업무를 위한 내용이 충분히 기술되어 있는가?	
		정보보호 마스터 플랜 수립에 대한 내용이 충분히 기술되어 있는가?	
		개인정보보호 관리 체계 구축 요구사항을 이행하기 위한 내용이 충분히 기술되어 있는가?	
		교육 콘텐츠 개발 요구사항을 이행하기 위한 내용이 충분히 기술되어 있는가?	
		교육 운영에 대한 내용이 충분히 기술되어 있는가?	
		모의 해킹 요구사항을 이행하기 위한 내용이 충분히 기술되어 있는가?	
		취약점 진단 요구사항을 이행하기 위한 내용이 충분히 기술되어 있는가?	
	보안성 지속서비스	시스템 운영 및 유지 관리에 대한 내용이 충분히 기술되어 있는가?	
		시스템 유지 관리 서비스 데스크 운영에 대한 내용이 충분히 기술되어 있는가?	
	보안관제	원격관제, 파견관제, 보고 체계, 관제시스템 연계 등에 대한 내용이 충분히 기술되어 있는가?	
		보안관제 부가서비스(분석, 진단, 관제시스템 기획운영, 개별서비스 등)에 대한 내용이 충분히 기술되어 있는가?	
	SI서비스	시스템 장비 설치 요구사항을 이행하기 위한 내용이 충분히 기술되었는가?	
		시스템 테스트 요구사항을 이행하기 위한 내용이 충분히 기술되었는가?	
		조직 및 인력관리에 대한 내용이 충분히 기술되어 있는가?	
		시스템 유지관리를 위한 예방 점검 및 보안 관리가 충분한가?	
	물리보안 및 기타서비스	영상보안의 관제, 모니터링, 장애처리, 녹화영상 확인 등의 기능을 수행하기 위한 내용이 충분히 기술되어 있는가?	
		출동 보안에 대한 내용이 충분히 기술되어 있는가?	
		기타서비스(Iot, 블록체인, 클라우드 등)에 대한 내용이 충분히 기술되어 있는가?	
합계			100

※ 위의 기술평가표에 평가되는 세부요구사항별 평가항목은 발주기관의 요구사항에 따라 추가되거나 삭제될 수 있습니다.

3. 제안요청서 확정 및 법제도 요건 반영여부 검토

가. 제안 요청서 확정

○ 정보보호시스템 개발사업 제안요청서를 작성하기 위해 제안요청서 목차를 작성하고, 이전 단계에서 파악된 현황과 목표 시스템에 대한 요구사항 상세내역을 기술합니다. 또한 입찰 관련 규정, 계약 체결 관련 유의사항, 필요한 서류 및 제안서에서 사용되는 서식 등을 제안요청서 내에 포함합니다.

나. 법제도 요건 반영여부 등 최종검토

○ 작성된 제안요청서에 대해 관련 법제도 요건 반영여부를 검토 및 보완하고 제안요청서를 최종 확정합니다. 계약 조건 작성에 필요한 용역계약 일반 조건, 정보보호산업진흥법 등 관련법령에 따른 계약 조건으로 다음과 같은 사항이 제안요청서 상에 명시되어야 합니다.

※ 정보보호사업 관련 주요법령
- 국가를 당사자로 하는 계약에 관한 법률
- 지방자치단체를 당사자로 하는 계약에 관한 법률
- 정보보호산업진흥법
- 전자정부법
- 기획재정부 계약예규 등

※ 정보보호사업 관련 주요제도
- 소프트웨어 분리발주
- 대기업인 소프트웨어 사업자가 참여할 수 있는 금액의 하한
- 정보보호사업의 경우 협상에 의한 계약체결방식의 우선 적용
- 기술능력 중심의 사업자 선정 (기술능력평가 : 입찰가격 평가비중 = 90:10 권장)
- 소프트웨어기술성 평가기준
- 소프트웨어사업 작업장소의 협의결정
- 계약목적물의 지식재산권 공동소유 원칙
- 정보보호사업 산출물의 하자담보책임기간은 1년 이하로 정함
- 정보보호사업 하도급 사전승인제도
- 제안서 보상제도(20억원 이상 사업에서 권장)

제 2 절 제안 평가 및 계약

1. 입찰공고

○ 사업담당자는 사업자가 사업의 입찰에 참여할 수 있도록 정해진 기한 내에 제안요구사항을 반영한 제안요청서를 공고합니다.

○ 사업담당자는 입찰부터 계약까지를 내부에서 수행할 것인지 외부기관(조달청 등)에 의뢰할 것인지 검토 한 후 입찰방침이 수립되면 사업일정을 고려하여 입찰공고매체에 공지합니다.

○ 입찰공고 후 발주기관의 내부규정 또는 외부기관(조달청 등)에서 정한 소정의 절차에 의거 제안서를 접수하며, 수의계약일 경우에는 관련 법령에서 정한 별도의 절차를 따릅니다.

2. 제안서 평가 및 사업자 선정

가. 제안서 평가 위원회 구성

○ 발주기관 자체평가의 경우 평가의 중립성과 전문성을 높이기 위해 평가 위원회 구성 방안 및 평가위원 자격 요건을 정의하고 그에 따른 평가 위원회를 구성합니다.

나. 우선협상대상자 선정 및 협상 수행

○ 기술능력평가 및 입찰가격평가를 통한 종합평가결과 순으로 협상대상 순위를 선정하고, 최고점을 받은 우선협상 대상자와 기술 및 가격협상을 수행합니다. 협상이 결렬될 경우 차순위 업체와 협상을 재개하거나 차순위 업체가 없을 경우 재입찰 공고를 합니다.

다. 계약 체결

○ 계약 절차는 국가계약법, 지방계약법 등 관계규정에 따라 수행하며, 계약상대자가 하도급계약을 체결하기 전에 발주자에게 하도급 승인을 받아야 합니다.

제4장
사업 수행 및 검사

제 4 장 사업 수행 및 검사

제 1 절 사업이행 및 관리

○ 사업이행 및 관리단계에서는 사업자와의 계약 체결 후, 정보보호사업이 수행되는 단계에서 필요한 관리 내용을 기술합니다. 본 단계에서는 제안요청서 및 제안서 내용을 바탕으로 사업자가 작성한 사업수행계획서 및 요구사항 상세내역에 대해 누락되었거나 신규로 추가 반영되어야 하는 요구사항을 정의하고 최종 작성된 내용에 대해 검토 및 승인하게 됩니다.

- 사업 착수단계에서는 제안요청서의 상세 요구사항이 사업수행계획서 및 요구사항 정의서에 누락없이 모두 반영되어 있는지 “과업대비표”를 작성하여 추적하고 변경사항에 대해서는 근거와 사유를 기록하여 관리하여야 합니다.

[표 3-5] 과업대비표 (예시)

제안요청서		제안서	사업수행계획서	요구사항정의서	
요구사항 고유번호	요구사항내용			요구사항 ID	요구사항명

○ 최종 승인된 사업수행계획서 및 요구사항 상세내역은 사업관리 및 인수에 있어 기준이 됩니다. 사업에 대한 진도 및 성과는 사업수행계획서에서 기술한 내용에 근거하여 관리가 되며, 요구사항의 변경 이력은 요구사항 상세내역에 기록됩니다. 아울러 사업수행계획서와 요구사항 상세내역의 내용은 사업 종료 및 인수 시 검수에 있어 가장 중요한 기초자료가 됩니다.

1. 사업수행계획서 검토 및 승인

○ 사업자가 제출한 사업수행 계획서(수정된 요구사항 상세내역 포함)는 발주기관의 사업담당자의 검토 하에 수행 가능 여부 및 요구사항 누락 여부가 확인되어야 합니다. 사업수행 계획서의 내용이 사업수행에 문제가 없다고 판단되는 경우, 발주기관의 사업담당자는 사업수행계획서를 승인하고 사업에 착수하게 됩니다.

2. 사업관리

가. 사업 관리

○ 사업수행계획서와 사업관리 관련 각종 지침을 기준으로 사업관리 활동을 수행합니다. 사업관리 활동에는 범위, 일정, 의사소통, 리스크, 이슈, 품질, 형상, 자원관리 등을 포함합니다.

나. 요구사항 관리체계 검토 및 승인

○ 사업담당자는 발주기관의 변경관리 절차 등을 기준으로 사업수행자에게 요구사항 추적, 변경관리방안이 포함된 요구사항 관리방안을 제시토록 요청하고, 변경절차, 서식 등 세부내용을 상호 협의하여 최종 승인합니다.

다. 요구사항별 충족여부 확인

○ 사업담당자 및 이해관계자는 정의한 요구사항이 정보보호사업 개발 단계별로 누락없이 적정하게 반영되었는지를 확인합니다. 이를 위해 “요구사항 추적표” 등의 사업관리 도구를 활용하여 단계별 활동과 산출물을 검토할 수 있습니다.

○ 요구사항 충족여부 확인 결과, 요구사항을 충족하지 못한 사항들을 정리하여 인수 시 최종 확인을 위한 이슈목록을 정의합니다.

[표 3-6] 요구사항추적표 (예시)

분석단계		설계단계	구현단계	시험단계	출처
요구사항 ID	요구사항명	화면/보고서 ID	프로그램 ID	시험시나리오 ID	(변경 근거)

라. 인수전략 수립

○ 사업담당자는 대상사업의 완료 시 검사 및 인수 등을 위하여 인수전략과 조건을 정의해야 합니다. 정보보호 제품 및 서비스의 인수전략은 일반적으로 사업자의 계약상 책임 범위(검수 불합격, 지체상금 부과 등)와 관련되므로 인수전략과 조건을 신중하게 고려해야 합니다. 정보시스템 개발사업의 경우 고려해야 할 주요 요소는 다음과 같습니다.

- 사업자가 수행할 테스트의 범위·테스트 요구사항·테스트 장소
- 발주기관이 수행할 운영테스트를 위한 지원
- 예비자원, 지원 장비 등을 포함하는 유지관리사항
- 사업자에 대한 후속 지원
- 시스템 설치 및 운영, 유지관리 전환 지원
- 인수 후 교육·훈련에 관한 지원
- 최종 산출물에 대한 보증(warranty) 등

○ 정보보호 제품 도입시 설치 HW 및 사용자 수 등에 따른 SW 라이센스를 확인해야 합니다.

제 2 절 검사 및 종료

1. 인수 준비

○ 사업담당자는 정의한 인수전략을 기준으로 인수를 위한 준비를 수행합니다.
- 발주자는 사전에 수립된 인수전략과 이슈목록을 검토하고 인수계획을 수립합니다.
- 사업수행계획서 및 계약서상에 명시된 산출물의 종류와 산출물의 유형을 정리합니다.
- 각 산출물의 적합성여부를 평가하기 위한 방법을 수립합니다.
- 인수계획에 따라 인수를 추진하며 필요 시 인수위원회나 평가위원회를 별도로 구성합니다.

○ 인수계획은 아래의 사항들을 고려하여 수립해야 합니다.
- 인수계획서에는 시험사례, 시험자료, 시험절차 및 시험환경에 대한 준비와 공급자의 참여 정도를 정의해야 합니다.
- 발주자는 인수시험을 준비할 때 최종 사용자 참여를 고려해야 하며, 시스템, 소프트웨어 및 정보보호 서비스에 대한 발주사업 유형에 따라 발주조직 내의 운영 및 유지보수 조직을 포함해야 합니다.
- 자격시험, 검증 및 확인과 같은 프로세스의 결과는 인수준비를 위한 자료로 사용될 수 있습니다.
- 발주자는 인수시험 및 검토를 개발자의 지원 없이 독자적으로 수행할 수 있습니다.
- 효과적인 검사를 위해 사업자와의 협의에 의해 검사기준서를 활용할 것을 권고합니다.

2. 검사 및 인수시험

○ 사업담당자는 사업자가 납품하는 소프트웨어 및 정보보호 서비스를 인수하기 위한 검사 및 시험 절차에 따라 수행합니다.
- 인수계획서에 따라 인수에 참여하는 요원들의 임무와 책임을 부여하고 필요한 교육을 실시합니다.
- 산출물별로 정해진 인수담당요원의 책임 하에 검사 및 시험을 실시합니다.
- 각 산출물별 검사 및 시험결과를 문서로 정리합니다.
- 부적합 판정된 산출물이나 결과에 대해 조치방안을 수립하고 별도의 검사 및 시험 절차에 의거 처리합니다.

○ 검사 및 인수시험은 아래의 사항들을 고려하여 수행해야 합니다.
- 발주자는 시스템, 소프트웨어 및 정보보호 서비스가 계약서와 사업 수행계획서에 명시된 인수기준과 조건들을 만족하는지 검사하고, 운영시험을 활용하여 최종사용자의 시험을 수행합니다.
- 정보보호시스템의 특성을 반영하여 평가 및 시험을 수행합니다.
- 시험기준 및 자료가 초기에 작성된 것이라면, 인수시험에서 수정하여 적용할 수 있습니다.

3. 인수 및 사업종료

○ 사업담당자는 사업자가 납품하는 모든 인도물이 계약서상의 요구사항을 충족하는지에 대해 아래의 절차를 기준으로 검사하고, 검사 및 인수시험 결과에 따라 인수하고 사업을 종료합니다.
- 인수한 산출물 품목을 인수계획서와 대조하고 확인합니다.
- 인수한 모든 산출물의 검사 및 시험 결과를 확인합니다.
- 인수계획서에 의거하여 정상적으로 인수 절차가 수행되었는지 확인 합니다.
- 사업담당자와 사업자 상호간 사업종료에 합의하고 사업종료 보고서와 함께 문서로 남깁니다.

○ 인수 및 사업종료는 아래의 사항들을 고려하여 수행해야 합니다.
- 사업담당자는 사업자가 인도하는 산출물의 특성에 따라 하드웨어 또는 소프트웨어 산출물만 인수하거나 관련 컴퓨터 하드웨어 및 내장형(embedded) 소프트웨어를 포함하는 전체 시스템을 인수할 수 있습니다.
- 사업담당자가 산출물을 인수한 이후에는 납품 소프트웨어 산출물의 형상관리에 대한 책임을 져야하며, 형상관리 프로세스를 활용합니다.

○ 또한, 성질상 분할할 수 있는 용역의 일부 기성부분에 대해 인수할 수 있으며, 장기 계속 계약의 경우 연차별 계약금액에 지체상금을 부과할 수 있습니다.

관련근거

정보보호산업 진흥법
제9조(정보보호시스템의 하자담보 책임) ① 정보보호기업은 공공기관등과 정보보호시스템 구축 사업 계약을 체결한 경우 사업을 종료한 날(사업에 대한 시험 및 검사를 수행하여 최종산출물을 인도한 날을 말한다)부터 1년 이내의 범위에서 발생한 하자에 대하여 담보책임이 있다.
② 제1항에도 불구하고 정보보호기업은 다음 각 호의 어느 하나의 사유로 발생한 하자에 대하여는 담보책임이 없다. 다만, 발주자가 제공한 물품 또는 발주자의 지시가 적절하지 아니하다는 것을 알고도 이를 발주자에게 고지하지 아니한 경우에는 그러하지 아니하다.
1. 발주자가 제공한 물품의 품질이나 규격 등이 제7조제2항의 기준에 미치지 못하는 경우
2. 발주자의 지시에 따라 정보보호시스템을 구축한 경우
3. 그 밖에 발주자의 고의 또는 과실로 하자가 발생한 경우

별첨 및 부록

별첨. 서식

[붙임 1호 서식]

일반현황 및 연혁

회 사 명		대 표 자	
사 업 분 야			
주 소			
전 화 번 호			
회 사 설 립 년 도	년 월		
해당부문 종사기간	년 월 ~ 년 월 (년 개월)		

주요연혁

[붙임 2호 서식]

자본금 및 매출액 (최근 3년)

(단위 : 천원)

구 분			M-2 년도	M-1 년도	M 년도
자 본 금					
매출액	정보보호 서비스	보안컨설팅			
		보안관제			
		보안성지속서비스			
		물리보안서비스			
		정보보호시스템 개발			
	정보보호 제품	정보보호 제품 도입 · 구축			
		물리보안 제품 도입 · 설치			
	합 계				

※ 정보보호 서비스 매출액의 경우 보안컨설팅, 보안관제, 보안성지속서비스, 물리보안서비스, 등으로 구분하여 상세히 기재한다.

주요사업실적

사 업 명	사 업 기 간	계 약 금 액	발 주 처	비 고

※ 연도순으로 기재하며, 제안과제와 유사하거나 동일한 업무영역이나 사업형태에 관한 것만 기재한다. 단, 현재수행중인 사업은 비고란에 현재수행중임을 명시한다.
※ 하도급은 발주처가 승인한 경우에 한하여 작성하며 비고란에 원도급회사를 기재한다.
※ 공동도급계약일 경우에는 계약금액란에 제안사의 지분만을 기재한다.
※ 사업별 사용 개발방법론을 비고에 기재한다.
※ 한국소프트웨어산업협회에서 발급하는 이행실적확인서를 가능한 활용.
※ 실적을 확인할 수 있는 실적증명서, 계약서 등의 증거서류제출, 확인이 불가능한 실적은 인정하지 않음
※ 실적증명자료는 붙임으로 첨부하여야 하며, 실적증명 첨부서류에 페이지를 명시하여 주요사업실적 비고란에 페이지를 표시하여야 함

[붙임 3호 서식]

핵심 참여인력 이력사항

성 명		소 속		직 책		연 령	세
참여인력 등급				근무경력 및 기술경력		년 개월	
학술연구용역기준 ( ) SW기술자 기준 ( ) 엔지니어링기술자 기준 ( ) 기타 ( )				자 격 증			
본사업 참여임무						목표투입공수	

경 력				
사 업 명	참 여 기 간 (년월 ~ 년월)	담 당 업 무	발 주 처	비 고

※ 「파견근로자보호 등에 관한 법률」 등에 의한 파견근로자인 경우에는 파견업체명과 원소속사를 함께 명기하여야 함 (예시) 업체명 (원소속사명)

※ 근무 경력확인서, 기술 경력확인서는 「소프트웨어산업 진흥법 시행규칙」 제13조(소프트웨어 기술자의 신고절차 등)에 근거하여 근무 경력확인서 및 기술 경력확인서를 사용자(대표자) 또는 소프트웨어 사업 발주자 확인을 받아 제출(소프트웨어기술자 경력관리기관의 소프트웨어 기술경력증명서 또는 기타 경력을 증빙할 수 있는 서류로도 제출 가능)

※ 자격증, 경력 및 수행업무와 관련된 사항을 증명할 수 있는 자료를 붙임으로 첨부하여야 하며, 첨부되지 않은 자료에 대하여는 인정하지 않음

※ 참여인력이 대표사 또는 공동수급업체 인원인 경우에는 재직증명서를 붙임으로 첨부하고, 그 외 인력(채용예정인력 등)은 추후 추가 협상과정에서 발주기관의 요청이 있을 시 증빙자료를 제출해야 함

※ 핵심 투입인력 평가 심사기준일은 입찰서 제출 마감일 전일로 하며 입찰서 제출마감일 이후 발생신고 또는 수정된 자료는 평가에서 제외됨

※ 입찰자가 하도급 계약할 경우는 하도급 예정자의 기술자 등급별 인원 현황만 제출하고 하도급 예정자에 대한 증빙서류는 제출하지 않음

[붙임 4호 서식]

[ ] 기술적용계획표, [ ] 기술적용결과표

사업명	
작성일	

□ 법률 및 고시

구분	항 목
법률	o 국가정보화 기본법 o 공공기관의 정보공개에 관한 법률 o 개인정보 보호법 o 소프트웨어산업 진흥법 o 인터넷주소자원에 관한 법률 o 전자서명법 o 전자정부법 o 정보통신기반 보호법 o 정보통신망 이용촉진 및 정보보호 등에 관한 법률 o 통신비밀보호법 o 국가를 당사자로 하는 계약에 관한 법률 o 하도급거래 공정화에 관한 법률 o 지방자치단체를 당사자로 하는 계약에 관한 법률
고시 등	o 보안업무규정(대통령령) o 행정기관 정보시스템 접근권한 관리 규정(국무총리훈령) o 장애인·고령자 등의 정보 접근 및 이용 편의 증진을 위한 지침(과학기술정보통신부고시) o 전자서명인증업무지침(과학기술정보통신부고시) o 전자정부서비스 호환성 준수지침(행정안전부고시) o 정보보호시스템 공통평가기준(과학기술정보통신부고시) o 정보보호시스템 평가·인증 지침(과학기술정보통신부고시) o 정보시스템 감리기준(행정안전부고시) o 전자정부사업관리 위탁에 관한 규정(행정안전부고시) o 전자정부사업관리 위탁용역계약 특수조건(행정안전부예규) o 행정전자서명 인증업무지침(행정안전부고시) o 행정기관 도메인이름 및 IP주소체계 표준(행정안전부고시) o 개인정보의 안전성 확보조치 기준(행정안전부고시) o 정보보호 관리체계 인증 등에 관한 고시(과학기술정보통신부고시) o 지방자치단체 입찰 및 계약 집행 기준(행정안전부예규) o 지방자치단체 입찰시 낙찰자 결정기준(행정안전부예규) o 표준 개인정보 보호지침(행정안전부고시) o 엔지니어링사업대가의 기준(산업통상자원부고시) o 소프트웨어 기술성 평가기준(과학기술정보통신부고시) o 소프트웨어사업의 제안서 보상기준 등에 관한 운영규정(과학기술정보통신부

구분	항 목
	고시) o 분리발주 대상 소프트웨어(과학기술정보통신부고시) o 대기업인 소프트웨어사업자가 참여할 수 있는 사업금액의 하한(과학기술정보통신부고시) o 소프트웨어 품질인증의 세부기준 및 절차(과학기술정보통신부고시) o 소프트웨어사업의 하도급 승인 및 관리 지침(과학기술정보통신부고시) o 소프트웨어 품질성능 평가시험에 관한 지침(과학기술정보통신부고시) o 용역계약일반조건(기획재정부계약예규) o 협상에 의한 계약체결기준(기획재정부계약예규) o 하도급거래 공정화지침(공정거래위원회예규) o 정보보호조치에 관한 지침(과학기술정보통신부고시) o 개인정보의 기술적·관리적 보호조치 기준(방송통신위원회고시)

210mm×297mm[백상지 80g/㎡]

□ 서비스 접근 및 전달 분야

구 분	항 목	적용계획/결과				부분적용/미적용 시 사유 및 대체기술
		적용	부분적용	미적용	해당없음	
기본 지침						
o 정보시스템은 사용자가 다양한 브라우저 환경에서 서비스를 이용할 수 있도록 표준기술을 준수하여야 하고, 장애인, 저사양 컴퓨터 사용자 등 서비스 이용 소외계층을 고려한 설계·구현을 검토하여야 한다.						
세부 기술 지침						
외부 접근 장치	o 웹브라우저 관련 - HTML 4.01/HTML 5, CSS 2.1					
	- XHTML 1.0					
	- XML 1.0, XSL 1.0					
	- ECMAScript 3rd					
	- 한국형 웹 콘텐츠 접근성 지침 2.1					
	o 모바일 관련 - 모바일 웹 콘텐츠 저작 지침 1.0 (KICS.KO-10.0307)					
서비스 요구사항	서비스관리(KS X ISO/IEC 20000)/ ITIL v3					
서비스 전달 프로토콜	IPv4					
	IPv6					

□ 인터페이스 및 통합 분야

구 분	항 목	적용계획/결과				부분적용/미적용시 사유 및 대체기술
		적용	부분적용	미적용	해당없음	
기본 지침						
o 정보시스템간 서비스의 연계 및 통합에는 웹서비스 적용을 검토하고, 개발된 웹서비스 중 타기관과 공유가 가능한 웹서비						

구 분	항 목	적용계획/결과				부분적용/미적용시 사유 및 대체기술
		적용	부분적용	미적용	해당없음	
스는 범정부 차원의 공유·활용이 가능하도록 지원하여야 한다.						
세부 기술 지침						
서비스 통합	o 웹 서비스 - SOAP 1.2, WSDL 2.0, XML 1.0					
	- UDDI v3					
	- RESTful					
	o 비즈니스 프로세스 관리 - UML 2.0/BPMN 1.0					
	- ebXML/BPEL 2.0/XPDL 2.0					
데이터 공유	o 데이터 형식 : XML 1.0					
인터페이스	o 서비스 발견 및 명세 : UDDI v3, WSDL 2.0					

□ 플랫폼 및 기반구조 분야

구 분	항 목	적용계획/결과				부분적용/미적용 시 사유 및 대체기술
		적용	부분적용	미적용	해당없음	
기본 지침						
o 정보시스템 운영에 사용되는 통신장비는 IPv4와 IPv6가 동시에 지원되는 장비를 채택하여야 한다.						
o 하드웨어는 이기종간 연계가 가능하여야 하며, 특정 기능을 수행하는 임베디드 장치 및 주변 장치는 해당 장치가 설치되는 정보시스템과 호환성 및 확장성이 보장되어야 한다.						
세부 기술 지침						
네트워크	o 화상회의 및 멀티미디어 통신 : H.320~H.324, H.310					
	o 부가통신: VoIP - H.323					
	- SIP					
	- Megaco(H.248)					
운영체제 및 기반 환경	o 서버용(개방형) 운영 체제 및 기반환경 : - POSIX.0					
	- UNIX					
	- Windows Server					
	- Linux					
	o 모바일용 운영 체계 및 기반환경 - android					
	- IOS					
	- Windows Phone					
데이터베이스	o DBMS					

구 분	항 목	적용계획/결과				부분적용/미적용 시 사유 및 대체기술
		적용	부분적용	미적용	해당없음	
	- RDBMS					
	- ORDBMS					
	- OODBMS					
	- MMDBMS					
시스템 관리	o ITIL v3 / ISO20000					
소프트웨어 공학	o 개발프레임워크 : 전자정부 표준프레임워크					

□ 요소기술 분야

구 분	항 목	적용계획/결과				부분적용/미적용 시 사유 및 대체기술
		적용	부분적용	미적용	해당없음	
기본 지침						
o 응용서비스는 컴포넌트화하여 개발하는 것을 원칙으로 한다.						
o 데이터는 데이터 공유 및 재사용, 데이터 교환, 데이터 품질 향상, 데이터베이스 통합 등을 위하여 표준화되어야 한다.						
o 행정정보의 공동활용에 필요한 행정코드는 행정표준코드를 준수하여야 하며 그렇지 못한 경우에는 행정기관등의 장이 그 사유를 행정안전부장관에게 보고하고 행정안전부의“행정기관의 코드표준화 추진지침”에 따라 코드체계 및 코드를 생성하여 행정안전부장관에게 표준 등록을 요청하여야 한다.						
o 패키지소프트웨어는 타 패키지소프트웨어 또는 타 정보시스템과의 연계를 위해 데이터베이스 사용이 투명해야 하며 다양한 유형의 인터페이스를 지원하여야 한다.						
세부 기술 지침						
데이터 표현	o 정적표현 : HTML 4.01					
	o 동적표현 - JSP 2.1					
	- ASP.net					
	- PHP					
	- 기타 ( )					
프로그래밍	o 프로그래밍 - C					
	- C++					
	- Java					

구 분	항 목	적용계획/결과				부분적용/미적용 시 사유 및 대체기술
		적용	부분적용	미적용	해당없음	
	- C#					
	- 기타 ( )					
데이터 교환	o 교환프로토콜: - XMI 2.0					
	- SOAP 1.2					
	o 문자셋 - EUC-KR					
	- UTF-8(단, 신규시스템은 UTF-8 우선 적용)					

□ 보안 분야

구 분	항 목	적용계획/결과				부분적용/미적용 시 사유 및 대체기술
		적용	부분적용	미적용	해당없음	
기본 지침						
o 정보시스템의 보안을 위하여 위험분석을 통한 보안 계획을 수립하고 이를 적용하여야 한다. 이는 정보시스템의 구축 운영과 관련된 “서비스 접근 및 전달”, “플랫폼 및 기반구조”, “요소기술” 및 “인터페이스 및 통합” 분야를 모두 포함하여야 한다.						
o 보안이 중요한 서비스 및 데이터의 접근에 관련된 사용자 인증은 공인 전자서명 또는 행정전자서명을 기반으로 하여야 한다.						
o 네트워크 장비 및 네트워크 보안장비에 임의 접속이 가능한 악의적인 기능 등 설치된 백도어가 없도록 하여야 하고 보안기능 취약점 발견 시 개선·조치하여야 한다.						
세부 기술 지침						
관련 규정	o 전자정부법 o 국가정보보안기본지침(국가정보원) - 국가 사이버안전 매뉴얼 o 네트워크 장비 구축·운영사업 추가특수조건(조달청 지침)					
제품별 도입 요건 및 보안 기준 준수	o 국정원 검증필 암호모듈 탑재·사용 대상(암호가 주기능인 정보보호제품) - PKI제품					
	- SSO제품					
	- 디스크·파일 암호화 제품					
	- 문서 암호화 제품(DRM)등					
	- 메일 암호화 제품					
	- 구간 암호화 제품					
	- 키보드 암호화 제품					
	- 하드웨어 보안 토큰					
	- DB암호화 제품					
	- 상기제품(9종)이외 중요정보 보호를 위해 암호기능이 내장된 제품					

구 분	항 목	적용계획/결과				부분적용/미적용 시 사유 및 대체기술
		적용	부분적용	미적용	해당없음	
	- 암호모듈 검증서에 명시된 제품과 동일 제품 여부					
	o CC인증 필수제품 유형군(국제 CC인 경우 보안적합성 검증 필요) - (네트워크)침입차단					
	- (네트워크)침입방지(침입탐지 포함)					
	- 통합보안관리					
	- 웹 응용프로그램 침입차단					
	- DDos 대응					
	- 인터넷 전화 보안					
	- 무선침입방지					
	- 무선랜 인증					
	- 가상사설망(검증필 암호모듈 탑재 필수)					
	- 네트워크 접근통제					
	- 네트워크 자료유출방지					
	- 망간 자료전송					
	- 안티 바이러스					
	- 가상화(PC 또는 서버)					
	- 패치관리					
	- 호스트 자료유출 방지(매체제어제품 포함, 자료저장 기능이 있는 경우 국정원 검증필 암호모듈 탑재 필수)					
	- 스팸메일 차단					
	- 서버 접근통제					
	- DB접근 통제					
	- 스마트카드					
	- 소프트웨어기반 보안USB(검증필 암호모듈 탑재 필수)					
	- 디지털 복합기 (비휘발성 저장매체 장착 제품에 대한 완전삭제 혹은 암호화 기능)					

구 분	항 목	적용계획/결과				부분적용/미적용 시 사유 및 대체기술
		적용	부분적용	미적용	해당없음	
	- 소스코드 보안약점 분석도구					
	- 스마트폰 보안관리					
	- CC인증서에 명시된 제품과 동일 제품 여부					
	o 모바일 서비스(앱·웹) 등 - 보안취약점 및 보안약점 점검·조치 (모바일 전자정부 서비스 관리 지침)					
백도어 방지 기술적 확인 사항	o 보안기능 준수 - 식별 및 인증					
	- 암호지원					
	- 정보 흐름 통제					
	- 보안 관리					
	- 자체 시험					
	- 접근 통제					
	- 전송데이터 보호					
	- 감사 기록					
	- 기타 제품별 특화기능					
	o 보안기능 확인 및 취약점 제거 - 보안기능별 명령어 등 시험 및 운영방법 제공					
	- 취약점 개선(취약점이 없는 펌웨어 및 패치 적용)					
	- 백도어 제거(비공개 원격 관리 및 접속 기능)					
	- 오픈소스 적용 기능 및 리스트 제공					

※ 최신 기준은 '국가정보원 홈페이지(www.nis.go.kr/AF/1_7_2_1.do)' 참조

[붙임 5호 서식]

하도급 대금지급 비율 명세서

원도급자			하도급자			
사 업 명			하 도 급 사 업 명			
회 사 명			회 사 명			
사업기간			하 도 급 기 간			
			하도급 지급대금			원
하도급 지급대금 세부내역	①구 분	②SW 월 노임단가	③투입인력 (MM)	④MM당 하도급 대가	⑤지급금액 (③×④)	⑥지급 비 율
	합 계					

상기와 같이 합의하였음을 확인합니다.

년 월 일

(원도급자) 직인

(하도급자) 직인

첨부서류 : 하도급 부문 산출 내역서

① 구분 : 소프트웨어산업진흥법 제2조 5항에서 정한 소프트웨어 기술자

② SW 월노임단가 : 한국SW산업협회에서 공표하는 일노임단가 × 근무일수

④ MM당 하도급 대가 : 원도급자가 하도급자에게 지급하는 직접인건비 + 제경비 + 기술료

⑥ 지급비율 : Σ지급금액 ÷ Σ(SW 월노임단가 × 투입인력)

[붙임 6호 서식

정보보호시스템 구축 사업 [ ] 하 도 급 [ ] 재하도급 계약승인신청서

※ [ ]에는 해당되는 곳에 √표를 하시고, 아래 바탕색이 어두운 난은 신청인이 적지 않습니다.

(앞쪽)

접수번호	접수일자	처리기간 14일

하도급 거래 계약 당사자	원도급자	상호		대표자		
		사업자등록번호		소재지		
	하도급자	상호		대표자		
		사업자등록번호		소재지		
	재하도급자	상호		대표자		
		사업자등록번호		소재지		

사업 내용	계약명		계약번호		계약금액	
	계 약 일	년 월 일	계약기간	. . .부터 . . . 까지		

하도급 내용	계약명			하도급액		
	계약예정일	년 월 일	계약기간	. . .부터 . . . 까지		
	하도급 내역 및 사유	(※ 필요한 경우 별지 사용)				

재하도급 내용	계약명			재하도급액		
	계약예정일	년 월 일	계약기간	. . .부터 . . . 까지		
	재하도급 내역 및 사유	(※ 필요한 경우 별지 사용)				

「정보보호산업의 진흥에 관한 법률」 제8조 및 같은 법 시행규칙 제2조제1항에 따라 위와 같이 신청합니다.

년 월 일

신청인 (서명 또는 인)

발주기관의 장 귀하

신청인 제출서류	1. 하도급(또는 재하도급) 계약서안(세부 산출내역서 포함) 1부 2. 하도급(또는 재하도급) 사업수행계획서(세부 사업추진일정표 포함) 1부	수수료 없 음

210mm×297mm(백상지 80g/㎡)

[별지 1]

사업수행업체 보안 준수사항

※ 작성근거 : 국가정보보안기본지침(국정원), 정보보안지침(행안부 훈령19호) 등

1. 공통사항

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

○ 사업자는 사업 수행에 사용되는 문서, 인원, 장비 등에 대하여 물리적, 관리적, 기술적 보안을 유지하여야 하며, '누출금지 대상정보' 누출 시 발주기관은 국가계약법 시행령 제76조에 따라 사업자를 부정당업체로 등록한다.

〈 누출금지 대상정보 〉

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 네트워크 장비 설정 정보
⑧ '공공기관의 정보공개에 관한 법률' 제9조1항에 따라 비공개 대상정보로 분류된 기관의 내부문서
⑨ '개인정보 보호법' 제2조1호의 개인정보
⑩ 사업 수행 중 습득·인지한 보안정보
⑪ 그 밖의 발주자가 공개가 불가하다고 판단한 자료

○ 사업자는 발주기관의 보안정책을 위반하였을 경우 발주기관의 위규처리 기준에 따라 위규자 및 관리자를 행정조치하고 손해배상 책임을 진다.

※ 보안 위약금 부과기준에 따라 해당금액을 발주기관에 납부한다.

○ 사업자는 사업 최종 산출물에 대해 정보보안전문가 또는 전문보안 점검도구를 활용하여 보안 취약점을 점검, 도출된 취약점에 대한 개선을 완료하고 그 결과를 제출해야 한다.

2. 용역사업 참여인원에 대한 보안관리

○ 용역사업 참여인원 중 최고 직급자를 보안책임관으로 지정, 발주기관의 승인을 받아야 한다.
○ 용역사업 참여인원은 보안서약서를 작성 후, 발주기관에 제출하여야 한다.
○ 용역사업 참여인원은 업체 임의로 교체 할 수 없으며, 신상변동(해외여행 포함)사항 발생 시 즉시 보고하여야 한다.
○ 용역사업 시작 전 참여인원에 대한 비밀유지의무 준수 등의 교육을 실시하고, 발주기관의 확인을 받아야 한다.
○ 용역사업 참여인원이 업무를 수행할 장소는 외부인의 출입을 통제하여야 하며, 부재시에는 반드시 시건장치를 하여야 한다.
○ 용역사업 수행 중 발주기관 정보시스템에 위해를 가할 수 있는 행위는 절대 불가하며, 정보시스템 접근이 필요한 경우에는 발주기관의 사전승인을 득한 후 보안관리 담당자의 입회하에 실시하여야 한다.

3. 내부자료에 대한 보안관리

○ 전산망구성도·IP 현황 등 발주기관에서 제공하는 내부자료에 대해서는 상호간의 책임자가 직접 서명한 후 인수·인계하여야 한다.
○ 사업수행을 위해 제공된 내부 자료는 복사 및 외부반출을 금지한다.
○ 제공된 내부 자료는 매일 퇴근 시 반납하여야 하며, 다만 비밀문서를 제외한 일반문서는 제공된 사무실에 시건장치가 된 보관함이 있을 경우 이를 보관함에 보관할 수 있다.
○ 발주기관 보안관리 담당자가 사업수행업체에 제공된 사무실에 보관된 자료에 대해 수시로 확인할 수 있도록 하여야 한다.

4. 용역사업 관련 장비에 대한 보안관리

○ CD-RW 등의 보조매체 기록장치는 발주기관과의 상호협의 하여 제한된 PC에서만 사용하여야 한다.
○ USB, 외장하드디스크 등의 탈착이 용이한 보조기억매체의 사용은 금지한다. 다만, 산출물작성 등의 보조기억매체가 필요한 경우에는 발주기관의 관리 하에 사용하도록 한다.
○ 용역사업 종료 시까지는 반입된 PC의 반출을 금지한다. 다만, 사업 수행 상 외부 반출이 필요한 경우는 자료 유출에 대비한 보안대책을 발주기관에 제출하여 발주기관 보안관리 담당자의 승인 후 최소한의 장비만 반출 할 수 있다.
  • 용역사업 참여인원이 퇴근 시에 외부로 반출 할 수 없으며, 반드시 제공된 사무실내의 시건장치가 있는 보관함에 보관하여야 한다.
○ 용역사업 종료 시 계약자의 PC 및 보조기억장치는 완전 삭제 후 반출하여야 한다.

5. 내·외부망 접근에 대한 보안관리

○ 사업 수행 시 발주기관 내부망에 대한 접속은 반드시 발주기관의 승인을 득한 후 하여야 한다.
○ 사업자가 사용하는 PC는 인터넷 연결을 금지함을 원칙으로 한다. 다만, 사업 수행상 필요 한

경우는 사업체의 보안책임관이 접속이 필요한 PC와 웹사이트·서버를 선정하여 직접 발주기관 보안담당자에 요청하여, 승인을 득한 후 사용하여야 한다.

6. 산출물에 대한 보안관리

○ 사업 수행 시 생산되는 모든 산출물은 업체의 보안책임관의 관리 하에 있는 파일서버에 저장하여야 하며, 계정관리 및 접근권한 부여하여 관리를 철저히 하여야 한다.

○ 사업 수행 시 생산된 산출물 및 기록은 발주기관 보안관리 담당자가 인가하지 않은 비인가자에게 제공·대여·열람을 금지한다.

○ 사업종료 후 최종산출물에 대해 “대외비”임을 표기하여 발주기관에 제출하여야 하며, 기타 자료는 삭제 및 세단 후 폐기하고 발주기관 보안관리 담당자의 점검을 받아야 한다.

○ 최종산출물 및 관련 자료는 사업 수행업체의 보관을 금지함을 원칙으로 한다. 다만, 유지보수 등으로 필요한 경우에는 발주기관보안관리 담당자의 승인을 득한 후 사용할 수 있다.

○ 정보시스템 구축 사업인 경우 사업자는 사업 완료전에 정보보안 전문가 또는 전문 보안점검도구를 활용하여 보안 취약점을 점검하고, 도출된 취약점에 대한 개선을 완료하여 그 결과를 제출하여야 한다.

- 정보시스템 도입·운용하기 전 보안취약점 진단 및 조치
- 소프트웨어 보안취약점 진단 및 조치

※ 소프트웨어개발보안(시큐어코딩) 준수 : 행정기관 및 공공기관 정보시스템 구축·운영 지침, 소프트웨어 개발보안 가이드 참조

· 신규개발의 경우 : 소스코드 전체

· 유지보수의 경우 : 유지보수로 인해 변경된 소스코드 전체

- 웹 어플리케이션에 대한 웹서비스인 경우 취약점 진단 및 조치

※ 전자정부서비스 웹 취약점 표준 점검 21개 항목 참조

[별지 2]

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 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 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 용역 사업 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 연결사용 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

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. 캐비닛 · 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. 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 모니터옆 등 외부에 노출 바. 비인가 보조기억매체 무단 사용	○ 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. 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

※ 사업자 보안위규 처리 절차

경위 확인 ▶ 보안위규 처리기준에 따라 조치 ▶ 재발방지 대책 ▶ 보안조치 이행여부 점검

[별지 3]

보안 위약금 부과 기준

1. 위규 수준별로 A~D 등급으로 차등 부과

구 분	위규 수준			
	A급	B급	C급	D급
위 규	심각 1건	중대 1건	보통 2건 이상	경미 3건 이상
위약금 비중	부정당업자 등록	총계약금의 5%	총계약금의 3%	총계약금의 1%

* 위규 수준은 [붙임1] 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

부록. 발주가이드 참고 자료

1. 사업유형 분류표

[표] 정보보호사업 유형

구분	정보보호 사업 유형	정의
정보보호 제품	정보보호 제품 도입 · 구축 사업	보안관리, 침입탐지, 분석대응 및 복구 관련 제품 도입 및 적용
	물리보안 제품 도입 · 설치 사업	CCTV 설치사업 등의 특성 조사 후 별도 분리 여부 결정 예정
정보보호 서비스	정보보안 컨설팅 사업	취약점 분석 평가, 정보보호관리체계(ISMS), 개인정보보호 (PIMS, PIA), 기본·종합컨설팅, 개발보안컨설팅 등
	보안성지속서비스 사업	정보보호 제품 보안성 유지 관리, 사고 분석, 인증 및 자문 등
	보안관제 사업	보안관제, 원격관제, 모의훈련 등
	물리보안 서비스 사업	영상보안, 출동보안 서비스, 교육훈련 포함
	정보보호시스템 개발 사업	개인정보보호시스템, 보안관리시스템, 보안관제시스템, 사이버안전센터 구축 등 특정 목적의 정보보호시스템을 개발하는 사업 ※ 정보보호제품 통합/분리발주 가능

2. 요구사항 표준 패키지

[표] 정보보호 요구사항 대비 SW사업 요구사항 비교표

	Level 1		Level 2		Level 3			SW사업 RFP 가이드
유 형 분류	Code	요구사항명	Code	요구사항 명	Code	요구사항 명	Code	**요구사항 명**
사 업 공 통 요 구 사항	CFI	프로젝트 기밀성 유지 요구사항	AMS	관리적 보안 준수사항			MSE	관리적보안관리
			PHS	물리적 보안 준수사항			PSE	물리적보안관리
			TES	기술 보안 준수사항				신규추가
			LAS	법률 및 인증 준수사항				신규추가
	PMR	프로젝트 관리	HUM	인력 관리			HUM	인력구성방안
			CON	공동 수급 관련 요구사항			CON	공동수급관련 요구사항
			COO	하도급 협력 방안			COO	하도급 협력방안
			SCH	사업 일정 관리			SCH	일정관리
			SCO	요구사항 관리			SCO	요구사항 관리
			RIS	위험 관리 사항			RIS	위험관리
			DOC	산출물 관리 사항			DOC	산출물관리
			QAL	품질 관리 사항			QAL	품질관리
	PSR	프로젝트 지원	DEF	하자 보수 사항			DEF	하자 보수
			EDT	교육 훈련			EDT	교육 및 기술이전
			TTR	기술 이전			TTR	기술이전
			PRS	문제 상황 대응				시스템안정화(STA)를 좀 더 넓은 범위로 확장(조달청)
	COR	제약사항	HRE	수행 업체 제한				신규추가
			CRE	하도급 제한				
			IPR	지적 재산권 제한				
			DAT	데이터 제약사항			DAT	데이터 제약사항
			SDC	시스템 개발 제한			SDC	시스템 개발 제한
			DEG	설계 및 구현 제약사항			DEG	설계 및 구현 제약사항
			BIZ	업무 제약사항			BIZ	업무 제약사항
			STD	표준 제약사항			STD	표준 제약사항
	QUR	품질 요구사항	REL	신뢰성			REL	신뢰성
			USE	사용성			USE	사용성
			INT	이식성			INT	이식성
			MAT	유지 관리성			MAT	유지관리성
				효율성				신규추가
				기능성				

	Level 1		Level 2		Level 3			SW사업 RFP 가이드
유 형 분류	Code	요구사항명	Code	요구사항 명	Code	요구사항 명	Code	**요구사항 명**
사 업 선 택 요 구 사항	OFR	자산 관리 기능 요구사항	IAM	정보 자산 관리 기능				
			HAM	하드웨어 자산 관리 기능				
			SAM	소프트웨어 자산 관리 기능				
	PER	성능 요구사항	GEN	성능 일반			GEN	성능 일반
			SPD	처리 속도 및 시간 성능			SPD	처리 속도 및 시간 성능
			THR	처리량 요구사항			THR	처리량
			RES	자원 사용량 요구사항			RES	자원 사용량
	TER	테스트 요구사항	하드웨어T	통합 테스트			하드웨어T	통합 테스트
			PIL	성능 테스트			PER	성능테스트
			UNT	단위 테스트			UNT	단위 테스트
			SYT	시스템 테스트			SYT	시스템 테스트
			UST	사용자 테스트				기존 장비 및 시험개발 테스트를 사용자테스트로 수정(조달청)
			UAT	인수 테스트			UAT	인수 테스트
	DAR	데이터 요구사항	GAI	데이터 수집 및 입력 요구사항			GAI	데이터 수집 및 입력
			IND	초기 데이터 구축 요구사항			IND	초기 데이터 구축
			QUA	데이터 품질 요구사항			QUA	데이터 품질
			BKR	백업 및 복구 요구사항			BKR	백업 및 복구
	INR	인터페이스 요구사항	UIR	사용자 인터페이스 요구사항			UIR	사용자 인터페이스
			SIR	시스템 인터페이스 요구사항			SIR	시스템 인터페이스
	CNR	제품 컨설팅 요구사항	ENV	환경분석			ENV	환경분석
			STA	현황분석			STA	현황분석
			WOR	개선 과제 도출			WOR	개선 과제 도출
			TOB	목표 모델 설계			TOB	목표 모델 설계
			PLN	개선 계획 수립			PLN	개선 계획 수립
			ACT	실행 계획 수립			ACT	실행 계획 수립
			GOA	정보보호시스템 방향성 수립			GOA	정보시스템 방향성 수립
			ASI	업무 및 정보 기술 요건 분석			ASI	업무 및 정보기술요건 분석
			REQ	정보 보호 시스템 구조 및 요건 정의			REQ	정보시스템 구조 및 요건 정의

	Level 1		Level 2		Level 3			SW사업 RFP 가이드
유 형 분류	Code	요구사항명	Code	요구사항 명	Code	요구사항 명	Code	**요구사항 명**
			IMP	정보보호 시스템 구축 사업 계획 수립			IMP	정보시스템 구축사업 이행방안 수립
			RFP	제안서 작성			RFP	제안요청서 작성
			BAS	기반 정립			BAS	기반정립
			ASR	현행 아키텍처 수립			ASI	현행아키텍처 수립
			TAR	목표 아키텍처			TAR	목표아키텍처 구축
			MPP	이행계획 수립			IMP	이행계획 수립
			MAG	관리체계 수립			MAG	관리체계 수립
정보보호제품선택요구사항	ECR	시스템 장비 구성 요구사항	P/M	보안 관리(Protection & Management) 장비 구성	ACM	접근통제		개정된 정보보호사업유형 구분에 따라 신규추가
					PAM	암호/인증관리		
					DCS	데이터·콘텐츠 보안		
					NWS	네트워크 보안		
					MOS	모바일 보안		
					BIO	바이오인식		
					SSM	보안운영		
			D/M	침입 탐지(Detection & Monitor) 장비 구성	PDS	침입방지 및 탐지		
					MON	모니터링		
			R/R	대응 및 복구(Response & Recovery) 장비 구성	IVM	침해 관리		
					RNB	복구 및 백업	BKR	백업 및 복구
			EEC	기타 장비 구성	IMR	영상 기록		물리보안제품(CCTV, 영상보안 등)의 주요 기능에 따른 요구사항 신규추가
					IRP	영상 기록 보호		
	SFR	보안 기능 요구사항	P/M	보안 관리(Protection & Management) 기능	ACM	접근통제		개정된 정보보호사업유형 구분에 따라 신규추가
					PAM	암호/인증관리		
					DCS	데이터·콘텐츠 보안		
					NWS	네트워크 보안		
					MOS	모바일 보안		
					BIO	바이오인식		
					SSM	보안운영		
			D/M	침입 탐지(Detection & Monitor) 기능	PDS	침입방지 및 탐지		
					MON	모니터링		
			IAM	침해관리(infringement accident management) 기능	IAR	침해 대응		
					RNB	복구 및 백업 (Recovery & backup)	BKR	백업 및 복구
			ESF	기타 기능 구성	IMR	영상 기록		물리보안제품(C

	Level 1		Level 2		Level 3			SW사업 RFP 가이드
유 형 분류	Code	요규사항명	Code	요구사항 명	Code	요구사항 명	Code	**요구사항 명**
					IRP	영상 기록 보호		CTV, 영상보안 등)의 주요 기능에 따른 요구사항 신규추가
	TSC	정보 보안 컨설팅	GSC	보안 컨설팅 일반 요구사항				정보보안컨설팅 하위 분류에 따른 요구사항 항목 신규추가
			ISMS	정보보안 인증체계 요구사항				
			SCG	솔루션 컨설팅 요구사항				
			AMR	접근 관리 요구사항				
			AUT	정보 감사				
			ISMP	정보보호 마스터 플랜 수립			ISM	ISMP
			PIM	개인정보보호 관리 체계 구축 요구사항				정보보안컨설팅 하위 분류에 따른 요구사항 항목 신규추가
			EDC	교육 콘텐츠 개발 요구사항				
			PTR	모의 해킹			HAK	모의해킹
			VSR	취약점 진단			VLS	취약점 점검
	PSS	보안성지속 서비스	OMT	시스템 운영 및 유지 관리 대상			OMT	운영 및 유지관리 대상
			HLD	시스템 유지 관리 서비스 데스크운영			HLD	서비스데스크
	SMS	보안관제	BCS	원격·파견관제 서비스				보안관제 기본서비스 및 부가서비스에 대한 요구사항 항목 신규 추가
			SOS	보안관제 부가서비스				
	SIM	SI 서비스 사업 요구사항	HRM	조직 및 인력관리			ONM	조직과 인력
			SAA	시스템 분석·설계				신규추가
			INS	시스템 장비 설치			INS	설치
			SYT	시스템 테스트			SYT	시스템 테스트
			PRI	시스템 유지 관리를 위한 예방 점검 및 보안 관리			PRI	예방점검
	PEI	물리보안 및 기타 정보보호 서비스	VMS	영상 보안				물리보안 서비스에 따른 요구사항 항목 신규추가
			SPS	출동 보안				
			EDM	정보보안 및 개인정보보호 교육			UST	사용자 교육
			ICS	기타 서비스				물리보안외 신규 정보보호서비스에 대한 요구사항 항목 신규추가

3. 사업유형별 요구사항 매핑표

[표] 정보보호사업 발주 요구사항 매핑표

필수 평가 부분			정보보호제품		정보보호서비스				
			정보보호제품 도입 및 구축	물리보안제품 도입 및 구축	보안 컨설팅	보안성 지속서비스	보안 관제	물리보안 서비스	정보보호시스템 개발
공통 요구사항	프로젝트 기밀성 유지 요구사항		●	●	●	●	●	●	●
	프로젝트 관리		●	●	●	●	●	●	●
	프로젝트 지원		●	●	●	●	●	●	●
	제약사항		●	●	●	●	●	●	●
	품질 요구사항		●	●	●	●	●	●	●
선택 요구사항	자산관리 기능 요구사항		●	●				○	●
	성능 요구사항		●	○				○	●
	테스트 요구사항		●	○				○	●
	데이터 요구사항		●	○				○	●
	인터페이스 요구사항		●	○				○	●
	제품 컨설팅 요구사항		●	●				○	●
정보보호 제품 요구사항	시스템 장비 구성	보안관리 장비구성	●						
		침입탐지 장비구성	●						
		대응 및 복구 장비구성	●						
		기타 장비 구성		●					
	보 안 기능	보안관리 기능	●						
		침입탐지 기능	●						
		침해관리 기능	●						
		기타 기능 구성		●					
정보보호 서비스 요구사항	정보 보안 컨설팅	보안컨설팅 공통 일반			●	○	○	○	○
		정보보호관리체계 인증			●				
		개인정보보호관리체계 구축			●				
		개인정보영향평가			●				
		정보보호 마스터 플랜 수립			●				
		교육체계 및 콘텐츠 개발			●				
		모의해킹			●				
		보안취약점 진단			●				
	보안성 지속 서비스				○	●	○	○	○
	보안 관제	원격 파견관제 서비스			○	○	●	○	○
		보안관제 부가서비스			○	○	●	○	○
	SI 서비스 사업 요구사항				○	○	○	○	●
	물리보안 및 기타 정보보호서비스				○	○	○	●	○

4. 제안요청서 적용 법제도 목록

[표] 정보보호사업 발주 시 적용 규정 (SW사업과 비교)

(○ 적용 △ 참조)

No	적용 규정	SW 사업	정보보호사업
1	SW분리발주 및 SW품질성능 평가시험(BMT)	○	○
2	대기업(상출제 포함) 참여제한	○	△
3	사업금액하한 적용기준 (일괄발주/장기계속 유지보수 계약)	○	△
4	대기업 공동수급제한	○	△
5	하도급 제한	○	○
6	작업장소 상호협의	○	○
7	지식재산권 공동귀속	○	○
8	개발SW의 공동활용 사전명시	○	△
9	하자담보 책임기간 및 범위	○	○
10	특정규격 명시 금지	○	○
11	협상에 의한 계약 방식 적용	○	○
12	기술능력평가비중 (90%) 도입	○	○
13	SW기술성평가기준 적용	○	○
14	SW사업 제안서 보상	○	△
15	무상유지보수 용어 사용 금지	○	△
16	요구사항 상세화	○	○
17	SW사업 적정사업기간 산정	○	×
18	투입인력 관리 금지	○	△
19	SW사업정보 제출	○	×
20	정보보호 서비스의 적정대가 지급		○
21	표준계약서 사용		○
22	보안관제사업 입찰참가자격 제한		○
23	정보보호컨설팅사업 입찰참가자격 제한		○
24	정보보호시스템 유형별 도입여건 만족 여부(CC인증)		○
25	개인정보영향평가기관 입찰참가자격 제한		○

[표] SW사업 대비 정보보호사업 관련 법제도 준수요건

No	대상 제도	법적 근거	판단기준	정보보호 사업
★1	SW분리발주 및 SW품질성능 평가시험(BMT)	• 법 제20조제2항・제13조의2 • 분리발주 대상 SW(고시) • SW 품질성능 평가시험에 관한 지침(고시)	• 총 사업규모가 5억원 이상인 SW사업에서 상용SW 도입이 있는 경우 • 조달청 종합쇼핑몰 등록제품 또는 5천만원 이상이며 소프트웨어품질인증・NEP 등 국가인증을 획득한 5종의 제품 • 예외사유 적용시 제안요청서에 제외사유서 첨부여부 • 분리발주 대상 SW를 경쟁입찰(조달청 종합쇼핑몰 등록제품 예외)로 구매하는 경우 BMT 실시 및 결과 반영 명시 여부	소프트웨어산업 진흥법 제20조 제2항
★2	대기업(상출제 포함) 참여제한	• 법 제24조의2 • 대기업인 SW사업자가 참여할 수 있는 사업 금액의 하한(고시) • 대기업의 공공SW사업자 참여제한 예외사업(고시)	• 발주사업금액에 따른 대기업참여하한 적용 및 입찰참가자격 명시여부 • 상출제기업 참여제한 명시여부 • 예외사업 해당 시 명시여부	
★3	사업금액하한 적용기준 (일괄발주/장기계속 유지보수 계약)	• 법 제24조의2제2항	• 2개 이상의 다른 사업을 통합하여 일괄 입찰하는 경우 낮은 사업예산으로 적용여부 • 장기계속계약인 유지보수사업의 경우 총 사업금액의 연차별 평균금액으로 참여제한 적용여부 • 장기계속계약인 유지보수사업이면서 2개 이상의 다른 사업을 통합 발주하는 경우 각각 사업별 연차별 평균금액을 산출하고 그 중에서 낮은 사업금액을 기준으로 적용	
★4	대기업 공동수급제한	• SW 사업 관리감독에 관한 일반기준(고시) 제5조제2항	• 매출액 8천억원 이상인 대기업이 참여가능한 사업(사업예산 80억원이상 또는 예외사업)에서 대기업간 공동수급 금지 명시여부	

No	대상 제도	법적 근거	판단기준	정보보호 사업
★5	하도급 제한	• 법 제20조의3 • SW사업의 하도급 승인 및 관리지침(고시)	• 하도급을 허용하는 경우 계약상대자가 하도급계약시 반드시 발주기관 사전승인을 받도록 명시여부 • 하도급 비율(50%초과) 제한 및 재하도급 원칙적 금지 명시여부 • 하도급 적정성 판단 세부기준 명시여부 • 하도급 계획서(입찰시, 계약체결시) 제출 요청 명시여부 • 하도급 비율 10%초과 시 공동수급체 구성 요청 명시여부	정보보호산업법 제8조 시행령 제2조
6	작업장소 상호협의	• 용역계약일반조건(기재부 계약예규) 제52조 • 행정기관 및 공공기관 정보시스템 구축·운영지침(행안부 고시) 제41조	• SW사업수행을 위한 작업장소 협의결정 명시 여부 • 작업장소비용의 사업예산 계상여부	행정기관 및 공공기관 정보시스템 구축·운영 지침 제41조
7	지식재산권 공동귀속	• 국유재산법 제65조의12 • 용역계약일반조건(기재부 계약예규) 제56조 • 행정기관 및 공공기관 정보시스템 구축·운영지침(행안부 고시) 제60조	• 지식재산권 공동소유 원칙 명시여부 • 국방·국가안보 등 이유로 발주기관 귀속 시 그 사유를 명시하였는지 여부	행정기관 및 공공기관 정보시스템 구축·운영 지침 제60조 용역계약일반조건 제56조
8	개발SW의 공동활용 사전명시	• 국유재산법 제65조의12 • 용역계약일반조건(기재부 계약예규) 제56조	• 개발SW가 타 기관에 공동활용 되는지 사전에 안내하고, 공동활용 시 타 기관을 명시하였는지 여부	
★9	하자담보 책임기간 및 범위	• 법 제20조의5 • 용역계약일반조건(기재부 계약예규) 제58조	• 검수후 최종산출물을 인도한 날부터 1년 이내로 하자담보책임기간 명시여부 • 적법한 하자담보책임의 범위내 명시여부 (범위를 넘은 사항은 유지관리에 해당)	정보보호산업법 제9조 / 용역계약일반조건 제58조

No	대상 제도	법적 근거	판단기준	정보보호 사업
10	특정규격 명시 금지	• 정부입찰・계약집행기준(기재부 계약예규) 제5조제4항제5호	• 특정상표 또는 모델・규격 등 명시여부	정부 입찰·계약 집행기준 제2장
11	협상에 의한 계약 방식 적용	• 국가를 당사자로 하는 계약에 관한 법률 시행령 제43조・제43조의2 • 지방자치단체를 당사자로 하는 계약에 관한 법률 시행령 제43조・제44조 • 협상에 의한 계약체결기준(기재부 계약예규) • 법 제20조제1항	• 지식기반산업인 SW사업에 대한 협상에 의한 계약체결방식(낙찰자결정) 채택여부	국가를 당사자로 하는 계약에 관한 법률 제10조 시행령 제43조, 제43조의2 정보보호산업법 제7조제1항 -협상에 의한 계약체결기준 적용
12	기술능력평가 비중 (90%) 도입	• 협상에 의한 계약체결기준(기재부 계약예규) 제7조 • 행정기관 및 공공기관 정보시스템 구축・운영지침(행안부 고시) 제18조	• 협상방식 적용사업에서 기술능력 대 가격점수 비중을 90:10로 제시여부	행정기관 및 공공기관 정보시스템 구축·운영 지침 제18조
★13	SW기술성평가 기준 적용	• 법 제20조제4항 • SW 기술성 평가기준(고시)	• 기술능력평가 시 평가기준을 SW기술성평가기준을 적용・활용하였는지 여부 • 각 평가부문별 배점한도를 30점 이하로 준수하였는지 여부	정보보호산업법 제7조제2항 -정보보호시스템의 요구사항을 분석.적용할수있는기준 -정보보호시스템의 사업자 선정을 위한 기술평가기준

No	대상 제도	법적 근거	판단기준	정보보호 사업
★14	SW사업 제안서 보상	• 법 제21조 • SW사업의 제안서 보상기준 등에 관한 운영규정(고시)	• 20억원 이상의 SW사업에서 제안서보상에 대한 명시 여부 (단, 유지보수사업, 단순 하드웨어구축사업, 데이터베이스구축사업 및 시스템운용환경구축사업은 제외)	
15	무상유지보수 용어 사용 금지	• 용역계약일반조건(기재부 계약예규) 제58조	• 하자보수와 혼용하여 '무상유지보수' 사용여부 • 용역계약일반조건에서 정하는 유지보수 사항(범위내)을 하자보수로 명시하는지 여부	
★16	요구사항 상세화	• 법 제20조제3항 • SW사업 관리감독에 관한 일반기준(고시) 제4조제1항 · 제7조제1항	• SW사업의 상세요구사항 작성표 사용여부	정보보호산업법 제7조제2항 -정보보호시스템의 요구사항을 분석.적용할수있는기준
17	SW사업 적정사업기간 산정	• 정보통신융합법* 제23조 • SW사업 관리감독에 관한 일반기준(고시) 제6조	• SW개발과 관련된 사업의 경우 적정사업기간 산정기준에 따른 사업 명시 및 종합 산정서 첨부 여부 * 정보통신 진흥 및 융합 활성화 등에 관한 특별법	
★18	투입인력 관리 금지	• SW사업 관리감독에 관한 일반기준(고시) 제3조·제7조제3항·제9조제2항	• SW개발과 관련된 사업의 경우 제안요청서 내 투입인력 관련 사항 명시가 불가능하며, 핵심인력에 대한 사항만 명시 여부	
★19	SW사업정보 제출	• 법 제22조 제2항,제3항	• SW개발·재개발·유지보수 및 운영과 관련된 사업의 경우 제안요청서 내 SW사업정보 제출 명시 여부	

No	대상 제도	법적 근거	판단기준	정보보호 사업
★	정보보호 서비스의 적정대가 지급	• 정보보호산업법 제10조제1항, 시행령 제5조	• 보안성 지속 서비스 예산은 유지관리와 별도로 편성하여야 하며, 보안성 지속 서비스 예산은 보안성 유지에 직접적인 영향을 줄 수 있기 때문에 다른 예산으로 전용해서는 안 된다.	정보보호사업 고유
★	표준계약서 사용	• 정보보호산업법 제10조제2항, 약관법 제17조	• 정보보호산업의 합리적 유통 및 공정한 거래를 위하여 공정거래위원회와 협의를 거쳐 표준계약서를 마련하고, 공공기관등에 이를 사용하도록 권고	정보보호사업 고유
★	보안관제사업 입찰참가자격 제한	• 국가사이버안전관리규정 제10조의2	• 국가 공공기관 보안관제센터 운영 지원 전문기업 지정여부 – 보안관제 전문기업 지정 등에 관한 공고(과학기술정보통신부 공고)	정보보호사업 고유
★	정보보호컨설팅 사업 입찰참가 자격 제한	• 정보보호산업 진흥법 제23조 • 시행규칙 제8조~제15조	• 전문업체 지정여부 – 정보보호 전문서비스 기업 지정 등에 관한 고시(과학기술정보통신부 고시)	정보보호사업 고유
★	정보보호시스템 유형별 도입여건 만족 여부(CC인증)	• 국가정보화기본법 제38조(정보보호시스템에 관한 기준 고시 등) • 국가정보보안기본지침 제115조(정보보호시스템 도입 등)	• 정보보호제품에 CC인증 요건 명시	정보보호사업 고유
★	개인정보영향 평가 입찰참가 자격 제한	• 개인정보보호법 제33조 • 시행령 제38조	• 등록기관 지정여부 – 개인정보 영향평가에 관한 고시 (행안부 고시)	정보보호사업 고유

5. 사업유형별 제안요청서 표준 템플릿 (별도 파일 제공)

[표] 정보보호사업 유형별 템플릿

유형	구분	정보보호 사업 유형	비고
Ⅰ	정보보호 제품	1-1 정보보호 제품 도입 · 구축 사업	
		1-2 물리보안 제품 도입 · 설치 사업	
Ⅱ	정보보호 서비스	2-1 정보보안 컨설팅 사업	
		2-2 보안성지속서비스 사업	
		2-3 보안관제 사업	
		2-4 물리보안 서비스 사업	
		2-5 정보보호시스템 개발 사업	SW사업 참조

정보보호시스템 구축
실무가이드

과학기술정보통신부
KISA 한국인터넷진흥원