제 안 요 청 서

사 업 명	자살예방교육 시스템 개인정보영향평가
주관기관	한국생명존중희망재단

2026. 10.

담당	운영지원팀(조달)	대리 김영현	TEL:02-3706-0496
	정보화관리팀(사업)	사원 김하늘	TEL:02-3706-0488

목 차

Ⅰ. 과업 개요 ····· 1

1. 추진배경 ····· 1
2. 과업내용 ····· 2
3. 추진체계 및 역할 ····· 3

Ⅱ. 과업 안내사항 ····· 4

1. 과업내용 ····· 4
2. 영향평가 방법 및 절차 ····· 4
3. 추진일정(안) ····· 6
4. 일반사항 ····· 7
5. 상세요구사항 ····· 8

Ⅲ. 준수사항 ····· 20

1. 일반사항 ····· 20
2. 참여인력 관리 ····· 20
3. 보고서 및 산출관리 ····· 21
4. 준공 및 정산 ····· 21
5. 보안준수사항 ····· 21

[붙임 1] 용역사업 수행업체 보안 준수사항 ····· 22
[붙임 2] 사업자 보안위규 처리기준 예시 ····· 26
[붙임 3] 보안 위약금 부과 기준 ····· 28

Ⅰ 사업 개요

1. 추진 배경 및 필요성

가. 추진배경

○「개인정보 보호법」제33조와 「개인정보 보호법 시행령」 제35조 및 개인정보 영향평가에 관한 고시(행정안전부고시 제2020-4호)에 의해 개인정보 영향평가실시

○ 공공기관 지정에 따라 운영 중인 '자살예방교육 시스템'의 '일반회원정보' 개인정보 파일이 개인정보 영향평가 대상이 되어 개인정보 영향평가를 수행함

- 이를 통해, 잠재 위험식별 · 침해요인 분석 · 취약점에 대한 개선방안 도출 · 불필요한 개인정보 보유 제거 · 개인정보 취급 프로세서 개선 등 개인정보보호 수준 및 개인정보보호 관련 법령에 대해 법적 준거성을 확보하고자 함

○ 개인정보보호 관련 법령의 의무 준수사항 점검과 미비 사항을 보완하여 개인정보 관리체계 및 유출 예방 강화

○ 개인정보 침해위험요인과 위험요소에 대한 분석 및 개선사항 조치를 통한 개인정보 침해 예방

나. 필요성

○ 개인정보 유출 등 위험요소를 식별하여 개인정보주체의 권리를 보장하기 위한 방안 도출 필요

○ 개인정보영향평가 전문기관에 의한 개인정보 영향도 분석과 취약점 진단 · 결과 반영을 통해, 시스템 보안성 강화 및 개인정보 침해사고를 사전 예방하기 위한 대책 필요

2. 과업내용

○ 과업명 : 자살예방교육 시스템 개인정보 영향평가

○ 사업예산 : 20,000,000원(VAT포함)

※ 기초금액은 공고문 및 나라장터 공고에서 확인

○ 과업범위 : 개인정보영향평가 대상사업의 본 사업 입찰공고

○ 선정방식 : 제한경쟁입찰(견적에 의한 가격결정)

○ 참가자격

- 개인정보 보호법 제33조(개인정보영향평가)에 의한 행정안전부 장관이 지정한 기관으로서, 국가종합전자조달시스템 입찰참가자격등록규정에 의하여 나라장터(G2B)에 **"개인정보 영향평가기관" 업종(업종코드 : 6525)**으로 입찰참가를 등록한 업체

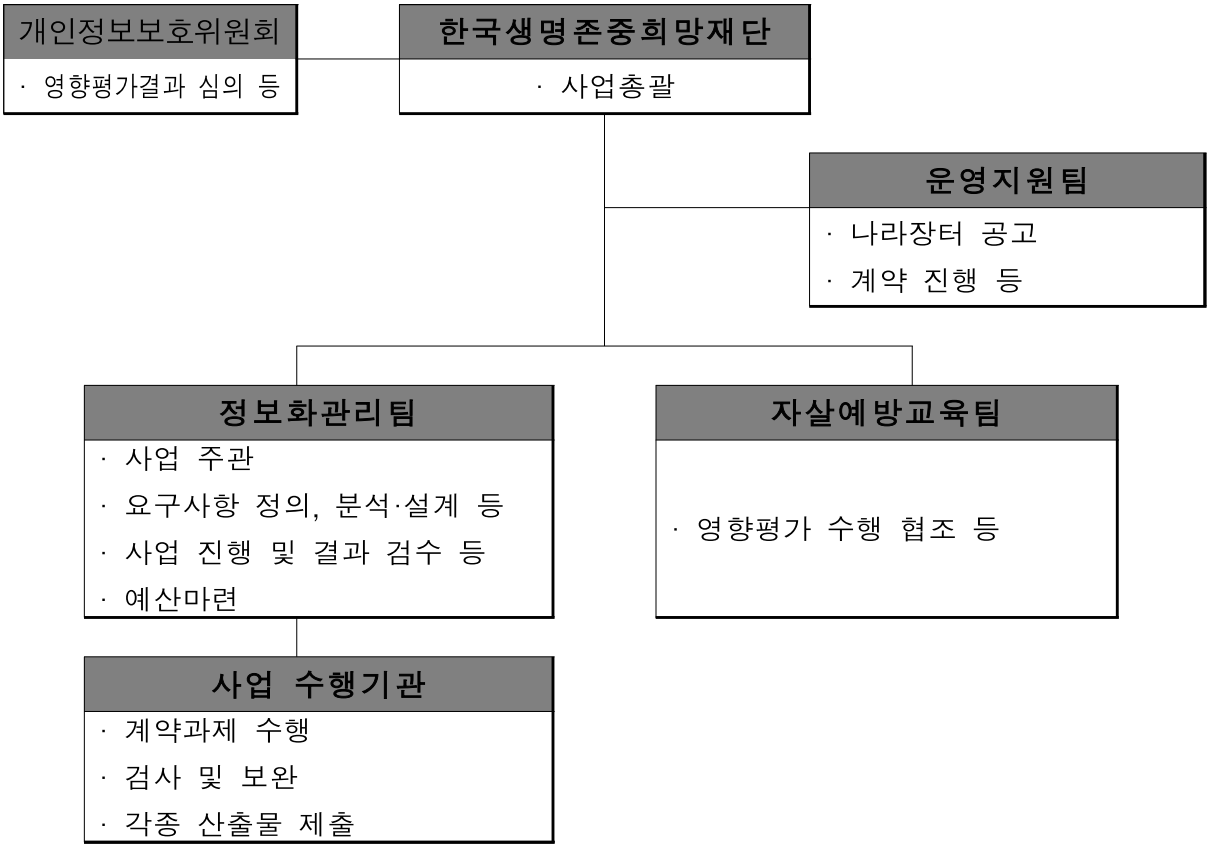
※ 개인정보 영향평가기관으로서 공고일 전일부터 입찰일(낙찰자는 계약체결일까지) 해당 자격을 계속 유지하여야 함

3. 추진체계 및 역할

○ 기관별 역할 및 책임

기 관		주 요 역 할
한국생명존중희망재단		· 사업 총괄
사업부서	정보화관리팀	· 사업 주관 · 요구사항 정의, 분석·설계 등 · 사업 진행 및 결과 검수 등 · 예산 마련
	운영지원팀	· 계약 체결 관련 지원
	자살예방교육팀	· 영향평가 수행 협조 등
사업 수행기관		· 사업추진에 따른 계약의 이행 · 운영교육 및 기술전수 · 사업 관련 수행할 필요가 있는 업무 등
개인정보보호위원회		· 영향평가 결과 심의 등

○ 추진조직도


개인정보보호위원회
· 영향평가결과 심의 등
한국생명존중희망재단
· 사업총괄
운영지원팀
· 나라장터 공고
· 계약 진행 등
정보화관리팀
· 사업 주관
· 요구사항 정의, 분석·설계 등
· 사업 진행 및 결과 검수 등
· 예산마련
자살예방교육팀
· 영향평가 수행 협조 등
사업 수행기관
· 계약과제 수행
· 검사 및 보완
· 각종 산출물 제출

Ⅱ 과업 안내사항

1. 과업내용

○ ‘자살예방교육 시스템’의 개인정보보호 관리체계의 적정성 분석

- 개인정보파일 관리, 개인정보 처리방침에 대한 적정성 등

○ 개인정보 처리단계별 보호의 적정성 분석

- 개인정보 수집, 저장, 보유, 이용 및 연계·제공, 파기에 이르기까지 각 단계별 보호조치에 대한 분석 등

○ ‘자살예방교육 시스템’의 기술적 보호조치 분석

- 접근권한 관리, 접근통제, 개인정보의 암호화, 접속기록의 보관 및 점검, 악성프로그램 등 방지, 물리적 접근방지, 개인정보의 파기, 기타 기술적 보호 조치 분석 등

○ 기타 관련 법령에 따라 수행이 필요한 부분 등 분석

※ 기타 관련 법령: 개인정보 보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 위치정보의 보호 및 이용 등에 관한 법률 등

○ 영향평가 결과에 따른 개선계획 수립 및 개선조치 기술지원

- 개인정보 흐름 및 개인정보 침해요인 분석, 위험평가를 실시 후 도출된 개인정보 침해요소에 대해 관련 법규, 지침 등 관련 내용을 반영하여 개선방안 및 개선계획 수립
- 개선조치에 대한 기술지원 및 반영 검토, 개인정보보호교육 지원

2. 영향평가 방법 및 절차

○ 문서 확인, 인터뷰, 현장방문을 통한 실사 등의 방법을 병행

○ 개인정보영향평가 대상 사업(이하 ‘대상사업’)에 적용되는 개인정보 보호 관련 법령 · 지침 및 가이드라인 · 내부지침 등 관련 정책 분석

○ 개인정보의 종류 · 성질, 정보주체의 수, 개인정보의 흐름 및 개인정보 침해 요인 분석, 위험평가 실시

○ 개인정보보호 관련 법령, 지침 등 관련 내용을 반영한 개선방안 및 개선계획 수립

○ 법적 쟁점사항 발생 시 개인정보보호 관련 전문가 또는 변호사, 법학 교수 등에 법률 자문 등



※ 평가방법 및 절차는 「공공기관 개인정보 영향평가 수행 안내서」에 따라 수행

※ 개인정보 영향평가에 관한 고시(행정안전부고시 제2020-4호)」 및 「개인정보의 안전성 확보조치 기준 고시(행정안전부고시 제2021-2호)」 준수

3. 추진 일정(안)

○ 계약일로부터 한달(1개월)이며, 통합사업의 사업 수행계획서 일정에 따라 계약기간 내 1개월 이상 프로젝트 수행

추진 내용	추진일정
	M
□ 사전분석	
· 역할 정의	
· 사업계획 수립	
□ 개인정보영향평가(시스템 성능진단, 보안취약점 점검)	
· 평가자료 수집 및 분석	
· 개인정보흐름 분석	
· 침해요인 분석	
· 개선계획 수립	
· 영향평가 보고서 작성 및 제시 (시스템 성능진단, 보안취약점 점검)	

4. 일반사항

○ 「개인정보 영향평가에 관한 고시(행정안전부고시 제2020-4호, 시행 2020.8.11.)」와 「개인정보의 안전성 확보조치 기준 고시(행정안전부고시 제2021-2호, 시행 2021.9.15.)」 및 『개인정보 영향평가 수행안내서』를 준수해야 함

○ 과업지시서에 명시되지 않은 사항은 주관기관과 협의·조정하도록 하며 본 사업 진행상 불가피하거나 마땅히 시행하여야 할 경미한 사항은 본 계약에 포함된 것으로 간주함

○ 본 사업의 목표달성을 위해 필요하다고 판단되는 추가적인 진단 및 방안 등을 제안할 수 있으며, 추가적인 제안 및 구현에 대한 모든 비용은 제안사가 부담함

- 사업 내용이 변경될 경우 사업변경절차에 따라 상호 협의하여 결정하며, 제안서 작성 시 제안요청서 요구사항에 명시되지 않았으나 주관사업자 판단으로 추가되어야 할 요구사항에 대해서는 별도 표시하여 추가 작성 가능

○ 제안사는 과업지시서에 기술된 요구사항을 기반으로 제안하되, 업무분석 단계에서 보다 창의적인 방법으로 요구사항을 해석하고, 정제하여 사업에 반영

- 사업기간 중 본 과업지시서에 기술한 업무 외에 수요기관과의 상호 협의에 따라 추가 및 변동 가능

○ 본 사업에 대한 과업을 수행하면서 알게 된 사업과 관련된 모든 사항은 외부로 유출하거나 인용 불가함

- 배포된 과업지시서는 작성 목적 외 사용 및 제공 금지
- 사업 관련 정보(문서, 현황 등)는 수요기관의 승인 없이 외부에 공개 또는 제공 금지
- 과업 수행 중은 물론 사업 완료 후에도 비밀 준수

- 과업지시서 작성 시 열람한 대외비 자료 및 사업 수행 중 취득한 자료의 외부유출 문제 발생 시 사업자가 모든 민·형사상 책임을 지고 배상해야 함

○ 산출물에 포함된 주관기관과 관련된 주요 정보(대외비, 민감정보 등)는 본 사업 이외에 활용을 금지하며, 해당 정보를 본 사업 이외에 활용하였을 경우 사업자가 모든 민·형사상 책임을 지고 배상해야 함

○ 사업참여인력은 본 사업의 개인정보영향평가 현장점검 기간 동안 기 수행 중이거나 제안 중인 타 사업 일정과 중복될 수 없음

○ 기타 준수사항

- 본 사업은 발주기관이 제시하는「전자정부지원사업 관리지침」과「전자정부지원사업 운영지침」및 「전자정부지원사업 관련 계약특수조건」 등의 절차를 준수하여야 함

5. 상세요구사항

○ 요구사항 총괄표

요청사항 구분	약자	설 명	요구사항수
컨설팅 요구사항	CSR	Customer Service Request	7
보안 요구사항	SER	Security Requirement	4
품질 요구사항	QUR	Quality Requirement	2
제약사항	COR	Constraint Requirement	1
프로젝트 관리 요구사항	PMR	Project Management Requirement	2
프로젝트 지원 요구사항	PSR	Project Support Requirement	2
합 계			18

○ 요구사항목록

요구사항	고유번호	요구사항 명칭
컨설팅 요구사항	CSR-001	개인정보 영향평가 일반사항
	CSR-002	개인정보 영향평가 계획 수립
	CSR-003	개인정보 영향평가 수행 요구사항 - 개인정보 흐름 확인
	CSR-004	개인정보 영향평가 수행 요구사항 - 개인정보 침해요인 도출
	CSR-005	개인정보 영향평가 수행 요구사항 - 개선 계획 수립
	CSR-006	개인정보 영향평가 수행 요구사항 - 영향평가 보고서 작성
	CSR-007	영향평가 이행점검 요구사항
보안 요구사항	SER-001	공통 보안요구사항
	SER-002	사업 착수시 보안요구사항
	SER-003	사업 수행시 보안요구사항
	SER-004	사업 완료시 보안요구사항
품질 요구사항	QUR-001	품질관리 및 보증 방안
	QUR-002	산출물 관리
제약사항	COR-001	계약의 일반사항 및 계약 이행 조건
프로젝트 관리 요구사항	PMR-001	사업수행 관리 및 업무보고 요구사항
	PMR-002	사업수행 조직구성
프로젝트 지원 요구사항	PSR-001	교육계획 수립
	PSR-002	하자보수 계획

○ 상세 요구사항

- 컨설팅 요구사항(CSR)

요구사항 고유번호		CSR-001		
요구사항 명칭		개인정보 영향평가 일반사항		
요구사항 분류		컨설팅 요구사항	응낙수준	필수
요구사항 세부내용	정의	영향평가 일반사항		
	세부 내용	○'자살예방교육 시스템' 대상으로 영향평가를 수행 (이하 '대상사업') ○관리적·기술적 보호조치의 적정성 및 법적 의무사항 준수여부 등을 확인하여야 함 ○「개인정보 영향평가에 관한 고시」 및 「공공기관 개인정보 영향평가 수행안내서」 등을 준용하여 사업을 수행하여야 함 ○개인정보보호 관리체계의 적정성 분석과 개선방안 수립을 수행하여야 함 - 대상시스템의 개인정보 취급자, 취급 내용, 보유기간 등의 적정성 및 개선방안 제시 ○개인정보 처리단계별 보호의 적정성 분석 및 조치방안을 마련하여야 함 - 개인정보 수집, 저장 및 보유, 이용 및 연계·제공, 파기단계에 이르는 각 단계별 보호조치의 적정성 분석 ○개인정보보호 점검결과에 따른 개선방안 및 후속조치방안을 마련하여야 함 - 개인정보보호 관련 법규 위반사항에 대한 개선방안 마련 등 - 개인정보영향평가 결과에 따른 시스템 개선방안 도출 * 개선방안 및 후속조치방안은 조치가 가능하도록 상세히 제시(내부정책자료의 경우 초안, 양식 제공 등의 컨설팅 지원)되어야 함		
산출정보				

요구사항 고유번호		CSR-002		
요구사항 명칭		개인정보 영향평가 수행 요구사항 – 개인정보 영향평가 계획 수립		
요구사항 분류		컨설팅 요구사항	응낙수준	필수
요구사항 세부내용	정의	개인정보 영향평가팀 구성 및 운영계획 수립		
	세부 내용	○ 개인정보영향평가팀 구성 방안 및 운영계획 수립 - 평가하고자 하는 사업 자체에 대한 이해와 개인정보보호 관련 법제 및 정책·전략 수립, 기술·시스템 분석 및 정보보안(Security) 등의 광범위하고 다양한 전문지식과 정보를 보유한 기관 내 유관 부서, 사업을 구축하는 업체(개발 용역업체), 외부 전문가 등으로 팀을 구성 - 영향평가팀에 참여하는 부서 및 유관기관 담당자의 역할 및 책임 배분 ※ 역할 및 책임 배분 시 담당자의 업무를 명확히 정의하고 업무의 중복을 가급적 지양할 것 ○ 효율적인 평가 수행을 위한 영향평가 수행계획 수립 ○ 개인정보 영향평가 계획 수립 - 평가목적, 평가대상 및 범위, 평가주체(평가팀), 평가기간, 평가절차(방법), 주요 평가사항, 평가기준 및 항목, 자료 수집 및 분석 계획 등을 포함		
산출정보		개인정보 영향평가팀 운영계획서, 개인정보 영향평가 계획서		

요구사항 고유번호	CSR-003
요구사항 명칭	개인정보 영향평가 수행 요구사항 – 개인정보 흐름 확인

<table>
<tr><td colspan="2">요구사항 분류</td><td>컨설팅 요구사항</td><td>응낙수준</td><td>필수</td></tr>
<tr><td rowspan="2">요구사항
세부내용</td><td>정의</td><td colspan="3">평가대상 업무 현황 분석 자료 검토, 평가대상 업무 흐름도 작성, 개인정보 흐름표 작성, 정보시스템 구조도 및 정보보호 시스템 목록 작성</td></tr>
<tr><td>세부
내용</td><td colspan="3">○ 대상사업을 면밀히 분석하고 업무를 정의하여, 해당 사업을 통해 처리되는 업무 중 개인정보 취급이 수반되는 업무를 도출
○ 개인정보 처리업무 현황 분석 자료 검토
- 대상 정보시스템 개발 관련 산출물 분석 및 담당자 인터뷰 등을 통해 수행
- (영향평가 업무명) 영향평가 대상시스템에서 개인정보가 취급되는 업무를 주요 업무단위로 기재
- (취급 개인정보) 평가 업무명 단위로 취급되는 개인정보 기재
- (개인정보 영향도) 취급개인정보의 중요도에 따라 영향도를 산정
※ 개인정보 처리업무 현황 분석으로 도출된 업무별로 개인정보 취급 업무 흐름표 작성할 것
○ 도출된 개인정보 취급 업무별로 개인정보 취급 업무표의 개인정보 취급 업무별 세부 업무절차를 작성
○ 개인정보 처리업무 흐름도 작성
- 해당 업무를 수행하는 인력 및 부서 등을 함께 표시하고, 연계기관(개인정보를 제공하거나 제공받는 기관)이 있는 경우 해당 기관도 포함하여 작성
※ 개인정보 업무 흐름도는 해당 업무를 수행하는 인력 및 부서 등을 함께 표시하고, 연계 기관(개인정보를 제공하거나 제공받는 기관)이 있는 경우 해당 기관도 포함하여 작성할 것
○ 개인정보 취급 단계별로 취급되는 개인정보 현황 및 처리 내역 등을 용이하게 식별 할 수 있도록 개인정보 흐름표를 작성
○ 개인정보를 취급 업무별로 개인정보의 수집·보유·이용/제공·파기로 구분하여 구체적으로 작성
○ 개인정보 흐름표 작성
- 해당 업무를 수행하는 인력 및 부서 등을 함께 표시하고, 연계기관(개인정보를 제공하거나 제공받는 기관)이 있는 경우 해당 기관도 포함하여 작성
※ 개인정보 흐름표에는 업무명을 기반으로 개인정보의 수집·보유·이용/제공-파기에 이르는 Life-Cycle 별 현황 등을 기재하여 개인정보의 흐름을 한눈에 이해할 수 있도록 작성할 것
○ 개인정보 취급이 수반되는 업무별로 개인정보의 수집·보유·이용/제공·파기되는 개인정보의 흐름을 한 눈에 파악할 수 있도록 개인정보 흐름도를 작성
○ 개인정보 흐름도 작성
- 개인정보와 관련한 업무를 기재하고, 업무와 관련하여 개인정보 취급과 관련한 담당자 및 담당부서, 정보주체 등을 포함하여 기재
- 개인정보를 취급하는 관련업무, 취급과 관련하여 사용되는 매체(PC, 노트북, 신청서 등의 문서)와 수집한 개인정보를 처리할 때 관련한 IT시스템(DB, 웹서버 등)을 표시하고 각 요소들 간의 이동 시 전송되는 개인정보 항목을 기재
※ 개인정보 흐름도는 개인정보를 취급 업무별로 개인정보 흐름표를 기준으로 수집・보유・이용/제공・파기 등의 생명주기를 기반으로 해당 업무처리자 및 시스템의 구성사항을 고려하여 구체적으로 작성할 것
○ 정보시스템 구조도 작성</td></tr>
</table>

		○ 정보보호 기술적·물리적·관리적 보안 메커니즘 목록 작성 ※ 방화벽, 침입탐지시스템과 같은 보안 메커니즘을 포함하여 전송 데이터 암호화, DB 암호화 등 개인정보보호를 위한 기술적·물리적·관리적 보안 메커니즘의 타당성을 검토할 것
산출정보		개인정보 취급 업무흐름표 및 업무흐름도, 개인정보 처리업무 흐름도, 개인정보 흐름표 및 흐름도, 정보시스템 구조도 및 정보보호 시스템 목록

요구사항 고유번호		CSR-004		
요구사항 명칭		개인정보 영향평가 수행 요구사항 – 개인정보 침해요인 도출		
요구사항 분류		컨설팅 요구사항	응낙수준	필수
요구사항 세부내용	정의	○ 평가 기준 수립 및 개인정보보호 조치 사항 파악을 위한 평가항목 작성 ○ 자료 분석, 현장 실사, 담당자 인터뷰 등을 통해 개인정보보호 조치 현황 파악 ○ 도출된 개인정보 침해 요소에 대한 위험도 산정 ○ 침해요소에 대한 위험 관리 방안 수립		
	세부 내용	○ 「공공기관 개인정보 영향평가 안내서」의 영향평가 항목을 기준으로 영향 평가 영역을 구성 ○ 영향평가 기준 및 평가항목 수립 - 개인정보 취급 업무 및 개인정보 흐름이 다수 존재하는 경우에는 각 흐름별로 평가항목을 각각 작성 - 평가항목 외에도 관련 근거, 항목 설명, 확인 자료 등을 제시하여 작성 ○ 개인정보 조치사항 및 계획 등을 파악 ○ 평가기준 및 평가항목에 따라 자료분석, 현장실사, 담당자 및 취급자 대상 인터뷰를 통한 분석 수행 ○ 개인정보 흐름분석 시 도출된 업무 흐름표를 활용하여 개인정보 라이프 사이클별로 구분한 후, 위험요소별 개인정보 침해요인 분석 ○ 위험요소 분석 및 위험도 산정 - 자산별 침해요인 연계 개념도 작성 - 중요도와 취약점, 위협요소 등을 고려하여 위험요소 분석 및 위험도 산정 ○ 위험도의 우선순위에 따라 나열하여 해당 기관이 수용 가능한 수준을 정하여 단기, 중·장기로 구분하여 개선방안을 도출		
산출정보		개인정보 평가 기준 및 평가항목 정의서, 개인정보 보호조치 현황 분석서, 개인정보 침해요인 위험도 산정표, 개인정보 침해요인별 개선방안표		

요구사항 고유번호		CSR-005		
요구사항 명칭		개인정보 영향평가 수행 요구사항 – 개선 계획 수립		
요구사항 분류		컨설팅 요구사항	응낙수준	필수
요구사항 세부내용	정의	개선 과제 도출 및 계획 수립		
	세부 내용	○ 도출된 개인정보 침해요소 및 도출된 개선방안을 기반으로 개선 과제 도출 - 위험 요소를 제거하거나 최소화할 수 있는 대처 방안 마련 - 위험 요소 해결을 위해 유사 사례에 대한 벤치마킹 등을 수행		

		- 담당자(개인정보취급자)들이 취약 사항을 시정하기 위해 취해야 할 조치사항과 책임 사항 등을 마련 ○ 법적 쟁점사항 발생시 개인정보보호 관련 전문가 또는 변호사, 법학교수 등에 법률 자문 ○ 개선계획은 위험평가를 참고하여 위험도가 높은 순서의 개선방안을 먼저 실행하도록 개선계획표 작성 - 당해 기관 내 보안 조치 현황, 예산, 인력, 정보화 사업 일정 등을 고려
산출정보		개선과제 정의서, 개선계획표

요구사항 고유번호		CSR-006		
요구사항 명칭		개인정보 영향평가 수행 요구사항 – 영향평가 보고서 작성		
요구사항 분류		컨설팅 요구사항	응낙수준	필수
요구사항 세부내용	정의	개인정보 영향평가 결과 보고서 작성 및 주요 이슈 사항 검토		
	세부 내용	○ 개인정보 영향평가 결과서 작성 - 영향평가 전 과정 및 산출물을 정리하여 개선계획서, 영향평가서 등 결과 보고서 작성 ○ 시스템 성능진단 - 운영 시스템에 대한 성능진단 실시 및 결과보고 ○ 보안취약점 점검 - 신규 구축 정보조회서비스 및 정보유통서비스 전반에 대한 취약점 진단을 실시하고, 주요 취약점에 대한 소스코드를 분석·검증 ○ 주요 이슈 사항 검토 - 잔존 위험이나 이해관계자 간의 의견 충돌이 있는 경우에는 최고의사 결정권자(기관장 등)를 토론에 참여시킴으로써 해당 사업의 중단·지속 여부 및 개인정보보호 정도에 대한 합의 도출		
산출정보		개인정보 영향평가 결과 보고서, 시스템 테스트결과서 (성능진단결과보고서), 보안취약점점검 결과보고서		

- 보안 요구사항(SER)

요구사항 고유번호		SER-001		
요구사항 명칭		공통 보안요구사항		
요구사항 분류		보안 요구사항	응낙수준	필수
요구사항 세부내용	정의	공통 보안		
	세부 내용	○ 당해 업무수행 과정을 통하여 취득한 정보는 절대 외부에 누설, 유출해서는 안되며, 이를 위반한 경우에는 민·형사상 또는 관계법규에 따라 조치함 ○ 과업수행 인력의 전산실 출입 등 업무수행 시 발주자가 요구하는 보안관련 규정을 충실히 이행하여야 함 ○ 「개인정보 보호법」준수 ○ 대검찰청 정보보안업무지침 준수		

		○ 기타 정보보호 관련 법규 및 지침 준수 - 행정기관 등 웹사이트 운영 가이드라인(행정안전부) - 공공기관의 개인정보보호를 위한 기본지침(행정안전부) ○ 참여인원 보안 - 참여인원은 보안서약서를 작성·제출하고 임의교체 불가 - 보안의식 강화를 위한 주기적인 보안 교육 및 실태 점검 - 사업관련 자료 보유 불가, 사업수행으로 취득한 정보에 대한 외부유출, 누설 금지 등 비밀유지의무 준수, 위반 시 관련 법령에 의한 처벌 - 사업 착수 시 대표명의 보안서약서, 완료 시 대표명의 확약서 ○ 자료보안 - PC 등 장비의 반·출입에 대해 관리대장에 등록 및 관리 - 자료관리대장 작성, 시건장치가 된 보관함에 서류보관 - 비인가자에게 제공·대여·열람 금지 - 전자우편을 이용할 경우 참여인원의 회사메일 사용, 첨부자료 암호화하여 수·발신, 대외비 이상은 전자우편을 이용한 자료 수·발신 금지 - 본 사업과 관련이 있는 모든 기록 및 자료에 대하여 발주기관의 사전 승인 없이는 이용(반출, 인용, 공개 등 유·무형의 행위)할 수 없으며, 사업종료 시 완전 폐기 또는 반납하여야 하며, 발주기관에서 요구하는 보안사항을 철저히 준수하여야 한다.(미이행시 위약금 부과) - 사업 수행에 사용되는 문서, 인원, 장비 등에 대하여 물리적, 관리적, 기술적 보안대책 및 '누출금지 대상정보'에 대한 보안관리계획을 제안서에 기재하여야 하며, 해당 정보 누출 시 발주기관은 국가계약법 시행령 제76조에 따라 사업자를 부정당업체로 등록
산출정보		

요구사항 고유번호		SER-002		
요구사항 명칭		사업 착수시 보안요구사항		
요구사항 분류		보안 요구사항	응낙수준	필수
요구사항 세부내용	정의	사업 착수시 보안		
	세부 내용	○ 사업수행에 사용되는 문서, 인원, 장비 등에 대한 물리적, 관리적, 기술적 보안대책 및 보안관리 계획을 수립하여 용역에 투입되는 인력(대표자 포함)에 대한 보안서약서와 함께 제출하여야 하며, 해당 정보 누출시 주관기관은 「국가를 당사자로 하는 계약에 관한 법률」 시행령 제76조에 따라 해당 사업자를 부정당업체로 등록 ○ 투입인력에 대해 법률 또는 규정에 의한 비밀유지의무 준수 및 위반 시 처벌내용 등에 대한 보안교육 실시		
산출정보				

요구사항 고유번호	SER-003

요구사항 명칭		사업 수행시 보안요구사항		
요구사항 분류		보안 요구사항	응낙수준	필수
요구사항 세부내용	정의	사업 수행시 보안		
	세부 내용	○ 보안인식 강화를 위하여 주기적으로 자체 보안교육을 실시하여야 하며, 주관기관이 요구하는 보안교육에 참석해야 함 ○ 사업수행 중 주관기관의 보안정책을 위반하였을 경우, 위규자 및 관리자를 행정조치하고, 보안위약금을 주관기관에 납부하여야 함 ○ 과업수행을 위해 제공받은 내부자료에 대해 용역수행책임자(PM)는 "자료관리대장"을 작성하여, 인수인계시 직접 서명·관리해야 함		
산출정보				

요구사항 고유번호		SER-004		
요구사항 명칭		사업 완료시 보안요구사항		
요구사항 분류		보안 요구사항	응낙수준	필수
요구사항 세부내용	정의	사업 완료시 보안		
	세부 내용	○ 사업 수행과정상 취득한 모든 자료와 정보는 사업수행 중은 물론, 사업완료 후에도 이를 유출해서는 안 되며, 사업종료 시 정보보안담당자 입회하에 반환, 소각 및 완전 폐기 등 필요한 조치 이행 ○ 사업 종료시, 사업수행업체의 노트북, PC 등은 포맷 후 반출 ○ 제공받은 제반자료, 장비, 서류와 중간·최종산출물 등을 전량 반납하고, 업체에 복사본 등 별도 보관은 금지한다.		
산출정보				

- 품질 요구사항(QUR)

요구사항 고유번호		QUR-001		
요구사항 명칭		품질관리 및 보증 방안		
요구사항 분류		품질 요구사항	응낙수준	필수
요구사항 세부내용	정의	품질관리 및 보증 방안		
	세부 내용	○ 사업자는 최근의 자료를 이용하여야 하며, 지침 등에 저촉되지 않도록 함 ○ 사업자는 각종 과업을 신중히 검토하여야 하며, 그 정당성, 정확도 및 안정성 등에 섬세하고 세밀한 평가를 하여야 함 ○ 본 사업 수행목적으로 사용한 모든 공식자료 및 통계는 서면으로 그 근거를 제시하여야 함 ○ 사업자는 본 사업에 관련된 모든 보고서의 조사.분석된 사항과 정리된 자료의 출처, 연도, 참고사항 등과 분석 자료 등 이에 관련된 기타서류를 제출함		
산출정보				

요구사항 고유번호		QUR-002		
요구사항 명칭		산출물 관리		
요구사항 분류		품질 요구사항	응낙수준	필수
요구사항 세부내용	정의	품질관리(프로젝트 관리 관점)		
	세부 내용	○ 선정된 사업자는 사업추진 과정에서 생산되는 제반 작업 단위별 산출물에 대하여 작업 일정계획 및 품질보증계획과 연계하여 산출물의 종류, 주요 내용, 작성 및 제출 시기, 제출 부수 등을 제시하여야 함 ○ 산출물 관리방안을 제시하여야 함		
산출정보		산출물 관리계획서		

- 제약사항(COR)

요구사항 고유번호		COR-001		
요구사항 명칭		계약의 일반사항 및 계약 이행 조건		
요구사항 분류		제약사항	응낙수준	필수
요구사항 세부내용	정의	계약의 일반사항 및 계약 이행 조건		
	세부 내용	○ 사업자가 계약의무를 다하지 못하였을 경우 지연배상금은「지방자치단체를 당사자로 하는 계약에 관한 법률 시행령」제90조(지연배상금),「지방자치단체 입찰 및 계약 집행기준」용역계약 일반조건에 따름 ○ 사업자는 규정에 의한 분쟁이 발생 시, 분쟁 기간 중 용역의 수행을 중지할 수 없음 ○ 발주기관과 사업자가 상호협의 시에도 문제를 해결하지 못하고 부득이 소송할 필요가 있을 때에는 발주기관의 주소지 관할법원으로 함 ○ 본 계약에 정하지 아니한 사항이나 본 계약의 각 조항과 다른 사항을 특약할 경우에는 발주기관과 사업자가 따로 서면으로 합의함으로써 그 효력을 발생 ○ 손해배상 책임 - 계약업체는 사업 대상 시스템 취급 시 관리자로서의 의무를 충실히 시행 - 계약업체의 부주의, 고의 또는 과실로 대상 시스템을 망실, 훼손한 것과 사고에 대하여 손해를 끼쳤을 경우 계약업체는 그에 상응한 보상 또는 교환 등의 손해배상 책임을 짐 - 계약업체는 지연처리로 인하여 피해가 발생하였을 경우에는 이에 대한 손해배상 책임을 짐 - 계약업체는 본 사업기간동안 정보를 수집, 가공에 있어 위법 또는 부당한 방법을 사용해서는 안 되며, 발주자가 제공한 정보 및 자료와 관련하여 저작권법 및 기타관련법 등에 따른 권리 침해를 이유로 국내외의 제3자로부터 소송, 청구, 이의제기, 형사고소 등을 당한 경우에는 계약업체는 자신의 책임과 비용으로 주관기관(대검찰청)의 권리를 보호하며, 그에 따라 주관기관이		

		입은 일체의 손해를 배상해야 함
산출정보		

- 프로젝트 관리 요구사항(PMR)

요구사항 고유번호		PMR-001		
요구사항 명칭		업무보고 요구사항		
요구사항 분류		프로젝트 관리	응낙수준	필수
요구사항 세부내용	정의	업무 보고 및 산출물 관리		
	세부 내용	○ 계약일로부터 10일 이내 제출 서류 - 착수계 - 사업수행계획서(일정표/사업 목적 및 범위/산출물 목록 및 정의서/사업관리, 품질관리 방법 및 절차서/보안관리 계획/인력투입 계획/교육지원 계획/비상연락체계/기타 사업 추진 시 고려사항 등 사업관련 내용을 상세하게 기술) - 업체대표 및 참여인력에 대한 재직증명서, 보안서약서, 개인정보보호 서약서 - 개인정보처리위탁 계약서, 비밀유지 계약서, 외주 용역사업 보안특약서 ○ 협의된 양식에 의거 정기보고서(주간, 월간 등)를 작성/제출하고 업무보고를 실시하여야 한다. ○ 사업 종료 7일 전까지 결과보고서(요약보고서 포함) 제출 - 대표자 보안 확약서, 하자보수 계획서, 교육자료 제출 ○ 사업 완료 후 이행점검 계획서(점검 후 이행점검 결과보고서) 제출 ○ 사업진행 중 착수보고회, 완료보고회를 개최하여야 하며 개최방법은 주관기관과 협의한다. ○ 사업수행 중 발생하는 비정기적인 사안에 대해서 주관기관은 수시보고서 제출을 요구할 수 있다.		
산출정보		사업수행계획서, 결과보고서, 정기보고서		

요구사항 고유번호		PMR-002		
요구사항 명칭		사업수행 조직구성		
요구사항 분류		프로젝트 관리	응낙수준	필수
요구사항 세부내용	정의	사업수행 조직구성		
	세부 내용	○ 본 사업을 수행할 추진 조직, 인력 구성 및 프로파일과 단계별 인력 투입계획 및 역할, 투입률 등을 제시하여야 하고, 투입인력의 기술 수준을 상세히 제시하여야 하며, 추후 인력은 본 기관의 동의 없이 사업자 임의로 변경할 수 없음 - 용역 수행 책임자(PM)는 반드시 주관사업자 소속이어야 한다. - 특별한 사유가 없는 한 인력 교체는 불가하며, 불가항력 사유로 인력교체 필요 시 인력교체 안정화 및 품질저하방지대책을 제시해야 함 ○ 프로젝트 추진 일정에 따른 인력 투입계획을 제시하여야 함 ○ 참여인력은「개인정보 영향평가에 관한 고시 제5조(영향평가 수행인력 자격)」의		

		수행인력 자격을 갖추어야 함 ○ 사업자는 투입인력의 개인정보 영향평가 관련 자격 및 경력, 기술등급 등을 확인할 수 있는 서류(자격증 사본, 경력증명서 또는 소프트웨어산업협회의 SW 기술자경력증명서 등)를 제안 시 제출해야 함 ○ 용역 수행에 있어 자격미달, 근무태도 불량, 기술능력 부족 등으로 판단될 경우에는 해당 기술 인력의 교체를 요구할 수 있으며, 사업자는 특별한 사유가 없는 한 해당 기술 인력을 즉시 교체하여야 하며 인력 교체 시 동급이상의 인력으로 교체하여야 함
산출정보		

- 프로젝트 지원 요구사항(PSR)

요구사항 고유번호		PSR-001		
요구사항 명칭		교육계획 수립		
요구사항 분류		프로젝트 지원	응낙수준	필수
요구사항 세부내용	정의	교육계획		
	세부 내용	○ 개인정보 영향평가 결과물에 대한 사항을 전문가를 통해 담당자에게 교육을 실시하여야 함 ○ 사업수행기간 중 개인정보에 필요한 교육을 실시하며, 사업수행계획서에 교육계획서를 포함하여 제출하여야 함 - 전 직원 및 개인정보취급자 대상 교육 - 교육에 필요한 교재 및 소요경비는 업체가 부담 ○ 개인정보 영향평가 결과물로 주관기관의 업무 처리시 유의사항을 정리하여 직원교육용 자료를 제공하여야 함 ○ 사업종료 이후에도 추가적인 교육 요구 및 개인정보보호에 대한 자문 역할을 수행하여야 함		
산출정보		교육계획서 및 교육자료		

요구사항 고유번호		PSR-002		
요구사항 명칭		하자보수계획		
요구사항 분류		프로젝트 지원	응낙수준	필수
요구사항 세부내용	정의	하자보수계획		
	세부 내용	○ 무상하자보수기간은 검수일로부터 1년으로 하며, 하자보수 방안을 상세하게 제시하여야 함 - 하자보증 이행으로 발생하는 모든 비용은 제안사가 부담 ○ 개인정보 영향평가 결과물을 개인정보보호위원회에 제출 후 지적된 사항에 대한 보완을 위하여 사업자는 지원체계, 인력을 제시하여야 함 - 개인정보보호위원회에 제출한 영향평가서에 대한 보완이 있을 경우 사업자는 추가비용 없이 영향평가서를 보완하여야 함 ○ 사업 완료 후 도출된 취약점 개선 완료 시까지 자문을 수행하여야 함		

		- 개인정보 영향평가 개선방안 이행 점검 내용을 필히 포함하여야 함
산출정보		하자보수 계획서

3 준수사항

1. 일반사항

○ 용역사는 과업내용서 및 관련 법 규정에 의하여 수행함을 원칙으로 하며, 과업내용서의 문구, 용어의 해석과 과업의 범위 등에 대하여 발주기관과 의견을 달리하는 경우는 상호간 협의를 통해 정한다.

○ 본 과업 수행으로 인하여 제3자의 권리침해, 불법S/W 및 특허권 등 사용으로 법적·물질적 위반할 경우 용역사가 모든 책임을 진다.

○ 계약 후 10일 이내에 다음사항이 포함된 착수계를 제출하여야 한다.

- 사업수행계획서 1부
- 보안관리 계획서(보안서약서 포함)
- 산출내역서 1부
- 참여인력 이력서 및 소프트웨어기술 경력증 또는 소프트웨어기술자 경력증명서 등 소프트웨어 경력 증빙자료

○ 과업 완료 7일 전에 최종보고서(안)을 발주처에 제출 협의 후 수정사항에 대해서는 즉시 보완토록 하고 보고서 작성과정에서 항상 발주처와 긴밀한 협의를 하여야 한다.

○ 본 과업 수행 상 특별한 사유가 없는 한 다음과 같은 행위가 발생하였을 때에는 계약위반 행위로 간주하여 관계규정에 의거 조치할 수 있다.

- 발주기관의 지시사항을 기한 내에 이행하지 않을 때
- 계약기간 내에 과업을 충실히 완료할 능력이 없거나 현저하게 수행공정이 미달될 때
- 용역사의 부주의로 인한 과실이 인정될 때

2. 참여인력 관리

○ 발주기관은 참여인력이 임무 수행에 있어 부적당하다고 판단되거나 태만하다고 인정될 때에는 해당요원의 교체를 요구할 수 있다.

○ 참여인력을 부득이한 사유로 인하여 교체하고자 할 경우에는 반드시 사전에 주관기관의 승인을 득하여야 한다.

○ 참여인력은 반드시 동급이상의 기술자이어야 하며 인계인수를 위한 중복 투입기간(7일 이상)을 충분히 확보하여야 한다.

○ 본 사업의 투입인력은 **업무일과시간의 100%를 통합사업자의 사업장에서 상주하여 개인정보영향평가를 실시해야 한다.**

3. 보고서 및 산출관리

○ 용역사는 다음의 보고체계를 갖추어 보고서를 제출하여야 한다.

구 분	보고서	시기	보고 내용
착수보고	사업수행계획서	계약 후 10일 이내	- 사업범위, 사업추진일정계획, 인력 투입계획, 보안관리계획 등
최종보고	최종보고서	사업종료전 7일 이내	- 사업수행내역 및 최종결과보고
수시 보고	수시 보고서	요구시	- 긴급 변경사항, 서면 요구사항

※ 발주기관과 용역사가 협의하여 보고회를 개회할 수 있으며 모든 성과품은 관련 원본파일을 포함하여 산출물 인쇄물 추가 요청 시 즉시 제출

4. 준공 및 정산

○ 본 과업이 정상적으로 종료되었을 경우 용역사는 검사를 계약 종료일까지 공문에 의해 제출한다.

○ 발주기관은 과업비의 단가적용, 과업물량 및 정산에 대한 부당함이 발견되었을 경우에는 그에 해당하는 금액을 감액 또는 환불이 가능하다.

5. 보안준수사항

○ 용역사는 과업수행과정에서 취득한 정보, 참고자료, 산출물, 반·출입하는 각종 전산장비에 대해 주관기관이 규정하는 관리계획과 보안대책을 수립·시행하여야 한다.

○ 참여인력 전원 보안서약서를 작성하여 제출하고 서약내용을 반드시 준수하여야 한다.

[붙임 1] 용역사업 수행업체 보안 준수사항

용역사업 수행업체 보안 준수사항

1. 공통사항

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

○ 사업자는 사업 수행에 사용되는 문서, 인원, 장비 등에 대하여 물리적, 관리적, 기술적 보안대책 및 '누출금지 대상정보'에 대한 보안관리 계획을 사업제안서에 기재하여야 하며, 해당 정보 누출시 발주기관은 국가계약법 시행령 제76조에 따라 사업자를 부정당업체로 등록한다.

< 누출금지 정보 >

① 기관 소유 정보시스템의 내·외부 IP주소 현황
② 세부 정보시스템 구성현황 및 정보통신망구성도
③ 사용자계정 및 패스워드 등 정보시스템 접근권한 정보
④ 정보통신망 취약점 분석·평가 결과물
⑤ 용역사업 결과물 및 프로그램 소스코드
⑥ 국가용 보안시스템 및 정보보호시스템 도입현황
⑦ 침입차단시스템·방지시스템(IPS) 등 정보보호제품 및 라우터·스위치 등 네트워크장비 설정 정보
⑧ 「공공기관의 정보공개에 관한 법률」제9조제1항에 따라 비공개 대상정보로 분류된 기관의 내부문서
⑨ 「개인정보 보호법」제2조제1호의 개인정보
⑩ 「보안업무규정」제4조의 비밀, 同 시행규칙 제7조제3항의 대외비
⑪ 그 밖의 발주자가 공개가 불가하다고 판단한 자료

○ 사업자는 발주기관의 보안정책을 위반하였을 경우 (붙임1)의 위규처리 기준에 따라 위규자 및 관리자를 행정조치하고 손해배상 책임을 진다.

※ 보안 위약금 부과기준이 명시되는 경우 해당금액을 발주기관에 납부한다.

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

2. 용역사업 참여인원에 대한 보안관리

○ 용역사업 참여인원 중 용역책임자를 보안책임관으로 지정, 발주기관의 승인을 받아야 한다.

○ 용역사업 참여인원은 보안서약서를 작성 후, 발주기관에 제출하여야 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 보안관리자의 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 퇴근시 반납하여야 하며, 다만 비밀문서를 제외한 일반문서는 제공된 사무실에 시건장치가 된 보관함이 있을 경우 이를 보관함에 보관할 수 있다.

○ 발주기관 보안관리자는 용역사업을 수행하는 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 관리하에 사용하도록 한다.

○ 용역사업 종료 시까지는 반입된 PC의 반출을 금지한다. 다만, 사업 수행상 외부 반출이 필요한 경우는 자료 유출에 대비한 보안대책을 발주기관에 제출하여 발주기관 보안관리자의 승인 후 최소한의 장비만 반출할 수 있다.

- 용역사업 참여인원이 퇴근시에 자료를 외부로 반출 할 수 없으며, 반드시 제공된 사무실내의 시건장치가 있는 보관함에 보관하여야 한다.

○ 용역사업 종료시 계약자의 PC 및 보조기억장치는 완전 삭제 후 반출하여야 한다.

5. 내·외부망 접근에 대한 보안관리

○ 사업 수행시 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 수행시 생산되는 모든 산출물은 발주기관 파일서버 또는 지정PC에 저장하여야 하며, 계정관리 및 접근권한 부여하여 관리를 철저히 한다.

○ 사업 수행시 생산된 산출물 및 기록은 발주기관 보안관리자가 인가하지 않은 비인가자에게 제공·대여·열람을 금지한다.

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

○ 최종산출물 및 사업관련 자료는 용역사업 수행업체의 보관을 금지함을 원칙으로 한다. 다만, 유지보수 등으로 필요한 경우에는 발주기관 보안관리 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
  ※ SW개발보안(시큐어코딩) 준수 : 행정기관 및 공공기관 정보시스템 구축·운영 지침, SW 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

※ 사업자 보안위규 처리기준(붙임1) 및 위약금 부과기준(붙임2)은 사업규모에 따라 조정

[붙임 2] 사업자 보안위규 처리기준 예시

사업자 보안위규 처리기준 예시

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 (부정당업체 등록) ○ 위규자 및 직속 감독자 OO 등 중징계 ○ 재발 방지를 위한 조치계획 제출 ○ 위규자 대상 특별 보안교육 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 용역사업 관련 자료 수발신 다. 개발·유지보수 시 원격작업 사용 라. 저장된 비공개 정보 패스워드 미부여 마. 인터넷망 연결 PC 하드디스크에 비공개 정보를 저장 바. 외부용 PC를 업무망에 무단 연결 사용 사. 보안관련 프로그램 강제 삭제 아. 사용자 계정관리 미흡 및 오남용(시스템 불법접근 시도 등)	○ 위규자 및 직속 감독자 OO 등 중징계 ○ 재발 방지를 위한 조치계획 제출 ○ 위규자 대상 특별 보안교육 실시
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	○ 위규자 및 직속 감독자 OO 등 경징계 ○ 위규자 및 직속 감독자 사유서 /경위

구 분	위 규 사 항	처 리 기 준
	가. 캐비넷 · 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	서 징구 ○ 위규자 대상 특별 보안 교육 실시
경 미	1. 업무 관련서류 관리 소홀 가. 진행중인 업무자료를 책상 등에 방치, 퇴근 나. 복사기 · 인쇄기 위에 서류 방치 2. 근무자 근무상태 불량 가. 각종 보안장비 운용 미숙 나. 경보 · 보안장치 작동 불량 3. 전산정보 보호대책 부실 가. PC내 보안성이 검증되지 않은 프로그램 사용 나. 보안관련 소프트웨어의 주기적 점검 위반	○위규자 서면 · 구두 경고 등 문책 ○위규자 사유서 / 경위서 징구

※ 출처: 국가·공공기관 용역업체 보안관리 가이드라인<국가정보원 2014.3.>

[붙임 3] 보안 위약금 부과 기준

보안 위약금 부과 기준

1. 위규 수준별로 A~D 등급으로 차등 부과

구분	위규 수준			
	A급	B급	C급	D급
위규	심각 1건	중대 1건	보통 2건 이상	경미 3건 이상
위약금 비중	부정당업자 등록	총 사업비의 OO%	총 사업비의 OO%	총 사업비의 OO%

* 위약금 규모는 기관별 사업규모에 따라 조정
* 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 종료시 지출금액 조정을 통해 위약금 정산

※ 출처: 국가·공공기관 용역업체 보안관리 가이드라인<국가정보원 2014.3.>