

**정보보호관리체계  
(ISMS)  
인증 컨설팅  
과업지시서**

2022. 04

**고신대학교복음병원**

# 목 차

I. 사업 안내	3
1. 사업개요	3
2. 추진배경 및 필요성	3
3. 사업범위	3
4. 기대효과	5
II. 사업추진 방안	6
1. 추진방향 및 전략	6
2. 추진체계 및 역할	6
3. 추진일정	7
III. 과업 내용	8
1. 상세 요구사항	8
1-1. 컨설팅 요구사항	8
1-2. 보안 요구사항	12
1-3. 제약 요구사항	13
1-4. 프로젝트 관리 요구사항	14
1-5. 프로젝트 지원 요구사항	16

# I 사업 안내

## 1. 사업개요

- 사업명 : 정보보호관리체계(ISMS) 인증 컨설팅
- 사업기간 : 계약일로부터 정보보호관리체계(ISMS) 인증 심사  
3회차[매년 심사 시 준비 기간 2개월(추후 협의 가능)]

## 2. 추진배경 및 필요성

- 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 ‘정보통신망법’) 제 47조(정보보호 관리체계의 인증) 기준에 따른 종합적인 보호 대책 수립
- 조직 내·외부 위협 요소의 변화 또는 새로운 취약점 발견 등에 대응하기 위하여 지속적 유지관리가 필요
- 갱신 인증 심사

## 3. 사업 범위

- 정보보호관리체계(ISMS) 수립
  - 정보보호 현황분석 및 위험분석
  - 정보보호 계획수립 및 정보보호 정책 · 지침 · 절차 정비
  - 정보보호관리체계(ISMS) 인증에 적합한 정보보안 관리방안 수립
- 시스템 보안취약점 진단
  - 서버/네트워크 취약점 진단 및 분석
  - 모의 해킹 시도 및 대응방안 제시
  - 정보보안 가이드 및 이행 방안 제시
  -
- 홈페이지 및 EMR 및 PACS 시스템에 대한 정보보호관리체계

## (ISMS)구축

- 정보보호 관리체계 현황 및 미비점 분석
- 정보보호 관리체계 인증 모의심사 수행 및 심사준비 등
- 정보보호 관리체계(ISMS) 운영지원
- 인증심사 사전 준비 및 심사 결함 사항 상주 지원
- 정보보안 교육

## ○ 조직 및 정보시스템 현황

구 분	세부내역	비 고
대상조직 및 임직원	5개부서, 100여명	전산과, 의무기록실, 총무부, 홍보실, 원무부
시스템 정보	서버시스템(30대)	
	네트워크장비(80대)	
	보안시스템(3대)	
	DBMS(3식)	

\* 2022.02.24 현재 병원 전체 시스템 현황으로 타 기관 연동시스템 및 인증범위에서 제외되는 시스템 등이 포함되어 실제 수량은 조정될 수 있음.

## ○ 웹 취약점 점검대상

홈페이지명	URL	비고
고신대학교복음병원(대표 홈페이지)	www.kosinmed.or.kr	
고신대병원복음병원 의학도서관	lib.kosinmed.or.kr	
고신대병원복음병원 사이버연수원	study.kosinmed.or.kr	
고신대병원복음병원 임상시험센터	ctc.kosinmed.or.kr/	

#### 4. 기대효과

- 주요정보자산 및 시설에 대한 잠재적인 정보보안 위험요소 감소
  - 전문 보안컨설팅 업체를 통한 객관적 정보보호 수준 진단으로 자체 보안 점검의 한계점 보완
  - 종합적인 취약점을 개선하여 안정적 서비스 제공
- 정보보호 관리체계 구축을 통한 고신대학교복음병원 운영 신뢰도 향상
- 모의훈련을 통한 사이버 위기 대응능력 강화
- 임직원 교육을 통한 정보보호 의식 수준 향상

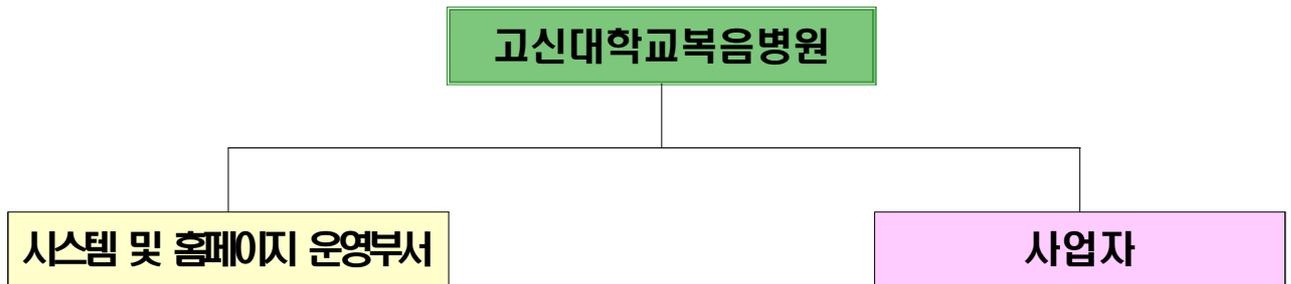
## II 사업추진 방안

### 1. 추진방향 및 전략

- 정보보호관리체계(ISMS) 구축을 통해 본원의 정보자산에 대한 비밀성·무결성·가용성을 향상하고 시스템의 안정적인 서비스 제공
- 최신 정보보호 기술, 국내·외 표준, 정보보호 관리체계 인증 기준 반영을 통한 고신대학교복음병원 정보보호 관리체계 수준 향상
- 정보보안의 일회성 관리 및 부분적 보안이 아닌 지속적 관리·운영을 위한 예방중심의 정보보호관리체계(ISMS) 구축

### 2. 추진체계 및 역할

- 추진체계



- 조직별 역할

조직 구분	수행내용
시스템 및 홈페이지 운영부서	<ul style="list-style-type: none"> <li>- 정보보호관리체계 관련 자산 및 조직 범위 파악</li> <li>- 사업이행사항 및 산출물 검토 등 사업관리</li> <li>- 보안현황분석 및 위험분석 지원 및 발견된 취약점 조치</li> <li>- 정보보호관리체계 운영 등</li> </ul>
사업자 (사업수행)	<ul style="list-style-type: none"> <li>- 정보보호관리체계 인증 사업 수행</li> <li>- 정보보호관리체계 인증 모의심사 및 증적자료 확인</li> <li>- 사업실적, 진도관리 및 보고, 산출물 관리 등</li> </ul>

### 3. 추진일정

추진구분	추진항목	사업 기간								인증서 획득시점
		M				M+1				
정보보호 관리체계 구축 및 운영	정보보호관리체계 구축 용역 수행	■	■	■	■	■	■	■	■	
	정보보호관리체계 인증심사 대비 증적 운영					■	■	■	■	
정보보호 관리체계 인증 심사	정보보호관리체계 인증 신청			■						
	인증심사 보완조치 및 인증서 획득									■

\* 단, 사업 진행에 따라 일정이 조정될 수 있음

### Ⅲ 과업 내용

#### 1. 상세 요구사항

##### ○ 컨설팅 요구사항(ConSulting Requirement)

요구사항 고유번호		CSR-001
요구사항 상세설명	정의	○ 사업 수행 계획 수립
	세부내용	○ 사업 수행에 대한 전반적인 계획 수립 - 사업 수행 방법 및 내용 제시 - 세부 과업 별 수행 범위, 내용, 일정 제시 - 투입 인력 별 역할 제시 - 정기(주/월간) 비정기 보고 방안 제시 - 교육훈련에 대한 내용 및 방법 제시
산출 정보		○ 사업수행계획서

요구사항 고유번호		CSR-002
요구사항 상세설명	정의	○ 정보보호관리체계(ISMS) 인증 컨설팅 수행 계획 수립
	세부내용	○ 정보보호관리체계 구축 과업을 위한 세부 계획 수립 - 정보보호관리체계 구축 수행 절차 제시 - 현황 및 위험 평가 분석 방안 제시 - 관리적/물리적/기술적 취약점 진단 항목 및 방법 제시 - 정보보호관리체계 구축 관련 산출물 제시
산출 정보		○ 정보보호관리체계 인증 컨설팅 수행 계획서

요구사항 고유번호		CSR-003
요구사항 상세설명	정의	○ 정보보호관리체계(ISMS) 자산 분류 및 중요도 평가
	세부내용	○ 정보보호관리체계 자산을 식별하고 그룹화하여, 취약점 분석·평가 자산분석 대상목록 작성 - 자산 분류 기준 제시 - 자산 중요도 평가 기준 제시 - 자산에 대한 중요도 산정
산출 정보		○ 자산 분석 보고서

요구사항 고유번호		CSR-004
요구사항 상세설명	정의	○ 정보보호관리체계 자산 취약점별 위험도 산정 및 조치대상 분류
	세부내용	○ 각 취약점 점검항목별 위험도 산정 및 우선 조치대상 분류 - 자산 위험도 평가 세부 방법 정의 - 잠재 위험 수준 평가 결과 도출
산출 정보		○ 위험분석.평가 보고서

요구사항 고유번호		CSR-005
요구사항 상세설명	정의	○ 정보보호관리체계(ISMS) 현황 및 문제점 분석.평가
	세부내용	○ 정보보호 관리체계 인증 등에 관한 고시(미래창조과학부고시 제 2013-36호)에 의거, 104개 정보보호관리체계 인증기준에 대한 보안현황 분석 - 담당자 인터뷰, 실사 등의 방법으로 진단 수행 - 점검 항목에 대한 상세 진단결과 및 개선방안 제시 ○ 『보건복지부 취약점 분석.평가 가이드라인』 기술적 분야 항목을 대상으로 기술적 취약점을 진단 - 점검 항목에 대한 상세 진단결과 및 개선방안 제시
산출 정보		○ 정보보호관리체계 운영 명세서 ○ 정보시스템 취약점 분석 결과 보고서 ○ 웹 모의해킹 보고서

요구사항 고유번호		CSR-006
요구사항 상세설명	정의	○ 정보보호관리체계(ISMS) 위험 조치방안 수립
	세부내용	○ 취약점 제거 및 경감방안에 대하여 세부 개선방안 수립 - 각 점검항목별 세부 조치 방법 도출 - 서비스에 대한 실질적인 조치방안 제시
산출 정보		○ 취약점 개선 가이드

요구사항 고유번호		CSR-007
요구사항 상세설명	정의	○ 정보보호관리체계(ISMS) 웹어플리케이션, 모의해킹 취약점 진단
	세부내용	○ 고신대학교복음병원 서비스에 대한 수작업 점검 실시 - 진단을 위한 세부 시나리오 작성 - 웹 취약점 분석 항목 및 OWASP 10대 취약점 활용 - 각 취약 항목 별 결과 도출 및 대응방안 제시
산출 정보		○ 웹어플리케이션, 모의해킹 진단 결과 보고서

요구사항 고유번호		CSR-008
요구사항 상세설명	정의	○ 정보보호관리체계(ISMS) 정보보호 수준 분석
	세부내용	○ 정보보호(ISMS) 현황 분석 - 정보보호관리과정(5단계, 12개 통제사항), 정보보호대책(13개 분야, 92개 통제사항)에 대한 현황 파악 - 현황 파악 후 미비점에 대한 보완 및 개선 계획 마련
산출 정보		○ 정보보호관리체계(ISMS) 정보보호 수준 분석서 ○ 정보보호관리체계 운영 명세서

요구사항 고유번호		CSR-009
요구사항 상세설명	정의	○ 정보보호관리체계(ISMS) 표준 모형 및 문서 제.개정
	세부내용	○ 정보보호관리체계 보안 운영 표준 분석 및 개선사항 반영 - 관련 법규, 지침 등을 기준으로 반영이 필요한 항목 개정 실시 - 개정 사유, 대상, 기준등에 대한 세부 내용 도출
산출 정보		○ 정보보호관리체계(ISMS) 보안 운영 표준 문서 제.개정(안)

요구사항 고유번호		CSR-010
요구사항 상세설명	정의	○ 정보보호관리체계(ISMS) 인증 심사 지원 등
	세부내용	○ 정보보호관리체계 인증을 위한 인증 본심사 지원(12월 중 신청) - KISA 정보보호관리체계 인증신청서 양식을 활용하여 신청서 작성 ※ 인증 심사비는 사업자 부담 사항이 아님
산출 정보		○ 인증 심사 신청서

요구사항 고유번호		CSR-011
요구사항 상세설명	정의	○ 정보보호관리체계(ISMS) 결함 보완 지원
	세부내용	○ 심사를 통해 도출된 결함에 대한 보완 - 정보보호관리체계(ISMS) 인증 심사의 결함사항 보완에 대한 조치 가이드
산출 정보		○ 정보보호관리체계(ISMS) 인증심사 결함 보완 조치 가이드

요구사항 고유번호		CSR-012
요구사항 상세설명	정의	○ 정보보호관리체계(ISMS) 인증 유지 방안 수립
	세부내용	○ 정보보호관리체계 인증 유지 방안 수립 - 사후관리심사를 위한 필요사항 정의 - 정보보호관리체계의 지속적인 유지를 위한 관리방법 제시
산출 정보		○ 정보보호관리체계(ISMS) 인증 유지 관리 가이드

요구사항 고유번호		CSR-013
요구사항 상세설명	정의	○ 정보보안 인식제고 교육
	세부내용	○ 임직원 보안인식 제고를 위한 보안교육 실시 - 교육대상 및 내용, 일정은 담당자와 협의하여 진행
산출 정보		○ 정보보안 교육자료

○ 보안 요구사항(SECURITY Requirement)

요구사항 고유번호		SER-001
요구사항 상세설명	정의	○ 사업수행 시 보안 준수
	세부내용	○ 본원의 보안업무 규정 및 행자부 "정보화용역사업 보안 관리 매뉴얼"에 의거 보안 사항을 준수하여야 함

요구사항 고유번호		SER-002
요구사항 상세설명	정의	○ 장비 및 자료보안
	세부내용	<ul style="list-style-type: none"> <li>○ 과업수행에 따른 조사 및 분석자료 등이 타 용도에 임의로 사용되거나 외부에 유출되지 않도록 조치하여야 함</li> <li>○ 제공된 내부자료에 해안 복사 및 외부반출을 할 수 없으며, 과업완료 후 본원에 반환하여야 함</li> <li>○ 참여인력의 노트북, 휴대용저장매체 등 관련 장비를 반입, 반출할 때에는 휴대용 저장매체(전산장비 포함) 반출입 대장을 작성하여 제출하고, 악성코드 감염 및 자료 무단반출 여부를 확인하는 등 보안조치를 하여야 함</li> <li>○ 과업수행으로 생산되는 모든 산출물 및 기록은 본원에서 전량 회수하고 인가하지 않은 자에게 제공·대여·열람을 금지함</li> <li>○ 본 용역사업관련 모든 기록, 자료 및 산출물을 본원의 파일서버 또는 보안담당자가 지정한 PC에서 관리하여야 하며, 웹하드 등에 공유 및 개인 메일함 저장을 금지</li> <li>○ 사업수행에 사용되는 PC에 대해 네트워크 접근제어, 최신 백신 등 본원이 지정하는 보안 프로그램을 설치하고 실행하여야 함</li> <li>○ 용역 수행 시의 PC는 원칙적으로 인터넷 연결을 금지하되, 사업수행상 불가피한 경우에는 본원의 승인하에 제한적으로 사용하여야 함</li> <li>○ 외부에서 본원의 업무망에 원격접속을 원칙적으로 금지하되, 사업수행상 불가피한 경우에는 본원의 승인하에 접속하도록 함</li> </ul>

요구사항 고유번호		SER-003
요구사항 상세설명	정의	○ 사업 종료 시 보안 사항
	세부내용	○ 용역사업 종료 시 사업관련 모든 자료를 반납하고 정보보안담당자 입회하에 복구가 불가능 하도록 완전삭제 등의 보안 조치를 한 후 휴대용 저장매체 관리대장을 작성하여야 하며, 사업 관련 자료를 보유하고 있지 않다는 대표자 명의의 보안확약서를 제출하여야 함

○ 제약사항(CONstraint Requirement)

요구사항 고유번호		COR-001
요구사항 상세설명	정의	○ 수행업체 제한
	세부내용	○ 최근 정보보호 관리체계(ISMS) 인증 컨설팅 수행실적은 입찰공고문의 기준으로 제한함

요구사항 고유번호		COR-002
요구사항 상세설명	정의	○ 컨소시엄 불가 및 하도급 제약사항
	세부내용	○ 본 사업은 컨소시엄 구성 및 하도급을 허용하지 않음

요구사항 고유번호		COR-003
요구사항 상세설명	정의	○ 지적재산권 귀속
	세부내용	○ 당해 계약에 따른 계약목적물에 대한 지식재산권은 본원이 소유함

요구사항 고유번호		COR-004
요구사항 상세설명	정의	○ 데이터 수집·관리 시 제약사항
	세부내용	○ 필요시 본 사업관련 저작권, 사용권, 특허 등에 대해 일체의 하자가 없도록 사전에 면밀히 분석하여 해결하여야 하며 문제발생 시 제반 비용을 포함한 모든 책임을 져야 함

○ 프로젝트 관리 요구사항(Project Mgmt. Requirement)

요구사항 고유번호		PMR-001
요구사항 상세설명	정의	○ 조직구성 및 인력관리
	세부내용	<ul style="list-style-type: none"> <li>○ 사업을 수행할 적절한 사업수행 조직과 단계별 인력 투입공수계획 및 작업 단위별 업무분장 내역(역할), 투입률을 제시하여야 함</li> <li>○ 수행기간 2개월</li> <li>○ 고급(PM) 2M/M, 중급 2M/M, 초급 2M/M (단. 등급별 투입공수는 협의에 의해 조정 가능하나, PM은 고급이상 인력으로 1M/M 이상 상주)</li> <li>○ 과업수행 도중 참여인력에 대한 불성실, 기준미달, 기술력 미흡 등을 이유로 참여인력 교체요구를 받은 경우, '낙찰사'는 즉시 대안을 마련하여 본원의 승인을 받은후 대체 인력을 투입시켜야 함</li> </ul>

요구사항 고유번호		PMR-002
요구사항 상세설명	정의	○ 과업 요구사항 관리
	세부내용	<ul style="list-style-type: none"> <li>○ 과업지시서에 명시된 모든 항목은 최소한의 사항만을 규정하였으므로 상세히 기술되지 않았거나 누락된 사항에 대하여 '낙찰사'는 운영상 문제가 발생하지 않도록 사전 조치를 하여야 함</li> <li>○ 본 과업지시서 상에 명시된 사항 중 해석상의 이견이 있을 경우에는 본원과 '낙찰사'간에 상호 협의하여 조정함</li> <li>○ 본원은 계약내용 전부에 대하여 권리행사를 할 수 있으며, '낙찰사'는 이에 대하여 전적으로 동의하여야 함</li> <li>○ '낙찰사'는 공급하는 제품의 품질에 대하여 최종적인 책임을 져야 하며, 기술환경 및 기타사정 등으로 인하여 일부사업의 내용 및 범위 등의 변경이 필요한 경우에는 쌍방의 협의 하에 조정할 수 있음</li> </ul>

요구사항 고유번호		PMR-004
요구사항 상세설명	정의	○ 프로젝트 일정관리
	세부내용	○ '낙찰사'는 사업추진과정에서 생산되는 제반 작업 단위별 산출물에 대하여 작업 일정계획 및 품질보증계획과 연계하여 산출물의 종류, 주요내용, 작성 및 제출시기, 제출 부수 등 제시 ○ 컨설팅 결과물, 보고서등 산출물 전체 : 출력물 2부, USB 1매 ○ 정보보호규정, 지침 및 ISMS 인증심사에 필요한 증적자료 등

○ 프로젝트 지원 요구사항(Project Support Requirement)

요구사항 고유번호		PSR-001
요구사항 상세설명	정의	○ 교육 및 기술이전
	세부내용	○ '낙찰사'는 정보보호 관리체계 구축 컨설팅이 본원의 업무 담당자 및 관련 담당자에게 이전될 수 있도록 이에 필요한 교육을 실시하여야 하며, 교육은 업무 담당자들이 완전히 이해하여 활용할 수 있도록 충분히 이루어져야 함

요구사항 고유번호		PSR-002
요구사항 상세설명	정의	○ 하자 유지보수
	세부내용	○ ISMS 심사 결함 사항 지원 시 원내에 상주하며 결함 사항에 대한 적극적인 유지보수 지원이 이루어져야 함 ○ <b>ISMS 인증심사 불합격 시 합격 될 때까지 인증심사를 지원하여야 하며 지원 기간동안 컨설팅 업체는 추가 심사비용은 업체 부담</b> ○ '낙찰사'는 사업을 종료한 날(사업에 대한 시험 및 검사를 수행하여 최종산출물을 인도한 날을 말한다)부터 1년 이내의 범위에서 발생한 하자에 대하여 담보책임을 부담함