**정보보호관리체계 컨설팅 범위 및 요구사항 (사전접수)**

1. **제안서 작성 (온라인 제출 : admin@uuh.ulsan.kr)**

제안서는 요구사항을 반영하되 아래와 같은 내용을 포함하여야 함

\* 주요 정보보호관리체계 컨설팅 수행 실적

\* 수행조직의 구성 및 업무분장 (보안점검 및 취약점점검, 기타를 구분할 것)

\* 추진일정계획(1개월 기준)

\* 제안가 기재 불필요, A4 크기 가로 (PPT 또는 PDF파일) 20장 이내

1. **요구사항**

|  |  |  |
| --- | --- | --- |
| **구 분** | **요구사항** | **참 고** |
| **보안점검**  **(내부감사)** | **∙ 자격요건**  - PM은 최소 고급 이상 인력으로 유사규모 보안점검을 실시한 경험이 있을 것  - 2인이상 4인이하의 보안점검반을 구성할 것  - 보안점검반 인력 내 ISMS-P 또는 유사 정보보호 심사원자격(ISO27001) 보유자가 최소 1명 이상 포함될 것  **∙ 점검기간**  - 5일이내 (2020.08) 협의  **∙ 점검내용**  - ISMS(신) 인증기준에 부합하는 체크리스트의 작성  - 법적요구사항을 포함한 관리적 / 기술적 영역을 점검  - 보안점검의 결함사항에 대한 해결책 제시  **∙ 산출물**  - 보안점검 계획서  - 보안점검 결과보고서 | ∙ 2017년 ISMS(구) 인증 후 정보보호관리체계 운영 中  ∙ 사후심사 자체적으로 이행  ∙ 2020년 11월 인증심사 예정  ∙ 계획서 및 결과보고서는 최소요구사항임 |
| **취약점 점검** | **∙ 점검기간**  - 10일이내 (2020.08) 협의  **∙ 점검내용 및 대상**  - ISMS(신) 인증기준에 부합하는 체크리스트의 작성  - ISMS 인증범위 내 정보자산  ※ 서버(52),DB(5),보안장비(41),웹(8),모바일(4), PC(70) 등  ※ 점검대상은 일부 변경될 수 있음  **∙ 산출물**  - 인프라 취약점 점검 계획서  - 인프라 취약점 점검 결과 보고서(전체, 자산그룹별) | ∙ 병원 내 기도입된 솔루션 (SolidStep, NetHelper 등) 활용 가능 (단, 최신 기준을 확인 및 적용)  ∙ 일부 보안장비 및 네트워크 장비는 수동점검 필요  ∙ 계획서 및 결과보고서는 최소 요구사항임 |
| **기 타** | ∙ ISMS(신) 기준에 따라 정보보호흐름도의 작성 지원  ∙ 2020년 기준 주요 법적요구사항 및 인증 변화 및 제공  ∙ 인증심사 시 도출된 결함에 대한 가이드 지원 |  |