

채용분야	정보보안	분류체계	대분류	중분류	소분류	세분류
			20. 정보통신	01. 정보기술	06. 정보보호	01. 정보보호관리운영 02. 정보보호진단분석 03. 보안사고분석대응
설립이념	○ 한국과학기술원법 - 깊이 있는 이론과 실체적인 응용력으로 국가 산업 발전에 기여할 고급 과학기술 인재 양성 - 국가 정책으로 추진하는 중장기 연구 개발과 국가 과학기술 저력 배양을 위한 기초응용 연구 수행 - 각 분야 연구 기관 및 산업계와 연계한 연구 지원					
KAIST 주요사업	○ 교육: 과학기술 글로벌 인재 양성 ○ 연구: 인류 난제 해결을 위한 연구 ○ 국제화: 글로벌 리더십 역량 강화 ○ 창업: 창업혁신 생태계 구축 및 발전					
성장 동력	○ Vision : 국가와 인류, 지구를 위한 독특한 빛깔의 세계 10위권 대학 ○ Mission: 인류의 행복과 번영을 실현하는 과학기술혁신대학 ○ QAIST: 창의인재, Post AI 융복합 연구, 글로벌 인재, 기술가치창출, 소통의 신뢰 ○ 3C Spirit : Challenge, Creativity, Caring					
담당 업무	○ 정보보안 기획 및 정책수립 ○ 정보보안활동(교육,훈련,점검) ○ 정보보안 침해사고 분석 및 대응(보안관제) ○ 정보보호시스템 구축 및 운영 ○ 개인정보보호시스템 관련 업무 수행					
직무수행내용	정보보호관리운영	○ (정보보호 거버넌스 구현) 정보보호 전략 수립하기, 정보보호 자원 할당하기, 정보보호 성과 관리하기 ○ (정보보호 정책 기획) 정보보호 정책 수립하기, 정보보호 정책 유지관리하기 ○ (보안 위협관리) 위협관리 계획 수립하기, 위협 분석하기, 위협 분석 결과 조치하기 ○ (정보보호 계획 수립) 정보보호 목표 및 대상범위 설정하기, 정보보호 중장기 계획 수립하기, 정보보호 세부 실행 계획 수립하기 ○ (개인정보보호 사고대응) 개인정보 침해사고 대응하기 ○ (네트워크 보안 운영) 네트워크 보안솔루션 운영 및 개선하기, 네트워크 보안 신규 위협 대응하기, 네트워크 보안솔루션 업데이트 적용하기 ○ (애플리케이션 보안 운영) 애플리케이션 보안솔루션 운영.개선.업데이트 적용하기, 애플리케이션 보안 신규 위협 대응하기 ○ (시스템 보안 운영) 시스템 보안솔루션 운영.개선.업데이트 적용하기, 시스템 보안 신규 위협 대응하기 ○ (관리적 보안 운영) 정보보호 이행 점검하기, 침해사고 대응하기, 정보보호 정책 교육하기, 외부자 보안 관리하기 ○ (물리 보안 운영) 물리 보안솔루션 운영하기, 물리 보안솔루션 운영 개선하기, 물리 보안 신규 위협 대응하기 ○ (보안 장비 운영) 보안시스템 상태 체크하기, 정책요청 적용하기, 보안시스템 가용성 관리하기 ○ (보안성 검토) 보안성 검토 기준 수립하기, 보안성 검토 수행하기, 보안 대책 권고하기 ○ (내부 보안 감사 수행) 보안 감사 계획 수립하기, 보안 감사 실행하기, 보안 감사 결과 보고하기				
	정보보호진단분석	○ (보안전략수립 컨설팅) 보안 전략 현황 분석하기, 보안 위협 평가하기, 보안 전략 수립하기 ○ (보안감리) 보안감리 계획하기, 보안감리 수행하기, 보안감리 사후관리하기 ○ (보안감사) 보안감사 계획하기, 보안감사 수행하기, 보안감사 사후관리하기 ○ (정보보호관리체계 인증) 정보보호관리체계 인증심사 체계 및 기준 수립하기, 정보보호관리체계 인증심사 수행하기 ○ (정보보호제품 도입평가) 정보보호제품 평가체계 수립하기, 정보보호제품 평가기준 수립하기, 정보보호제품 평가 수행하기 ○ (보안대책설계 컨설팅) 보안현황 분석하기, 보안위험 평가하기, 보안통제 설계하기 ○ (정보시스템 진단) 정보시스템 진단 기준 마련하기, 정보시스템 진단 결과 도출하기, 정보시스템 대응책 마련하기 ○ (모의해킹) 모의해킹 준비하기, 모의해킹 수행하기				
	보안사고분석대응	○ (보안관제 기획운영) 보안관제센터 설계하기, 보안관제센터 구축하기, 보안관제센터 관리하기 ○ (침해대응팀(CERT) 구축) 침해대응 조직 구성하기, 침해대응 활동계획 수립하기, 외부기관과의 침해사고 공조대응 체계 구성하기 ○ (디지털 포렌식) 증거자료 수집하기, 디지털포렌식 분석하기 ○ (사이버수사) 디지털포렌식 관련법규 활용하기, 증거수집기술 활용하기, 사이버사건 해결하기 ○ (침해사고 분석) 분석기반 조성하기, 침해사고 원인 분석하기, 침해사고 사후처리하기 ○ (악성코드 분석) 악성코드 분석환경 구축하기, 악성코드 분석도구 운용하기, 악성코드 대응하기 ○ (보안로그 분석) 보안시스템 로그 분석하기, 보안로그 상관분석하기, 탐지패턴 개발하기 ○ (보안이벤트 대응) 보안이벤트 모니터링하기, 보안이벤트 후속 조치하기				
필요지식	○ 정보통신 일반에 대한 이해 ○ 정보시스템 및 OS에 대한 경험과 지식 ○ S/W 설계 또는 개발 경험 ○ 패킷분석 기술 및 해킹 ○ 정보시스템 및 보안시스템 구성 및 네트워크 운영 지식(방화벽, IPS, 웹방화벽, DDoS차단시스템, 라우터, 스위치, DNS, QoS )					

필요기술	<div>○ 침해사고 및 취약점 분석 기술</div> <div>○ 포렌식 기술</div> <div>○ 악성코드 분석 기술</div> <div>○ 보안시스템 활용 기술 및 시스템 로그 분석</div> <div>○ 프로그램 언어 활용</div> <div>○ 시스템 활용 및 OS 사용 기술</div>
직무수행태도	<div>○ 사전 점검과 예상되는 예측가능한 상황에 대비하는 자세가 필요함</div> <div>○ 신속한 조치로 문제를 해결한 후 문제점의 근본 원인을 알아내어 조치하려는 의지가 필요함</div> <div>○ 보안에 대한 개념과 정보보호에 대한 명확한 인식이 필요함.</div> <div>○ 기술발달에 따른 신기술 및 보안대응에 대한 지속적인 모니터링과 학습하는 자세가 필요함</div>
직업기초능력	○ 문제해결능력, 대인관계능력, 직업윤리, 의사소통능력, 자기개발능력, 자원관리능력, 조직이해능력, 기술능력, 정보능력, 수리능력
참고사이트	<a href="http://www.ncs.go.kr">www.ncs.go.kr</a> , <a href="http://www.kaist.ac.kr">www.kaist.ac.kr</a>