

광주과학기술원 2022년 직원(무기계약직) 채용 직무기술서

1	직종	일반직	채용분야	정보보안지원
NCS 분류 체계	20.정보통신	01.정보기술	06.정보보호	01.정보보호관리운영 02.정보보호진단분석 03.보안사고분석대응
기관 주요사업	<ul style="list-style-type: none"> • 고급 과학기술인재 양성, 산업계와의 협동연구 및 외국과의 교육연구 교류촉진, 기술의 이전·사업화의 촉진 및 창업 지원 등을 통한 국가 과학기술 및 지역 균형발전에 이바지 			
능력단위	<ul style="list-style-type: none"> • (정보보호 관리운영) 정보보호 정책 기획, 보안위험관리, 개인정보보호 운영, 네트워크 보안 운영, 애플리케이션 보안 운영, 시스템 보안 운영, 관리적 보안 운영, 물리 보안 운영, 보안 장비 운용, 보안성 검토, 내부 보안 감사 수행, 협력사 보안 관리 • (정보보호진단분석) 정보시스템 진단, 정보보호관리체계 심사컨설팅, 정보보호제품 평가 컨설팅, 모의해킹 • (보안사고분석대응) 보안관제 기획운영, 디지털 포렌식, 사이버수사, 침해사고 분석, 악성코드 분석, 보안로그 분석, 보안이벤트 대응 			
직무수행 내용	<ul style="list-style-type: none"> • (정보보호 정책 기획) 정보보호 정책 유지관리 • (보안 위험관리) 위험 분석, 위험 분석 결과 조치 • (개인정보보호 운영) 개인정보보호 이행 점검, 개인정보 침해사고 대응 • (네트워크 보안 운영) 네트워크 보안솔루션 운영 및 개선, 네트워크 보안 신규 위협 대응, 네트워크 보안솔루션 업데이트 적용 • (애플리케이션 보안 운영) 애플리케이션 보안솔루션 운영 및 개선, 애플리케이션 보안 신규 위협 대응, 애플리케이션 보안솔루션 업데이트 적용 • (시스템 보안 운영) 시스템 보안솔루션 운영 및 개선, 시스템 보안 신규 위협 대응, 시스템 보안솔루션 업데이트 적용 • (관리적 보안 운영) 정보보호 이행 점검, 침해사고 대응, 정보보호 정책 교육, 외부자 보안 관리 • (물리 보안 운영) 물리 보안솔루션 운영 및 개선, 물리 보안 신규 위협 대응 • (보안 장비 운영) 보안시스템 상태 체크, 정책요청 적용, 보안시스템 가용성 관리 • (보안성 검토) 보안성 검토 수행, 보안 대책 권고 • (내부 보안 감사 수행) 보안 감사 실행, 보안 감사 결과 보고 • (협력사 보안 관리) 협력사 보안 운영, 협력사 보안 감사 <ul style="list-style-type: none"> • (정보시스템 진단) 정보시스템 진단 기준 마련, 정보시스템 진단 결과 도출, 정보시스템 대응책 마련 • (정보보호관리체계 심사컨설팅) 정보보호관리체계 심사 준비, 정보보호관리체계 인증 취득, 정보보호관리체계 인증 사후관리 • (정보보호제품 평가 컨설팅) 정보보호제품평가 준비, 정보보호제품인증 취득, 정보보호제품인증 사후관리 • (모의해킹) 모의해킹 준비, 모의해킹 수행 <ul style="list-style-type: none"> • (보안관제 기획운영) 보안관제센터 관리 • (디지털 포렌식) 증거자료 수집, 디지털포렌식 분석 • (사이버수사) 디지털포렌식 관련 법규 활용, 증거수집기술 활용, 사이버사건 해결 • (침해사고 분석) 침해사고 원인 분석, 침해사고 사후처리 			

	<ul style="list-style-type: none"> • (악성코드 분석) 악성코드 분석도구 운용, 악성코드 대응 • (보안로그 분석) 보안시스템 로그 분석, 보안로그 상관분석, 탐지패턴 개발 • (보안이벤트 대응) 보안이벤트 모니터링, 보안이벤트 후속 조치 	
일반요건	연령·성별	• 제한 없음 ※ 단, 직원인사규정에 의거 만61세에 도달한 자 지원불가
교육요건	학력·전공	• 제한 없음
필요지식	<ul style="list-style-type: none"> • 정보통신 일반에 대한 이해 • 정보시스템 및 OS에 대한 경험과 지식 • S/W에 설계 개발 경험 • 패킷분석 기술 및 해킹 • 정보시스템 및 보안시스템 구성 및 네트워크 운영 지식(방화벽, IPS, 웹방화벽, DDoS차단시스템, 라우터, 스위치, DNS, QoS) 	
필요기술	<ul style="list-style-type: none"> • 침해사고 및 취약점 분석 기술 • 포렌식 기술 • 악성코드 분석 기술 • 보안시스템 활용 기술 및 시스템 로그 분석 • 프로그램 언어 활용 • 시스템 활용 및 OS 사용 기술 	
직무수행 태도	<ul style="list-style-type: none"> • 올바른 직업관, 원만한 대인관계, 책임감, 적극적 협업자세 • 최신 기술을 습득하여 전문성을 기르려는 태도 • 규정, 관련 법규, 표준 기술 기준에 대한 준수 의지 • 능동적이고 적극적으로 업무에 임하려는 태도 • 즉각적이고 신속하게 대처하려는 자세 • 성실하게 업무에 임하는 자세 • 창의적으로 사고하려는 노력 • 책임지고 맡은 업무를 완성하려는 태도 • 복잡한 사회 환경에 대한 전반적인 이해와 통찰력 • 고객 요청에 최대한 부합하고자 하는 서비스 자세 	
필요자격	자격 사항	<ul style="list-style-type: none"> • 아래 자격 중 1개 이상의 자격 소지자 - 정보보안기사 - 한국인터넷진흥원 정보보호관리체계 인증 심사원 또는 정보보호전문가(SIS) - 국제정보시스템감사통제협회 공인정보시스템감사사(CISA) - 국제정보시스템보안자격협회 공인정보시스템보호전문가(CISSP)
	외국어 능력	<ul style="list-style-type: none"> • TOEIC 700점 이상(TOEFL 79점, New TEPS 264점, TOEIC SPEAKING IM2, OPIc IM2) 중 하나를 충족 ※ 글로벌 교육환경 구축, 외국인 학생 및 연구원 대상 서비스 제공, 해외 연구네트워크 구축 등 기관 전략과제 추진을 위해 업무 전반에 영어능력이 필요함
직업기초 능력	<ul style="list-style-type: none"> • 의사소통능력, 수리능력, 문제해결능력, 자원관리능력, 대인관계능력, 자기개발능력, 정보능력, 기술능력, 직업윤리 	
참고사이트	<ul style="list-style-type: none"> • 직업기초능력 관련: 국가직무능력표준 홈페이지(www.ncs.go.kr) 	