

직무기술서(정보보안)

□ 분류

대분류(직군)	중분류(직렬)	소분류(직종)	세분류(직무)
20. 정보통신	01. 정보기술	06. 정보보호	01. 정보보호관리·운영 01. 보안사고분석대응

□ 직무 기본 정보

직무명	정보보안	NCS 분류코드	2001060101_19v2
직무정의	<ul style="list-style-type: none"> ○ 위험관리에 기반한 정보보호 대책을 도출하고 실행, 정보 자산 안정적 운영 ○ 보안사고의 위험정보를 사전 탐지하고 예방, 보안사고 시 증거 확보 후 분석하여 신속 대응 		
관련 자격증	○ 정보보안기사(산업기사), 정보처리기사, 정보보호 및 개인정보보호 관리체계 인증(ISMS-P) 등		

□ 직무 주요업무 및 역할

구분	주요업무 및 역할
정보보호 계획수립	<ul style="list-style-type: none"> ○ 조직의 정보보호 목표 설정을 위한 정보보호정책 분석 ○ 정보보호 관리체계 내의 서비스, 업무, 조직, 정보시스템, 설비 파악 및 분석 ○ 정보보호 정책과 관리체계의 분석에 의한 조직의 관리적, 물리적, 기술적 목표 설정
보안시스템 운영	<ul style="list-style-type: none"> ○ 시스템 보안요구사항 파악 및 준수, 시스템구조 및 보안솔루션 현황 파악 ○ 보안 요구사항에 의거한 시스템 보안솔루션 운영
관리적보안 운영	<ul style="list-style-type: none"> ○ 정보보호 관련 법 준수를 위한 규정과 정책에 기반한 정보보안 교육 수행 ○ 보안 요구사항에 의거한 시스템 보안솔루션 관리, 정보보호정책 이행 여부 점검
보안감사	<ul style="list-style-type: none"> ○ 보안 감사 규정에 의거하여 보안 감사 수행을 위한 사전 예비조사 수행 및 계획 수립 ○ 감사에 필요한 자료 수집·분석, 감사 결과에 대한 시정조치
보안사고 대응	<ul style="list-style-type: none"> ○ 공격별 대응 기능을 제공하는 보안시스템 식별 ○ 정보 유출 또는 침해사고 발생 원인 분석 및 조치

□ 필요 지식 및 역량

구분	능력단위
지식	<ul style="list-style-type: none"> ○ (정보보호계획수립) 정보보호정책에 대한 이해 ○ (시스템보안운영) 정보보호 관리체계, 정보보안 실무지침 이해, 정보보안 운영 정책 ○ (관리적보안운영) IT 보안 교육, 정보보호 및 개인정보보호 관리체계, 정보보안 사고관리 ○ (보안감사) 관련 법규정, 정보보호 및 개인정보보호 관리체계(ISMS-P) ○ (보안사고대응) 로그 분석 절차, 보안사고 대응 절차, 보안사고 유형 분석, 해킹이론
기술	<ul style="list-style-type: none"> ○ (정보보호계획수립) 정보보호 정책 체계파악 능력, 정보보호 보안 대책에 관한 기술 ○ (시스템보안운영) 서버 보안 소프트웨어 설치 및 운영 기술, 운영체제 취약점 분석 능력 ○ (관리적보안운영) 정보보호 교육 수행 능력, 정보보호시스템 운영 기술 ○ (보안감사) 감사 자동화 도구 사용 기술, 감사자료 수집 및 분석 기술 ○ (보안사고대응) 네트워크 복원 기술, 로그 분석 능력, 모의해킹 능력, 보안사고 간 연관성 분석 기술, 보안사고 별 후속 조치 수행 능력
태도	<ul style="list-style-type: none"> ○ (정보보호계획수립) 관련 규정 준수 의지, 정보자산을 누락 없이 식별하려는 자세 ○ (시스템보안운영) 설계된 서버 보안을 준수하여 구현하려는 노력, 문제 해결을 위한 적극적 자세 ○ (관리적보안운영) 요구사항을 적극적으로 반영하려는 태도, 책임감, 교육훈련 개선 의지 ○ (보안감사) 감사 대상 및 범위 선정 시 합리적인 태도, 공정하고 객관적인 자세 ○ (보안사고대응) 종합적으로 분석하려는 의지, 지속적으로 연구하려는 자세
필요역량	의사소통능력, 문제해결능력, 자원관리능력, 대인관계능력, 정보능력, 조직이해능력, 직업윤리