IT 인프라(정보보안) 분야 직무기술서

채용분야	IT 인프라(정보보안) 분야				
대분류	20. 정보통신				
중분류	01. 정보기술				
소분류	02. 정보기술개발	06. 정보보호			11. 개인정보보호
세분류	06. 보안엔지니어링	01. 정보보호관리·운영	02. 정보보호진단·분석	03. 보안사고분석대응	01. 개인정보보호관리운영
주요사업	미래 선도 원천기술 확보, 국가·사회적 현안 해결기술 개발, 융합·협력 개방형 플랫폼 구축				
능력단위	○ **(보안엔지니어링)** 01. 보안 구축 계획 수립, 03. 보안 구축 요구사항 분석, 04. 관리적 보안 구축, 05. 물리적 보안 구축, 10. 보안인증 관리, 11.SW개발 보안 구축, 12. DB보안 구축, 13. 시스템 보안 구축, 14. NW보안 구축				
	○ **(정보보호관리·운영)** 03. 정보보호 정책 기획, 05. 보안 위험관리, 06. 정보보호 계획 수립, 08. 네트워크 보안 운영, 09. 애플리케이션 보안 운영, 10. 시스템 보안 운영, 11. 관리적 보안 운영, 13. 보안 장비 운용, 14. 보안성 검토, 15. 내부 보안 감사 수행, 16. 협력사 보안 관리				
	○ **(정보보호진단·분석)** 03. 보안감사, 04. 정보보호관리체계 인증, 07. 정보시스템 진단, 10. 모의해킹				
	○ **(보안사고분석대응)** 03. 디지털 포렌식, 04. 사이버조사, 05. 침해사고 분석, 06. 악성코드 분석, 07. 보안로그 분석, 08. 보안사고 대응				
	○ **(개인정보보호관리운영)** 01. 개인정보보호 법령·정책 분석, 02. 개인정보보호 기획, 04. 개인정보보호 위험관리, 05. 개인정보보호 운영, 10. 개인정보 수탁자 관리				
직무수행 내용	○ **(보안엔지니어링)** 정보보호 및 개인정보보호 관련 법률/정책 등의 이해를 바탕으로 연구원 정보보호정책을 수립하고 네트워크/시스템에 적용/운용하는 업무				
	○ **(정보보호관리·운영)** 연구원의 비전과 미션을 수행하기 위하여 정보 자산을 안정적으로 운영하는 데 필요한 정보보호 전략 및 정책을 수립하고, 관련 법제도 준수, 정보보호관리 활동을 수행하며, 위험관리에 기반한 정보보호대책을 도출하고 실행하는 업무. 정보보호시스템을 운영하는 업무				
	○ **(정보보호진단·분석)** 연구원에 대한 외부 보안감사 대응 및 자체 보안감사를 실시하며 관련된 정보시스템 대상 취약점 진단 및 조치, 모의해킹을 수행하는 업무				
	○ **(보안사고분석대응)** 연구원 사이버공격 및 침해사고의 예방활동, 위협정보를 탐지/분석, 피해 현황 파악 및 복구 등 침해사고 대응절차를 수행하는 업무				
	○ **(개인정보보호관리운영)** 개인정보보호 법령 및 정책을 분석하여 연구원의 개인정보보호 체계를 수립하고 이행하는 업무				
필요지식	○ **(보안엔지니어링)** 정보보호관리체계에 관한 국제표준 규격(ISO27001), 정보보호 및 개인정보보호 관리체계, (ISMS-P), 서비스 공격유형, 시스템 아키텍처, 암호알고리즘, 접근통제, 식별 및 인증, 보안 솔루션 종류 및 유형별 제공 기능, 네트워크 기반 공격유형 및 QoS, 소프트웨어 개발 보안 가이드, 프로그래밍 언어 관련 지식				
	○ **(정보보호관리·운영)** 정보보호시스템 운영, 네트워크 시스템 운영, 서버 시스템 운영, 웹서비스 운영 관련 지식				
	○ **(정보보호진단·분석)** 정보시스템 보안 진단 및 취약점 진단/분석 과 조치, 물리적/관리적 보안운영 정책/이행 관련 지식				
	○ **(보안사고분석대응)** 침입대응, 분석 실무에 필요한 정보수집 및 활용 방법, 침해사고 대응절차, 원인과 사고과정 분석, 보안위협 이벤트 관련 지식				
	○ **(개인정보보호관리운영)** 개인정보보호 법령 및 정책, 개인정보침해사고 대응 관련 지식				

필요기술	○ **(보안엔지니어링)** 정보화/정보보호 기획, 내/외부 환경분석, 정보보호 및 개인정보보호 법령/규정 분석 기술
	○ **(정보보호관리·운영)** 네트워크 시스템 운영 기술, 서버 운영 기술, 웹서비스 운영 기술, 운영체제의 환경 설정 기술, 응용 프로그램 실행 제어 기술
	○ **(정보보호진단·분석)** 취약점 진단 도구 운영 기술, 수동 취약점 진단 기술, 취약점 조치 기술
	○ **(보안사고분석대응)** 침해사고 분석 기술(분석도구, 원인, 사고과정 분석 등), 네트워크시스템 로그/보안취약점/분석 도구 사용기술, 악성코드 행위분석 기술, 파일/프로세스/레지스트리구조 동작방식 분석기술
	○ **(개인정보보호관리운영)** 개인정보보호 법령 및 정책 분석 기술, 개인정보 침해사고 분석기술, PC 분석기술, 암호화 관련 기술
직무수행 태도	○ 고객의 요청에 대한 적극적인 수용, 다양한 가능성에 대해 유연하게 사고하는 태도, 이해관계자 의견을 경청하는 태도, 자신의 업무에 책임감을 갖고 역할을 다하려는 태도, 합리적인 사고능력을 기반으로 정확한 업무 수행을 위해 집중하려는 태도, 정보시스템을 세심하게 관리하는 태도, 취약점을 지속적으로 점검하는 태도, 보안 위협에 신속하게 대응하는 태도, 정보보호 정책을 철저히 준수하는 태도, 보안 상황을 정확하게 분석하는 태도, 정보보호 시스템을 안정적으로 운영하는 태도, 개인정보보호에 대한 책임감 있는 태도, 보안감사에 적극적으로 대응하는 태도, 사이버 침해 예방활동을 꾸준히 수행하는 태도, 관계자와 협력하여 보안 문제를 해결하는 태도
자격사항	○ 정보처리기사, 정보보안기사, CISSP(국제공인정보시스템보안전문가), CISA(국제공인정보시스템감사사), ISMS-P 인증심사원 등
직업기초 능력	○ 의사소통능력, 수리능력, 자원관리능력, 문제해결능력, 조직이해능력, 기술능력
참고	○ 위 직무기술서는 한국산업인력공단의 표준 분류를 참고하여 KIST에서 자체 작성한 직무기술서로, 향후 NCS 개발동향 등 내·외부 사정에 따라 변경될 수 있음을 알려드립니다. ○ 참고사이트 : www.ncs.go.kr