NCS 기반 채용 직무기술서 (행정-2)

<table>
<tr><td>배치(예정)
본부 및 부서</td><td>기획본부
정보전산실</td><td>전략분야
R&R</td><td>상위역할
주요역할</td><td>-
-</td></tr>
<tr><td>채용분야</td><td colspan="4">정보보안</td></tr>
<tr><td rowspan="4">NCS
분류체계</td><td>대분류</td><td>중분류</td><td>소분류</td><td>세분류</td></tr>
<tr><td rowspan="3">20.정보통신</td><td rowspan="3">01.정보기술</td><td>02.정보기술개발</td><td>06.보안엔지니어링</td></tr>
<tr><td rowspan="2">06.정보보호</td><td>01.정보보호관리·운영</td></tr>
<tr><td>03.보안사고분석대응</td></tr>
<tr><td>연구원
주요사업</td><td colspan="4">○ 기계 관련 미래 원천 기술, 산업 핵심 기술 및 사회 난제 해결 기술의 연구개발,
기계류·부품 공인시험 및 신뢰성 향상 기준·기술 개발 보급, 중소·중견기업 기술 지원 및 육성</td></tr>
<tr><td>직무수행내용</td><td colspan="4">○ 연구원의 비전과 미션을 수행하기 위하여 정보 자산을 안정적으로 운영하는 데 필요한 정보보호 전략 및 정책을 수립하고, 관련 법제도 준수, 정보보호관리 활동을 수행하며, 위험관리에 기반한 정보보호 대책을 도출하고 실행하는 업무
○ 연구원 사이버공격 및 침해사고의 예방활동, 위협정보를 탐지/분석, 피해 현황 파악 및 복구 등 침해사고 대응절차를 수행하는 업무
○ 정보보호 및 개인정보보호 관련 법률/정책 등의 이해를 바탕으로 연구원 정보보호정책을 수립하고 네트워크/시스템에 적용/운용하는 업무
○ 연구보안평가, 정보보안 관리실태 평가 등 내/외부 감사 대응 업무</td></tr>
<tr><td>전형방법</td><td colspan="4">○ 1차 서류전형 → 2차 필기전형 → 3차 종합면접 → 신원조사·합격자발표·신체검사 → 임용</td></tr>
<tr><td rowspan="2">일반요건</td><td colspan="2">연령</td><td colspan="2">제한 없음</td></tr>
<tr><td colspan="2">성별</td><td colspan="2">제한 없음</td></tr>
<tr><td rowspan="2">교육요건</td><td colspan="2">학력</td><td colspan="2">제한 없음</td></tr>
<tr><td colspan="2">전공</td><td colspan="2">제한 없음</td></tr>
<tr><td>필요지식</td><td colspan="4">○ (정보보호관리·운영) 정보보안 및 개인정보보호 시스템(방화벽, IPS, 유해사이트차단시스템, 보조기억매체 관리시스템 등) 운영·관리, 통합정보시스템 보안 진단 및 취약점 진단/분석과 조치, 네트워크 보안시스템 운영·관리, 물리적/관리적 보안운영 정책/이행 관련 지식,국가망보안체계(N^2SF) 지식
○ (보안사고분석대응) 침입대응, 분석 실무에 필요한 정보수집 및 활용 방법, 침해사고 대응절차, 원인과 사고과정 분석에 관한 지식, 보안위협 이벤트/원리이론분석, 침해사고 관련 휘발성/비휘발성 증거 수집 방법, 네트워크와 시스템 취약점 관련 지식
○ (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</td></tr>
<tr><td>필요기술</td><td colspan="4">○ (정보보호관리·운영) 정보보호 관련 법 및 규정 분석 능력, 정책/표준/지침/절차의 분석 능력, 정보보호 정책 체계파악 능력, 정보자산의 구성과 현황 파악 기술, 국가망보안체계(N^2SF) 분석 능력
○ (보안사고분석대응) 침해사고 분석 시술(분석도구, 원인, 사고과정 분석 등), 네트워크시스템 로그/보안취약점/분석 도구 사용기술, 악성코드 행위분석 기술,, 후속조치 및 보고서 작성 기술
○ (보안엔지니어링) 시스템/네트워크 취약점분석 도구 사용기술, 로그분석 도구 사용 기술, 서버보안 소프트웨어 설치 및 운영기술, 보안 아키텍처 수립기술</td></tr>
<tr><td>직무수행태도</td><td colspan="4">○ 조직의 일원으로 구성원과 융화하며 상호 협력하려는 자세
○ 새로운 기술 지식을 탐구하려는 자세, 적극적인 업무 태도, 긍정적인 업무 태도
○ 원칙을 준수하고 청렴하며 공정한 업무 처리 태도
○ 상황을 종합적, 현실적으로 판단하는 통찰력 있는 자세</td></tr>
<tr><td>관련자격</td><td colspan="4">○ (우대) 정보보안기사, CISSP, CISA, CCIE, 개인정보관리사, 네트워크관리사, 정보처리기사, 전자계산기기사 등 정보기술 관련 자격증 소지자</td></tr>
<tr><td>직업기초능력</td><td colspan="4">○ 의사소통능력, 수리능력, 문제해결능력, 자기개발능력, 대인관계능력, 정보능력, 기술능력,
조직이해능력, 직업윤리</td></tr>
<tr><td>참고 사이트</td><td colspan="4">○ www.ncs.go.kr 참조</td></tr>
</table>

※ 직무기술서에 기술된 **교육요건(전공), 필요지식 및 필요기술은 별도로 표기되어 있지 않는 한 1개 항목 이상 해당 시 지원 가능**