

【NCS기반 직무 설명자료】

채용 분야	정보보안			
NCS 분류 체계	대분류	중분류	소분류	세분류
	20. 정보통신	01. 정보기술	02. 정보기술개발 06. 정보보호	06. 보안엔지니어링 01. 정보보호관리·운영 03. 보안사고분석대응
직무 수행 내용	<p>○ (직무개요) 발매전산·발매지원 시스템 운영 및 품질관리, IT 인프라 및 정보시스템 운영관리, 빅데이터 관리, 공공데이터 개방, 데이터 기반 행정지원, IT 아웃소싱 관리 등에 관한 업무</p> <p>○ (주요업무) 사이버 위협 및 침해사고 예방 대응관리, 국가 사이버 안전센터 공조체계 확립, 정보보안, 개인정보보호 관리체계 시행, 정보보안 및 개인정보보호시스템 도입, 구축, 운영, 유지관리, 정보화사업 보안성 검토 및 교육계획 수립, 정보보안 관리실태 점검, 정보보안 보안감사 수검 지원, 정보보안, 개인정보보호 점검 및 감사지원, 정보보안, 개인정보보호 관련 규정, 지침, 업무절차서, 제개정 및 관리, 개인정보영향평가 및 개인정보파일 관리</p> <p>○ (채용 후 배치 가능 직무) 정보화전략, 정보보안및보호</p>			
능력 단위	<p>(보안엔지니어링) 01.보안 구축 계획 수립 03.보안 구축 요구사항 분석 04.관리적 보안 구축 10.보안인증 관리 11.SW개발 보안 구축 12.DB보안 구축 13.시스템 보안 구축 14.NW보안 구축</p> <p>(정보보호관리운영) 03. 정보보호 정책 기획 05.보안 위험관리 08.네트워크 보안 운영 10.시스템 보안 운영 14.보안성 검토</p> <p>(보안사고분석대응) 05.보안사고 현황분석 09. 분석대응 체계수립 10.보안위협 대응 11.보안사고 사후처리</p>			
필요 지식	<ul style="list-style-type: none"> - 정보보안, 개인정보보호 법·제도 지침 - 정보시스템 취약점 동향, 개인정보 유출 사고 동향 - OWASP TOP 10, OWASP MOBILE 10 - 상급기관(국정원·농식품부,개인정보보호위원회) 정보보안 및 개인정보보호 정책 - 가명·익명정보 처리 - 침해사고 분석 및 대응 - 개인정보보호 법·제도 지침, 상급기관(개인정보보호위원회·농식품부) 개인정보보호 정책 			
필요 기술	<ul style="list-style-type: none"> - ISMS-P 인증제도 - 개인정보영향평가 - 정보보호기술(기술적 보안) - 정보기술(SW·서버·네트워크) 관련 이해 - 소프트웨어 개발보안 진단 - 웹 취약점 진단 능력 - 개인정보흐름도 작성 및 분석 			
필요 태도	<ul style="list-style-type: none"> - 객관적인 시각으로 보안 기능을 분류·분석하려는 사고 - 설계된 서버 보안을 준수하여 구현하려는 노력 및 객관적인 테스트와 적극적인 문제해결 태도 - 설계된 네트워크 보안을 준수하여 구현하려는 노력 - 정보보호 관련 법률 준수하려는 태도 - 취약점 발생환경의 분석환경을 구축하고 보안위협을 신속하게 분석·대응하는 자세 - 신규 보안취약점을 지속적으로 연구하는 노력 			
필요 자격	○ 자격제한 없음			
지식 능력	○ 의사소통능력, 문제해결능력, 조직이해능력, 자원관리능력, 정보능력, 수리능력, 직업윤리			
참고 사이트	○ 국가직무능력표준 www.ncs.go.kr 및 한국마사회 홈페이지 www.kra.co.kr			

※ 별첨: 직무수행요건

- 본 내용은 국가직무능력표준(NCS)과는 별도로 자체 개발하였으며,
해당 직무를 수행하기 위해 필요한 한국마사회만의 요구 역량 및 수준에 대한 세부 사항입니다.

직무역량	No.	역량	등급	요구 수준
직무 공통역량	1	설득력 및 협상력 : 이해관계자와 자신에게 주어진 상황을 정확히 이해하여 자신의 주장을 합리적으로 설득하여 본인 혹은 양자가 이득이 될 수 있도록 최적의 합의를 도출해 낸다.	적용 단계	<ul style="list-style-type: none"> - 다른 사람들의 수준이나 관심사에 어필하기 위해 발표나 토론에 변화를 준다. - 자신에 대한 이미지나 행동의 효과를 예측한다. - 구체적인 영향력을 미치기 위해 심사숙고 하여 극적이거나 독특한 행동을 취한다. - 설득 과정에서 다른 사람들의 반응을 예측하고 대응방안을 준비한다. - 청중들의 관심사에 어필하기 위해 커뮤니케이션 전략이나 방법을 적용한다.
			최소 단계	<ul style="list-style-type: none"> - 토론이나 발표에서 직접적인 설득법을 사용한다. - 근거, 자료, 다른 사람들의 개인적 관심사에 어필하여 설득한다. - 구체적인 예, 시각적 자료 등을 사용하여 설득한다. - 청중의 수준과 관심사를 발표에 반영하려는 명백한 시도를 하지 않는다
	2	의사소통 : 상대의 기대나 의도를 명확히 이해하고 자신의 의사를 명확하고 간결하게 표현,전달,이해시키며, 타 부서와의 원활한 의사소통을 위해 노력한다.	적용 단계	<ul style="list-style-type: none"> - 의사소통의 목적에 따라 적절한 정보와 사실을 제시하고 추후 의사결정에 활용한다. - 다양한 정보를 효과적으로 문서화 혹은 구두로 표현한다. - 다양한 의사소통 채널을 파악하고 있으며, 상황에 따라 적절히 활용한다. - 설득/협상 시 효과적인 의사소통을 위해 내용과 관련된 사실, 입장 및 정황 등 관련 정보를 파악하여 타인의 이해와 공감대를 형성한다.
			최소 단계	<ul style="list-style-type: none"> - 상대방이 하는 말을 경청하고 상대가 의도하는 바와 기대 수준을 정확히 파악한다. - 상대방에게 전달하려는 내용을 뒷받침할 수 있는 근거를 제시할 수 있다. - 서류나 보고서를 원래의 작성 방식에 맞추어 적절히 작성한다. - 팀원들과 일하는데 있어 원활한 사적, 비공식적 의사소통 수준을 보인다.
	3	관계형성 : 업무에서 만나는 내외부 사람들과 친밀한 관계를 유지하고 정보 습득을 위해 노력한다.	적용 단계	<ul style="list-style-type: none"> - 다른 사람들과의 관계를 개선하거나 강화시키기 위해 모임 등을 열거나 참석한다. - 인맥을 넓히기 위해 폭넓은 사회적 활동(동아리, 클럽, 연구회, 등)에 참여한다. - 조직 내외부 인맥을 통해 업무와 관련된 정보를 습득한다.
			최소 단계	<ul style="list-style-type: none"> - 다른 사람들과 업무에서 만나는 사람들과 친구나 지인으로서의 관계를 형성하고 유지한다. - 동료, 고객들과 식당, 클럽, 스포츠 등의 활동을 통해 친밀한 관계를 추구한다.

직무역량	No.	역량	등급	요구 수준
직무 전문역량	1	보안 및 개인정보 사고 대응	적용 단계	사고 대책을 마련하고 관련조치를 수행하고 재발방지 대책을 수립할 수 있으며 정보보안 및 개인정보 유·노출사고 발생 시 ICT 기술을 기반으로 사고 원인을 분석할 수 있다.
			최소 단계	정보보안 및 개인정보 유·노출사고 발생을 감지하고 신고절차를 능숙하게 수행할 수 있다.
	2	관리적, 물리적, 기술적 보안	적용 단계	관리적, 물리적, 기술적 정보보호 목표를 설정하고 보안 대책과 자원 계획을 수립할 수 있다.
			최소 단계	서비스, 업무, 조직, 정보시스템, 설비를 파악하고 보안 관련 문제점의 분석과 개선방안을 제시할 수 있다.
	3	보안성 검토	적용 단계	도출된 보안 대책 요구사항에 따라서 보안대책서를 작성할 수 있으며 자체 보안성 검토 기준을 수립하고 검토 대상 사업의 사업계획서를 분석할 수 있다.
			최소 단계	법령 및 보안성 검토 관련 규정에 의거하여 필요한 보안 요구사항을 도출할 수 있다.
	4	개인정보 보호조치 이행	적용 단계	개인정보 생명주기별 관리방은 수립과 기술적/관리적/물리적 보호조치를 수립할 수 있으며 개인정보/조직/정보자산 등 보호 대상을 식별할 수 있다.
			최소 단계	개인정보보호 관련 국내외 법령, 정책 등의 분석 하여 우리 회에 적용되는 항목을 식별할 수 있다.
	5	개인정보영향평가 및 개인정보 파일 관리	적용 단계	개인정보 영향평가 개선조치 이행점검하고 개인정보파일을 갱신할 수 있으며, 개인정보영향평가 수행계획을 수립하고 팀 구성 및 운영계획서를 작성할 수 있다.
			최소 단계	개인정보영향 평가 대상을 식별하고 개인정보파일을 관리할 수 있다.