국가과학기술연구회 NAIS 연구직 채용 직무기술서

<table>
<tr><td>채용직종</td><td>연구직-3 플랫폼</td><td>채용인원</td><td>2명</td></tr>
<tr><td>모집 분야</td><td colspan="3">AI 보안 아키텍처· AI 시스템 보안</td></tr>
<tr><td>수행업무</td><td colspan="3">국가 망 보안체계(N2SF) 기반 과학 AI 서비스 보안 아키텍처를 연구·설계 및 보안성 검토
AI 모델·에이전트 고유 위협에 대한 레드팀·안전 평가·방어 기법 연구</td></tr>
<tr><td>대분류</td><td>중분류</td><td>소분류</td><td>세분류</td></tr>
<tr><td colspan="4">NCS 미개발분야로 자체 직무분석을 통해 도출한 내용임</td></tr>
<tr><td>기관소개</td><td colspan="3">「국가과학AI연구센터」는 국가과학기술연구회 내부조직으로 과학기술 분야의 인공지능 활용 촉진 및 인공지능 기반 연구기관 간의 협업 생태계 조성을 위한 연구개발·지원 역할을 수행함</td></tr>
<tr><td>전형절차</td><td colspan="3">서류전형 → 전공면접(인성검사 포함) → 종합면접 → 임용</td></tr>
<tr><td>직무수행 내용</td><td colspan="3">· 과학 AI-OS·LLM API·AI 포털의 N2SF 정보 등급(C/S/O) 기반 보안 아키텍처 설계 및 보안성 검토 대응(위협 식별·보안통제 항목 매핑·증빙), 민감(S) 등급 확장 요건 설계
· AI·LLM 고유 위협(프롬프트 주입·데이터 유출·모델 탈취·에이전트 도구 오남용)의 위협 모델 연구와 통제 설계(실행 격리·권한 최소화·아웃바운드 차단·감사 기록) 및 AI-OS·하네스 설계 반영
· AI 서비스·에이전트 레드팀 방법론 개발과 정기 평가 수행, 취약점 발견·보고·조치 확인 체계 운영
· AI 안전·신뢰성 평가 기준(견고성·오남용 저항성) 설계, 마켓플레이스 등록 에이전트·도구의 보안 점검 기준 수립, 자율 연구 수행의 위험·이중용도 검토 기준 수립(도메인 전문가 검토 연계)
· 클라우드(CSAP)·슈퍼컴 연계 환경 보안 정책 수립, 이용 기관·검토 기관과의 보안 협의, AI 보안·안전 규범 동향 분석 및 보안 지침·교육 발간</td></tr>
<tr><td rowspan="2">채용예정직급</td><td colspan="3">원 또는 선임*</td></tr>
<tr><td colspan="3">*[선임연구원 임용자격]
· 대학이상의 과정을 이수한 자로서 국가기관 또는 연구기관에서 7년이상**의 연구경력을 가진 자
· 박사학위 소지자로서 국가기관, 대학 또는 연구기관에서 3년이상**의 연구경력을 가진자
· 상기 각 요건과 동등한 자격이 있다고 인정되는 자
** 직급결정 시 경력기간은 내부 경력산정기준에 따름</td></tr>
<tr><td>근무지</td><td colspan="3">대전광역시 또는 업무에 필요한 장소(세종 등)</td></tr>
<tr><td rowspan="2">일반요건</td><td>연령, 성별</td><td colspan="2">· 연령 및 성별 무관</td></tr>
<tr><td>기타</td><td colspan="2">· 「국가공무원법」제33조에 따른 결격사유가 없는 자
· 「병역법」제76조에 따른 병역의무 불이행자에 해당하지 않는 자
· 채용 신체검사 기준에 적합한 자
· 국가연구개발사업 참여 제한이 없는 자
· 연구회 및 출연연 또는 타 공공기관에서 최근 5년 이내 부정한 방법으로 채용된 사실이 적발되어 채용이 취소된 사실이 없는 자
· 「부패방지 및 국민권익위원회의 설치와 운영에 관한 법률」제82조에 따른 취업제한 대상에 해당하지 않는 자
· 임용시기에 근무가 가능한 자
· 대한민국 국적 소지자
· 병역의무 대상자(남성)는 군필자(전역 예정 군인 포함), 면제자</td></tr>
</table>

교육요건	학력	· 석사 이상 학위 소지자 [기졸업자 및 2027년 2월 졸업예정자 포함] ※ 최종 임용되더라도 2027년 2월말까지 학위 취득이 불가한 경우 임용 취소
	관련 전공	정보보호, 컴퓨터공학, AI 및 보안 관련 전공 (보안 아키텍처·보안성 검토 또는 AI 보안·안전 연구실적·실무경력)
필요지식	· 국가 망 보안체계(N2SF) 가이드라인·정보 등급 분류·보안통제 항목과 보안성 검토 절차에 관한 지식 · 클라우드 보안(CSAP)·제로트러스트·네트워크 분리·암호화(KCMVP)에 관한 지식 · 대규모 언어모델·에이전트 시스템의 공격 표면과 위협 유형, 적대적 공격·방어 및 레드팀 방법론에 관한 지식 · 실행 격리·샌드박스·권한 최소화 등 시스템 보안 원리와 보안 아키텍처 설계·위협 모델링 방법론에 관한 지식 · AI 안전·신뢰성 평가 지표, 국내외 AI 보안·안전 규범·표준과 개인정보·연구데이터 보호 법규에 관한 지식	
필요기술	· 보안 아키텍처 설계·위협 모델링 및 보안성 검토 문서(위협 식별·통제 매핑) 작성 기술 · 컨테이너·Kubernetes 환경 보안(정책·격리·이미지 검증)과 에이전트 실행 격리·권한 통제·감사 기록 설계·검증 기술 · AI 서비스·에이전트 레드팀 설계·수행, 적대적 입력·탈옥·데이터 유출 시나리오 구성과 자동화 평가 도구 개발 기술 · 안전·신뢰성 평가 기준 설계와 실험·통계 분석 기술 · 이용 기관·검토 기관과의 보안 요건 협의·증빙 작성 및 연구 논문·기술 보고서·보안 지침 작성 기술	
권장사항	· 공공기관 정보보안·보안성 검토 대응 실무 또는 보안 아키텍처 연구 실적 · AI·LLM 보안 또는 안전 연구 실적(논문·공개 도구·취약점 보고) · 레드팀·모의해킹·취약점 진단 수행 또는 클라우드·AI 서비스 보안 설계 경험 · 정보보호 관련 자격(정보보안기사·CISSP 등) 또는 관련 학위	
직무수행 태도	· 창의적이고 도전적인 연구자세, 객관적인 판단 및 논리적 분석태도 · 투명하고 공정한 업무수행의 청렴성, 문제해결을 위한 적극적 의지 · 조직의 일원으로 구성원과 융화하며 상호 협력하는 자세 · AI 기반 연구환경 변화에 유연하게 적응하고 지속적으로 학습하는 자세	
직업기초 능력	연구직의 경우 필기시험 미전형에 따라 별도의 직업기초능력평가 없음	
참고사이트	· https://nst.re.kr (국가과학기술연구회 홈페이지) · https://nst.fairy.im (국가과학기술연구회 지원서 접수 사이트)	