연구자를 위한
연구보안 현장 매뉴얼

RESEARCH SECURITY FIELD MANUAL

과학기술정보통신부

KISTEP 한국과학기술기획평가원
Korea Institute of S&T Evaluation and Planning

CONTENTS

- 연구자를 위한 연구보안 현장매뉴얼 사용설명서 ····· i
- 연구보안 Q&A ····· ii
- **일반과제 |** 연구자의 기본 연구보안 준수사항 ····· iii
- **보안과제 |** 연구자가 지켜야 하는 보안 법규정 준수사항 ····· iv
- 연구자를 위한 연구보안 CHECK LIST ····· vi

PART 1 연구보안 기본원칙

제1장 국가R&D 참여연구자의 연구보안

제1절 | 국가R&D 참여연구원의 일상 속 연구보안 규칙은 무엇인가요? ·· 3

1. IT 및 정보기기 사용 ····· 3
2. 원격·재택근무 및 영상회의 ····· 6
3. 해외 출장 ····· 9
4. 연구보안 인식제고 및 교육 ····· 12

제2절 | 국가R&D 연구산출물 및 성과를 어떻게 관리해야 하나요? ···· 14

1. 문서·연구노트·데이터 관리 ····· 14
2. 논문발표·특허출원·보고서 공개 ····· 18
3. 회의 참석, 학술발표로 인한 연구내용 대외공개 ····· 22

제2장 보안과제 참여연구자의 연구보안

제1절 | 보안과제 참여 시 주의가 필요한 연구보안 규칙은 무엇인가요? ·· 23

1. 보안과제 연구자의 보안교육 및 보안서약 ····· 23
2. 보안과제 연구자의 외국접촉 ····· 25
3. 보안과제 연구자의 IT 및 정보기기 사용 ····· 31
4. 보안과제 연구자의 보호지역 출입 관리 및 시설장비 사용 ····· 36

제2절 | 보안과제 연구산출물 및 성과를 어떻게 관리해야 하나요? ····· 39

1. 보안과제 창출 문서·데이터·연구노트 보안등급 구분 ····· 39
2. 보안과제 연구개발성과 외부공개 ····· 42

PART 2 주요 상황 별 연구보안 원칙

제3장
국제공동연구 추진 시 연구보안

◆◆◆
제1절 | 외국인 연구원과 일하게 되었어요! ····· 47
1. 외국인 연구원의 연구부서 배정 ····· 47
2. 일반과제에 외국인 연구원 참여 ····· 50
3. 보안과제에 외국인 연구원 참여 ····· 52
4. 보안과제 수행 연구실에 외국인이 상주하는 경우 ····· 57

제2절 | 국가R&D 국제공동연구 추진 시 지켜야 하는 것이 무엇인가요? 59
1. 협약·계약 시 연구보안 ····· 59
2. 보안과제에 외국기관 참여 ····· 64

제3절 | 안전한 국제협력을 추구하고 싶어요! ····· 67
1. 국외수혜정보 보고 추진 원칙 및 방법 ····· 67
2. 개인 국제협력 및 해외 기관 진출 ····· 71
3. 보안과제 수행 연구자의 외국과제 수행 ····· 76

제4장
기술사업화 단계의 연구보안

◆◆◆
제1절 | 기술이전 및 창업을 하려 해요! ····· 79
1. 기술이전, 양도, 해외수출 시 주의사항 ····· 79
2. 실험실 창업 ····· 82

제2절 | 품목화 된 기술보호를 위해 어떻게 해야 되나요? ····· 85
1. 산업보안·국방보안 판정절차 및 주의사항 ····· 85
2. 기술임치를 통한 지식재산 보호 ····· 90

제5장
연구보안 사고 대응

◆◆◆
제1절 | 연구보안 사고가 발생하고 말았어요! ····· 92
1. 연구보안 사고 대응절차 및 연구자 행동 ····· 92

제2절 | 연구보안 규정 위반 이후 어떻게 되나요? ····· 96
1. 연구보안 규정 위반 시 처분 ····· 96
2. 연구보안 위반행위에 대한 가중처벌 및 감경 요인 ····· 99

연구자를 위한 연구보안 현장매뉴얼 사용설명서

- 이 매뉴얼은 국가R&D 추진 시 연구자가 준수해야 하는 '연구보안 기본원칙(Part1)'과 '주요 상황 별 연구보안 원칙(Part2)'로 구성되어 있습니다.

- 일반과제 연구자는 '1장', 보안과제 연구자의 경우 '1~2장'을 검토하시며 '연구보안 기본원칙(Part1)'을 파악해 보세요.

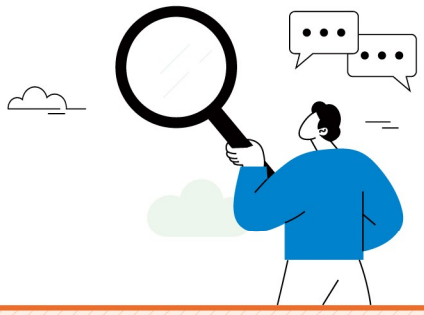
- 목차 별 '연구자를 위한 연구보안 Check List(vi쪽)'를 먼저 살펴보시면 전반적인 흐름을 확인하실 수 있습니다.

- 상기 '체크리스트'에 관련 법이 기재된 부분, 본문에 [법]이라고 표시된 내용은 연구자가 꼭 준수하셔야 하는 내용입니다. 해당 내용 관련해서는 소속기관 연구보안 담당부서와 상담하세요.

- 소속기관 연구보안 담당부서가 없다면 연구관리자·전문기관 담당자에게 문의하여 주세요. 해결하기 어려운 질의는 IRIS 신문고에 문의하세요.

- 연구보안은 과학·기술적 판단이 결부되는 만큼, 연구자 본인의 진실성이 가장 중요합니다. 체크리스트를 살펴보시며 연구자 스스로 판단하고 실천해 보세요.

- 연구보안은 연구자가 소속기관 및 연구 커뮤니티에 투명하게 정보를 공개하는 것으로부터 시작될 수 있음을 기억하세요!



연구보안 Q&A

연구보안이 무엇인가요?

- 연구보안은 국가R&D 과정 중 창출된 '연구자산'을 불법적인 기술유출 등 각종 위험으로부터 보호하면서 개방적 협력 관점에서 연구성과 확산을 촉진할 수 있는 관리체계 및 조치를 말합니다.
- 연구보안은 연구기관·연구자가 연구보안 절차(법규정)를 준수하고 '연구진실성'의 가치를 따르는 것으로 확립해 나갈 수 있습니다.

연구보안은 왜 갑자기 부상하게 되었나요?

- 안보 개념이 '군사'에서 '경제·기술'로 확장되며 해외 국가 간 연구자산을 탈취하는 사례가 증가하고 있으며 이에 따라 우리나라도 국가R&D 연구자산 보호를 강화해야 하는 시점입니다.
- 해외 주요 국가는 국제공동연구 파트너 선정 시, 상대 국가의 연구보안 수준을 중요한 평가 기준으로 삼고 있습니다. 국제적으로 우리나라가 신뢰받는 파트너로 거듭나기 위해 연구보안 체계를 국제 수준에 맞춰 강화해야 합니다.

연구보안의 범위는 어디인가요?

- R&D 전주기 상 연구자산 유출을 예방하기 위한 '과제 및 성과관리, 연구원 관리, 시설·정보통신 등'을 포괄합니다.

산업보안과 다른 점이 있나요?

- 연구보안은 '과제 전주기 상' '연구자, 연구자의 아이디어 및 연구성과물'을 지키고자 하는 '예방' 위주 접근방법을 취하고 있습니다.
- 산업보안은 '기술상업화 단계'의 '산업기술'에 중점을 두고 있으며 '처벌' 위주의 접근 방법을 택하고 있습니다.

보안과제 연구자만 연구보안을 지키면 되나요?

- 일반과제 연구자도 '연구자 자신과 연구자의 지식재산, 연구 커뮤니티'를 보호하기 위해 연구보안 절차(법규정)를 준수해야 합니다.

연구자산 보호와 지속적 국제협력을 위한
일반과제 연구자의 기본 연구보안 준수사항

	연구기획단계	연구수행단계	성과공개 및 활용단계
과제관리 및 연구원관리	국제공동R&D 협약 시 주의	국외수혜정보 보고 해외파견/출장 시 주의	
문서 및 성과관리		논문발간, 특허출원, 발표 시 영업비밀, 보안성 검토 산출물 보안등급 설정 및 관리	기술이전/창업 시 유출주의
IT 및 시설관리	업무용 IT 기기 보안관리, 기관인증 클라우드 사용, 온라인 회의 시 보안, 생성형 AI사용주의		

구분	상세내용	Page
국제공동R&D	• 국제공동R&D 협약 시, 소속기관 담당자와 IP보호·활용, 보안대책 수립 등에 대해 상의합니다.	59
국외수혜정보 보고	• 국가R&D 연구책임자는 과제 시작 전 또는 수행 중 외국 정부·기관·단체로부터 재정적·행정적 수혜 사항을 '연구개발계획서 또는 IRIS 연구자정보 시스템'에 투명하게 보고합니다.	67
해외출장	• 해외 출장 전후 소속기관에 출장 내용을 보고합니다. • 출장 전 IT 기기에 암호화하고 중요정보를 백업해 둡니다. • 해외출장 시 발표자료가 '보안과제·전략물자·국가핵심기술 또는 소속기관의 영업비밀'과 관련성이 있지 않은지 전문기관 담당자, 기관의 연구보안 담당부서와 상의 합니다.	9
해외파견	• 해외 기관에서 안내하는 정보접근 권한, 정보공개 요구사항, 수출통제 등에 관한 보안요건을 상세히 검토하고 준수합니다.	71
연구데이터·자료관리	• 필요 시 연구책임자는 연구보안 담당자와 논의하여 문서·연구데이터·연구노트에 대한 보안등급을 설정하고 보안관리를 차등화 합니다.	14
성과공개	• 국가R&D 연구보고서 및 데이터는 원칙적으로 공개해야 하나 일부 경우에 한해 비공개가 가능합니다. 비공개를 원할 경우 전문기관 담당자와 논의합니다.	18, 22
성과실시	• 기술이전 및 실험실 창업 시, 소속기관 담당자와 '보안대책 수립, 기술이전 범위, 비밀유지조약 체결 여부' 등에 대해 논의합니다.	79, 82
IT기기·정보통신	• 소속기관 방침에 따라 업무용 IT기기의 보안관리를 추진합니다. • 기관에서 공식적으로 인정한 클라우드만 사용합니다. • 온라인 회의 추진 시, 주소 암호화·접근제한 등 조치를 취합니다. • 생성형 AI 사용 시 민감한 정보를 입력하지 않도록 주의합니다.	3, 6

국가안보를 위해
보안과제 연구자가 지켜야 하는 보안 법규정 준수사항

※ 보안과제 수행 연구자 중심 확인사항 입니다. 해당 연구자는 일반과제 수준 권고사항 뿐 아니라 관계법령을 준수해야만 합니다 (회색: 일반과제, 분홍색: 보안과제).

	연구기획단계	연구수행단계	성과공개 및 활용단계
과제관리 및 연구원관리		국외수혜정보 보고	
	국제공동R&D 협약 시 주의		
		해외파견/출장 시 주의	
	외국과제 수행 전 승인		
	외국인/외국기관 참여 승인		
		외국 접촉 및 정보교환 주의	
		보안서약 및 교육	
문서 및 성과관리		논문발간, 특허출원, 발표 시 영업비밀, 보안성 검토	
		산출물 보안등급 설정 및 관리	
			기술이전/수출 시 승인
IT 및 시설관리	업무용 IT 기기 보안관리, 기관인증 클라우드 사용, 온라인 회의 시 보안, 생성형 AI사용주의		
	보호지역 설정, 출입권한 차등화 및 기록관리		

구분	상세내용	Page
외국지원연구	• 보안과제 연구자는 외국 수탁과제 추진 시 소속 기관에 승인을 요청해야 합니다.	76
외국기관 연구참여	• 보안과제에 외국기관 참여 시 소속 기관에 승인을 요청해야 합니다.	64
외국인참여	• 보안과제에 외국인 참여 시 소속 기관에 승인을 요청해야 합니다.	52
외국과 정보교류 (외국접촉)	• 보안과제 관련 사항에 대해 외국인과 유의미하고 지속적인 대화를 나누었다면 소속기관에 보고해야 합니다. • 국가핵심기술·전략물자·방위산업기술 등에 해당 시 외국인과 과제 관련 정보 교류가 위법 행위가 될 수 있으므로 주의해야 합니다.	25
보안서약/교육	• 필수적으로 보안교육을 수강하시고 보안서약서를 제출하셔야 합니다.	23

구분	상세내용	Page
연구데이터·자료관리	• 연구책임자 및 연구보안 담당자는 기관의 보안대책에 따라 보안과제 산출물의 보안등급을 지정합니다. • 보안등급에 따른 차등화 된 보안관리가 이뤄질 수 있도록 합니다 .	39
성과공개	• 보안과제의 경우 성과 비공개 요청이 가능합니다. 만약 국가핵심기술, 방위산업기술에 해당한다면 성과 공개 시 별도 승인이 필요하므로 연구보안·국가핵심기술관리책임자·전문기관담당자와 상의하셔야 합니다.	42
성과실시	• 국가보안이 필요한 기술의 경우, 기술이전·수출 시 관계 장관 사전 승인, 보안특약이 필요한 경우가 많습니다. 관련하여 기술이전담당자·보안담당자·전문기관 담당자와 상의하세요.	79, 82, 85
IT기기·정보통신	• 보안과제의 경우, 메신저·인터넷·클라우드 사용 및 전자자료 반출에 제한 받으므로 이를 염두에 두어야 합니다. • 생성형 AI 사용 시 민감한 정보의 입력은 금지됩니다. 소속기관의 보안 방침을 꼭 확인하세요.	31
보호지역 지정	• 보안과제 관련 보호지역 설정에 따른 출입권한 차등화·기록관리 등을 추진해야 합니다.	36
유출 및 위반행위	• 연구자는 보안과제·전략물자·방위산업기술·국가핵심기술 관련 규정을 숙지하고 위반하지 않아야 합니다. • 반드시 사전에 연구보안 교육을 받으시길 바랍니다.	85

연구자를 위한 연구보안 CHECK LIST

※ 법: 혁신법, 영: 혁신법 시행령, 대책: 보안대책(고시), 권고: 권고사항
※ 아래 내용 중 NO에 체크되는 항목이 있다면 소속기관 및 전문기관과 상담이 필요합니다.
※ [보안]으로 표시된 부분은 보안과제 관련 부분이 포함되어 있으니 유의하세요.

PART 1 | 연구보안 기본원칙

제1장. 국가R&D 참여연구자의 연구보안

제1절 | 국가R&D 참여 시 지켜야 할 일상적 연구보안 규칙은 무엇인가요?

주제	체크리스트	관련법	본문 (Page)
❶ IT 및 정보기기 사용	업무용 컴퓨터의 비밀번호를 주기적으로 변경하고 있나요?	권고	3
	업무용 컴퓨터 대상 보안 SW, 보안패치 등을 설치하고 업데이트 등의 관리를 추진하고 있나요?	권고	3
	타인의 주민등록번호가 포함된 데이터를 연구기관 방침에 따라 주기적으로 삭제하고 계신가요?	개인정보보호법 제24조의2	3
	업무용 장비, 정보통신매체 등을 소속 기관의 방침에 따라 안전 폐기해야 한다는 것을 알고 계신가요?	권고	3
	연구실 내 공용 PC 보안관리 담당자가 지정되어 있나요?	권고	3
	민감정보를 다룰 때 소속기관으로부터 보안성을 인정받은 클라우드를 사용하고 계신가요?	권고	3
	스팸메일로 의심되는 메일을 받았을 때, '스팸신고'를 추진하고 계신가요?	권고	3
	비공개 정보, 개인정보를 생성형 AI에 입력하지 않도록 주의하고 있나요?	권고	4
	생성형 AI 로그인 계정에 강력한 비밀번호를 설정하였나요?	권고	4
	생성형 AI 생성물 활용 시 지적재산권, 저작권 침해 여부 등을 검토하였나요(출처 검토)?	권고	4
	생성형 AI 관련 연계, 확장 프로그램 사용 시 보안 취약여부 등을 소속기관 담당자에게 문의 하였나요?	권고	4
❷ 원격근무 및 영상회의	연구부서장께서는 원격·재택근무 관련 부서원의 원격근무 관리대장을 관리하고 계신가요?	권고	6
	보안성이 확보된 장소에서 원격·재택근무를 실시하고 계신가요?	권고	6
	원격·재택근무 시 기관에서 제공된 단말기를 사용하여 사내망에 접속하고 계신가요?	권고	6
	원격·재택근무 시 보안성이 확보된 인터넷망을 사용하고 계신가요?	권고	6

주제	체크리스트	관련법	본문 (Page)
	⊘ 허가된 영상회의 접속자에게만 주소를 공개하거나 비밀번호를 설정 하였나요?	권고	6
	⊘ 영상회의 참가자들 간 파일공유 비활성화 작업으로 악성파일이 전송되지 않도록 설정하였나요?	권고	6
	⊘ 영상회의 전 참가자에게 녹화, 캡처 행위 금지에 대해 안내 하였나요?	권고	6
❸ 해외출장	⊘ 해외 출장 국가에서 위급 시 도움을 청할 수 있는 대사관, 경찰서, 지인 등 정보를 사전에 확보 하셨나요?	권고	9
	⊘ 업무용 노트북, 전산장비에 비밀번호를 설정하셨나요?	권고	9
	⊘ 업무용 노트북, 전산장비 내 데이터를 암호화 하셨나요?	권고	9
	⊘ 업무용 노트북, 전산장비를 분실하지 않기 위해 어떠한 노력을 할 예정 이신가요?	권고	9
	⊘ 기관의 렌탈 노트북을 활용하는 것을 검토해 보셨나요?	권고	9
	⊘ 소속기관에서 제공하는 해외출장 교육내용을 확인 하셨나요?	권고	9
	⊘ 해외출장 전 기관의 사전 승인을 받으셨나요?	권고	9
	⊘ 해외 출장 발표 자료 관련 보안성, 상업적 활용 가능성을 검토해 보셨나요?	권고	9, 22
	⊘ 해외 출장 중 여행사, 호텔 관계자 등 외부인에게 출장과 관련된 정보 노출을 최소화하고 있나요?	권고	10
	⊘ 연구자 신원이 특정되지 않도록, 사원증 및 소속기관 로고 등의 노출을 최소화 하였나요?	권고	10
	⊘ 보안을 요구하는 중요한 자료 취급 시 호텔이나 학회 측에서 제공하는 전산장비 및 공용 WI-FI 등의 이용을 자제하고 있나요?	권고	10
	⊘ 연구기관 방침에 따른 해외출장 보고를 추진하였나요?	권고	10
	⊘ 귀국 후 가능한 빠른 시일 내에 전산장비의 패스워드를 변경 하였나요?	권고	10
	⊘ 출장에서 돌아온 뒤 연구기관의 정보보안부서에 의뢰하여, 소지한 전산 장비에 악성프로그램이 설치 되었는지 점검하였나요?	권고	10
❹ 연구보안 인식제고 및 교육	⊘ 소속기관 연구보안 담당자가 누구인지 알고 계신가요? (또는 연구관리 담당자)	권고	12
	⊘ 소속기관의 연구보안 규정명을 알고 계신가요?	권고	12
	⊘ 연구부서 구성원들은 연구보안 소양 함양을 위한 교육을 수강하고 있나요?	권고	12

제2절 | 국가R&D 연구산출물 및 성과를 어떻게 관리해야 하나요?

주제	체크리스트	관련법	본문 (Page)
❶ 문서·데이터·연구노트 관리	✓ '대외비 여부, 영업비밀 보호 필요성'에 따른 문서 등급화를 고려해 보셨나요?	영업비밀보호법 제2조의2	14
	✓ '대외비, 영업비밀' 등에 대한 구분을 문서에 명확하게 표기 하였나요?	영업비밀보호법 제2조의2	14
	✓ 문서 등급에 따른 접근자, 외부 공개 범위를 설정 하였나요?	권고	14
	✓ 문서 등급에 따라 구체적 관리방법(보관방법, 보존기한 설정, 활용 기록 관리, 폐기 등)을 설정 하였나요?	권고	14
❷ 논문발표·출원·보고서 공개	✓ 특허출원을 고려하여 논문발표 시점을 설정 하였나요?	권고	18
	✓ 과제종료 후 3개월 이내에 최종보고서 및 연구개발성과 목록을 공개해야 함을 알고 계신가요?	영제35조 제1항	18
	✓ 보안유지 및 상업적 활용 가능성에 따라 최종보고서와 연구개발성과 목록에 대한 비공개 또는 부분공개를 검토해 보셨나요?	영제35조 제2항	18
❸ 회의 참석·학술발표로 인한 연구내용 대외공개	✓ 대외공개 예정인 자료에 보안과제, 국가핵심기술, 전략물자, 방위산업 관련 내용이 포함되어 있지 않은지 확인해 보셨나요?	대외무역법 제2조, 산업기술보호법 제2조, 방위산업보호법 제2조	22
	✓ 대외공개 시 지식재산권 확보에 문제가 있을지, 또는 기술상용화를 앞두고 있어 보호가 필요하지 않을지 검토해 보셨나요?	권고	22
	✓ 그 외 대외공개 시 소속기관에 불리한 내용이 있지 않은 지 검토해 보셨나요?	권고	22

PART 1 | 연구보안 기본원칙 - 보안과제 연구자

제2장 보안과제 참여연구자의 연구보안

제1절 | 보안과제 참여 시 주의가 필요한 연구보안 규칙은 무엇인가요?

※ 보안과제 수행 연구자는 일반과제 수행 연구자 대상 체크리스트도 함께 준수 필요

주제	체크리스트	관련법	본문 (Page)
❶ 보안교육 및 보안서약	**[보안]** 연구보안 교육을 수강하셨나요?	영제46조제3호 대책제7조제1항	23
	[보안] 연구보안서약서를 제출하셨나요?	대책제7조제2항	23
❷ 외국접촉	**[보안]** 보안과제를 수행 중이거나 수행 후 3년 이내인 시점에서 외국인과 과제관련 유의미한 접촉이 발생할 시 이를 10일 내에 연구기관에 알려야 한다는 사실을 알고 계신가요?	대책제8조제1항	25
	국가핵심기술, 전략물자 등인 경우, 이메일, 전화, 자료전송 등 행위가 기술이전에 해당되어 산업부장관 사전승인이 필요하다는 사실을 알고 계셨나요?	대외무역법 영제32조의3, 산업기술보호법 제11조, 산업기술보호지침 제17조 등	29
	[보안] 해외 출장 시 기관으로부터 보안 유의 사항을 안내 받으셨나요?	대책제4조 (별표)	26
	[보안] 해외 출장 시 발표자료의 보안성을 검토 하셨나요?		
	[보안] 해외 출장에서 복귀하였을 시 외국접촉을 포함한 귀국보고를 하셨나요?		
❸ IT 및 정보기기 사용	**[보안]** 업무용 정보기기에 대한 계정 및 비밀번호 관리를 꾸준히 하고 계신가요?	대책제4조 (별표)	31
	[보안] 업무용 정보기기에 대한 지속적인 보안SW 업데이트를 하고 계신가요?		
	[보안] 보안과제 관련 시설에 정보기기, 매체 반입 시 사전 승인을 받으셨나요?		
	[보안] USB, 정보통신망을 이용한 정보 반출 시 사전 승인을 받으셨으며 정보 관련 데이터를 반출 시 암호화 하였나요?		
	[보안] 불용 장비, 정보통신매체, 등의 안전 폐기에 대한 계획이 수립되어 있나요?		
	원격/재택근무 시 비밀 및 대외비 해당 정보·자료의 생산 및 처리를 지양해야 함을 알고 계신가요?	권고	32
	연구부서장은 원격/재택근무 관련 부서원의 원격근무 관리대장을 관리하고 계신가요?		
❹ 보호지역 출입관리 및 시설장비 사용	**[보안]** 보안과제 관련 보호지역을 설정하셨나요?	대책제4조 (별표)	36
	[보안] 보호지역에 대한 출입기록을 관리하고 있나요?	대책제4조 (별표)	36
	[보안] 보안과제 시설장비의 사용기록을 관리하고 있나요?		

제2절 | 보안과제 연구산출물 및 성과를 어떻게 관리해야 하나요?

주제	체크리스트	관련법	본문 (Page)
❶ 문서·데이터·연구노트 보안등급 표기와 관리	**[보안]** 보안과제 연구과정 중 창출된 '문서(연구노트·데이터 포함)'의 '보안등급' 기준을 수립하였나요?	대책제10조	39
	[보안] 보안등급 설정 시, 과대 또는 과소 분류를 지양하여 문서 별 독립적인 분류를 추진해야 한다는 사실을 알고 계신가요?	권고	40
	[보안] 보안등급에 따른 문서, 관리, 활용 방침에 따른 문서관리를 추진하고 있나요?	권고	40
	[보안] 보안과제 종료 후 연구성과물의 보안등급 재조정에 대해 고려해 보았나요?	권고	40
❷ 보안과제 연구개발성과 외부공개	**[보안]** 보안과제 관련 최종연구보고서 및 데이터 비공개 절차를 파악하고 계신가요?	영제35조	42
	[보안] 보안과제 관련 연구개발성과 대외 공개 및 정보 외부 제공 시 기관의 확인을 받아야 함을 알고 계신가요?	대책제4조 (별표)	42
	[보안] 보안과제 관련 연구개발성과 대외 공개 및 정보 외부 제공 시 과제 관련 전문기관 담당자와 논의해 보셨나요?	권고	22, 42

PART 2 | 주요 상황 별 연구보안 원칙

제3장. 국제공동연구 추진 시 연구보안

제1절 | 외국인 연구원과 일하게 되었어요!

주제	체크리스트	관련법	본문 (Page)
❶ 외국인 연구원의 연구부서 배정	(채용) 연구부서장(또는 연구책임자)은 외국인 채용 과정에서 적절한 보안조치(보안서약, 보안교육, 신원확인 등)가 이루어졌는지 인사부서에 확인 요청 하셨나요?	권고	47
	(채용) 연구부서장은 외국인의 내부 인트라넷 정보 접근 제한 및 출입제한 구역 설정 등에 대해 관련 부서와 검토 하셨나요?	권고	47
	(채용) 연구부서장은 외국인 접근을 제한해야 하는 연구 문서가 무엇인지 검토하셨나요(보안과제, 국가핵심기술, 전략물자, 방위산업기술)?	대외무역법영 제32조의3, 산업기술보호 지침제17조, 방위산업기술 보호지침제23조	47
	(채용) 연구부서장은 외국인에게 '국가 R&D 성과의 소유권이 기관에 있음' 등 혁신법 기본사항에 대해 설명하셨나요?	권고	48
	(채용) 연구부서장은 외국인에게 연구개발성과 발표 전에 적절한 보안성 검토 및 연구기관의 내부절차 준수가 필요함을 안내하셨나요?	권고	48
	(퇴사/과제참여 종료) 연구부서장은 외국인으로부터 연구자료, 연구노트, 성과물을 회수 하셨나요?	권고	48
	(퇴사/과제참여 종료) 연구부서장은 연구보안 담당자와 함께 외국인으로부터 자료 반출 이력을 점검 하셨나요?	권고	48
	(퇴사/과제참여 종료) 연구부서장은 정보보안, 시설보안 담당자와 함께 연구기관 정보시스템, 시설장비, 보호시설 접근 권한 등을 차단 하였나요?	권고	48
	(퇴사/과제참여 종료) 연구부서장은 해당 외국인에게 보안서약서를 징구한 사실을 확인 하였나요?	권고	48
❷ 일반과제에 외국인 연구원 참여	참여연구원 모두가 연구보안교육을 이수하였나요?	권고	50
	'3-1-1. 외국인 연구원의 부서 배정'의 안내사항을 확인 하셨나요?	권고	50
	외국인의 타 실험실 출입 시도, 자료 무단반출 등 수상한 행동을 발견한 즉시, 연구보안 담당부서에 통보해야 함을 알고 계신가요?	권고	50

주제	체크리스트	관련법	본문 (Page)
❸ 보안과제에 외국인 연구원 참여	**[보안]** (참여 전) 보안과제 외국인 참여 시, 연구보안심의회의 심의·의결 및 기관장 승인이 필요함을 알고 계신가요?	영제46조제4호	52
	[보안] (참여 전) 보안과제에 외국인 참여가 정말 필요한 것인지 주변 연구자, 연구보안 담당부서, 전문기관과 논의해 보셨나요?	대책제9조제1항	52
	[보안] (참여 전) 보안과제 참여 외국인의 신상은 확실한지, 범죄이력은 없는지 인사부서와 다시 검토해 보셨나요?	권고	52
	[보안] (참여 전 및 수행 중) 보안과제 참여 예정인 외국인의 국외수혜 현황에 대해 확인 하셨나요?	권고	52
	[보안] (참여 전) 보안과제에 참여 예정인 외국인의 과제 수행 시 과제 참여 범위, 정보접근 권한을 제한할 수 있나요?	대책제9조제4항	52
	[보안] (참여 전) 보안과제 참여 외국인의 업무 활동과 시설 접근을 추적하고 기록할 계획과 방법이 있으신가요?	권고	52
	[보안] (참여 전) 보안과제 참여 외국인의 불법적인 본국 자료 반출을 막을 수 있는 체계가 소속기관에 존재하나요?	권고	52
	[보안] (참여 시작) 보안과제에 외국인 참여 시, 연구보안 담당부서에서 연구보안 교육을 시행하고 보안서약서를 징구하였는지 확인 하셨나요?	영제46조제3호, 대책제7조 제1항 및 제2항	53
	[보안] (참여 시작) 보안과제에 참여하는 외국인에게 보안과제 참여 연구원의 의무 및 규칙 전반에 대해 설명하였나요?	권고	53
	[보안] (과제수행 중) 과제 수행 과정 중 외국인의 제한된 연구범위가 지켜질 수 있도록 노력하고 있나요?	권고	54
	[보안] (과제수행 중) 외국인의 출입 및 연구보안 위배 특이동향을 관찰하고 계신가요?	권고	54
	[보안] (참여종료) 외국인의 과제 참여 종료 시 각종 연구자료 등을 회수하였나요?	대책제4조 (별표)	54
	[보안] (참여종료) 외국인의 연구시설/정보 등에 대한 접근권한을 제한하였나요?	대책제4조 (별표)	54
	[보안] (참여종료) 연구책임자는 외국인의 자료반출입 이력 및 인쇄 이력을 점검 하였나요?	대책제4조 (별표)	54
	[보안] (참여종료) 보안과제 종료 시점에 외국인에게 추가 보안서약서 징구가 필요할지에 대해 연구보안 담당부서와 함께 검토해보셨나요?	권고	54
❹ 보안과제 수행 연구실에 외국인 상주	**[보안]** 보안과제에 참여하지 않는 부서 내의 외국인(연구원, 방문연구원, 교환학생, 인턴 등)에 대한 자료 및 시설접근 제한 계획을 마련하셨나요?	대책제4조 (별표)	57
	[보안] 보안과제 참여연구원이 연구부서 내 외국인에게 보안과제 관련 논의를 지속적으로 하는 경우에도 외국접촉 보고를 해야 함을 알고 계신가요?	대책제8조제2항	57

제2절 | 국가R&D 국제공동 연구 추진 시 지켜야 하는 것이 무엇인가요?

주제	체크리스트	관련법	본문 (Page)
❶ 협약·계약 시 연구보안	(협약 전) 공동 연구기관의 연구보안 규정 특이사항이 무엇인지 확인 하였나요?	권고	59
	(협약 전) 상호 지식재산, 대외발표 규정을 검토 하였나요?	권고	59
	(협약 전) 공동연구 결과가 군사적으로 사용될 가능성이 존재하는지 검토해 보셨나요?	권고	59
	(협약 전) 공동연구 내용과 각국의 수출통제 기술 관련성 여부에 대해 검토해 보셨나요?	권고	59
	(협약 전) 외국기관과 연구계획서를 작성할 때, 공유된 정보를 별도 저장 및 관리하는 보안체계가 마련되어 있나요?	권고	59
	(협약 당시) 계약서에 지식재산권(IP) 보호 정책과 소유권 배분 조항, 활용에 대한 내용이 명확히 포함되어 있으며, 해당 조항이 소속 기관에 불리하지 않은지 기관 내 지식재산 담당자와 논의해 보셨나요?	권고	60
	(협약 당시) 계약서 상 윤리적 문제(데이터 위조, 표절, 저작권침해)에 대해서도 다루었나요?	권고	60
	(협약 당시) 상호 충분히 동의할 수 있는 보안대책을 수립 하였나요?	권고	60
	(협약 당시) 국제공동연구 중 민감한 정보가 포함된 경우, 관련 내용을 보호하기 위해 비밀유지계약(NDA)을 체결하셨나요?	권고	60
	(협약 당시) 상대 기관의 참여연구진 신원(소속, 국적)과 연구범위를 확인 하였나요?	권고	60
	(협약 당시) 상대 기관의 R&D 자금 출처가 어디인지 명확히 알고 있나요?	권고	60
	(협약 당시) 국제공동연구와 관련하여 소속 기관에 보고하거나 승인을 받아야 하는 주요 사안을 확인하였나요?	권고	60
❷ 보안과제에 외국기관 참여	**[보안]** 국외 연구기관과 보안과제 공동연구 추진 시 강화된 보안관리 방안을 마련하셨나요?	영제44조 제2항제4호	64
	[보안] 전문기관 및 연구보안 담당자와 함께 보안과제 외국기관 참여가 필요한 것인지 검토해 보셨나요?	권고	64
	[보안] 외국기관 참여 시 연구기관의 사전승인, 담당 중앙행정기관장의 사전승인, 국정원 통보 절차가 필요하다는 사실을 알고 계신가요?	대책제9조제2항	64
	[보안] 보안과제 참여 외국기관에게 우리나라 관련법 및 소속기관 방침을 공식적으로 전달 하였나요?	권고	64

제3절 | 안전한 국제협력을 추진하고 싶어요!

주제	체크리스트	관련법	본문 (Page)
❶ 국외수혜정보 보고 원칙 및 방법	⊘ 국외수혜정보 보고 대상자, 보고 의무범위, 보고시기, 보고항목, 보고방법 전반에 대해 알고 계신가요?	영제9조제3항 제8호	67
	⊘ 협약 시 또는 과제수행 도중 국외수혜정보 보고를 하셨나요?		67
❷ 개인 국제협력 및 해외기관 진출	⊘ 개인의 과제수행, 자문이력, 겸직 등을 평소에 정리해 두고 계신가요?	권고	71
	⊘ 연구자 활동 국가의 정보공개 요구 사항을 확인 하셨나요?	권고	71
	⊘ 연구자 활동 국가의 수출통제 기술에 대해 알고 계신가요?	권고	71
	⊘ 연구자가 파견 대상 기관에는 어떠한 연구보안 규정이 있는 지 알고 계신가요?	권고	71
❸ 보안과제 수행 연구자의 외국과제 수행	⊘ **[보안]** 보안과제를 수행 중이거나 수행 후 3년 이내인 시점에서 국외 연구과제를 수행하기 전에 소속 기관장의 사전 승인을 받아야 한다는 것을 알고 계셨나요? (이직 및 퇴직도 포함)	대책제8조제2항	76

제4장. 기술사업화 단계의 연구보안

제1절 | 기술이전 및 창업을 하려 해요!

주제	체크리스트	관련법	본문 (Page)
❶ 기술이전·양도·해외수출	⊘ 기술이전 기획 단계에서 수요기업에 대한 신용평가, 재정상태에 대한 평판을 확인해 보셨나요?	권고	79
	⊘ 기술이전 상담 시 수요기업과 상담내용 관련 비밀유지 계약 체결하는 것을 고려해 보셨나요?	권고	79
	⊘ 기술이전 및 연구보안 담당자와 논의하시어, 기술이전 계약서에 명확하게 '기술 이전 범위, 손해배상 조항, 비밀유지 조항, 보안대책 수립' 등 내용이 포함되어 있는지 확인 하셨나요?	권고	79
	⊘ **[보안]** 보안과제 관련 성과의 소유권 이전은 원칙적으로 허용되지 않는다는 것을 알고 계신가요?	대책제15조제1항	80
	⊘ **[보안]** 보안과제 성과의 소유권 양도 시 이전 받는 기관이 보안대책 제3조~15조를 따르도록 계약해야 한다는 것을 알고 계신가요?	대책제15조제2항	80

주제	체크리스트	관련법	본문 (Page)
	[보안] 보안과제 기술이전 시 제3자 기술실시 금지 관련 내용을 포함시켜 계약을 체결해야 한다는 것을 알고 계신가요?	대책제15조제3항	80
	[보안] 보안과제 성과를 해외로 양도 및 기술이전 결정 시 중앙행정기관 장의 사전 승인을 받아야 함을 알고 계신가요?	대책제15조제3항	80
	[보안] 보안과제 성과 해외 수출 시, 전략물자, 국가핵심기술에 해당하는지 연구보안 담당부서와 함께 검토해 보셨나요?	대외무역법 제2조, 산업기술보호법 제2조·제9조 제6항·제11조, 방위산업보호법 제2조	80
❷ 실험실 창업	실험실 창업 전에 소속기관과 지식재산 및 보안관련 사항을 협의 하였나요?	권고	82
	실험실 창업 후 M&A 및 투자제안을 받았을 때 해당 내용을 원 소속기관과 검토해 보셨나요?	권고	82
	실험실 창업 투자 예정 기관이 혹시 제3국의 지배를 받지 않는 지, 연구보안 사고 사례가 있었는 지 평판을 검토해 보셨나요?	권고	82
	실험실 창업 투자 기관과 사업구상 시 NDA 체결을 고려해 보았나요?	권고	82
	국가핵심기술, 전략물자, 방위산업기술에 해당하는지를 점검해 보셨나요?	대외무역법 제2조, 산업기술보호법 제2조·제9조 제6항 방위산업보호법 제2조	82

제2절 | 품목화 된 기술보호를 위해 어떻게 해야 되나요?

주제	체크리스트	관련법	본문 (Page)
❶ 산업보안·국방보안 판정절차 및 주의사항	**[보안]** 국가핵심기술, 전략물자기술, 방위산업기술 위반 시 불이익과 판정 절차 등에 대해 교육을 받으셨나요?	대책제4조 (별표)	85
	국가핵심기술, 전략물자기술, 방위산업기술과 연관되는 분야를 연구하고 있다는 의심이 드는 경우, 연구보안 담당 부서에 판정지원을 요청해야 한다는 것을 알고 계신가요?	권고	85
❷ 기술임치를 통한 지식재산 보호	영업비밀원본증명서비스, 기술임치 제도 등 기술보호 제도를 알고 계신가요?	권고	90

제5장. 연구보안 사고 대응

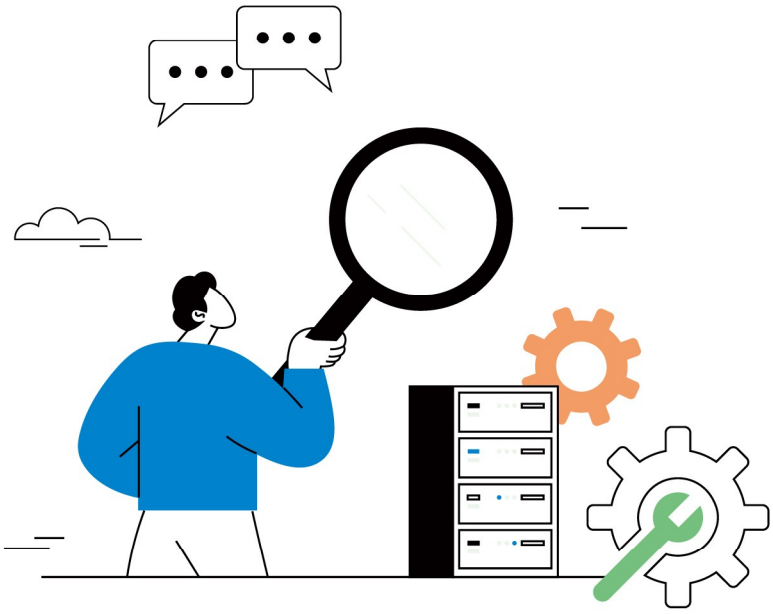
제1절 | 연구보안 사고가 발생 하였어요!

주제	체크리스트	관련법	본문 (Page)
❶ 대응절차 및 행동지침	✓ 연구보안 사고의 정의 및 종류에 대해 알고 계신가요?	영제48조 제1항 및 제2항, 대책제4조 (별표)	92
	✓ 연구자가 보안사고를 당하거나 목격했을 시, 즉시 관련자에게 보고해야 함을 알고 계신가요(부서장, 연구책임자, 연구보안 담당자)?	대책제4조 (별표)	93
	✓ 연구자는 보안사고에 관해 관계기관의 조사요청에 적극 협조해야 함을 알고 계신가요?		

제2절 | 연구보안 규정 위반 이후 어떻게 되나요?

주제	체크리스트	관련법	본문 (Page)
❷ 연구보안 규정 위반 시 처분, 가중 및 감경요인	✓ 혁신법 상 보안사고 관련 참여제한 기준을 알고 있나요?	영제59조 제1항 및 제2항	99
	✓ 혁신법 상 가중처벌 및 감면규정 등 처벌 규정을 알고 있나요?		

PART 01



연구보안 기본원칙

제1장 국가R&D 참여연구자의 연구보안

제1절 국가R&D 참여연구원의 일상 속 연구보안 규칙은 무엇인가요?

01. IT 및 정보기기 사용

1 연구보안 위험 포인트

» IT 발달은 빠른 정보교환을 가능하게 하여 연구 진행을 촉진 시키기도 하지만 불법적 침입 수단이 되기도 합니다.

» 연구자의 올바른 IT 활용으로 스스로를 지키려는 노력이 필수적입니다.

2 권고사항 및 의무

❶ 업무용 정보기기 보안관리

- **(로그인관리)** 연구자는 업무용 PC등 정보기기의 계정을 관리하고 비밀번호를 주기적으로 변경하여야 합니다.
- **(보안SW)** 연구자는 소속기관의 보안SW 업데이트 방침에 적극 협조해야 합니다.
- **(개인정보 포함 데이터관리)** 연구자는 소속기관의 방침에 따라 타인의 주민등록번호가 포함된 데이터를 주기적으로 삭제해야 합니다.
- **(폐기)** 개인의 업무용 노트북, 정보통신 매체(USB), 장비 등을 폐기할 시, 기관의 방침에 따라 안전하게 폐기해야 합니다. 기관 담당부서에 문의 하세요.
- **(기타)** 연구자가 개인 IT 기기를 업무용으로 사용하는 경우에도 연구기관의 보안 정책을 준수합니다. 연구책임자는 연구부서(연구실) 내 공용PC에 대해서도 연구실 내 관리자를 지정하여 기관의 정보보안 방침을 따를 수 있도록 합니다.

• 업무용 컴퓨터 비밀번호 주기적 변경	☐Yes ☐No
• 업무용 컴퓨터 보안SW 업데이트	☐Yes ☐No
• 개인정보 포함 데이터를 주기적으로 삭제하는 지 여부	☐Yes ☐No
• 업무용 컴퓨터, 정보통신매체 등의 안전폐기 방침 확인 여부	☐Yes ☐No
• 연구실 내 공용 PC 보안관리 담당자 지정 여부 확인	☐Yes ☐No

❷ 업무 시 IT 활용

- **(클라우드)** 연구자가 민감정보를 다룰 시 기관인증 클라우드를 활용해야 합니다.
- **(스팸메일)** 악성 이메일은 해킹의 경로가 될 수 있으므로 의심이 가는 메일은 일단 읽지 말고 '스팸신고' 합니다.

- **(생성형 AI)** 연구자가 생성형 AI등을 연구에 사용하는 경우, 아래 표와 같이 기본적인 보안수칙을 지킬 수 있도록 해야 합니다.

• 소속기관으로부터 보안성을 인정받은 클라우드를 사용	☐Yes ☐No
• 스팸메일로 의심되는 메일을 받았을 때, '스팸신고'부터 추진	☐Yes ☐No
• 비공개 정보, 개인정보를 생성형 AI에 입력 금지	☐Yes ☐No
• 생성형 AI 로그인 계정에 대한 보안설정 강화*	☐Yes ☐No
• 생성형 AI 생성물 활용 시 지적재산권, 저작권 침해 여부 등 검토	☐Yes ☐No
• 생성형 AI 관련 연계, 확장 프로그램 사용 시 보안 취약여부 등을 소속기관 담당자에게 문의	☐Yes ☐No

* 강력한 비밀번호 설정, Multi-Factor Authentication

3 연구보안 모의사례

❶ USB를 통한 악성코드 감염 방지

가상상황	• 연구자 B는 최근 참석한 컨퍼런스에서 USB를 증정받았다. B는 기관의 보안방침에 따라 USB 사용등록을 마쳤으며 악성코드 검사 후에 해당 USB를 사용하였다. USB 검사 중 악성코드를 발견해 제거할 수 있었고, 다행히도 해당 PC와 연결된 기관 시스템에 대한 감염 확산도 방지할 수 있었다.
연구보안 포인트	✓ 연구자는 연구자료를 다룰 때 기관에서 인증받은 USB를 사용하도록 하고 수시로 악성코드를 검사해야 합니다.

❷ 민감정보를 생성형 AI에 입력한 사례

가상상황	• 의대에서 박사과정 중인 B는 환자 빅데이터를 파이썬으로 분석하는 작업을 수행 중이다. B는 AI에게 파이썬 코드를 만들어 달라고 하거나 데이터 일부를 AI에 입력하여 수정사항을 찾아내기도 하였다. 환자 데이터라는 점이 마음에 걸렸지만 B는 환자 데이터가 개인정보 비식별처리 되어 있어 문제가 없을 것이라고 생각했다. • 그러던 어느 날 AI 사용 교육을 수강하였는데, 강사님께서 개인정보를 비식별 처리하였다고 하더라도 AI 출력물, 외부정보 결합을 통해 어느 정도의 개인정보 추출이 가능할 수도 있다고 하였다. 또한 사용자 입력정보가 AI 훈련 데이터로 활용되어 AI가 타인에게 관련 정보를 유출할 가능성도 존재한다고 하였다. B는 앞으로는 환자 데이터를 AI에 직접 입력하지 않겠다고 다짐하였다.
연구보안 포인트	✓ 생성형 AI 사용 시 민감정보 삭제 여부를 사전에 확인 합니다. ※ 만약 환자 데이터인 경우, 환자 동의 여부 확보 확인 필요 ✓ 생성형 AI 사용 시 폐쇄형 대화(비공개 모드 또는 학습 거부설정) 설정인지 여부를 확인 합니다.

❸ 연구과정 중 생성형 AI의 잘못된 사용사례

가상상황	• 신입 연구자인 A씨는 연구개발과제를 수주하기 위하여 연구개발계획서(제안서)를 작성 중에 있다. • A씨는 연구개발계획서 작성 시, 필요한 정보를 빠르게 정리하기 위하여 AI를 사용하였다. 또한 연구개발계획서의 보완점을 찾기 위하여 연구개발계획서 전체를 AI에 입력하기도 하였다. • 이러한 와중에 AI를 활용해서 연구계획서를 작성해도 되는 지, 다른 사람은 어떻게 하는지 의문이 들었다.
연구보안 포인트	✓ 연구개발계획서 작성 시 생성형 AI를 사용한 경우 해당 계획서에 AI 도구 사용 내역을 기술할 것을 권장합니다. ✓ 연구개발계획서에는 개인정보, 연구내용, 수행기관 정보, 대외비인 전략적 정보 등이 포함되어 있으므로 해당 계획서 전체를 AI 서비스에 업로드 해서는 안됩니다.

4 관련 법규 및 매뉴얼

- 연구자별 PC, 노트북 등의 단말기 사용 시 기본적인 보안사항들을 준수하여 보안위험 상황을 조기에 예방하는 것이 중요합니다.
- 국가정보원, 국가보안기술연구소는 '챗GPT 등 생성형 AI 활용 보안 가이드라인(2023)'을 발행하였으므로 아래와 같은 항목에 대해 확인하시길 바랍니다[1].

가이드라인 주제	포함내용
서비스 사용 주의사항	• 서비스접근, 계정관리법
서비스와 대화 시 주의사항	• 답변 검증(정확성, 유해성), 개인정보 및 민감정보 처리, AI모델이 생성한 데이터 관리, 책임감 있는 사용, 업무에서 올바르게 AI모델 활용하기
AI모델 플러그인 사용 주의사항	• 올바른 서비스 플러그인 사용 및 관리
AI모델 확장 프로그램 사용 주의사항	• 개인정보 및 민감정보 처리
AI모델 생성기반 공격대처 방안	• AI모델 생성기반 공격정의, AI모델 생성기반 공격대처

- 한국연구재단은 생성형 AI 관련 권고사항을 2024년에 발표 하였습니다[2].
- 한국연구재단 지원과제 신청자 및 수행자는 연구개발계획서 및 단계/최종보고서 작성 과정에서 생성형 AI도구를 사용한 경우, 해당 계획서 및 보고서에 AI도구 사용 내역을 기술할 것을 권장하고 있습니다.
- 개인정보보호법 제24조의2(주민등록번호 처리의 제한) 따라 특수한 경우를 제외하고 타인의 주민등록번호를 처리할 수 없습니다.

1) 국가정보원·국가보안기술연구소. (2023), 챗GPT 등 생성형 AI 활용 보안 가이드라인
2) 한국연구재단. (2024), 생성형 인공지능(AI) 도구의 책임 있는 사용을 위한 권고사항

02. 원격·재택근무 및 영상회의

1 연구보안 위험 포인트

» 코로나19 이후 '비대면 디지털 기반 근무(원격·재택 근무), 원격 영상회의'가 많은 연구기관의 근무 형태로 자리 잡아가고 있습니다.

» 갑작스러운 팬데믹으로 확산된 근무 형태이기에 충분한 준비 없이 '가정 및 온라인 환경'이 업무공간으로 변화된 경우가 많아 보안위험에 취약할 수 있습니다.

2 권고사항 및 의무

❶ 원격 및 재택근무

※ ICT 기술을 활용한 근무형태로 '재택근무, 공유 오피스 근무, 노트북을 활용해 임의 장소에서 일하는 모바일 근무' 형태를 포함

- **(관리자)** 연구부서장(연구실 책임자)은 '원격 및 재택근무'의 책임자이므로 소속기관 방침을 확인하고 원격근무에 대한 관리를 추진합니다.

• 연구부서장은 '원격근무 관리대장' 작성	☐Yes ☐No

- **(보안지침)** 연구자는 소속기관의 방침을 준수하며 '원격 및 재택근무'를 수행하여야 합니다. 일반적인 원격근무 수행자의 행동지침은 아래와 같습니다.

• (전용 공간 확보) 개방된 장소가 아닌, 보안성이 확보된 전용 공간에서 원격·재택근무 실시	☐Yes ☐No
• (단말기 보안) 기관에서 제공된 단말기를 사용하여 사내망 접속	☐Yes ☐No
• (네트워크 보안) 보안성이 확보된 인터넷망 사용	☐Yes ☐No

※ 보안과제의 경우, '보안과제 수행 시 원격/재택근무 주의사항' 별도참고 (p.32)

❷ 영상회의

- **(영상회의 관리자)** 연구부서장은 부서단위의 '영상회의'의 책임자로서 소속기관 방침, IT 환경을 확인하고 온라인회의를 승인 합니다.
- **(영상근무 보안지침)** 연구자는 소속 연구기관의 방침에 따라 영상회의를 진행 합니다. 일반적으로 영상회의에 대한 올바른 보안 행동 수칙은 아래와 같습니다.

• 허가된 영상회의 접속자에게만 주소를 공개하거나 비밀번호 설정	☐Yes ☐No
• 참가자들 간 파일공유 비활성화 작업으로 악성파일이 전송되지 않도록 설정	☐Yes ☐No
• 회의 전 참가자에게 녹화, 캡처 행위 금지에 대해 안내	☐Yes ☐No

※ 보안과제의 경우, '보안과제 수행 시 영상회의 주의사항' 별도참고 (p.32)

3 연구보안 모의사례

❶ 온라인 회의 시 보안조치

가상상황	• A, B 두 기업 간에 NDA 체결 후 사업 협업을 논의하는 도중, 온라인 회의를 개최하게 되었다. 이 때 A 기업 담당자의 부주의로 인하여 모두에게 공개된 상태로 온라인 회의를 진행 하였다. • 온라인 회의 도중 신원미상자가 참석하여 두 기업이 서로 발표 중이던 기밀사항 및 고객정보 등을 보게되는 사고가 발생하고 말았다.
연구보안 포인트	• 연구기관은 원격·재택근무 보안방침, 대응계획 및 처리절차를 임직원에게 전파하고, 주기적으로 교육을 진행해야 합니다. • 연구자는 소속기관이 안내한 방침에 따라 연구보안 수칙을 지키며 온라인 회의를 추진해야 합니다.

4 관련 법규 및 매뉴얼

- 한국인터넷진흥원은 『비대면 업무환경(원격근무, 영상회의) 도입·운영을 위한 보안 가이드』를 발표하여 연구기관·연구자가 어떠한 보안환경을 갖추고 행동해야 하는 지를 안내하고 있습니다. 보다 구체적 내용은 해당 가이드를 확인하세요[3].
- 연구기관장은 자체적으로 원격 및 재택근무 관련 보안규정을 마련하고 임직원들이 해당 규정을 따를 수 있도록 안내해야 합니다.
- 과학기술정보통신부 산하 기관 중 보안업무를 다루는 기관이라면 원격, 재택근무 규정 수립 시 아래와 같은 사항을 참고할 수 있습니다.

과학기술정보통신부 보안업무 시행세칙

제20조의2(원격·재택근무 관련 보안준칙) ① 모든 직원은 원격·재택근무시 다음 각 호의 사항을 준수하여야 한다.

1. 비밀 및 대외비에 해당하는 정보·자료의 생산 및 처리 금지
2. 불특정 다수가 사용하는 PC에서 원격근무서비스 접속 금지
3. 업무상 생성된 문서 및 데이터는 업무 종료시 PC에서 완전 삭제하되, 불가피한 경우 비밀번호를 설정하여 저장
4. 접속화면 캡쳐 및 카메라 등을 이용한 촬영 금지, 출력물 생성 최소화
5. OS, 백신 소프트웨어 등 최신 보안 업데이트 및 바이러스 점검 실행
6. 상용 P2P, 메신저, 웹하드, 영상회의시스템 등 사용 금지

② 각 부서장은 해당 부서의 원격·재택근무 보안전담관이 되며, 다음 각 호의 임무를 수행한다.

1. 소속 부서원의 원격·재택근무 계획서의 보안 적절성 확인
2. 원격·재택근무 승인 심사 및 보안서약서 징구
3. 원격·재택근무자에 대한 보안 유의사항 수시 교육
4. 원격·재택근무자의 보안지침 준수 및 비인가 직무 수행 여부 점검
5. 원격·재택근무자 현황 및 문서반출 기록 유지·관리
6. 원격·재택근무 종료시 반출문서 회수 확인 등 사후 보안조치

③ 소속기관 등의 보안담당관은 원격·재택근무 보안관리 실태를 정기적으로 자체평가하고 미비점을 보완하여야 한다.

제51조(중요 정책자료 등에 대한 보안대책) ① 중요 정책 및 사업에 대한 자료로서 누설되는 경우 그 정책 및 사업추진에 지장을 초래할 우려가 있거나, 직무수행 상 특별히 보호가 필요한 사항은 입안(立案) 단계에서부터 대외비로 분류하여야 한다.
② 중요 정책 또는 사업의 추진을 위하여 관계자회의 등을 개최하는 기관(부서)의 장은 참여자에 대하여 사전에 보안교육을 실시하고, 회의 시 배부하는 자료는 대외비로 분류하여 회의종료 후 회수하는 등 자료의 유출방지대책을 강구하여야 한다.
③ 제2항의 회의를 영상회의로 진행하는 경우 영상회의시스템의 보안성을 확보하여야 하며, 단계별·분야별 영상회의 운영 보안대책을 마련하여 시행하여야 한다

3) 한국인터넷진흥원. (2020), 비대면 업무환경(원격근무, 영상회의) 도입·운영을 위한 보안 가이드

03. 해외 출장

1 연구보안 위험 포인트

» 해외출장 시 생소한 환경에 적응하느라 물품을 분실하는 경우도 많고 긴장감이 풀려서 연구보안 규정을 허술하게 다루게 될 수도 있습니다.

» 해외 출장 중 중요한 자료나 물품을 분실 또는 도난당하면 되찾을 방법이 거의 없으므로 출국 전 보안 관련 준비를 철저히 해두는 것이 중요합니다.

2 권고사항 및 의무

❶ 해외 출장 전 보안조치

- **(출장교육 및 준비)** 해외 출장 전 연구자는 연구기관으로부터 해외출장 관련 주의사항에 대해 안내 받아야 합니다. 일반적인 주의 사항은 아래와 같습니다.

• 해외 출장 국가에서 위급 시 도움을 청할 수 있는 대사관, 경찰서, 지인 등 정보를 사전에 확보	☐Yes ☐No
• 업무용 노트북, 전산장비 비밀번호 설정 여부 확인	☐Yes ☐No
• 업무용 노트북, 전산장비 내 중요 데이터 암호화 여부 확인	☐Yes ☐No
• 업무용 노트북, 전산장비 분실 방지방안 고민	☐Yes ☐No
• 필요 시 렌탈 노트북 활용여부 검토	☐Yes ☐No
• 해외출장 사전 교육	☐Yes ☐No
• 소속기관에 해외 출장 사전 승인	☐Yes ☐No

- **(출장 사전승인)** 해외 출장 전 연구자는 연구기관 방침에 따라서 '해외출장 목적, 경로, 예상되는 국외 관계자 만남, 반출자료'에 대해 보고하고 승인 받도록 합니다.
- **(출장발표)** 연구자는 해외출장 시 발표 자료의 향후 상업적 활용 가능성, 보안성 저촉 여부 등에 대해 고민해 봐야 합니다.

※ 참고 : 1-2-3. 회의참석, 학술발표(p.22)

• 해외출장 발표 자료의 상업적 활용 가능성 검토	☐Yes ☐No
• 해외출장 발표 자료의 보안성 검토	☐Yes ☐No

❷ 해외 출장 중 보안조치

- 연구자는 소속 연구기관의 보안 행동 요령 방침에 대해 숙지하도록 합니다. 아래는 일반적인 행동 요령입니다.
  - 업무용 노트북 및 장비 분실은 연구보안 사고로 발전될 수 있는 가능성이 크기 때문에 소지품 관리에 각별히 주의합니다.

• 해외 출장 중 여행사, 호텔 관계자 등 외부인에게 체류 목적 등 출장과 관련된 언급 최소화	☐Yes ☐No
• 신원이 특정되지 않도록 해외 출장 중 사원증, 소속기관 마크 등 노출 금지	☐Yes ☐No
• 연구과제와 관련된 민감한 정보를 발설해야 할 경우에는 자체 연구보안 관리 규정 또는 지침 준수	☐Yes ☐No
• 보안을 요구하는 중요한 자료 취급 시 호텔이나 학회 또는 세미나 측에서 제공하는 전산장비, 공용 WI-FI 등 이용 자제	☐Yes ☐No

❸ 해외 출장 후 보안조치

- 연구자는 소속기관의 방침에 따라 출장보고를 추진하며 전산장비를 정비합니다.

• 연구기관 방침에 따른 해외출장 보고 추진	☐Yes ☐No
• 귀국 후 가능한 빠른 시일 내에 전산장비의 패스워드를 변경	☐Yes ☐No
• 출장 중 소지한 전산장비는 연구기관의 정보보안부서에 의뢰하여 악성프로그램 설치 여부를 점검	☐Yes ☐No

3 연구보안 모의사례

❶ 국외출장 보안수칙 준수로 연구정보 유출 방지

가상상황	• A연구기관에서는 연구자들이 해외 출장 신청 시 내부 시스템에서 "국외출장보안수칙"을 열람해야 출장비 신청이 가능하도록 강제하였다. 이를 통해 국외출장보안수칙에 익숙해진 연구자 B는 경쟁국에서 중요한 기술 정보를 염탐하지 못하도록 철저하게 출장 일정을 관리 하였다. 연구관련 회의를 추진할 때도 호텔로비나 카페가 아닌 연구자들으로만 이뤄진 공간에서 추진하였고 회사 로고를 노출하지 않도록 하였다.
연구보안 포인트	✓ 출장 중 연구기관, 연구과제 및 연구와 관련된 중요한 정보를 외부인이 들을 수 있는 공공장소 등의 환경에서 언급하지 않아야 합니다. ✓ 연구기관은 해외 출장 전 연구자들에게 보안 교육을 실시하고, 보안 위험 사례를 공유하여 경각심을 높여야 합니다.

4 관련 법규 및 매뉴얼

- 국가연구개발사업을 추진하는 연구기관이라면 연구자산 유출 방지를 위한 연구보안대책을 강구하고 연구자가 해외출장 시 임무를 무사히 마칠 수 있도록 안내해야 합니다.
- 보안과제를 수행하고 있거나 「산업기술보호법」에 따라 '산업기술'을 연구하고 있는 연구기관은 보안과제를 수행하는 연구자의 해외출장 및 해외접촉에 대한 규정을 마련해야 합니다.

국가연구개발사업 보안대책

연구기관보안대책에 포함되어야 하는 사항(보안대책 제4조 관련)

2. 보안과제 참여연구자(연구책임자 및 외국인을 포함한다) 관리

가. 참여연구자의 연구기관보안대책 위반 시 징계에 관한 사항

나. 퇴직하였거나 퇴직 예정인 자가 반출 또는 반출 예정인 자료에 대한 보안성 검토, 회수, 전산망 접속 차단 등의 조치에 관한 사항

다. 참여연구자의 국외 출장 시 사전 보안교육 및 귀국보고(출장기간에 접촉한 사람 및 협의 내용 등을 포함한다) 실시

라. 보안과제를 수행하거나 수행한 적이 있는 연구자의 외국 정부·기관·단체 접촉시 보고 및 외국 정부·기관·단체와의 연구 승인 등에 관련된 절차 및 형식 등 제반사항

- 과학기술정보통신부 산하 기관은 해외출장자에 대한 충분한 자체교육을 시행해야 합니다.

과학기술정보통신부 보안업무 시행세칙

제77조(보안교육) ① 보안담당관은 다음 구분에 따라 자체계획을 수립하여 보안교육을 실시하여야 한다.

1. 보안업무의 향상과 보안사고의 사전 예방을 위하여 소속 직원을 대상으로 반기 1회 이상 보안교육을 실시하여야 한다.
2. 신규 채용자에 대하여서는 채용과 동시에 보안업무 전반에 대한 교육을 실시하여야 한다.
3. **공무, 학술, 체육, 문화, 시찰, 유학 또는 국제기구·민간기업 파견 또는 취업 등을 목적으로 하는 해외여행자에 대하여는 출국 전에 충분한 자체 보안교육을 실시하여야 한다.**
4. 비밀·암호자재취급인가 예정자에 대하여는 보안담당관의 지도하에 소관 분임 보안담당관이 사전에 충분한 보안교육을 실시하여야 한다.

② 비밀교재 및 비밀교육 내용을 기록한 피교육자의 필기장 등에 대한 보안대책을 마련·이행하여야 한다.

04. 연구보안 인식제고 및 교육

1 연구보안 위험 포인트

» 외국의 연구자산 탈취 시도가 증가하고 연구개발 정보 유출 기법도 나날이 발전하고 있습니다.

» 순간의 방심으로 연구자산이 유출될 수 있으므로 연구자들은 지속적으로 경각심을 유지하며 연구보안에 친숙한 문화를 형성하도록 합니다.

2 권고사항 및 의무

- **(규정·담당자 사전파악)** 연구부서장(또는 연구책임자)은 소속기관의 연구보안 규정에 대해 숙지해야 하고 소속기관의 연구보안 담당자가 누구인지 사전에 파악 하도록 합니다.
  - 연구기관의 연구보안 담당자가 누구인지 확실치 않다면 '연구관리부서' 등에 문의 합니다.
- [법] **(교육·보안서약)** 연구부서장은 연구부서(또는 연구실) 구성원이 연구보안 소양을 함양할 수 있도록 교육 수강을 권장해야 합니다.
  - [법] 일반과제 수행 연구자라도 '소속기관, 중앙행정기관' 방침에 따라 보안교육을 받거나 보안서약서를 제출할 수도 있습니다.
- **(문화형성)** 연구부서장은 연구부서 구성원들이 연구보안, 이해상충, 산업보안 등의 주제에 대해서 기탄없이 논의할 수 있는 분위기를 형성하도록 해야 합니다.
  - 연구자는 자료 외부 반출 및 발표, 국외수혜, 국제공동연구 수행에 대해 연구책임자, 연구보안 담당자와 긴밀히 논의해야 합니다.

• 소속기관 연구보안 규정명 확인	☐Yes ☐No
• 소속기관 연구보안 담당자(또는 연구관리자) 연락처 확인	☐Yes ☐No
• 연구부서(또는 연구실) 구성원들의 연구보안 교육 수강	☐Yes ☐No

3 연구보안 모의사례

❶ 연구보안 인식 제고로 인한 유출사고 발생 예방

가상상황	• A대학은 '연구보안 교육 수강'을 대학원생 졸업 요건으로 지정하였다. A대학 B실험실에서는 구성원들이 돌아가며 반드시 1번은 정기 보안교육에 참석해야 했고 담당 교수는 교육 참석자들에게 보안교육 자료를 연구실에 공유하도록 하였다. • 처음에는 모두가 귀찮아했지만 정보공유 횟수가 누적되고 교육을 수강한 구성원들이 많아지자 점차 연구실 내에 연구보안 문화가 정착되기 시작하였다. • B실험실 전체가 국제 학회에 참여할 일이 발생했는데, 서로 발표자료에 민감한 내용이 있지는 않은지, 민감한 정보를 외국인에게 발설하지는 않는지, 노트북에 비밀번호를 설정하였는지 등에 대해 자발적으로 주의를 줄 수 있었다. 그 결과 모두가 불미스러운 일 없이 무사히 해외출장을 마칠 수 있었다.
연구보안 포인트	✓ 연구보안 문화는 연구자 간 신뢰와 공동체 의식을 통해 형성될 수 있습니다. ✓ 연구자는 연구기관이 제공하는 연구보안 교육을 반드시 이수하고, 연구자료의 공개 여부에 대해 사전에 연구책임자와 협의해야 합니다.

❷ 연구실의 연구보안 문화 조성

가상상황	• 국가전략기술 관련 연구실에서 석사과정을 진행 중인 대학원생 C는 대학원생을 대상으로 한 연구보안 교육을 최근 수강하였다. 해당 교육에서 강사는 연구자의 지식재산을 지키기 위해서는 평소에 '국외수혜 및 이해상충' 관련 정보의 투명한 공개가 중요하다고 강조하였다. C는 그 말이 잘 이해가 되지 않아 실험실 내 선배들에게 문의하였다. • 선배들은 연구자들이 '국외수혜 및 이해상충' 정보를 평상 시에 투명하게 공개 한다면 '연구보안 규정 위반 및 이해충돌 상황'을 예방할 수 있다고 하였다. 또한 선배들은 연구자가 과제 관련 정보를 투명하게 공개함으로 '신뢰받는 연구자'라는 긍정적인 평판을 얻고, '흠결 없는 연구'를 추구할 수 있다고 덧붙였다. • 선배들의 설명을 들은 C는 투명한 정보 공개의 중요성에 대해 다시 한번 생각해 보게 되었고 연구보안과 윤리적 책임에 대해 깊이 이해할 수 있었다.
연구보안 포인트	✓ 연구자들은 관련 연구보안 교육을 지속 수강하는 한편 기탄없이 관련 내용을 토론하는 문화를 만들어 나가야 합니다. ✓ 연구보안은 연구관리 전주기 동안 연구자의 투명한 정보공개와 절차준수를 통해 이뤄질 수 있습니다.

4 관련 법규 및 매뉴얼

- 국가연구개발사업을 추진하는 연구기관이라면 연구자산 유출 방지를 위한 연구보안대책을 강구하고 소속기관 연구자의 교육을 책임져야 합니다.
- 국가연구개발사업 보안대책에 따라 보안과제를 수행하는 연구기관의 장은 보안과제를 수행하지 않는 연구자에 대해서도 보안교육을 실시할 수 있고, 보안서약서를 징구할 수 있습니다.

국가연구개발사업 보안대책

제7조(보안교육 및 보안서약)

④ 연구기관의 장은 필요한 경우 보안과제를 수행하지 않는 소속 연구자와 기타 소속 직원에 대해서도 보안교육을 실시할 수 있으며, 특별히 보안상 필요한 경우 서약서를 제출하도록 할 수 있다.

[별표] 연구기관보안대책에 포함되어야 하는 사항(제4조 관련)

1. 보안관리체계

바. 소속 직원의 보안교육 이수 의무에 관한 사항

※ 연구기관보안대책에 따른 연구자의 의무, 우대사항 및 의무사항 위반시 「산업기술의 유출방지 및 보호에 관한 법률」, 「대외무역법」에 따라 받을 수 있는 불이익에 관한 사항과 연구성과에 대한 「산업기술의 유출방지 및 보호에 관한 법률」상 핵심기술 판정 필요성과 후속조치 등

제2절 국가R&D 연구산출물 및 성과를 어떻게 관리해야 하나요?

01. 문서·연구노트·데이터 관리

1 연구보안 위험 포인트

» 국가R&D 수행 중에는 문서, 연구노트, 데이터 등 많은 자료가 생성되며 이들 자료에는 중요한 정보가 포함되어 있습니다. 예방적 차원에서 이들 자료의 생성 단계부터 보안관리를 추진해야 할 필요성이 있습니다.

2 권고사항 및 의무

❶ 문서 연구보안

- **(문서정의)** 국가R&D를 수행하며 발생하게 되는 '보고서, 회의록, 보고자료, 연구정보 자료, 연구데이터, 연구노트, 파일' 등은 '문서'로 통칭될 수 있습니다.
- **(문서등급 구분)** 연구책임자를 중심으로 연구과정 중 창출된 '문서'가 '영업비밀', '대외비'에 해당하지 않는지 구분합니다.
  - (기준) 문서 분류에 대한 연구기관의 기준이 존재한다면 이를 따릅니다.
- **(문서등급 지정)** 문서생산자 및 연구책임자는 '영업비밀, 대외비'에 해당하는 문서등급을 '문서관리자' 등에게 통보하며 문서 관리자는 이에 따른 문서의 등급 지정을 추진 합니다.
  - (지정시기) 문서생산 단계부터 설정이 가능하나 생산 이후라도 등급 설정이 가능합니다.
- **(문서관리)** 연구기관 문서관리자는 문서등급에 따른 '표기'를 추진하고 연구책임자와 함께 열람권한자, 폐기 등에 대해서도 논의합니다.
  - (표기) 영업비밀*, 대외비 여부 등을 문서 앞면에 표기하고 관리번호를 부여해 누구든지 해당 문서의 중요성을 알 수 있도록 해야 합니다(예: Confidential, 대외비).

    * 공공연히 알려져 있지 않고 독립된 경제적 가치를 가지며 보안등급을 표기하는 등 영업비밀로 관리되고 있다면 「부정경쟁방지 및 영업비밀 보호에 관한 법률」에 의해 '영업비밀'로 인정 가능
  - (보관) 중요 문서에 대해서는 잠금장치가 있는 캐비넷 등에 관리하도록 하고 전자문서의 경우 보안문서 비밀번호 설정 등으로 보호합니다. 이 때 문서의 중요도에 따라 보관을 연구부서에서 할 것인지 연구기관에서 할 것인지도 정합니다.
  - (보존기한) 문서의 보존기한은 연구책임자-문서관리자 간 협의에 의해 설정합니다. 또한 정기적으로 문서 보존 필요성을 검토하여 필요 시에는 폐기하도록 합니다.
  - (활용) 문서의 열람, 복사, 복제는 영업비밀, 대외비 여부 등 문서 성격에 따라 권한이 있는 자에 한하여 허락 되어야 합니다. '문서를 활용한 자(권한을 부여받은 자 포함)'는 문서 기록 대장 등에 활용 현황을 기록해야 합니다. 전자문서일 경우 로그기록을 추적할 수 있도록 시스템화하여야 합니다.
  - (폐기) 문서폐기는 연구기관에서 자체적으로 정한 보존기한까지 문서를 보관하다가 해당 시기에 도달하면 파쇄 및 폐기를 진행합니다.

• 대외비, 영업비밀 보호 필요성 등에 따른 문서 등급화 검토	□Yes □No
• 대외비, 영업비밀 등에 대한 명확한 문서 표기 시행	□Yes □No
• 대외비, 영업비밀 등에 따른 문서 접근자, 외부공개 범위 명확화	□Yes □No
• 문서 등급에 따른 관리방법 설정(보관방법, 보존기한 설정, 활용기록 관리, 폐기방법)	□Yes □No

❷ 연구노트 연구보안

- **(연구노트 정의)** 연구노트는 R&D 수행을 통해 얻은 정보, 데이터, 노하우 등을 체계적으로 기록한 자료입니다.
  - 최근 연구노트 형태는 종이, 전자파일(음성, 영상 포함) 등으로 다양해 졌으므로 연구기관은 이러한 사안을 감안한 관리규정을 연구자에게 제시 합니다.
- **(연구노트 가치)** 연구노트는 그 자체가 '연구개발성과'로 인정받을 수 있으며 '연구진실성 입증, 발명자 보상, 자산유출 시 피해입증' 자료로 활용 가능합니다.
  - 연구자 개인 소유가 아닌 연구기관의 연구개발성과로 귀속됨을 유의합니다.
- **(연구노트 작성·관리)** 연구노트의 가치를 감안하여 연구자는 연구노트를 상시 작성하며 식별번호 부여, 관리대장 작성 등 체계적 관리를 추진해야 합니다.
  - 개별 연구노트에는 간략한 식별자료*를 기재하도록 합니다.

    * 연구노트 번호, 사용 시작 및 종료, 기록자 및 확인자 서명 등 포함
  - 연구책임자는 소속기관 규정에 따라 연구노트 관리대장을 만들고 사전에 연구노트 사용자를 등록해 분쟁 시 연구노트 진위성을 증명할 수 있어야 합니다.
- **(연구노트 회수)** [법] 연구수행 중에 연구노트는 참여연구원이 직접 관리하다 과제종료 후에는 연구노트 관리부서에 제출 합니다. 연구노트의 보존기간은 연구개발과제 종료일로부터 30년입니다.
  - 연구책임자는 연구과제 추진 중 하차하게 된 참여연구원의 연구노트를 회수 합니다.
  - 연구자가 연구노트 분실 시에는 연구책임자에게 즉각 알리고 연구노트 관리부서로부터 신규 연구노트 번호를 발급 받도록 합니다.
- **(연구노트 활용)** 연구자가 연구노트를 제출한 이후, 연구노트 열람·반출·복제에 대해서는 연구기관의 관리 방침을 따라야 합니다.
  - 일반적으로 연구노트의 기록자인 연구자의 열람권을 보장하고 있습니다. 그 외 내부인에게는 보안등급에 따라 열람을 허용할 수 있습니다.
  - 외부로 연구노트의 반출 및 복제는 허용되지 아니하나 연구심의위원회 개최를 통한 결정에 따라 사본 반출도 가능합니다.
  - '비밀유지의무'가 없는 외부인에게는 연구노트 열람을 금하되 '비밀유지서약'을 제출하거나 기관장이 허용하는 경우 연구노트 열람을 허락할 수 있습니다.

③ 연구데이터 연구보안

- **(연구데이터 정의)** 연구데이터는 연구과제 수행 시 각종 실험, 관찰, 조사 및 분석을 통해 산출된 자료로 연구결과의 검증에 필수적입니다.

  – 국가R&D에서 창출된 연구데이터는 연구기관의 소유로 귀속됩니다.

- **(연구데이터 관리계획)** 연구자는 연구과제 성격에 따라 연구계획서 제출 시 데이터관리계획(Data Management Plan)을 작성할 수 있습니다. 이 때 아래와 같이 연구보안 관점에서 데이터관리 계획 전반을 검토해 볼 수 있습니다.

  – 데이터 리포지터리 또는 스토리지 안전성, 장기보존 계획 검토

  – 데이터 수집 및 관리 시 윤리적 문제 검토

  – 데이터 관리, 저장, 공유를 담당할 수 있는 연구자 지정

- **(연구데이터 저장)** 연구데이터 생산 연구자는 데이터관리계획서(DMP)에 명시된 기간 이내에 연구데이터를 연구기관에서 지정하는 시스템에 등록해야 합니다.

- **(연구데이터 공개)** 국가R&D를 통해 창출된 연구데이터는 공개를 원칙으로 하되 연구기관의 담당부서, 전문기관 담당자 등과 협의하여 비공개, 내부공개, 대외공개 등의 공개 기준을 선택할 수 있고 엠바고를 설정할 수 있습니다.

- **(연구데이터 보존·폐기)** 연구데이터 보존 기간은 연구기관에서 방침을 정해 관리해야 하며 폐기 시에는 별도의 위원회를 거쳐야 합니다.

3 연구보안 모의사례

① 연구노트를 비밀로 관리한 사례[4)]

가상상황	• A대학 김교수는 상용화 연구에 열심이다. 최근에는 핸드폰 부품 관련 특수한 소재를 개발하기도 하였으며 특허출원을 앞두고 있다. 김교수는 평소 지식재산 보호를 위하여 관련 소재 연구를 진행하는 학생들의 연구노트에 모두 '대외비' 표시를 하게 하였고 이를 '연구노트 부서'에 별도 관리를 요청하기도 했다. 또한 해당 학생들을 별도의 잠금장치가 되어 있는 연구실에서 근무하게 하였다. • 그러던 어느 날 김교수 실험실에서 근무하던 C학생이 B기업에 취직하였는데 그 기업에서 C학생은 김교수가 상용화 중인 소재분야에 관한 제품개발에 착수하게되었다. 이 소식을 들은 김교수는 해당기업과 C학생을 '영업비밀보호' 침해 금지를 청구하는 소송을 제기하였고 증거물로 연구노트를 제출하였다. 법원은 해당 연구노트를 보고 이는 A대학의 특수한 지식재산을 인정해 주었다.
연구보안 포인트	✓ 연구노트 작성을 생활화하여야 합니다. ✓ 민감한 자료의 '등급표시, 비밀관리'를 추진하므로 상업적 가치가 있는 연구성과를 지킬 수 있습니다.

4) 국가과학기술인력개발원·한국지식재산전략원. (2016), 연구노트의 생활화. (참고하여 사례 재작성)

4 관련 법규 및 매뉴얼

- 국가연구개발사업을 추진하는 연구기관은 소속 연구자들이 체계적으로 문서, 연구노트, 연구데이터를 관리할 수 있도록 하여 대책을 마련해야 합니다.

국가연구개발사업 연구노트 지침(고시)

제2조(정의) 4. "연구노트"란 법 제35조제2항에 따른 연구노트로서 연구개발과제 수행을 통하여 얻은 정보, 데이터, 노하우 등을 체계적으로 기록한 자료를 말한다.

국가연구개발정보처리기준(고시)

제2조(정의) 6. "연구데이터"란 연구개발과제 수행 과정에서 실시하는 각종 실험, 관찰, 조사 및 분석 등을 통하여 산출된 사실 자료로서 연구결과의 검증에 필수적인 데이터를 말한다.
7. "데이터관리계획"이란 연구데이터의 생산·보존·관리 및 공동활용 등에 관한 계획을 말한다.

- 보안과제를 수행하고 있거나 「산업기술보호법」에 따라 '산업기술'을 연구하고 있는 연구기관은 기관의 보안대책에 보안과제 관련 보안등급 표기 정책을 포함 시켜야 합니다.

국가연구개발사업 보안대책

연구기관보안대책에 포함되어야 하는 사항(제4조 관련)
3. 연구개발내용 및 연구개발성과의 보고
가. 보안등급 표기가 필요한 문서 및 데이터의 종류
나. 연구개발성과의 대외 공개 및 제공 시 사전신고 등 확인절차

- 영업비밀로 관리하기 위해서는 비공지성(Secrecy), 경제적 가치(Value), 비밀로 보호했다는 노력(Manageability) 등을 입증할 수 있어야 합니다.[5)]

부정경쟁방지 및 영업비밀 보호에 관한 법률

제2조(정의) 2. "영업비밀"이란 공공연히 알려져 있지 아니하고 독립된 경제적 가치를 가지는 것으로서, 비밀로 관리된 생산방법, 판매방법, 그 밖에 영업활동에 유용한 기술상 또는 경영상의 정보를 말한다..

5) 특허청·지식재산보호원·영업비밀보호센터. (2021), 영업비밀 등급분류 가이드.

02. 논문발표·특허출원·보고서 공개

1 연구보안 위험 포인트

» 국가연구개발사업은 국민의 세금으로 추진된 것이기에 창출된 연구성과를 널리 활용하여 국민에게 혜택이 돌아가도록 하는 것이 원칙입니다.

» 하지만 일부 연구개발성과의 경우 섣부른 공개 시 오히려 소속기관이나 국가에 경제적 손해를 입힐 수 있고 안보 위협이 될 수도 있기에 예외적으로 비공개를 검토해 볼 수 있습니다.

2 권고사항 및 의무

❶ 논문발표·특허출원

- 국가R&D 수행을 통한 논문, 특허 창출에는 별도의 제약이 없으며 오히려 권장되는 활동입니다.
  - 다만, 공지된 기술은 특허출원이 어려운 점을 고려하여 논문작성 및 특허출원 시점을 달리하는 등 전략적 접근이 필요할 수 있습니다.

• 특허출원을 고려한 논문발표 시점 설정	☐Yes ☐No

❷ 과제종료 후 최종보고서 및 연구개발성과정보 공개

- **[법] (공개시점)** 연구개발과제 보고서를 제출한 시점(과제종료 후 60일 이내)으로부터 3개월 이내에 공개가 이뤄져야 합니다.
- **(공개대상)** 공개대상 연구개발성과는 최종보고서 및 '연구성과 관리·유통 전담기관*'에 등록·기탁한 연구개발성과 목록**을 말합니다.

  * 「국가연구개발사업 등의 성과평가 및 성과관리에 관한 법률」 제26조에 따른 기관

  ** 연구개발성과에 관한 정보(혁신법 제17조제2항)를 지칭하며, 혁신법 제2조제6호다목에 따른 연구개발성과의 명칭·종류·소유기관 등을 포함해야 함

- **(공개플랫폼)** 연구개발성과를 통합정보시스템(NTIS, IRIS)에 업로드해야 합니다.

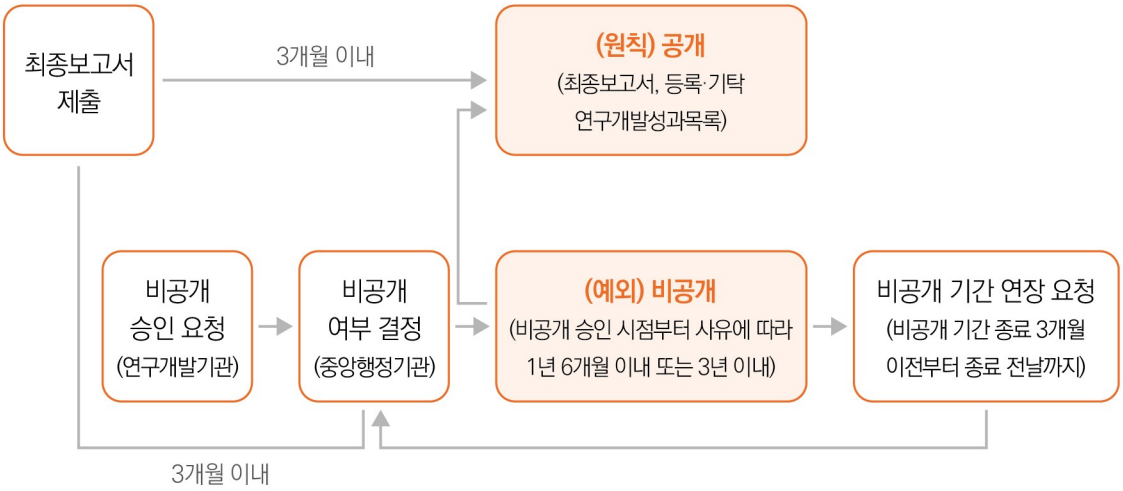
❸ 과제종료 후 최종보고서 및 연구개발성과정보 비공개 및 부분공개

- **(비공개 및 부분공개)** 연구책임자가 연구개발성과의 '부분공개 및 비공개' 필요성을 인지하였다면 전문기관 담당자와 상의하여 요건과 절차에 맞게 '부분공개 및 비공개'를 추진할 수 있습니다.
  - (요건) 혁신법 시행령 제35조제2항 각 호와 같이 '보안 및 상업적 보호' 필요성이 있을 경우 비공개 및 부분공개가 가능합니다.
  - (절차) 연구기관의 장이 중앙행정기관의 장에게 연구개발성과의 전부 또는 일부에 대하여 비공개 승인을 신청할 수 있고, 중앙행정기관의 장은 요청 사유에 따라 최대 3년 이내에서 연구개발성과의 비공개를 승인 할 수 있습니다.

〈표 〉 연구개발성과 비공개 승인을 요청할 수 있는 경우와 기간

상세 내용(혁신법 시행령 제35조제2항 및 제3항)	기간
• 국가핵심기술 관련 연구개발과제(산업기술의 유출방지 및 보호에 관한 법률 제2조 제2호) • 핵심전략기술 관련 연구개발과제(소재·부품·장비산업 경쟁력 강화를 위한 특별조치법 제2조 제3호) • 보안과제로 분류된 연구개발과제 (혁신법 제21조 제2항)	3년 이내
• 연구개발성과에 대해 지식재산권을 취득하려는 경우 • 외국의 정부·기관·단체와의 협정·조약·양해각서 등에 따라 비공개를 요청하는 경우 • 중소기업이 연구개발성과를 임치한 경우 (대·중소기업 상생협력 촉진에 관한 법률 제24조의2) • 기타 영업비밀 보호 등 정당한 사유가 있는 경우	1년 6개월 이내

- 비공개 기간의 연장은 비공개 기간이 끝나기 3개월 전부터 그 기간이 끝나기 전날까지 최초 비공개 승인 요청 절차와 동일하게 신청 가능하며, 비공개 요청 사유에 따른 비공개 기간 범위에서 연장 승인이 가능합니다.



[그림] 연구개발성과의 공개 및 비공개 절차

※ 출처: 혁신법매뉴얼(2024)

• 과제종료 후 연구개발성과 공개 절차 및 내용 확인	□Yes □No
• 보안유지 및 상업적 활용가능성에 따른 연구개발성과 비공개 및 부분공개 필요성 검토	□Yes □No

3 연구보안 모의사례

❶ 논문 발표와 특허 출원의 시점이 맞지 않아 난감한 경우[6)]

가상상황	• A는 박사과정을 받은 지 얼마되지 않은 생명분야 신진 연구자이다. 오랜 연구 끝에 최근 건강에 효능이 높은 물질을 개발하고 효과도 입증하였다. A는 이를 특허로 출원하기 위하여 선행기술조사를 의뢰하였다. • 그런데 A가 1년 전 경에 관련 내용을 학회에서 발표한 포스터 및 자료가 발견 되었으며 해당 자료에는 물질 명칭, 효과도 자세하게 기재되어 있었다. 담당 변리사는 이미 공지된 기술이므로 '신규성' 요건에 문제가 있을 수 있다고 하였다. 변리사는 청구범위를 변경하거나, 공지예외주장 출원(논문발표에 의한 공개 후 1년 이내)을 고려해 보겠다고 하였다.
연구보안 포인트	✓ 특허 출원 계획이 있다면 섣불리 발표해서는 안됩니다. 발표 전에 사업화 담당자 등과 협의가 필요합니다.

4 관련 법규 및 매뉴얼

• 보안과제 뿐 아니라 산업보안, 국방보안에 해당 시 다음 규정을 준수해야 하므로 확인 바랍니다.

구분	법령 내용	근거법
국가핵심기술	• 공공기관은 국가핵심기술 정보 비공개, 필요 시 장관승인	산업기술보호법 제9조의2
방위산업기술	• 성과 공개 시 부서장, 기술보호책임자 승인 필요	방위산업기술보호지침 제16조

• 국가연구개발혁신법 시행령에 따라 보안과제 성과라도 부분공개가 가능합니다.

국가연구개발혁신법 시행령

제18조(연구개발과제 수행 관련 보고서의 세부내용 등) ④ 연구기관과 연구책임자는 법 제12조제4항 및 제5항에 따라 연차보고서·단계보고서 및 최종보고서를 다음 각 호의 구분에 따른 날까지 중앙행정기관의 장에게 제출해야 한다.

1. 연차보고서: 연도별 연구개발기간 종료일까지
2. 단계보고서: 연구개발과제의 각 단계가 끝난 날
3. 최종보고서: 연구개발과제협약 종료일 후 60일

제35조(연구개발성과의 공개 등) ① 연구기관과 연구자는 법 제17조제2항 본문에 따라 최종보고서를 제출한 날부터 3개월 이내에 다음 각 호의 자료를 통합정보시스템을 통하여 공개해야 한다. 다만, 중앙행정기관의 장이 연구개발성과의 특성상 출판이나 학술지 게재가 필요한 경우 등의 사유로 3개월 이내에 공개가 불가능하다고 인정하여 공개 기한을 달리 정한 경우에는 그 기한까지 공개할 수 있다. 〈개정 2022. 6. 28.〉

1. 최종보고서
2. 제33조제3항 본문에 따라 전담기관에 등록·기탁한 연구개발성과 목록

6) 강선준(2023), 국제계약론. 퍼플출판사. (참고하여 재정리)

② 연구기관의 장은 다음 각 호의 어느 하나에 해당하는 경우에는 법 제17조제2항 단서에 따라 중앙행정기관의 장에게 연구개발성과의 전부 또는 일부에 대하여 비공개의 승인을 요청할 수 있다. 〈개정 2023. 12. 5., 2024. 2. 6.〉

1. 「산업기술의 유출방지 및 보호에 관한 법률」 제2조제2호에 따른 국가핵심기술 관련 연구개발과제를 수행한 경우
2. 「소재·부품·장비산업 경쟁력 강화 및 공급망 안정화를 위한 특별조치법」 제2조제3호에 따른 핵심전략기술 관련 연구개발과제를 수행한 경우
3. 법 제21조제2항에 따라 보안과제로 분류된 연구개발과제를 수행한 경우
4. 연구기관의 장이 해당 연구개발성과에 대하여 지식재산권을 취득하려는 경우
5. 외국의 정부·기관·단체와의 협정·조약·양해각서 등에 따라 해당 연구기관의 장이 비공개를 요청하는 경우
6. 「대·중소기업 상생협력 촉진에 관한 법률」 제24조의2에 따라 중소기업이 연구개발성과를 임치한 경우
7. 그 밖에 영업비밀 보호 등 정당한 사유가 있는 경우

③ 제2항에 따른 요청을 받은 중앙행정기관의 장은 다음 각 호의 구분에 따른 기간의 범위에서 연구개발성과의 비공개를 승인할 수 있다.

1. 제2항제1호부터 제3호까지의 규정의 어느 하나에 해당하는 경우: 3년 이내
2. 제2항제4호부터 제7호까지의 규정의 어느 하나에 해당하는 경우: 1년 6개월 이내

④ 연구기관의 장은 연구개발성과의 비공개 기간을 연장해야 할 사유가 있는 경우 제3항에 따라 승인된 비공개 기간이 끝나기 3개월 전부터 그 기간이 끝나기 전날까지 중앙행정기관의 장에게 비공개 기간의 연장을 요청할 수 있다.

⑤ 제4항에 따른 요청을 받은 중앙행정기관의 장은 그 사유를 검토하여 제3항 각 호의 구분에 따른 기간의 범위에서 비공개 기간의 연장을 승인할 수 있다.

03. 회의 참석, 학술발표로 인한 연구내용 대외공개

1 연구보안 위험 포인트

» 연구과제 수행 중 학회 및 회의에서 연구현황, 논문 등을 발표하는 것은 중요한 연구과정 중 하나입니다.

» 연구자가 연구성과를 공개하는 과정 중 예기치 못하게 보호해야 할 연구성과를 공개한 경우 소중한 연구자산이 유출될 위험도 있으므로 사전 검증이 필요합니다.

2 권고사항 및 의무

- 연구자는 소속기관의 방침에 따라 연구책임자, 담당부서와 함께 해당 연구를 대외에 발표해도 괜찮은 것인지에 대해 사전에 긴밀히 논의해야 합니다. 일반적으로 대외공개 시 판단 기준은 아래와 같습니다.
  - **(상업성 검토)** 공개된 기술은 특허등록을 받기 어려우므로, 특허출원 계획이 있다면 관련 내용을 발표하지 않도록 주의해야 합니다. 발표 이전에 소속기관의 '기술사업화 담당부서'와 함께 관련 내용을 논의 합니다. 아래는 상업성 검토를 위한 예시 항목입니다.

• 공개 시 지식재산권 확보에 문제가 있는지 여부 검토	□Yes □No
• 기술상용화를 앞두고 있어 보호할 가치가 있는 지 여부 검토	□Yes □No
• 소속기관에 유무형 손해를 끼칠 수 있는 지 여부 검토	□Yes □No

  - **(보안성 검토)** 발표자료가 국가핵심기술, 전략물자, 방위산업기술, 보안과제와 연관성이 있다고 의심된다면 '연구보안 담당부서'와 함께 상의가 필요합니다. 아래는 보완성 검토를 위한 예시 항목입니다.

• 보안과제 해당 여부 검토	□Yes □No
• 수출통제(전략물자, 국가핵심기술, 방위산업기술) 해당 여부	□Yes □No
• 그 외 국산화를 추진 중에 있어 보호가 필요한 지 여부 검토	□Yes □No

- 연구자는 되도록 충분한 기한을 두고 연구보안 담당부서에 검토를 요청하여야 하며, 필요할 경우 연구보안 담당부서에서는 내·외부 전문가를 활용하거나 연구보안심의회의를 개최하여 공개여부를 결정하도록 하는 절차를 진행하여야 합니다.
  - 특히 국가핵심기술아니 전략물자와 연관성이 있다고 의심되는 경우 관련 법규에 따라 해당 여부를 확인하고, 해외 또는 외국인에게 공개하기 전 허가를 받아야 할 수 있습니다.

3 관련 법규 및 매뉴얼

- 국가연구개발사업을 수행하는 연구기관은 기관의 규정 및 보안대책에 따라 대외 공개에 대한 정책 및 기준을 수립해 두어야 합니다.
- 보안과제를 수행하고 있거나 「산업기술보호법」에 따라 '산업기술'을 연구하고 있는 연구기관은 연구기관보안대책에 연구개발성과의 대외 공개 및 제공 시 사전신고 등 확인절차를 마련해야 합니다.

국가연구개발사업 보안대책

연구기관보안대책에 포함되어야 하는 사항(제4조 관련)

3. 연구개발내용 및 연구개발성과의 보고
   가. 보안등급 표기가 필요한 문서 및 데이터의 종류
   나. 연구개발성과의 대외 공개 및 제공 시 사전신고 등 확인절차

제2장 보안과제 참여연구자의 연구보안

제1절 보안과제 참여 시 주의가 필요한 연구보안 규칙은 무엇인가요?

01. 보안과제 연구자의 보안교육 및 보안서약

1 연구보안 위험 포인트

» 국가연구개발사업의 연구자산 유출은 주로 인력에 의한 암묵지적 지식전파, 고의적 범죄에 의해 발생하는 경우가 많습니다.

» 외부로 유출될 경우 기술적·재산적 가치에 상당한 손실이 예상되거나 국가안보를 위하여 보안이 필요한 보안과제 관련 연구자라면 일반과제 대비 더욱 수준 높은 보안교육을 이수해야 합니다.

2 권고사항 및 의무

- [법] 보안과제 참여 연구자의 경우 의무적으로 기관 내부 또는 외부의 연구보안 교육을 수강해야 하며, 보안서약서를 제출해야 합니다.

• 보안과제 연구자 보안교육 의무 수강	□Yes □No
• 보안과제 연구자 보안서약서 의무 제출	□Yes □No

3 연구보안 모의사례

❶ 보안과제와 무관한 국제공동연구 과정에서의 보안과제 정보 유출

가상상황	• 연구소 기업C에 근무하고 있는 A는 보안과제에 참여하며 보안서약서를 작성하게 되었다. 보안서약 관련 내용은 계약서 중 일부로 되어 있었고 추상적인 내용으로만 구성되어 있었다. 또한 A는 보안서약 관련하여 별도의 설명도 듣지 못하였다. • 1년 후 A는 다른 기업에 이직 하면서 C기업에서 익힌 연구내용과 노하우를 활용하면서 일하게 되었다. 이를 알게 된 C기업 관계자는 A를 영업비밀 침해, 보안과제 성과 유출 등으로 고발하였다. 증거자료로 A와 체결한 보안서약서를 제출 하였다. • 그러나 법원은, C기업이 A와 체결한 보안서약서가 너무 형식적이고 핵심 비밀이 무엇인지 구체적으로 기재되어 있지 않으며, 당사자에게 이에 대한 설명도 제대로 이루어지지 않은 점을 들어, 해당 보안서약서는 실질적인 의미가 있다고 보기 어렵다고 하였다.
연구보안 포인트	✓ 보안서약서에는 비밀로 할 내용을 구체적으로 명시하여 연구자와 관계자들이 명확하게 보안사항을 관리할 수 있도록 합니다.

4 관련 법규 및 매뉴얼

- 보안과제를 수행하고 있거나 「산업기술보호법」에 따라 '산업기술'을 연구하고 있는 연구기관은 보안과제를 수행하는 연구자에 대한 보안교육을 철저히 하고 보안서약을 받아야 합니다.

국가연구개발사업 보안대책

제7조(보안교육 및 보안서약) ① 연구기관의 장은 보안과제를 수행할 예정이거나 수행하고 있는 연구자에 대하여 다음 각 호의 사항을 포함하는 보안교육을 실시하여야 한다.

1. 이 지침에 따른 연구자의 의무 사항
2. 연구기관보안대책에 따른 연구자의 의무 사항
3. 보안과제 수행에 따른 우대조치에 관한 사항
4. 의무사항을 위반할 경우에 법, 「산업기술의 유출방지 및 보호에 관한 법률」, 「대외무역법」에 따라 받을 수 있는 불이익에 관한 사항
5. 그 밖에 보안사고의 예방을 위해 필요한 사항

② 제1항에 따른 교육을 받은 연구자는 연구기관의 장에게 보안서약서를 제출하여야 한다.

③ 제2항에 따른 보안서약서의 서식은 별지 제1호 서식을 따르며, 필요한 경우 연구기관의 장이 그 내용을 준용하여 정할 수 있다.

④ 연구기관의 장은 필요한 경우 보안과제를 수행하지 않는 소속 연구자와 기타 소속 직원에 대해서도 보안교육을 실시할 수 있으며, 특별히 보안상 필요한 경우 서약서를 제출하도록 할 수 있다.

[별표] 연구기관보안대책에 포함되어야 하는 사항(제4조 관련)

1. 보안관리체계
   바. 소속 직원의 보안교육 이수 의무에 관한 사항
   ※ 연구기관보안대책에 따른 연구자의 의무, 우대사항 및 의무사항 위반시 「산업기술의 유출방지 및 보호에 관한 법률」, 「대외무역법」에 따라 받을 수 있는 불이익에 관한 사항과 연구성과에 대한 「산업기술의 유출방지 및 보호에 관한 법률」상 핵심기술 판정 필요성과 후속조치 등
2. 보안과제 참여연구자(연구책임자 및 외국인을 포함한다) 관리
   다. 참여연구자의 국외 출장 시 사전 보안교육 및 귀국보고(출장기간에 접촉한 사람 및 협의 내용 등을 포함한다) 실시

02. 보안과제 연구자의 외국접촉

1 연구보안 위험 포인트

» 보안과제 참여연구원이 연구과제 관련하여 외국인·외국기관과 긴밀한 상호작용을 가진다면, 해당 연구원도 모르게 연구개발 관련 정보와 성과물이 외국에 무단으로 유출될 가능성이 높아질 수 있습니다.

» 보안과제 관련 내용이 해외로 유출될 경우 기술적·경제적 피해가 심각해 질 수 있기에 연구기관장, 중앙행정기관 장, 국정원 등의 현황 파악이 필요합니다.

» 기술적인 판단이 결부되는 만큼, 외국과 접촉 과정에서 언급되거나 전달된 정보가 보안 사항인지에 대해서는 연구자 본인의 진실성과 판단이 중요합니다.

2 권고사항 및 의무

❶ 외국접촉이란

- **[법] (정의)** '혁신법 및 관계법령'에서 외국접촉은 보안과제 참여연구자가 국내 및 해외에서 외국인 및 외국기관 관계자와 보안과제* 관련 상호작용 하는 경우 및 유의미하게 접촉을 반복하는 것을 말합니다.

  * 보안과제는 '주관·공동·위탁과제'를 포함

  - **(접촉 보고자)** 보안과제를 '현재 수행 중이거나 수행한 적(종료 후 3년 이내)'이 있는 연구자라면 주의가 필요합니다.
  - **(접촉 대상)** 대한민국 국적을 가지지 아니한 외국인, 외국법률에 따라 설립된 법인 등을 접촉하였을 때 외국접촉 보고를 고려할 수 있습니다.

    ※ 외국인 : 대한민국 국적을 가지지 아니한 자

    ※ 외국기관 : 외국법률에 따라 설립된 법인(정부·기업·단체 등을 포함)을 말하며 만약 본부(본사)와 지부(지사)의 소재가 다른 경우 본부(본사) 소재지 기준으로 판단

  - **(접촉 내용)** 모든 외국접촉이 보고 대상은 아니며, 유의미하게 보안과제 관련성이 있을 때 외국접촉 보고의 대상이 될 수 있습니다.
  - 유의미한 보안과제 관련성은 보안이 필요한 사항에 국한합니다. 접촉 시점에서 이미 공개되어 보안의 필요성이 없는 정보(접촉 시점에서 출판된 논문, 공개된 특허 등), 보안과제 관련 거래되는 재화, 단순 시장 동향에 대한 대화 등은 외국접촉 보고 대상이라고 보기 어렵습니다.
  - 다만 이러한 사항을 기계적으로 적용하기 어렵고 맥락에 따라 면밀한 검토가 필요합니다. 이를테면, 시장 동향에 대한 대화에서도 보고 대상인 경우와 그렇지 않은 경우가 모두 가능하기 때문입니다.
  - 유의미한 보안과제 관련성이 높은 대화라면 '간단한 질의응답(예/아니오)', '2회 이상 연락'도 외국접촉 보고 대상에 해당할 수 있습니다. 따라서 가급적 보안과제와 관련한 대화*에 주의를 기해야 하며 관련 대화 필요 시에는 기관에 보고를 추진하도록 합니다.

    * 온오프라인 대화 모두 포함

② 외국접촉에 대한 사전 준비

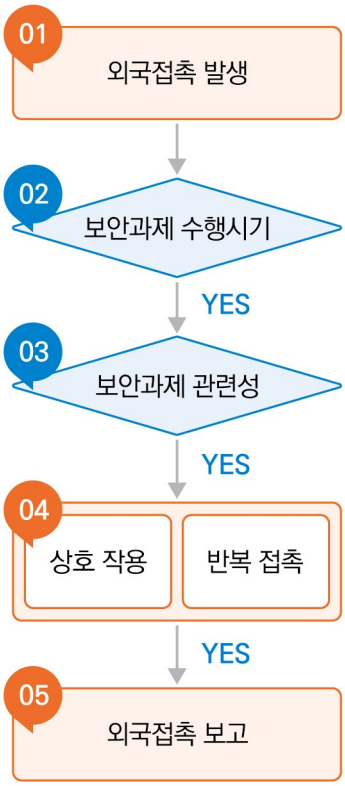
- **(접촉기준 수립)** 연구책임자는 보안과제와 관련해 어느 범위까지 '외국인, 외국기관'과 논의할 수 있을 지 참여연구원들과 토론 합니다.
  - 보안과제 참여연구원들은 외국접촉의 기준과 절차에 대해 사전에 숙지할 수 있도록 합니다.
    ※ 국가핵심기술, 전략물자 등인 경우, 이메일, 전화, 자료전송 등 행위가 기술이전에 해당되어 산업부장관 사전승인이 필요하므로 함께 주의 필요

- **(해외출장 접촉)** [법] 보안과제 연구자의 경우 해외출장 시 연구기관의 자체 보안대책에 따른 보안 교육을 필수적으로 이수해야 하며, 해외 발표자료에 대한 보안성을 검토 받아야 합니다.
  - 해외출장과 같이 외국접촉을 예상할 수 있는 경우, 보안과제 참여연구원(종료 후 3년이내 포함)은 '해외출장 경로, 만나게 될 외국인 및 외국기관'에 대해 사전 보고합니다.
  - 연구보안 담당부서는 해외출장 전 연구자 발표 자료의 보안성 등을 확인합니다.
  - 연구자는 해외출장 귀국 후 귀국보고를 하며 '접촉보고'도 함께 추진합니다.

  ※ 해외출장 유의사항은 1-1-3. 해외출장 참고(p.9)

• 보안과제 연구자 대상 국외출장 사전 교육 수강 여부	☐Yes ☐No
• 해외 발표자료 보안성 검토	☐Yes ☐No
• 연구기관 방침에 따른 해외출장 귀국보고 추진	☐Yes ☐No

- **(국내 접촉)** 해외출장과 같이 외국접촉을 예상할 수 있는 경우도 있지만 국내학회 등 예상 가능하지 않은 시점에 외국접촉이 발생할 수 있습니다.
  - 국내에서 외국인, 외국기관과 보안과제 관련 유의미한 접촉을 하였다면 보고 대상에 해당 합니다.



- **외국접촉**
  - 국내 또는 해외출장 중에 '외국인 및 외국기관 관계자'와 만나 대화한 경우
    * 외국인 : 대한민국 국적을 가지지 아니한 자,
    외국기관 : 외국법률에 따라 설립된 법인(정부·기업·단체 등을 포함)을 말하며 만약 본부(본사)와 지부(지사)의 소재가 다른 경우 본부(본사) 소재지 기준으로 판단
  - SNS, 이메일 등으로 '외국인 및 외국기관 관계자'와 대화하는 경우
- 보안과제* 수행시기
  * 보안과제는 '주관·공동·위탁과제'를 포함
  - 현재 보안과제 수행 참여연구원
  - 보안과제 종료 후 3년 이내인 참여연구원, 퇴사자라면 현재 소속기관, 은퇴자라면 마지막 소속기관에 보고
- 보안과제 관련성 있는 대화 여부 판단
  - 사전에 보안과제 관련 대화 범위를 연구원 간에 설정
  - 단순 통성명, Small talk 제외
- 상호 작용
  - 보안과제 관련 상호질의*·응답(YES·NO 답변 포함)
    * 이미 공개되어 보안이 필요 없는 내용 제외 등 검토
  - 보안과제 '연구개발정보(과제·성과·연구자), 진행상황' 공유
- 반복 접촉
  - 특정 외국인, 외국기관 관계자와 보안과제 관련 지속적인 온오프라인 연락이 2회 이상 반복
- 보안과제 관련 외국접촉 보고
  - 접촉 발생 후 10일 이내에 소속 연구기관에 보고

[그림] 보안과제 관련 외국접촉 판단 기준 및 절차

❸ 연구자의 외국접촉 시 조치사항

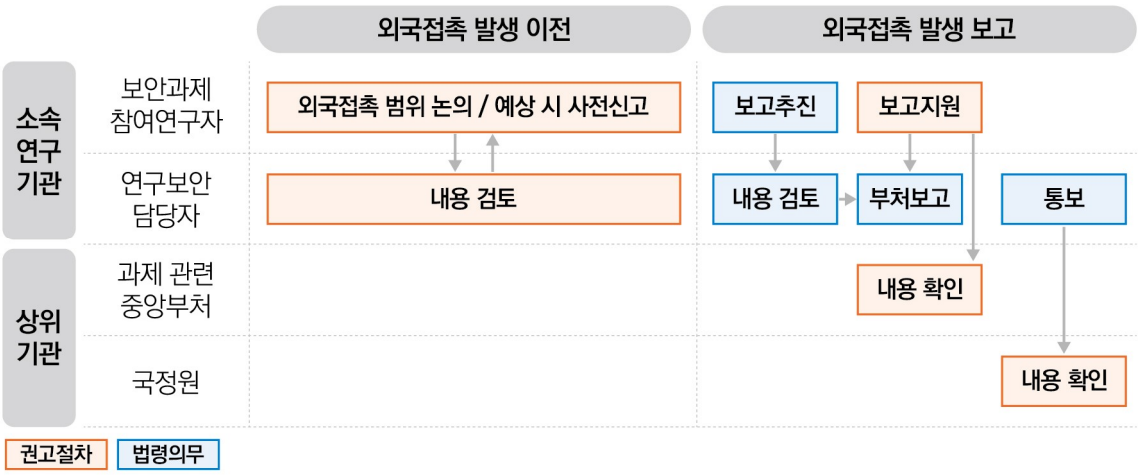
- **(접촉연구자)** [법] 보안과제를 '현재 수행 중이거나 수행한 적(종료 후 3년 이내)'이 있는 연구자의 경우 보안과제 관련 유의미한 외국접촉 시 이를 10일 이내에 소속 연구기관에 보고해야 합니다.
  - 보안과제 종료 후 3년 이내인 참여연구원인 경우, 이직자라면 현재 소속기관에 보고하면 되고 은퇴자라면 마지막 소속기관에 보고하시면 됩니다.
  - 연구자가 보안과제 관련 외국접촉 보고 여부를 판단하기 어렵다면 연구보안 담당부서, 연구책임자에게 도움을 구할 수 있습니다. '외국접촉' 발생 후 10일 이내에 '연구기관'에 보고해야 하므로 빠른 의사결정이 필요합니다.
  - 외국접촉에 대한 보고내용* 및 양식, 보고방법은 기관의 연구보안 담당부서에게 문의하도록 합니다.

    * 참여연구원 성명, 접촉 외국인 성명 및 국적, 접촉 일시·장소·방법·내용 포함
  - 대규모 외국접촉 보고가 발생한 경우, 연구기관의 양식에 따라 연구책임자가 대표로 외국접촉 보고를 진행할 수 있습니다.
  - 만약, 과제 관련 밀접하고 유의미한 외국 접촉으로 연구자산 유출이 의심되는 경우 연구책임자에게 관련 사항을 즉각 알릴 수 있도록 합니다.

• 보안과제 관련 유의미한 해외접촉 발생 시 연구기관에 보고	☐Yes ☐No
• 해외접촉으로 연구자산 유출 의심 시, 연구기관에 보고	☐Yes ☐No

❹ 연구자의 외국접촉 보고 이후 절차

- [법] **(연구보안 담당부서)** 연구자의 보고를 접수한 연구보안 담당부서는 과제 담당 중앙행정기관에 관련 내용을 한달 이내 공문(외국접촉보고서 첨부)으로 보고하도록 합니다.
  - 필요 시 연구자는 관련 내용을 과제 담당자에게 직접 설명할 수 있습니다.
- [법] **(연구보안 담당부서)** 연구보안 담당부서는 국정원에 관련 사실을 이메일, 공문, 문서 등으로 알리도록 합니다.



※ 보안과제에 외국인 또는 외국기관이 참여하는 경우, '3-1-3. 외국인 연구원의 보안과제 참여 (p.52)' 및 '3-2-2. 보안과제 외국기관 참여 (p.64)' 별도참조

3 연구보안 모의사례

❶ 보안과제 연구책임자의 해외접촉 여부 판단 (보고대상 미해당)

가상상황	• 보안과제의 '연구책임자'인 A책임은 해외 학회에서 우연히 동종 분야 외국기업 담당자를 만나 00연료의 국내 공급 일정에 대해서 정보를 공유하였다. 출장에서 돌아와 보니 해당 사항이 보안대책에서 말하는 유의미한 접촉인지 궁금해서 연구보안팀에게 문의하게 되었다. • 연구자A와 연구보안팀 담당자는 00연료 공급 일정에 대한 내용이 일반적인 시장동향에 관한 것으로 보안과제 관련성이 낮다고 판단하고 상황을 종결하였다.
연구보안 포인트	✓ 보안과제 연구자라 할지라도 해외 연구자와 일반적인 시장동향에 대해 이야기 한다면 '보안과제 관련성'이 없어 해외접촉 보고대상이 아닙니다. ✓ 다만, 연료 공급 자체를 물어본다는 것이 보안과제 수행 여부의 신호가 될 수 있으므로 연구진 간에 '보안과제 관련성' 여부에 대한 사전 논의가 중요합니다.

❷ 보안과제 연구책임자의 해외접촉 여부 판단 (보고대상 미해당)

가상상황	• 2024년 1월 미국의 X학회에서 국내 인공지능 기업의 보안과제 연구책임자 C와 중국의 B기업 연구자가 대화를 나누게 되었다. 대화 도중 연구책임자C는 중국 연구자에게 "미국의 T기업의 미국 특허 US20230099999와 유사한 가시광 카메라 기반의 자율주행 기계학습 알고리즘을 특허 출원 중"인 상황이라고 언급 하였다. • 연구책임자 C는 혹시 해당 대화도 외국접촉 보고대상인지 궁금하여 내부 연구진과 논의하게 되었다. 연구진은 해당 특허에 대한 논의는 일반적인 내용이므로 보안과제와 유의미한 관련성이 없다고 결론 내렸다. 또한 연구진의 조사결과 C가 언급한 특허는 T社가 2022년 출원하여 2024년 이미 공개된 특허였고 중국 B社도 이미 회피 특허까지 출원한 상태임을 알게 되었다.
연구보안 포인트	✓ 보안과제 관련 외국접촉은 보안과제와 관련 있는 사항에 대해서만 기관에 신고하는 것입니다. ✓ 보안과제 관련성이 있더라도 모두가 다 알고 있는 특허에 대한 논의를 한다면 유의미한 외국 접촉이라고 보기 어렵습니다. 하지만 이 또한 상황에 따라 다를 수 있으니 연구진 간 검토가 필요합니다.

❸ 보안과제 연구책임자의 해외접촉 여부 판단 (보고대상 해당)

가상상황	• 2025년 2월 미국의 Z학회에서 국내 인공지능 기업 D의 보안과제 연구자 C와 중국의 B기업 연구자가 미국의 T기업 기술개발 현황에 대한 대화를 나누게 되었다. 중국B기업, 미국T기업, 연구자가 속한 한국 D기업 모두 라이다 기술 관련 특허를 출원하였다는 소문이 업계에 파다하여 연구자C는 경각심을 잃어버린 채 대화를 이어나갔다. C는 중국 B기업 연구자에게 우리 회사도 "적외선 라이다 없이 가시광 카메라로 자율주행을 구현하는 기계학습 알고리즘의 특허를 출원하였다"라고 무심결에 말하게 되었다. • 숙소로 돌아온 C는 해당 대화 내용을 연구책임자에게 보고 하였고 연구진 내부에서 해당 대화가 외국 접촉 보고 대상인지에 대해 토론을 시작하였다. C가 언급한 특허는 2024년도에 출원되었고 업계에는 암암리에 알고 있는데 괜찮지 않냐는 내부 의견도 있었다. 그러나 해당 특허는 보안과제에서 창출된 것이고, 2024년 출원 되었으나 아직 공개되지 않은 시점이므로 보안을 꼭 지켰어야 했다고 결론이 났다. C는 외국접촉을 보고 하게 되었으며 해당 대화로 어떠한 파급효과가 있을지 연구진끼리 대책회의를 가지기도 하였다.
연구보안 포인트	✓ 외국인 연구원과 보안과제 관련성이 높은 대화는 되도록 자제 합니다.

4 관련 법규 및 매뉴얼

• 보안과제 뿐 아니라 산업보안, 국방보안에 해당 시 다음 규정을 준수해야 하므로 확인 바랍니다.

구분	법령 내용	근거법
국가핵심기술	• 외국기업에 국가핵심기술 자료 전송·양도·기술지도·위탁연구·인력파견 시 산업부장관 승인	산업기술보호지침 제17조
전략물자	• 정보통신망(전화·팩스·이메일), 구두나 행위 (이전·교육·훈련·실연), 정보처리장치(기록매체·컴퓨터)을 통한 기술이전 시 산업부장관 및 관계부처 승인	대외무역법 시행령 제32조의3

• 보안과제를 수행하고 있거나 「산업기술보호법」에 따라 '산업기술'을 연구하고 있는 연구기관은 보안과제를 수행하는 연구자의 해외출장 및 해외접촉에 대한 규정을 마련해야 합니다.

국가연구개발사업 보안대책

연구기관보안대책에 포함되어야 하는 사항(보안대책 제4조 관련)

2. 보안과제 참여연구자(연구책임자 및 외국인을 포함한다) 관리
   가. 참여연구자의 연구기관보안대책 위반 시 징계에 관한 사항
   나. 퇴직하였거나 퇴직 예정인 자가 반출 또는 반출 예정인 자료에 대한 보안성 검토, 회수, 전산망 접속 차단 등의 조치에 관한 사항
   다. 참여연구자의 국외 출장 시 사전 보안교육 및 귀국보고(출장기간에 접촉한 사람 및 협의 내용 등을 포함한다) 실시
   라. 보안과제를 수행하거나 수행한 적이 있는 연구자의 외국 정부·기관·단체 접촉시 보고 및 외국 정부·기관·단체와의 연구 승인 등에 관련된 절차 및 형식 등 제반사항

- 보안과제 참여 연구자(종료 후 3년 이내 포함)가 외국인과 보안과제 관련 상호작용하는 경우(또는 특정하여 유의미한 정도로 접촉이 반복되는 경우를 말한다.)의 경우, 해당 사실을 10일 내에 기관에 보고해야 합니다.

국가연구개발사업 보안대책

제8조(외국 정부 등과의 접촉 관리 등) ① 보안과제를 수행하고 있거나 수행한지 3년이 지나지 아니한 연구자가 외국에 소재한 정부·기관·단체 또는 외국인 등(본사와 지사의 소재가 다를 때에는 본사 위치를 기준으로 하는 것을 원칙으로 한다)과 보안과제와 관련하여 접촉(연구자가 상호작용하는 경우 또는 특정하여 유의미한 정도로 접촉이 반복되는 경우를 말한다.) 하는 경우에는 해당 접촉일로부터 10일 이내에 접촉 일시·장소·방법·내용 등에 관한 사항을 현재 소속된 연구개발기관의 장(퇴직으로 소속기관이 없거나 법 제2조제3호에 따른 연구개발기관이 아닌 기관으로 이직하는 경우에는 마지막으로 소속되었던 연구개발기관의 장)에게 보고하여야 한다.

② 보안과제를 수행하고 있거나 수행한지 3년이 지나지 아니한 연구자가 외국 정부·기관·단체 등의 지원을 받아 연구개발을 수행하는 경우 사전에 연구보안심의회의 심의를 거쳐 현재 연구자가 소속된 연구개발기관의 장(퇴직으로 소속기관이 없거나 법 제2조제3호에 따른 연구개발기관이 아닌 기관으로 이직하는 경우에는 마지막으로 소속되었던 연구개발기관의 장)의 사전 승인을 받아야 한다.

③ 연구개발기관의 장은 제1항에 따라 보고받은 사항, 제2항에 따라 사전 승인한 사항을 보고 및 승인 후 1월 이내에 중앙행정기관의 장에 보고하고 국가정보원장에 통보한다.

03. 보안과제 연구자의 IT 및 정보기기 사용

1 연구보안 위험 포인트

» 보안과제 수행 시에는 개인용 정보기기, 정보매체, 외부망을 경유한 자료 복사·전송·저장 등에 있어 평상시보다 더욱 주의해야 합니다.

2 권고사항 및 의무

- 보안과제를 수행하는 연구기관의 경우 정보통신망 및 IT 기기에 대한 내용을 포함하여 연구기관보안 대책을 수립해야 합니다.
- 아래는 법률에 따른 일반적인 내용이며 연구자는 반드시 소속 기관의 연구보안 관련 규정을 준수하도록 합니다.

❶ 업무용 개인 정보기기 및 매체관리

- **(기기관리)** [법] 보안과제 연구자의 업무용PC, 스마트폰, 태블릿에 대해서는 로그인 계정을 당사자만이 알도록 하고 타인이 쉽게 추측하지 못하도록 관리해야 합니다. 또한 기관 방침에 따라 꾸준히 보안패치 등을 설치하고 업데이트를 지속해야 합니다.
- **(매체반입)** [법] 보안과제 관련 보호시설에 업무 목적 외의 사전 승인되지 않은 개인용 저장매체*를 반입, 반출할 수 없으므로 연구자는 이에 유의해야 합니다.

  * 모바일 기기(스마트폰, 노트북, 패드류), 저장매체 (CD,DVD 테이프 등), 모든 형태의 카메라 등 촬영기기, USB, USB-C 플래시 드라이브, 외장하드(External HDD), 외장 SSD(External SSD), SD카드, 테이프 등 저장매체 일체

- **(자료반출)** [법] 만약 보안과제 수행 연구자가 보안과제 관련 정보를 개인용 매체(USB 등)에 담아 반출(전송·복사·저장 또는 보관을 포함)하고자 하는 경우에 연구기관에 관련 서약서를 제출해야 하니 연구보안 담당부서에게 문의하시기 바랍니다.

  – 정보통신망, USB 등을 활용하여 보안과제 관련 정보를 외부 반출 시 암호화를 적용하여야 합니다.

- **(기기폐기)** [법] 연구자는 보안과제에 사용된 USB, 스마트폰 기기, 업무용 PC를 폐기해야 할 경우, 임의로 하지 말고 기관의 시설보안 담당자에게 폐기를 요청해야 합니다. 폐기 전에는 자료를 포맷하도록 합니다.

• 업무용 정보기기에 대한 계정 및 비밀번호 관리	☐Yes ☐No
• 업무용 정보기기에 대한 지속적인 보안SW 업데이트	☐Yes ☐No
• 보안과제 관련 보호시설에 반입할 정보기기는 사전 승인	☐Yes ☐No
• USB, 정보통신망을 이용한 정보 반출 시 사전 승인	☐Yes ☐No
• USB, 정보통신망을 이용한 정보 반출 시 암호화	☐Yes ☐No
• 불용 장비, 정보통신매체 등에 대한 안전 폐기	☐Yes ☐No

❷ 분리된 정보통신망 사용

- [법] 보안과제 수행 연구자는 물리적으로 분리된 망을 사용하여야 하며, 연구기관의 승인을 얻어야만 정보망을 통한 연구개발정보의 반출을 허용할 수 있습니다. 다만 이 때에도 암호화를 적용해야 합니다.

• 물리적으로 분리된 망 사용	☐Yes ☐No

❸ 원격 및 재택근무 시 보안 주의사항[7)]

※ ICT 기술을 활용한 근무형태를 말하며 '재택근무, 공유 오피스 근무, 노트북을 활용해 임의 장소에서 일하는 모바일 근무'를 포함

- 보안과제를 수행 중에 있는 연구자의 경우 원격·재택근무 시 '보안과제를 포함한 비밀 및 대외비'에 해당하는 자료를 생산·처리하지 않도록 합니다. 또한 보안과제 수행 연구자가 재택근무를 시행하는 동시에 '영상회의'를 하는 것을 지양해야 합니다.

• 비밀 및 대외비에 해당하는 정보·자료의 생산 및 처리 금지 권고	☐Yes ☐No
• (전용 공간 확보) 개방된 장소가 아닌, 보안성이 확보된 전용 공간에서 원격·재택근무 실시	☐Yes ☐No
• (단말기 보안) 기관에서 제공된 단말기를 사용하여 사내망 접속불특정 다수가 사용하는 PC에서 원격근무 금지	☐Yes ☐No
• (네트워크 보안) 보안성이 확보된 인터넷망 사용	☐Yes ☐No

- 보안과제 연구부서장의 경우, 소속 부서원들이 재택 근무를 수행할 때 연구기관 방침에 따른 보안관리를 추진해야 합니다. 연구부서장은 아래와 같은 사항을 점검하는 것을 고려할 수 있습니다.

• 소속 부서원의 원격·재택근무 계획서 보안 적절성 확인	☐Yes ☐No
• 원격·재택근무자에 대한 보안 유의사항 수시 교육	☐Yes ☐No
• 원격·재택근무자의 보안지침 준수 및 비인가 직무 수행 여부 점검	☐Yes ☐No
• 원격·재택근무자 현황 및 문서반출 기록 유지·관리	☐Yes ☐No
• 원격·재택근무 종료시 반출문서 회수 확인 등 사후 보안조치	☐Yes ☐No

❹ 온라인 회의(영상회의) 시 보안 주의사항

- 보안과제 연구자 간 영상회의를 진행하는 경우 영상회의시스템의 보안성에 대한 연구자-정보보안 담당 부서 간에 철저한 점검이 필요하며 소속 기관의 보안대책을 따라야만 합니다.

※ 1-1-2번의 원격근무 및 온라인 회의 방침은 기본적으로 모두 준수 (p.6)

- 연구기관에서는 보안과제의 영상회의를 통한 유출 가능성 역시 고려하여 필요시 영상회의 서비스에 대해서도 내부망 접근을 차단하는 방안을 고려하여야 합니다.

7) 과학기술정보통신 보안업무 시행세칙에 따른 내용이며, 과학기술정보통신부 산하 기관이 아니더라도 보안과제를 수행하고 있다면 해당 내용을 준용하도록 권고

⑤ 생성형 AI 사용

- 보안과제 연구자가 생성형 AI를 사용하고자 하는 경우, 먼저 소속 연구기관의 정보보안 담당부서에 AI 사용 관련 연구기관의 보안대책, 보안 인프라 구축 정도에 대해 문의하고 이에 걸맞은 사용 범위를 확인하도록 합니다.

  ※ 연구기관이 국가정보원에서 관리하는 각급기관인 경우 '국가 정보보안 기본지침'을 준수하여 AI 사용 필요함

- 보안과제와 관련된 정보 일체를 생성형 AI에 입력하지 않도록 합니다.

  ※ 1-1-1번의 IT 및 정보기기 사용에서 다룬 생성형 AI 관련 지침은 모두 준수(p.4)

3 연구보안 모의사례

① 보안과제 수행 연구자의 원격근무

가상상황	• 보안과제 수행 연구자 B는 원격근무 중 공공장소에서 공용 PC를 사용하여 연구기관의 내부망에 접속하였다. 연구자는 연구자료를 확인한 후 보안 USB에 자료를 다운로드 받아서 활용하였기에 보안수칙을 준수했다고 생각하였다. 추후 연구보안 부서에 확인 결과, 기관 외부에서도 공용PC 대신 업무용 노트북 등을 사용하여 내부망에 접속하고 자료처리할 것을 조언받았다.
연구보안 포인트	✓ 보안과제 연구자는 불특정 다수가 사용하는 PC에서 연구자료를 처리하거나 내부망에 접속해서는 안 됩니다. ✓ 원격근무 중 보안과제 관련 비밀 및 대외비 자료를 생산 및 처리할 수 없습니다. ✓ 연구기관은 연구자들에게 안전한 원격근무 환경을 제공하고, 공용 네트워크 사용을 제한해야 합니다.

② 보안과제 수행 연구자의 개인 스마트폰 분실사례

가상상황	• 연구자 D는 평소 개인 스마트폰으로 소속 기관의 웹메일에 접속하고 스마트폰으로 자료를 자주 다운받아 업무 내용을 확인하는 편이다. • 연구자 D는 어느 날, 개인 여가 생활을 즐기던 중 스마트폰을 분실하고 말았다. 스마트폰 분실로 인해 D는 개인정보 유출 피해 뿐 아니라 소속기관과 연구자의 소중한 지식재산이 유출될 수 있는 위기에 처하게 되었다.
연구보안 포인트	✓ 개인 스마트폰 사용 시 보안설정 미비, 개인의 부주의가 보안사고로 이어질 수 있다는 것을 항상 기억해야 합니다. ✓ 기밀 자료는 보안 인프라가 철저한 환경에서 다루어야 합니다.

4 관련 법규 및 매뉴얼

- 보안과제를 수행하는 연구기관은 정보통신망, 시설장비 등에 대한 관리조치를 의무적으로 수행해야 합니다.

국가연구개발사업 보안대책

연구기관보안대책에 포함되어야 하는 사항(보안대책 제4조 관련)

5. 정보통신망 관리
   가. 보안사고 발생을 예방하기 위한 다음 사항을 포함하는 일반적인 정보통신망 관리 조치
      1) 정보통신망 보호를 위한 방화벽 시스템, 침입탐지시스템 등 각종 보안장비의 설치·운영
      2) 연구기관 외부에서 내부망 접속 시 사용자 인증으로 정보시스템 접근 제한 조치
      3) 업무용 컴퓨터 대상 보안 소프트웨어, 보안패치 등 설치 및 업데이트
      4) 정보시스템 사용기록(최소 6개월 이상) 보관
   나. 보안과제에 대한 다음 사항을 포함하는 강화된 정보통신망 관리 조치
      1) 메신저, 인터넷 저장소, 외부 이메일 등 자료 유출 가능 경로 접속차단
      2) 내부망의 물리적 또는 논리적(방화벽 등) 분리
      3) 정보통신 매체 및 인터넷 등을 이용한 외부 자료 전송 시 사전신고 등 보안조치
      4) 비인가 정보통신매체 사용 금지에 관한 사항
      5) 정보통신매체 폐기 및 외부 이관시 보안조치에 관련된 사항
      6) 직책 및 업무에 따른 각종 전자자료에 대한 차등적 접근권한 부여

- 국가정보원 관리대상인 '각급기관(보안업무규정제2조의제2호)', 과학기술정보통신부 산하 기관은 관련 지침에 따라 정보통신망, IT기기, 원격/재택근무 등의 보안관리를 추진해야 합니다.

국가정보보안 기본지침

제55조(로그기록 유지) ① 각급기관의 장은 정보시스템의 효율적인 통제·관리 및 사고 발생시 추적 등을 위하여 로그기록을 유지·관리하여야 한다.

제56조(업무용 통신단말기 보안) ① 각급기관의 장은 업무용 통신단말기를 이용하여 업무자료 등 중요정보를 소통·관리하고자 할 경우 다음 각 호의 사항을 포함한 보안대책을 수립·시행하여야 한다.

제57조(모바일 업무 보안) ① 각급기관의 장은 휴대폰·태블릿 PC 등을 이용한 모바일 업무환경(내부 행정업무, 현장 행정업무 및 대민서비스 업무 등)을 구축·운용하고자 할 경우 보안대책을 수립·시행하여야 한다.

제59조(원격근무 보안) ① 각급기관의 장은 소속 공무원등이 재택근무, 출장지 현장 근무 또는 파견 근무(제48조의2에 따라 기관 정보통신망 전용(專用) 단말기를 설치 운영하는 경우는 제외한다)시 인터넷을 통해 본인 인증을 거쳐 기관 정보시스템에 접속하여 온라인상으로 업무를 수행(이하 "원격근무"라 한다)하게 할 수 있다.

제61조(저장매체 불용처리) ① 각급기관의 장은 정보시스템 또는 저장매체(하드디스크·반도체 기반 저장장치(SSD) 등)를 외부수리·교체·반납·양여·폐기·불용 처리하고자 할 경우 정보시스템 및 저장매체에 저장된 자료가 외부에 유출되지 않도록 자료 삭제 등 보안조치를 실시하여야 한다. 이 경우 정보시스템 관리자 및 개별사용자는 분임정보보안담당관과 협의하여야 한다.

과학기술정보통신부 보안업무 시행세칙

제20조의2(원격·재택근무 관련 보안준칙) ① 모든 직원은 원격·재택근무시 다음 각 호의 사항을 준수하여야 한다.

1. 비밀 및 대외비에 해당하는 정보·자료의 생산 및 처리 금지
2. 불특정 다수가 사용하는 PC에서 원격근무서비스 접속 금지
3. 업무상 생성된 문서 및 데이터는 업무 종료시 PC에서 완전 삭제하되, 불가피한 경우 비밀번호를 설정하여 저장
4. 접속화면 캡쳐 및 카메라 등을 이용한 촬영 금지, 출력물 생성 최소화
5. OS, 백신 소프트웨어 등 최신 보안 업데이트 및 바이러스 점검 실행
6. 상용 P2P, 메신저, 웹하드, 영상회의시스템 등 사용 금지

② 각 부서장은 해당 부서의 원격·재택근무 보안전담관이 되며, 다음 각 호의 임무를 수행한다.

1. 소속 부서원의 원격·재택근무 계획서의 보안 적절성 확인
2. 원격·재택근무 승인 심사 및 보안서약서 징구
3. 원격·재택근무자에 대한 보안 유의사항 수시 교육
4. 원격·재택근무자의 보안지침 준수 및 비인가 직무 수행 여부 점검
5. 원격·재택근무자 현황 및 문서반출 기록 유지·관리
6. 원격·재택근무 종료시 반출문서 회수 확인 등 사후 보안조치

③ 소속기관 등의 보안담당관은 원격·재택근무 보안관리 실태를 정기적으로 자체평가하고 미비점을 보완하여야 한다.

제51조(중요 정책자료 등에 대한 보안대책) ① 중요 정책 및 사업에 대한 자료로서 누설되는 경우 그 정책 및 사업추진에 지장을 초래할 우려가 있거나, 직무수행 상 특별히 보호가 필요한 사항은 입안(立案)단계에서부터 대외비로 분류하여야 한다.

② 중요 정책 또는 사업의 추진을 위하여 관계자회의 등을 개최하는 기관(부서)의 장은 참여자에 대하여 사전에 보안교육을 실시하고, 회의 시 배부하는 자료는 대외비로 분류하여 회의종료 후 회수하는 등 자료의 유출방지대책을 강구하여야 한다.

③ 제2항의 회의를 영상회의로 진행하는 경우 영상회의시스템의 보안성을 확보하여야 하며, 단계별·분야별 영상회의 운영 보안대책을 마련하여 시행하여야 한다.

04. 보안과제 연구자의 보호지역 출입 관리 및 시설장비 사용

1 연구보안 위험 포인트

» 보안과제 관련 연구장소, 시설장비에 대한 보안관리를 철저히 하므로 보안사고를 예방할 수 있고 참여 연구원들이 안심하고 연구를 수행할 수 있습니다.

2 권고사항 및 의무

❶ 보호지역 관리

- **[법] (구역설정)** 보안과제 관련해서 연구기관은 '보호지역'을 설정할 수 있습니다. 시설보안 담당자는 연구기관 방침에 따라 해당 지역에 대한 출입기록을 관리하며 연구자는 이에 협조해야 합니다.

※ 보호지역 종류 :
① 보안상 중요한 곳으로 외부인 또는 내부 임직원의 출입이 필요할 경우 반드시 관리책임자의 안내를 받아 출입하여야 하는 '제한구역',
② 보안상 매우 중요한 곳으로 원칙적으로 외부인 출입을 불가하고 출입자 확인·통제를 위한 과학보안장비가 설치된 '통제구역(전산실, 비밀보관실 등)'

- **[법] (외부출입)** 만약 해당 보호지역에 외부인 또는 내부 임직원의 출입이 일시적으로 필요한 경우, '보안과제 연구부서장'은 이를 '연구보안 담당부서'에게 알려야 합니다. '연구보안 담당부서'는 해당 인원에 대한 보안서약서 징구, 모바일 기기 반출입 승인, 출입구역 관리 등을 추진 합니다.

• 보호지역 내 출입기록 관리	☐Yes ☐No

❷ 시설장비 관리

- **(시설장비 관리) [법]** 보안과제 관련 공용 시설장비, 정보기기가 존재한다면 연구부서 책임자는 해당 장비, 기기에 대한 관리자를 지정하고 '주기적인 비밀번호 변경, 보안SW업데이트, 로그기록, 정보 반출입 기록' 등을 추진할 수 있습니다.

- **(시설장비 수리)** 보안과제 관련 시설장비를 임대한 뒤 반납, 고장 수리를 위한 외부반출 등 특수사항이 생길 경우, 연구자는 전산장비에 포함된 자료를 필수적으로 삭제해야 하며 시설보안 담당자에게 점검을 요청해야 합니다.

• 보안과제 시설장비 사용 기록 관리	☐Yes ☐No

3 연구보안 모의사례

❶ 상시 출입 용역업체 직원에 대한 출입 허가 절차

가상상황	• 연구부서 C는 연구소 유지보수를 담당하는 용역업체 직원들이 보호지역에 정기적으로 방문할 때마다 절차에 따라 승인 후 출입을 허용하였다. 또한, 해당 업체 직원 방문 시 보안서약서를 별도로 징구하여 연구시설 내 연구자료를 몰래 촬영하는 등 허가되지 않은 행위는 처벌받을 수 있음을 명확하게 확인시켜 연구보안이 유출되는 사건을 예방하였다.
연구보안 포인트	✓ 연구기관은 보호지역 내 정기적으로 방문하는 용역업체 직원 등의 출입을 원칙적으로 금지해야 합니다. ✓ 연구부서는 용역업체 직원이 보호지역에 출입해야 하는 경우 보안서약서를 제출받고 출입 승인 절차를 거치도록 해야 합니다. ✓ 연구보안 담당부서는 보호지역 출입자 리스트를 정기적으로 점검하고, 필요 시 보안점검을 시행해야 합니다.

❷ 보호지역 내에 시설장비 무단 반입

가상상황	• 산학협력 보안과제를 수행하는 A기업의 연구실에 인근 B대학 신규 박사과정 학생이 보안교육을 받지 않은 채, 업무에 투입되었다. • 박사과정 학생은 무심코 자신의 노트북을 A기업 보호지역 내에 반입하려 하였다. 출입구에서 이 사실을 알게 된 A기업 시설보안 담당자는 노트북 반입이 금지됨을 공지 하였다. • A학생은 노트북을 집에다 두고 오기 위해 발걸음을 돌릴 수 밖에 없었다.
연구보안 포인트	✓ 보안과제 참여연구원은 보안교육을 필수적으로 수강해야 합니다. ✓ 보호지역 내에 허가받지 않은 개인 기기를 반입할 수 없습니다.

❸ 보호지역 상시출입자의 신원노출

가상상황	• A대학 박사과정 학생 B는 올해 C출연연과 학연협력 보안과제를 수행하게 되었으며 C출연연의 보호지역에도 상시출입자로써 승인을 받게 되었다. • 학생B는 해당 사실이 너무도 자랑스러워 C출연연의 출입증을 목에 걸고 C출연연 로고와 함께 사진을 찍었다. B학생은 SNS에 사진을 올리며 본인이 국가적으로 중요한 연구를 수행하고 있음을 암시하는 글을 올렸다. • 이것을 목격한 A대학 선배는 B학생에게 해당 행동은 보안과제 수행 연구자의 신원을 노출하여 연구자산 위험 유출을 높이므로 주의가 필요할 것 같다고 경고하였다.
연구보안 포인트	✓ 보안과제 수행 연구자의 경우 사원증, 출입증 등을 철저히 관리할 것을 권고합니다.

4 관련 법규 및 매뉴얼

- 보안과제를 수행하는 연구기관은 '연구기관보안대책'에 시설관리에 대한 내용을 포함시켜야 합니다.

국가연구개발사업 보안대책

연구기관보안대책에 포함되어야 하는 사항(보안대책 제4조 관련)

4. 연구시설 관리
   가. 보안과제 수행에 사용된 노트북, 외장형 하드디스크 드라이브 등 정보통신매체에 대한 출입 절차
   나. 연구개발기관 외곽, 주요 시설물에 폐쇄회로 텔레비전, 침입감지센터 등 장비 등의 설치·운용
   다. 연구개발과제와 관련된 핵심기술 및 정보를 보관하는 전산실 및 중요시설물에 대한 보안관리 조치
   라. 연구실 및 연구개발기관에 대한 출입권한 차등화의 방법·기준, 출입현황 관리 방법 등에 관한 사항
   마. 외부인 및 외부입주기관(벤처기업 포함)의 보안과제 관련 연구시설의 내부 출입통제 조치에 관련된 사항
   바. 화재, 홍수, 재난, 재해 등 비상시 대응계획 수립에 관련된 사항

- 과학기술정보통신부 산하기관이라면 보호지역 보호대책 및 출입통제 관련 규정을 준수합니다.

과학기술정보통신부 보안업무 시행세칙

제55조(보호지역의 보호대책) ②제한구역을 출입하고자 할 때에는 사전에 제한구역 책임자의 승인을 받아야 하며 승인된 자는 안내원이 항시 수행하여야 한다.
③통제구역을 출입하고자 할 때에는 통제구역을 관리하는 보안담당관(분임보안담당관을 포함한다)의 사전 승인을 받아야 하며, 승인된 자는 안내원이 항시 수행하여야 한다. 다만, 동일기관에 소속된 자가 업무수행을 위하여 출입하는 경우에는 통제구역 책임자의 승인을 받고 출입할 수 있다.
제56조(보호지역 내의 출입통제) ①제한구역 및 통제구역은 기관장 또는 보안담당관의 승인을 받아 출입이 허용된 자(이하 "상시출입인가자"라 한다) 이외의 출입을 통제하되, 출입통제대장(별지 제25호 서식)를 비치하여 출입상황을 기록·유지하여야 한다. 다만, 장기간 동일 제한구역 및 통제구역에 출입하는 경우에는 출입기간을 명시하고 1회만 기록할 수 있다.
③보호지역에 대해서는 일반인의 출입을 제한할 수 있는 보안대책을 수립·시행하여야 하며, 제한구역 및 통제구역에는 그 구역의 기능 및 구조에 따라 다음 각 호의 대책이 마련되어야 한다.
1. 출입할 수 있는 사람의 지정과 비인가자에 대한 출입 통제대책
   (자동잠금장치, 카드키, 지문인식시스템 등)
2. 주야간 경계대책
3. 외부로부터의 투시, 도청 및 파괴물질의 투척 방지 대책
4. 방화대책
5. 경보대책
6. 그 밖에 필요한 보안대책

제2절 보안과제 연구산출물 및 성과를 어떻게 관리해야 하나요?

01. 보안과제 창출 문서·데이터·연구노트 보안등급 구분

1 연구보안 위험 포인트

» 보안과제 수행 도중 생성되는 '문서, 연구노트, 데이터'에는 보안성을 요구하는 자료 및 일반적인 자료가 혼재되어 있습니다.

» 생성 단계부터 철저한 기밀 유지가 필요한 자료, 외부 공개 시에 문제가 되지 않는 자료 등을 구분하여 '보안'과 '성과활용'의 균형을 찾을 수 있도록 합니다.

2 권고사항 및 의무

❶ 보안등급 분류 기준 마련

- [법] 연구기관은 연구기관의 보안대책에 따라 보안과제 연구과정 중 창출된 '문서(연구노트·데이터 포함)'의 '보안등급'을 기준을 수립할 수 있습니다.

※ 기본적인 정의 및 내용은 1-2-1. 문서·데이터·연구노트 관리 참고 (p.14)

- 보안등급 분류 기준은 연구기관 자율로 정할 수 있으며 아래 표와 같은 기준 등을 고려해 볼 수 있습니다.
- 보안문서 등급에 따른 접근권한자, 관리자, 열람가능자를 지정할 수 있으며 경우에 따라 공개범위 설정 등에 대해서도 논의할 수 있습니다.

〈보안과제에서 창출된 보안문서의 보안등급 분류기준(예시)〉

구분	내용	접근가능자(예)	공개범위(예)
Ⅰ급 비밀	• 유출될 경우 대한민국과 외교관계가 단절되고 전쟁을 일으키며, 국가의 방위계획·정보활동 및 국가방위에 반드시 필요한 과학과 기술의 개발을 위태롭게 하는 등의 우려가 있는 보안과제의 핵심적인 정보	생산자, 과제책임자, 부서장	외부유출 절대 금지
Ⅱ급 비밀	• 유출될 경우 국가안전보장 및 국가경쟁력 확보에 막대한 지장을 끼칠 우려가 있는 보안과제의 핵심적인 정보로 문서나 전자매체 유출이 과제 중요사항의 직접적 유출로 이어질 수 있는 경우	생산자, 과제책임자, 부서장	중앙행정기관 승인 후 공개
Ⅲ급 비밀	• 유출될 경우 국가안전보장 및 국가 경쟁력 확보에 해를 끼칠 우려가 있는 보안과제의 핵심적인 정보로 문서나 전자매체 유출이 과제 중요사항의 직접적 또는 간접적인 유출로 이어질 수 있는 경우	생산자, 과제책임자, 부서장	중앙행정기관 승인 후 공개
대외비	• 연구 비밀에 속하지 않으나 누설될 경우 간접적으로 손실을 초래할 수 있는 문건 (상기 비밀 외 중요 정보, 관련자 외 공개가 제한되는 정보 등) • 공개되지 아니한 정보이면서 경제적 가치가 있는 정보	생산자, 과제책임자, 부서장, 지식재산 담당자	특허출원 후 공개
일반	• 상기 외 보호조치가 필요하지 않은 문건 자료	연구기관 소속직원	학회발표 가능

※ 참고: 보안대책(고시) 제10조 및 과학기술정보통신부 보안업무 시행세칙 제4장을 참고하여 재정리한 부분

❷ 보안등급 분류 과정

- **(분류 주체)** 보안문서의 생산자(연구자)와 연구책임자는 연구기관 보안대책에 따른 보안문서 등급분류 기준에 근거하여 문서를 분류 합니다.
- **(분류 주의사항)** 보안등급은 문서 가치에 따라 적정 분류가 이뤄지도록 하고 개별 문서 별 독립적 분류를 추진해야 합니다.
  - (적정 분류) 보안문서를 과대하게 분류하여 과다 보호가 되지 않도록 주의해야 하며 과소 분류로 정보 유출 가능성을 높여서는 안됩니다.
  - (독립 분류) 관련 문서를 연관지어 추정 분류하지 말고 개별 문서에 포함된 연구내용 및 정보, 가치에 따라 독립적으로 분류 합니다.
- **(등급 조정)** [법] 연구기관은 보안과제 종료 시 성과물의 보안등급 조정에 대해 다시 고려해 볼 수 있습니다.
  - 기존 보안등급이 높은 문서의 등급을 하향한다던지 보안등급이 낮은 문서를 상향 등급화하여 관리할 수 있습니다.

❸ 보안등급 분류 절차

- **(최상위 등급 분류)** 최상위 보안등급의 경우 연구책임자가 연구보안심의회의에 요청하여 등급을 지정 합니다.
  - 또는 연구책임자의 판단으로 등급분류가 어려운 경우에도 연구보안심의회의에 등급분류를 요청할 수 있습니다.
- **(그 외 보안등급)** 연구책임자의 자율적 판단에 의지하되 해당 내용을 연구관리자, 연구보안 부서에 통보해야 합니다.

❹ 보안등급 별 관리

- **(관리 전반)** 보안등급 별 표기, 보관장소 및 주체 결정, 활용, 폐기 등 문서관리 전반은 1-2-1의 내용을 기본적으로 모두 준용 합니다.

  ※ 기본적인 정의 및 내용은 1-2-1. 문서·데이터·연구노트 관리 참고 (p.14)
- **(주의 사항)** 보안과제에서 창출된 보안문서의 경우 일반문서에 대비하여 보관, 활용, 폐기에 보다 주의를 기울여야 합니다.
  - (표기) 모든 보안등급 별 명확한 '표기'를 추진합니다. 상위 등급의 보안문서를 이메일로 주고 받을 경우에는 이메일 상에도 보안등급을 표기하여 수신자에게 알리도록 합니다.
  - (보관) 최상위 등급의 보안문서의 경우에 연구실에서 관리하기 보다는 기관의 보안담당자의 책임하에 보호장비가 설치된 안전한 장소에서 보관 합니다.
  - (활용) 보안문서 등급별로 접근 가능자를 철저히 제한하며 권한을 부여받은 자 일지라도 활용 기록을 철저히 남기도록 합니다. 원칙적으로는 보안과제에서 창출된 문서의 경우 복사 등을 금하는 것이 바람직 합니다.
  - (폐기) 연구기관에서 정한 보존기한 만료 시기에 도달하면 문서책임자, 연구책임자, 보안관리자의 상의 하에 문서 폐기를 결정합니다. 연구기관에서 정한 최상위 등급 문서의 경우 기관의 연구보안 책임자 등의 입회하에 물리적, 영구적으로 문서를 폐기 하도록 합니다.

3 연구보안 모의사례

❶ 보안등급을 메일에 표기하는 규칙의 연습

가상상황	• 미국 A기관으로 파견 간 김박사는 해당 기관의 특수한 문서관리에 대해 교육을 받았다. A기관은 보안문서를 4등급으로 나누고 있었고 해당 보안문서 등급에 따라 이메일을 보낼 때도 등급표기를 해야 한다고 하였다. 특히 가장 보안등급이 높은 문서를 보낼 때에는 꼭 비밀 번호를 설정해야 하는 규칙이 있었다. 자유로운 대학생활을 주로 하였던 김박사는 보안등급을 표기하는 게 많이 헷갈리긴 했지만 구성원 모두가 따르는 분위기라 금방 적응할 수 있었다.
연구보안 포인트	✓ 만약 소속 기관에 보안문서를 다루는 규칙이 있다면 이를 따를 수 있도록 합니다.

4 관련 법규 및 매뉴얼

• 보안과제 뿐 아니라 산업보안, 국방보안에 해당 시 다음 규정을 준수해야 하므로 확인 바랍니다.

구분	법령 내용	근거법
보안과제	• 보안등급세분화, 접근권한 설정	국가연구개발사업 보안대책 제10조, 과학기술정보통신부 보안업무 시행세칙 제52조 등
국가핵심기술	• 보호등급 부여, 취급인력 권한관리, 암호화, 이력유지관리, 자료반출 승인	산업기술보호법 제10조, 산업기술보호지침 제3장
방위산업기술	• 일반기술과 방위산업 기술을 표시·보관	방위산업기술 보호지침 제14조

• 국가연구개발혁신법에 따라 보안과제를 수행하는 연구기관은 보안문서 등급 관리에 대한 기준을 수립하고 관리하도록 합니다.

국가연구개발사업 보안대책

제10조(보안등급 표기) ① 연구기관의 장은 보안과제 수행과정에서 산출되는 문서와 다양한 형식의 자료 및 데이터에 대하여 추가적인 보안이 필요한지 여부를 판단하고, 추가적인 보안이 필요한 경우 보안등급을 구분하여 표기하여야 한다.

② 연구기관의 장은 연구기관보안대책에 따라 보안등급의 구분을 자율적으로 정할 수 있다. 다만, 보안등급을 정하기 어려울 경우 다음 각 호와 같은 구분을 준용할 수 있다.

1. Ⅰ급 : 유출될 경우 대한민국과 외교관계가 단절되고 전쟁을 일으키며, 국가의 방위계획·정보활동 및 국가방위에 반드시 필요한 과학과 기술의 개발을 위태롭게 하는 등의 우려가 있는 보안과제의 핵심적인 정보
2. Ⅱ급 : 유출될 경우 국가안전보장 및 국가경쟁력 확보에 막대한 지장을 끼칠 우려가 있는 보안과제의 핵심적인 정보로 문서나 전자매체 유출이 과제 중요사항의 직접적 유출로 이어질 수 있는 경우
3. Ⅲ급: 유출될 경우 국가안전보장 및 국가 경쟁력 확보에 해를 끼칠 우려가 있는 보안과제의 핵심적인 정보로 문서나 전자매체 유출이 과제 중요사항의 직접적 또는 간접적인 유출로 이어질 수 있는 경우

③ 제1항에 따라 보호가 필요한 문서의 종류와 보안등급에 관한 사항은 연구기관보안대책으로 정한다.

02. 보안과제 연구개발성과 외부공개

1 연구보안 위험 포인트

» 국민경제 및 안보위협이 되지 않으면서 국민에게 혜택이 돌아갈 수 있도록 보안과제에서 창출된 연구성과의 공개를 결정 합니다.

2 권고사항 및 의무

❶ 보안과제 논문·특허 출원

- 보안과제 관련 '주관/공동/위탁 및 용역기관'은 특허출원 및 논문발표에 주의를 기울어야 합니다.
  - 연구책임자는 해당 과제를 발주한 중앙행정기관(또는 전문기관)의 담당자, 연구보안 담당부서와 함께 어디까지 특허출원, 논문발표가 가능할지 논의해야 합니다.
  - 연구기관의 보안대책에 따른 보안등급별 논문발표, 특허출원 기준이 존재한다면 이를 따릅니다.

❷ 과제종료 후 최종보고서 및 연구개발성과정보 공개

- 보안과제에 해당할 경우 '최종보고서 및 연구개발 성과'의 '비공개 및 부분공개'가 가능하므로 연구책임자는 요건과 절차에 맞춰 적절한 성과공개를 추진합니다.

  ※ 기본적인 내용은 1-2-2. 논문·특허출원·보고서 공개 참고 (p.18)

  - 보안과제라 할지라도 자동으로 과제 전체가 자동으로 비공개 되는 것이 아니며 전문기관 담당자와 협의하여 적절한 공개 수준을 결정하고 비공개 신청 절차를 진행해야 합니다.

• 보안과제 논문, 특허 출원 시 전문기관 담당자와 상담 추진	☐Yes ☐No
• 보안과제 성과 비공개 및 부분공개 시 전문기관에 관련 사항 문의	☐Yes ☐No

3 연구보안 모의사례

❶ 보안과제 일부 성과만 공개하는 경우

가상상황	• C 출연연 보안과제의 위탁연구개발과제를 진행하고 있는 A교수는 과제 종료를 앞두고 막바지 작업을 진행하고 있다. 마침 주관기관인 C 출연연으로부터 해당 과제의 '최종보고서'가 '비공개'될 예정이라는 이야기를 듣게 되었다. A교수는 승진심사를 앞두고 있어 논문실적이 하나라도 중요한데, 논문도 내지 못할까봐 걱정이 되기 시작하였다. A교수는 연구관리팀에 이런 상황에 대해 공유하게 되었다. • 연구관리팀 담당자는 혁신법시행령제35조제2항의 개정(24.2.6)에 따라 연구개발성과의 부분공개가 가능함을 안내하며 최종보고서 제출 시, 연구개발성과 비공개 승인신청을 함께 하자고 제안하였다. • A교수는 위탁연구 보고서 제출 시점에 '비공개 승인신청서'를 해당 전문기관에 제출하였으며 이에 대해 C출연연에게 설명하였다. 전문기관은 A교수의 의견을 받아들여 위탁연구개발 부문만 보고서가 공개되었으며 A교수는 무리없이 논문을 발행할 수 있었다.
연구보안 포인트	✓ 혁신법시행령제35조제2항에 따라 보안과제 성과의 일부 공개도 가능합니다.

4 관련 법규 및 매뉴얼

- 보안과제 뿐 아니라 산업보안, 국방보안에 해당 시 다음 규정을 준수해야 하므로 확인 바랍니다.

구분	법령 내용	근거법
국가핵심기술	• 공공기관은 국가핵심기술 정보 비공개, 필요 시 장관승인	산업기술보호법 제9조의2
방위산업기술	• 성과 공개 시 부서장, 기술보호책임자 승인 필요	방위산업기술 보호지침 제16조

- 국가연구개발혁신법 시행령에 따라 보안과제 성과라고 하더라도, 보안성이 낮은 부분에 대해서는 절차에 따라 신청하여 부분공개가 가능합니다.

국가연구개발혁신법 시행령

제35조(연구개발성과의 공개 등) ① 연구기관과 연구자는 법 제17조제2항 본문에 따라 최종보고서를 제출한 날부터 3개월 이내에 다음 각 호의 자료를 통합정보시스템을 통하여 공개해야 한다. 다만, 중앙행정기관의 장이 연구개발성과의 특성상 출판이나 학술지 게재가 필요한 경우 등의 사유로 3개월 이내에 공개가 불가능하다고 인정하여 공개 기한을 달리 정한 경우에는 그 기한까지 공개할 수 있다. 〈개정 2022. 6. 28.〉

1. 최종보고서
2. 제33조제3항 본문에 따라 전담기관에 등록·기탁한 연구개발성과 목록

② 연구기관의 장은 다음 각 호의 어느 하나에 해당하는 경우에는 법 제17조제2항 단서에 따라 중앙행정기관의 장에게 연구개발성과의 전부 또는 일부에 대하여 비공개의 승인을 요청할 수 있다. 〈개정 2023. 12. 5., 2024. 2. 6.〉

1. 「산업기술의 유출방지 및 보호에 관한 법률」 제2조제2호에 따른 국가핵심기술 관련 연구개발과제를 수행한 경우
2. 「소재·부품·장비산업 경쟁력 강화 및 공급망 안정화를 위한 특별조치법」 제2조제3호에 따른 핵심전략기술 관련 연구개발과제를 수행한 경우
3. 법 제21조제2항에 따라 보안과제로 분류된 연구개발과제를 수행한 경우
4. 연구기관의 장이 해당 연구개발성과에 대하여 지식재산권을 취득하려는 경우
5. 외국의 정부·기관·단체와의 협정·조약·양해각서 등에 따라 해당 연구기관의 장이 비공개를 요청하는 경우
6. 「대·중소기업 상생협력 촉진에 관한 법률」 제24조의2에 따라 중소기업이 연구개발성과를 임치한 경우
7. 그 밖에 영업비밀 보호 등 정당한 사유가 있는 경우

③ 제2항에 따른 요청을 받은 중앙행정기관의 장은 다음 각 호의 구분에 따른 기간의 범위에서 연구개발성과의 비공개를 승인할 수 있다.

1. 제2항제1호부터 제3호까지의 규정의 어느 하나에 해당하는 경우: 3년 이내
2. 제2항제4호부터 제7호까지의 규정의 어느 하나에 해당하는 경우: 1년 6개월 이내

④ 연구기관의 장은 연구개발성과의 비공개 기간을 연장해야 할 사유가 있는 경우 제3항에 따라 승인된 비공개 기간이 끝나기 3개월 전부터 그 기간이 끝나기 전날까지 중앙행정기관의 장에게 비공개 기간의 연장을 요청할 수 있다.

⑤ 제4항에 따른 요청을 받은 중앙행정기관의 장은 그 사유를 검토하여 제3항 각 호의 구분에 따른 기간의 범위에서 비공개 기간의 연장을 승인할 수 있다.

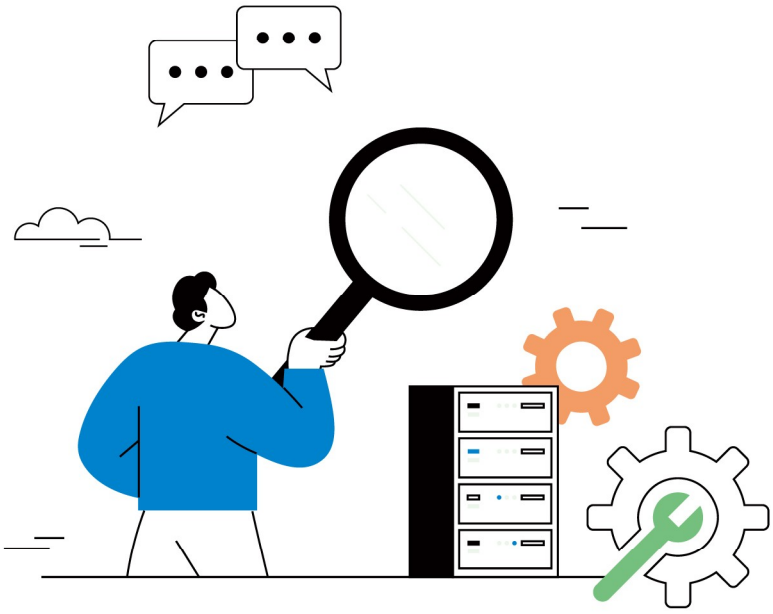
- 보안과제를 수행하는 연구기관은 연구기관보안대책에 연구개발성과의 대외 공개 및 제공 시 사전신고 등 확인절차를 마련해야 합니다.

국가연구개발사업 보안대책

연구기관보안대책에 포함되어야 하는 사항(제4조 관련)

3. 연구개발내용 및 연구개발성과의 보고
   가. 보안등급 표기가 필요한 문서 및 데이터의 종류
   나. 연구개발성과의 대외 공개 및 제공 시 사전신고 등 확인절차

PART 02



주요 상황 별 연구보안 원칙

제3장 국제공동연구 추진 시 연구보안

제1절 외국인 연구원과 일하게 되었어요!

01. 외국인 연구원의 연구부서 배정

1 연구보안 위험 포인트

» 연구기관들의 채용 형태가 다변화되고, 구성원의 국적 또한 다양해지며 연구기관에 외국인이 상주하는 경우가 많아졌습니다.

» 이 경우 동일한 기관이라는 소속감과 친밀감 때문에 자신도 모르게 중요 정보를 누출하여 연구개발정보 및 성과가 국외로 유출될 가능성이 있습니다.

» 다양한 근무 형태(정직원, 학생연구원, 방문연구원 등)의 외국인과 근무하게 될 경우에 대비하여 적절한 보안조치를 수립해 두는 것이 중요합니다.

2 권고사항 및 의무

❶ 외국인 채용

- **(신원조사 및 보안교육)** 연구기관은 외국인 채용 시 신원조사, 보안준수 사항이 명시된 보안서약서 징구, 보안 교육 등을 추진해야 합니다. 연구부서장(또는 연구책임자)은 해당 절차가 제대로 이뤄졌는지 인사담당 부서 등에 재확인할 수 있습니다.

• 외국인 연구원의 신원, 보안교육, 보안서약 등 재확인	☐Yes ☐No

- **(접근권한 설정)** 연구부서장은 외국인 연구원이 배속되기 전에 연구기관의 내부 정보, 시설 등에 대한 외국인의 접근권한을 어디까지 허용할 것인지에 대해 연구보안, 시설보안, 인사 담당부서 등과 논의하고 결정해야 합니다.
  - 시설보안 및 정보보안 담당자는 외국인의 접근 제한이 이뤄질 수 있도록 시스템을 마련 합니다.
  - 만약, 부서에서 보안과제를 수행하고 있거나 전략물자·국가핵심기술·비밀문서 등에 해당되는 문서를 다루고 있는 경우 부서장은 해당 문서에 대한 외국인 접근을 제한할 수 있도록 대책을 강구해야 합니다.

  ※ 보안과제 수행부서에 외국인이 상주하게 되는 경우에 대해서는 '3-1-4. 보안과제에 외국인이 상주하는 경우(p.57)'에서 자세히 다루니 참고하시기 바랍니다.

• 외국인이 허가된 구역만 출입할 수 있는 출입증 발급	☐Yes ☐No
• 외국인의 내부 정보 접근 제한 사전 설정 여부 검토	☐Yes ☐No
• 보안과제, 국가핵심기술, 전략물자 등에 따른 제한 필요한 문서 등 검토	☐Yes ☐No

- **(R&D 일반교육)** 연구부서장은 부서에 배속된 외국인에게 지식재산권 관련 기본법령, 연구성과 공개에 관한 사항, 데이터 공유 시 유의 사항에 대해 설명해야 합니다.

• 국가R&D 성과소유권이 기관에 있음을 설명	☐Yes ☐No
• 연구개발성과 발표 전에 적절한 보안성 검토 및 내부절차 준수가 필요함을 안내	☐Yes ☐No
• 연구개발성과의 무단 반출 금지에 대한 사안 안내	☐Yes ☐No

❷ 외국인 퇴사 및 과제참여 종료

- **(자료회수)** 외국인의 과제참여 종료 및 퇴사 시에 연구부서장은 연구보안 담당자와 함께 외국인으로부터 각종 연구자료, 성과물, 연구노트를 회수해야 합니다.
- **(자료반출 시 보안검토)** 만약 외국인이 외부로 자료, 시료 등을 반출할 예정이라면 연구부서장은 이에 대한 보안성을 검토하고 승인을 진행 합니다.
- **(반출이력 검토)** 정보보안, 시설보안 담당자 등은 외국인의 퇴사 시기 전후로 대용량 연구자료 반출입, 인쇄이력이 있지 않은지 연구부서장은 해당 내용을 함께 확인합니다.
- **(접근권한 제한)** 정보보안, 시설보안 담당자 등은 연구시설·장비 및 정보 등에 한 접근이 신속히 제한되도록 합니다.
- **(보안서약)** 연구보안 담당자는 외국인에게 연구기밀에 대한 보안유지 의무를 고지하며 위법 행위 처벌 등이 포함된 영문 보안 서약서를 징구 합니다.

• 퇴사/과제참여 종료 시 관련 자료 회수	☐Yes ☐No
• 퇴사/과제참여 종료 시 자료 반출 이력 검토	☐Yes ☐No
• 퇴사/과제참여 종료 시 정보 및 시설 관련 접근 제한	☐Yes ☐No
• 퇴사/과제참여 종료 시 보안서약 징구	☐Yes ☐No

3 연구보안 모의사례

❶ 채용 시 신원검증을 하지 않은 사례

가상상황	• D연구기관은 우수 인재 확보 차원에서 외국인 연구원 A를 채용하였다. 그러나 채용 과정에서 A에 대한 신원조사와 보안서약서 징구를 소홀히 하였고, 보안교육도 실시하지 않았다. 채용 후 A는 연구기관의 핵심 연구자료에 접근할 수 있었으며, 이를 외부로 유출하는 사고를 일으키고 말았다. 조사 결과, A가 전에도 유사한 보안 사고를 일으킨 전력이 있었으나 채용과정에서 신원조사를 하지 않아 이를 확인하지 못한 것으로 나타났다.
연구보안 포인트	✓ 외국인 채용 시 철저한 신원조사를 통해 과거 이력과 보안위험 요소를 확인해야 합니다. ✓ 채용 시 보안 준수사항이 명시된 보안서약서를 연구자에게 징구하여 보안의무를 명확히 하도록 합니다. ✓ 외국인의 내부 정보 및 시설 접근권한을 별도로 설정하고, 필요 시 연구보안 담당부서와 협의하여 결정해야 합니다.

4 관련 법규 및 매뉴얼

- 국가연구개발사업을 수행하는 연구기관이라면 자체적으로 국내외 참여연구원에 대한 보안관리대책을 수립합니다.
- 과학기술정보통신부 산하의 연구기관이라면 관련 규정을 준용하여 외국인 참여연구원을 관리하도록 합니다.

과학기술정보통신부 보안업무 시행세칙

제22조(외국인 공직임용 관련 보안대책) ① 외국인을 공무원으로 임용하는 경우 임용 30일전 까지 국가정보원에 신원조사를 요청하여야 하며, 신원 특이사항 발생시 보안심사위원회의 심의를 거쳐 임용 여부를 결정하여야 한다.
② 외국인과 고용계약을 체결할 때에는 근무 중 알게 된 기밀사항을 계약기간중이나 계약만료 후에 누설할 경우의 손해배상책임과 피고용인 업무의 한계설정 등 보안유의사항을 명시하여 계약서를 작성하여야 하며, 보안담당관이 서약을 집행하여야 한다.
③ 보안담당관은 공직에 임용된 외국인에 대해 보안교육을 포함한 공직자로서의 기본자세 및 보안준수 등 의무사항에 대한 기본교육을 실시하여야 한다.
④ 국가 중요정책 등 민감한 내용을 다루는 회의의 주재자는 외국인 공직자의 참석여부를 신중히 결정하여야 하며, 회의 종료 후 외국인 공직자에게 보안 유의사항을 명확히 알려주어야 한다.
⑤ 외국인에게 상시적으로 비밀취급 인가를 부여하는 것은 극히 제한해야 하며, 외국인을 대상으로 열람 등 비밀 취급이 반드시 필요한 경우에 한해 규칙 제46조제1항에 따라 일시적인 비밀 열람·취급을 허용할 수 있다.
⑥ 보안담당관은 재직 중인 외국인이 퇴직할 경우에는 업무기간 중 지득한 비밀 등 중요자료에 대한 누설 및 사적이용 금지를 내용으로 하는 보안서약서를 집행하여야 하며, 각종 자료의 무단반출 여부를 확인하여야 한다.

- (우려거래자 검토) 산업통상자원부에서 고시하는 우려거래자 목록에 외국인 연구원이 포함되어 있는지를 확인해야 합니다.

02. 일반과제에 외국인 연구원 참여

1 연구보안 위험 포인트

» 외국인 참여 연구원이라도 우리나라의 연구보안 제도 전반에 대해 숙지할 수 있도록 교육해 안전하고 윤리적인 연구환경을 만들어갈 수 있도록 해야 합니다.

2 권고사항 및 의무

- **(연구보안 문화)** 연구책임자(또는 부서장)는 외국인 연구원을 포함한 모든 참여연구원들이 온·오프라인 연구보안 교육을 수강할 수 있도록 지원하며 연구보안 준수 분위기가 조성될 수 있도록 합니다.
- **(연구보안 교육)** 연구책임자는 외국인 연구원에게는 '3-1-1. 외국인 연구원의 부서 배정(p.47)'에 포함된 '지식재산 방침, 자료 무단 반출 금지, 성과보호 방침'에 대해 다시 안내하도록 합니다.
- **(관리감독)** 외국인 연구원의 '협의되지 않은 주말 출입, 타 실험실 출입시도' 등 수상한 행동을 한 정황이 확인된다면 연구책임자는 이를 연구보안 담당부서에 즉시 알려 법령과 내규에 따라 조치해야 합니다.

• 연구개발과제 참여연구원(내·외국인) 모두 연구보안 교육 이수	☐Yes ☐No
• 3-1-1. 외국인의 부서 배정(p.47) 유의사항 재확인	☐Yes ☐No
• 수상한 행동 또는 정황 확인 시 연구보안 담당부서에 즉시 통보	☐Yes ☐No

3 연구보안 모의사례

❶ 과제 내 외국인 활용을 위한 사전 준비 사례

가상상황	• 모 과제에서 외국인 연구원 A를 채용하여 과제에 참여시키고자 하였다. 연구책임자 B는 외국인 참여 시 주의사항에 어떠한 것이 있는 지 연구보안 담당부서에 문의 하였다. 연구보안 담당부서는 '외국인의 불필요한 야근, 공휴일 연구실 출입 자제, 연구실 단독 출입 금지' 등의 안내 사항을 연구책임자 B에게 공지하였다. • 연구책임자 B는 필수적인 실험 일정으로 인하여 부득이 A가 야근 또는 공휴일 근무를 하게 될 경우 내국인 직원이 함께 근무하도록 일정을 계획하기로 하였다.
연구보안 포인트	✓ 외국인의 과제 참여가 결정되었다면, 연구보안 담당부서 등과의 확인을 통해 사전에 적절한 조치를 해야 합니다.

4 관련 법규 및 매뉴얼

- 국가연구개발사업을 수행하는 연구기관이라면 자체적으로 국내외 참여연구원에 대한 보안관리 대책을 수립합니다.
- 과학기술정보통신부 산하의 연구기관이라면 관련 규정을 준용하여 외국인 참여연구원을 관리하도록 합니다.

과학기술정보통신부 보안업무 시행세칙

제22조(외국인 공직임용 관련 보안대책) ① 외국인을 공무원으로 임용하는 경우 임용 30일전 까지 국가정보원에 신원조사를 요청하여야 하며, 신원 특이사항 발생시 보안심사위원회의 심의를 거쳐 임용여부를 결정하여야 한다.
② 외국인과 고용계약을 체결할 때에는 근무 중 알게 된 기밀사항을 계약기간중이나 계약만료 후에 누설할 경우의 손해배상책임과 피고용인 업무의 한계설정 등 보안유의사항을 명시하여 계약서를 작성하여야 하며, 보안담당관이 서약을 집행하여야 한다.
③ 보안담당관은 공직에 임용된 외국인에 대해 보안교육을 포함한 공직자로서의 기본자세 및 보안준수 등 의무사항에 대한 기본교육을 실시하여야 한다.
④ 국가 중요정책 등 민감한 내용을 다루는 회의의 주재자는 외국인 공직자의 참석여부를 신중히 결정하여야 하며, 회의 종료 후 외국인 공직자에게 보안 유의사항을 명확히 알려주어야 한다.
⑤ 외국인에게 상시적으로 비밀취급 인가를 부여하는 것은 극히 제한해야 하며, 외국인을 대상으로 열람 등 비밀 취급이 반드시 필요한 경우에 한해 규칙 제46조제1항에 따라 일시적인 비밀 열람·취급을 허용할 수 있다.
⑥ 보안담당관은 재직 중인 외국인이 퇴직할 경우에는 업무기간 중 지득한 비밀 등 중요자료에 대한 누설 및 사적이용 금지를 내용으로 하는 보안서약서를 집행하여야 하며, 각종 자료의 무단반출 여부를 확인하여야 한다.

03. 보안과제에 외국인 연구원 참여

1 연구보안 위험 포인트

» 보안과제에는 내국인만 참여하는 것이 원칙입니다.

» 예외적으로 불가피한 경우에 성공적인 연구개발성과 도출을 위하여 외국인 연구원이 보안과제에 참여하는 경우가 발생할 수 있습니다. 이때 보안사고를 방지하기 위해 철저한 현황 파악과 검토가 필요합니다.

2 권고사항 및 의무

❶ 보안과제 외국인* 연구원 참여 시 사전검토

* 외국인: 대한민국 국적을 가지지 않은 사람(보안대책제9조제1항)

- **(필요성 검토)** [법] 보안과제에 외국인 참여는 지양해야 하므로, 연구책임자는 철저히 외국인의 연구 참여가 필요한 것인지 숙고하고 보안과제 관계자와 긴밀히 논의해야 합니다.

• 보안과제 목표 달성에 외국인 참여연구원이 정말 필요한 것인지 보안과제 연구자, 연구보안 담당부서, 전문기관과 논의	☐Yes ☐No

- **(보안수단 검토)** 보안과제에 외국인 참여를 긍정적으로 고려하고 있다면 연구책임자는 연구자산 유출을 예방하기 위한 방안이 구비되어 있는지 확인합니다.

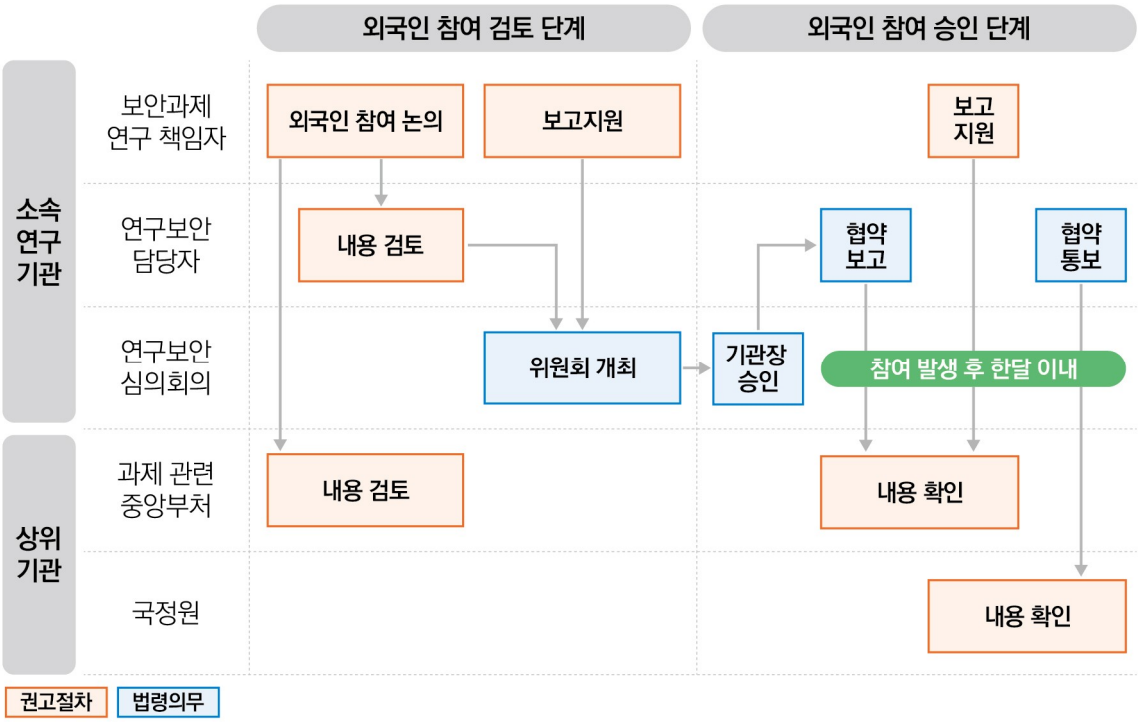
• 외국인의 신상은 확실한지, 범죄이력은 없는지 인사부서와 재확인	☐Yes ☐No
• 보안과제 참여 외국인의 본국 및 제3국으로부터의 수혜 사항 및 네트워크 확인	☐Yes ☐No
• 외국인 연구원의 연구수행 범위를 제한할 수 있는지 검토	☐Yes ☐No
• 외국인 연구원의 중요시설 출입 및 정보접근 기록을 관리할 수 있는 체계 마련 검토	☐Yes ☐No
• 외국인 연구원의 불법적인 자료 반출 통제 및 본국 송부를 막을 수 있는 체계 마련 검토	☐Yes ☐No

❷ 보안과제 외국인 연구원 참여 관련 의사결정 절차

- **(연구책임자)** 보안과제에 외국인 참여를 결정하였다면 연구책임자는 연구보안 담담자에게 연구보안심의회의 심의를 요청해야 하며 심의자료 작성을 지원합니다.
- **(연구보안심의회의)** [법] 외국인 연구원의 보안과제 참여 불가피성, 외국인 참여 시 보안 관리방안을 다각도로 검토하고 의결합니다.
- **(연구보안 담당부서)** [법] 보안과제 외국인 과제 참여 사실 발생 1달 이내에 연구보안 담당부서는 '협약서 또는 그에 준하는 내용', '외국인의 신상, 과제참여 범위', 과제 관련 정보 접근 권한의 범위' 등을 과제 담당 중앙행정기관 장에게 보고합니다.

  – 연구책임자는 중앙행정기관 담당자에게 관련 내용을 상세히 보고하는 것을 지원할 수 있습니다.
- **(연구보안 담당부서)** 중앙행정기관장 보고 시기에 동일한 내용을 국정원 담당자에게 통보해야 합니다.

• 보안과제 외국인 참여에 대해 연구보안심의회 의결 및 기관장 승인 획득	☐Yes ☐No



❸ 보안과제 외국인 참여 확정 후 외국인 연구원에 대한 교육 및 보안서약서 징구

- **(연구보안 담당부서)** [법] 보안과제 참여 외국인에 대한 보안교육을 추진해야 하며 보안서약서 내용을 충분히 해당 외국인이 숙지할 수 있도록 합니다.

• 보안과제 참여 외국인 연구원 보안교육 시행	☐Yes ☐No
• 보안과제 참여 외국인 연구원 대상 보안서약서 징구	☐Yes ☐No

- **(연구책임자)** 보안과제 전반에 대한 연구보안 수칙(연구성과 관리, 외국접촉 주의 사항 등)을 외국인에게 반복적으로 주지시킵니다. 이 때, '3-1-1. 외국인 연구원의 부서 배정(p.47)'에 포함된 내용도 함께 확인합니다.
  - 외국인 참여연구원이 소속된 보안과제의 연구책임자는 필요한 경우 연구보안 담당부서로부터 기관의 연구보안 방침 전반에 대해 안내받도록 합니다.

• 3-1-1. 외국인의 연구부서 배정 유의사항 재안내	☐Yes ☐No
• 보안과제 관련 정보를 타 외국인과 긴밀하게 지속적으로 논의할 경우 '외국접촉 신고' 필요함을 안내(보안과제 종료 후 3년 이내)	☐Yes ☐No
• 보안과제 참여 외국인이 한국 이외의 국가로부터 연구개발과제를 수탁받아 진행할 시, 사전에 소속 연구기관의 장의 승인을 얻어야 함을 설명(보안과제 종료 후 3년 이내)	☐Yes ☐No
• 보안과제 수행 시 이동 매체 사용 제한, 망분리 등을 설명	☐Yes ☐No

④ 보안과제 참여기간 동안 외국인 연구원에 대한 지속 관리

- **(연구책임자)** 연구책임자는 외국인 참여연구원의 정해진 연구범위가 지켜지도록 하고 외국인이 정해진 범위에 벗어난 정보시스템 또는 연구장비에 접근하는 것을 통제하고 관리·감시하여야 합니다.
  - 그 외 과제시작 전 확인하였던 보안과제 참여 외국인의 본국 및 제3국으로부터의 수혜 사항에 변화가 있는지에 대해서도 검토 합니다.
- **(주요 담당부서)** 연구보안 담당부서, 시설 담당부서 등은 보안과제 참여 외국인 연구원의 출입 동향, 연구보안 위배 특이동향을 관찰해야 합니다.

• 연구책임자는 외국인 참여연구원의 정해진 연구범위가 지켜질 수 있도록 노력	☐Yes ☐No
• 보안과제 참여 외국인 연구원의 출입 및 연구보안 위배 특이동향을 관찰	☐Yes ☐No

⑤ 보안과제 참여 외국인 연구원 참여 종료 시 관리

- 연구책임자는 참여가 종료된 외국인 연구원으로부터 자료 회수, 연구시설·장비 및 정보 접근제한, 보안서약서 징구 등 전반적 보안조치 사항을 연구보안 담당자와 함께 검토합니다.

※ 3-1-1. 외국인 연구원의 연구부서 배정 : 퇴사 시 및 과제종료 유의사항(p.47)을 기본적으로 모두 준수

• 과제 종료 시 외국인 참여연구원으로부터 각종 연구자료 등 회수	☐Yes ☐No
• 과제 종료 시 외국인 참여연구원의 연구시설/정보 등에 대한 접근권한 제한	☐Yes ☐No
• 참여종료 또는 고용 종료 시점에 연구책임자는 외국인의 자료반출입 이력 및 인쇄 이력 점검	☐Yes ☐No
• 보안과제 종료 시점에 필요 시 외국인 대상 추가 보안서약서 징구 논의	☐Yes ☐No

3 연구보안 모의사례

① 외국인 유학생이 승인 없이 보안과제 연구를 하며 자료를 유출하는 사례

가상상황	• 지방국립대 반도체 연구실 박사과정의 A외국인 학생은 연구실에서 보안과제를 포함하여 여러 과제를 동시에 연구하고 있다. 외국인의 경우 보안과제에 참여하기 위해서는 총장의 허가를 사전에 승인받아야 하지만 상황이 워낙 바쁘다 보니 A학생은 어느 순간 자연스럽게 보안과제 일부를 맡아서 하게 되었다. • A학생은 본국에서 석사과정을 마쳤는데 한국에서 연구를 하다 보니 본국의 친구들에게 참고 자료를 보내주면 좋을 것 같아서 실험 데이터의 일부를 정리해서 보내주었다. 그 과정에서 부지불식간에 보안과제에서 창출된 연구데이터 일부를 전송하게 되었다. • 담당 교수는 우연히 실험실에 들렀다가 이 장면을 목격하게 되었고 결국 해당 학생을 연구실에서 내보내기로 하였다.
연구보안 포인트	✓ 외국인이 보안과제에 참여할 경우 기관장의 사전승인이 필요합니다. ✓ 외국인 연구자가 보안과제에 참여할 시에는 제한된 업무 범위 설정이 중요합니다. ✓ 보안과제 관련 성과의 경우 기관 차원의 데이터 유출 제한 방침이 필요합니다.

4 관련 법규 및 매뉴얼

- 보안과제 뿐 아니라 국방보안 해당 시 다음 규정을 준수해야 하므로 확인 바랍니다.

구분	법령 내용	근거법
방위산업기술	• 상시출입 외국인의 출입통제, 기술보호서약, 교육, 출입통제, 정보통신 매체 이용 전반에 대한 계획 수립	방위산업기술 보호지침제21조
	• 외국인이 대상기술을 취급할 수 없으나 필요 시 방위사업청장·국가정보원장 신고	방위산업기술 보호지침제22조
	• 상시출입 외부인·외국인을 보호지역에서 근무하게 할 수 없으며 필요 시 범위 설정 필요	방위산업기술 보호지침제26조
	• 외부인·외국인 방문은 특정목적(단순방문, 견학 제외)이 있을때만 허가, 보호대책 및 출입현황 기록관리 필요	방위산업기술 보호지침제28조

- 보안과제에 외국인 연구원 참여 결정 시 관련 내용을 중앙행정기관, 국정원이 모두 관련 현황을 파악할 수 있도록 합니다.

국가연구개발사업 보안대책

제7조(보안교육 및 보안서약) ① 연구개발기관의 장은 보안과제를 수행할 예정이거나 수행하고 있는 연구자에 대하여 다음 각 호의 사항을 포함하는 보안교육을 실시하여야 한다.

1. 이 지침에 따른 연구자의 의무 사항
2. 연구기관보안대책에 따른 연구자의 의무 사항
3. 보안과제 수행에 따른 우대조치에 관한 사항
4. 의무사항을 위반할 경우에 법, 「산업기술의 유출방지 및 보호에 관한 법률」, 「대외무역법」에 따라 받을 수 있는 불이익에 관한 사항
5. 그 밖에 보안사고의 예방을 위해 필요한 사항

② 제1항에 따른 교육을 받은 연구자는 연구개발기관의 장에게 보안서약서를 제출하여야 한다.

③ 제2항에 따른 보안서약서의 서식은 별지 제1호 서식을 따르며, 필요한 경우 연구개발기관의 장이 그 내용을 준용하여 정할 수 있다.

④ 연구개발기관의 장은 필요한 경우 보안과제를 수행하지 않는 소속 연구자와 기타 소속 직원에 대해서도 보안교육을 실시할 수 있으며, 특별히 보안상 필요한 경우 서약서를 제출하도록 할 수 있다.

제8조(외국 정부 등과의 접촉 관리 등) ① 보안과제를 수행하고 있거나 수행한지 3년이 지나지 아니한 연구자가 외국에 소재한 정부·기관·단체 또는 외국인 등(본사와 지사의 소재가 다를 때에는 본사 위치를 기준으로 하는 것을 원칙으로 한다)과 보안과제와 관련하여 접촉(연구자가 상호작용하는 경우 또는 특정하여 유의미한 정도로 접촉이 반복되는 경우를 말한다.) 하는 경우에는 해당 접촉일로부터 10일 이내에 접촉 일시·장소·방법·내용 등에 관한 사항을 현재 소속된 연구개발기관의 장(퇴직으로 소속기관이 없거나 법 제2조제3호에 따른 연구개발기관이 아닌 기관으로 이직하는 경우에는 마지막으로 소속되었던 연구개발기관의 장)에게 보고하여야 한다.

② 보안과제를 수행하고 있거나 수행한지 3년이 지나지 아니한 연구자가 외국 정부·기관·단체 등의 지원을 받아 연구개발을 수행하는 경우 사전에 연구보안심의회의 심의를 거쳐 현재 연구자가 소속된 연구개발기관의 장(퇴직으로 소속기관이 없거나 법 제2조제3호에 따른 연구개발기관이 아닌 기관으로 이직하는 경우에는 마지막으로 소속되었던 연구개발기관의 장)의 사전 승인을 받아야 한다.

③ 연구개발기관의 장은 제1항에 따라 보고받은 사항, 제2항에 따라 사전 승인한 사항을 보고 및 승인 후 1월 이내에 중앙행정기관의 장에 보고하고 국가정보원장에 통보한다.

제9조(외국 연구자 등의 보안과제 참여 등) ① 보안과제에의 대한민국 국적을 가지지 아니한 외국인의 참여는 내국인을 통한 목적달성이 어려울 경우 보충적으로 인정하는 것을 원칙으로 한다.
② 연구기관의 장은 보안과제에 관하여 외국 정부·기관·단체 등과 공동연구를 수행하려거나 이들에게 연구의 일부를 수행하게 하려는 경우 중앙행정기관의 장의 사전 승인을 얻어야 한다.
③ 연구기관의 장은 보안과제에 대한 외국인의 참여를 승인하려할 경우 제6조에 따른 연구보안심의회의 심의를 거쳐야 한다. 이 때 연구보안심의회는 외국인의 보안과제에의 기여 가능성, 기술격차 등을 고려할 때 향후 외국에의 기술 유출 가능성 등을 종합적으로 검토하여야 한다.
④ 연구기관의 장은 제2항에 따라 중앙행정기관의 장의 사전승인을 얻었거나 제3항에 따라 보안과제에 외국인을 참여시킨 경우 해당 사항이 발생하고 1월 이내에 해당 보안과제에서 외국 연구기관 등과 공동연구 등을 위한 협약사항 또는 이에 준하는 사항, 또한 참여 외국인의 신상 및 과제 참여 범위, 과제 관련 정보 접근 권한의 범위 등의 정보를 중앙행정기관의 장에 보고하고 국가정보원장에게 통보하여야 한다.

04. 보안과제 수행 연구실에 외국인이 상주하는 경우

1 연구보안 위험 포인트

» 외국인 연구원이 연구기관에 상주하는 사례가 많아지며 보안과제를 추진하는 부서에 외국인이 함께 일하는 경우가 발생할 수 있습니다.

» 외국인 연구원과 보안과제 수행 연구자가 함께 생활하다 보면 상호 부주의함으로 보안과제 관련 정보가 유출될 가능성이 있습니다.

» 보안과제 연구책임자, 연구보안 담당부서는 보안사고 방지를 위한 조치를 해두어야 합니다.

2 권고사항 및 의무

※ 3-1-1. 외국인 연구원의 연구부서 배정(p.47)의 유의사항을 기본적으로 모두 준수

- [법] 보안과제 연구책임자는 외국인 연구원에게 보안과제 관련 정보, 시설에 일체 접근할 수 없음을 강조해야 합니다.
- [법] 보안과제 연구책임자는 참여연구원들에게 부서에 상주하는 외국인 일지라도 보안과제에 참여하지 않는 외국인과 보안과제 관련 긴밀한 논의를 하였다면 10일 이내에 기관에 '외국접촉 신고'를 해야 함을 교육 시킵니다.
  - 연구책임자는 보안과제 참여연구원들에게 보안과제 관련 사항을 부서 내 외국인 연구원에게 공유하지 않도록 주의를 주어야 합니다.
  - 연구진 간 회의더라도 보안과제 관련 내용을 다룰 가능성이 있다면 외국인 연구원의 참석 여부를 신중히 결정 합니다.

• 외국인 연구원에게 보안과제 관련 정보, 시설에 일체 접근할 수 없음을 강조	☐Yes ☐No
• 상주 외국인과 보안과제 관련 긴밀한 논의를 지속하였다면 10일 이내에 기관에 외국접촉을 신고해야 함을 보안과제 참여연구원들에게 교육	☐Yes ☐No

3 연구보안 모의사례

❶ 보안과제 수행 부서에 외국인 인턴학생 상주하는 경우

가상상황	• 일부 부서원이 보안과제를 수행하는 부서에 외국인 인턴 A가 배정되었다. 해당 인턴A는 보안과제에 참여하지는 않았다. • 같은 부서에서 보안과제를 수행하는 연구원 B와 C는 실험실 내에 외국인 인턴 A가 있는 것을 인지하지 못한 상태에서 보안과제 관련 내용을 논의하였고, 해당 대화를 A도 듣게 되었다. • 이를 인지한 B와 C는 즉시 연구보안 담당부서, 연구책임자에게 상황을 공유하며 상담을 요청하였다. 토의 결과, 관계자들은 B,C의 대화를 A가 우연히 엿듣는 것만으로는 보안과제 내용을 파악하는 것은 불가능하다는 결론에 이르렀다. 따라서 '외국접촉보고'를 하지 않기로 하였으며 B, C 연구원은 보안과제 관련 긴밀한 대화 시 주의해야겠다고 다짐하였다.
연구보안 포인트	✓ 보안과제 연구원들은 외국인 연구원과 연구정보를 공유해서는 안 되며, 외국인 연구원이 있는 공간에서 보안과제 관련 논의를 하지 않아야 합니다. ✓ 보안과제와 관련하여 외국인 연구원과 긴밀한 논의가 이뤄진 경우, 10일 이내에 연구보안 담당부서에 외국접촉을 신고해야 합니다.

② 외국인의 수상한 행동 확인 사례

가상상황	• 보안과제 연구책임자 C는 일요일 저녁에 연구실에 출근하였다가 같은 연구실의 외국인 D가 보안과제 관련 장비 앞을 서성이고 있는 것을 목격하였다. 연구책임자 C가 외국인 D에게 해당 시설 접근 이유를 물어보니 얼마 전 새로운 장비 도입을 위해 공사하던 것을 보고 궁금하여 서성거렸다고 하였다. • 평소 같으면 지나칠 수 있는 일이라는 생각도 들었지만 주말 저녁에 D가 혼자 출근하였다는 점, 보안과제 장비에 접근했다는 점 등이 미심쩍어 연구책임자C는 해당 사실을 연구보안 담당부서에 알리게 되었다. • 연구보안 담당부서는 현재 보안사고 발생 건은 없지만 혹시 모를 상황에 대비하여 해당 외국인의 자료반출 이력, 인쇄이력, 출입국 이력 등에 대해 검토해 보겠다고 응답하였다.
연구보안 포인트	✓ 외국인의 협의 되지 않은 주말 출입, 타 실험실 출입 시도 등 수상한 행동을 하거나 자료의 무단 반출 정황이 확인되면 이를 목격한 사람은 즉시 연구보안 담당부서에 알려야 합니다.

4 관련 법규 및 매뉴얼

• 보안대책(고시)에 따라 보안과제를 수행하는 연구기관은 연구기관 보안대책에 '보안관리 체계, 연구시설관리, 정보통신망 관리' 등을 마련하여 외국인 연구원을 통한 정보 유출을 예방합니다.

국가연구개발사업 보안대책

제4조(연구기관의 보안대책 수립 등) 연구기관의 장은 법 제21조제1항 및 영 제44조에 따른 보안대책(이하 "연구기관보안대책"이라 한다.)으로써 별표1에 따른 사항을 포함하는 자체규정을 마련하여야 한다. 다만, 공동연구기관이 자체 보안대책을 마련하기 어려운 경우 또는 주관연구기관과 공동연구기관의 보안대책을 통일성 있게 운영할 필요가 있는 경우에는 주관연구기관의 보안대책에 공동연구기관이 따르도록 한다.

[별표] 연구기관보안대책에 포함되어야 하는 사항(제4조 관련)

2. 보안과제 참여연구자(연구책임자 및 외국인을 포함한다) 관리
   가. 참여연구자의 연구기관보안대책 위반 시 징계에 관한 사항
   나. 퇴직하였거나 퇴직 예정인 자가 반출 또는 반출 예정인 자료에 대한 보안성 검토, 회수, 전산망 접속 차단 등의 조치에 관한 사항
   다. 참여연구자의 국외 출장 시 사전 보안교육 및 귀국보고(출장기간에 접촉한 사람 및 협의 내용 등을 포함한다) 실시
   라. 보안과제를 수행하거나 수행한 적이 있는 연구자의 외국 정부·기관·단체 접촉시 보고 및 외국 정부·기관·단체와의 연구 승인 등에 관련된 절차 및 형식 등 제반사항

제8조(외국 정부 등과의 접촉 관리 등) ① 보안과제를 수행하고 있거나 수행한지 3년이 지나지 아니한 연구자가 외국에 소재한 정부·기관·단체 또는 외국인 등(본사와 지사의 소재가 다를 때에는 본사 위치를 기준으로 하는 것을 원칙으로 한다)과 보안과제와 관련하여 접촉(연구자가 상호작용하는 경우 또는 특정하여 유의미한 정도로 접촉이 반복되는 경우를 말한다.) 하는 경우에는 해당 접촉일로부터 10일 이내에 접촉 일시·장소·방법·내용 등에 관한 사항을 현재 소속된 연구개발기관의 장(퇴직으로 소속기관이 없거나 법 제2조제3호에 따른 연구개발기관이 아닌 기관으로 이직하는 경우에는 마지막으로 소속되었던 연구개발기관의 장)에게 보고하여야 한다.

제2절 국가R&D 국제공동연구 추진 시 지켜야 하는 것이 무엇인가요?

01. 협약·계약 시 연구보안

1 연구보안 위험 포인트

» 해외 주요 국가는 국제공동연구 파트너 선정 시 상대 국가의 연구보안 수준도 함께 고려하고 있습니다. 글로벌 스탠다드에 걸맞는 연구보안 규정을 준수하여 우리나라의 국제적 위상을 높이도록 노력해야 합니다.

» 국외로 연구자산이 유출되는 경우 국가 간 법·제도, 보안에 대한 인식의 정도 및 문화가 달라 발 빠른 대처가 어려울 수 있습니다. 따라서 협약 체결 시 연구자산 유출 위험성에 대한 철저한 검토를 거치도록 합니다.

2 권고사항 및 의무

❶ (협약 전) 국제공동연구 상대 연구기관 및 주제에 대한 검토

- **(평판검토)** 연구책임자 및 연구보안 담당부서는 국제공동연구를 진행할 상대 연구기관의 지배구조, 참여 연구원 정보, 보안사고 이력, 보안수준 등 보안관련 평판에 대해 최대한 상세하게 파악하도록 노력합니다.
- **(보안규정)** 연구계약, 연구보안 담당자는 국제공동연구 대상 기관의 연구보안 규정을 사전에 확인할 수 있도록 하고 특이사항이 있는지를 확인 합니다.
- **(수출통제)** 국제공동연구를 추진하고자 하는 내용이 각국의 '수출통제' 품목에 해당하지 않는 지 또는 군사적 악용 가능성은 없는지 상호 검토 합니다.
- **(지식재산)** 국제공동연구로 위해 창출된 지식재산의 소유활용, 연구자료 대외발표 등을 어떻게 할 것인지에 대해 연구책임자 간 사전 협의를 추진해야 합니다.
  - 만약 해외 위탁한 연구의 지식재산권을 국내 연구기관 단독 소유로 하지 않을 경우 연구책임자는 상대 기관 선정의 타당성 등을 재검토해 보아야 합니다.
- **(정보제공 수준)** 국제공동연구를 진행할 상대 연구기관이 연구보안 관련 전반 정보제공에 협조하는 수준을 보며 연구보안 위험성을 파악해 볼 수 있습니다.

• 상대 기관의 연구보안 규정 사전 확인	☐Yes ☐No
• 공동연구 결과가 군사적으로 사용될 가능성이 존재하는지 검토	☐Yes ☐No
• 공동연구 내용이 각국의 수출통제 기술과 관련되는 지 검토	☐Yes ☐No
• 상대 기관과 지식재산, 대외발표 사항 사전 협의	☐Yes ☐No

❷ (협약 전) 상대 연구기관 또는 연구진과의 정보 공유 시 보안

- 국제공동연구 과정에서 상대 연구기관의 연구자와 연구과제와 관련된 자료를 주고 받는 과정에서의 정보 유출을 막을 방안을 강구해야 합니다. 보안성이 높은 이메일 계정, 보안인증 클라우드 등을 활용하도록 상호 논의할 수 있습니다.

• 국제공동연구 진행 시 상대기관과 공유된 정보를 별도 저장 및 관리하는 보안체계 마련 여부	☐Yes ☐No

❸ 협약서 작성

- 협약서 작성 시 연구책임자는 반드시 기관의 연구보안 및 지식재산 담당부서와 논의하여 지식재산 보호, 비밀유지계약 체결 등 전반 사항을 점검합니다.
  - 수출통제 기술과 연관되는 경우 사전에 많은 협의가 필요합니다. 특히, 혁신법 시행령 및 각 부처 연구개발사업 보안관리지침 등에 따라 전략물자 등에 해당하는 경우 보안과제로 보안등급을 분류하여야 합니다. 이 경우, 무역안보관리원 등 전문기관에 판정을 신청할 수 있습니다.
  - 협약 시 기관 간 상호 보안대책이 충돌하지 않도록 협의해야 합니다.
  - 지식재산, 개인정보, 연구윤리에 대한 각국의 법규정, 문화가 다를 수 있으니 사전에 해당 사항에 대해 알아보도록 합니다.
  - 연구책임자 및 연구보안 담당부서는 상대 기관의 참여 연구진(포닥, 석·박사 학생 등)의 소속 및 국적, 연구 활동 범위, 자금출처를 명확히 해달라고 요청해야 합니다.

• 협약(계약)서에 지식재산권(IP) 보호 정책과 소유권 배분 조항 존재	☐Yes ☐No
• 협약(계약)서에 공동연구 기관 간 데이터 출처 명시, 공저자 합의, 표절 검사 툴(Tool) 사용 관련 내용 포함	☐Yes ☐No
• 상호 동의할 수 있는 보안대책 수립	☐Yes ☐No
• 국제공동연구 중 민감한 정보가 포함된 경우, 관련 내용을 보호하기 위해 비밀유지계약(NDA)을 체결	☐Yes ☐No
• 상대 기관의 참여연구진 신원, 연구범위 검토	☐Yes ☐No
• 매칭 시 상대 기관의 자금출처 기재 요청	☐Yes ☐No
• 국제공동연구와 관련하여 소속 기관에 보고하거나 승인을 받아야 하는 주요 사안을 확인하고 기관의 규정을 준수	☐Yes ☐No

  - 연구책임자는 국제공동연구와 관련하여 소속 기관에 보고하거나 승인을 받아야 하는 주요 사안을 확인하고 기관의 규정을 준수 합니다.

3 연구보안 모의사례

❶ 파트너 국가의 지식재산 정책을 잘못 이해함

가상상황	• 국내 A 연구기관은 외국B국가의 C기관과 공동으로 우리나라 및 B국가에 특허를 출원하였다. • 몇 년 후 A 연구기관 연구자들은 C기관이 공동발명 특허를 B국가에서 활용하고 있다는 사실을 뒤늦게 알게 되었다. • 국내의 경우 상대방의 동의없이 특허권 실시가 불가하였으나 외국 B국가는 동의 없이도 실시가 가능한 점을 미쳐 몰랐기 때문에 발생한 사건이었다.
연구보안 포인트	✓ 협약 시 법률 전문가의 지원을 받아 상대방의 지식재산권 정책에 대해서 파악하고 협의하도록 해야 합니다.

❷ 국가 간 보안대책의 충돌

가상상황	• 외국 A국가에 위치한 B기업과 우리나라 C기업은 A국가에서 함께 보안과제 관련 국제 협력을 진행하게 되었다. C기업은 '국내 방첩규정'에 따라 연구 공간에 보안 감시장치를 설치하고자 하였으나 B기업이 A국가의 방침에 따라 해당 보안 감시장치 설치를 반대하여 갈등이 발생하였다.
연구보안 포인트	✓ 가급적 협약 이전에 상대 국가 및 기업의 보안방침을 사전에 파악하여 협의할 수 있도록 해야 합니다. ✓ 연구책임자 혼자 힘으로 많은 것을 알기 어려우므로 '소속기관'은 변호사 등을 지원할 수 있도록 해야 합니다. '전문기관'은 관련 노하우를 연구자에게 전달하도록 합니다.

4 관련 법규 및 매뉴얼

- 국제공동R&D매뉴얼(24.3)에 따르면 국제공동연구 협약 시, '파트너 선정, 협약서 상 보안대책 수립, 연구기관 단위 보안대책 수립'을 권고하고 있습니다.

구분	국제공동연구 협약 추진 시 주의사항
국외 기관 선정	• 국외계약금액이 특정 금액*이상이거나 해외로 위탁한 연구의 지식재산권을 국내 연구기관 단독소유로 하지 않을 경우 연구책임자는 상대기관 선정의 타당성 등 검토 * 30만불 또는 원화 3억원 이상 등 연구기관 내부 규정으로 결정
협약 주의 사항	• (IP보호) 영업비밀보호, 물질이전계약, 특허출원 등에 대한 선제적 조치 • (비밀유지계약) 비밀정보와 유지 기간을 상호 합의하여 정하고 핵심정보 적극 보호 • (소유권) 개량 발명, 신규 창출된 지식재산권에 대한 소유권을 사전 정리 • (보안대책) 주관/공동/위탁기관은 연구추진 시 보안대책 상호 논의
보안 대책 수립	• 국제공동연구 관련 사항을 포함한 연구기관의 보안대책 수립, 보안심의회의 의결

※ 참고 : 과학기술정보통신부·한국과학기술기획평가원. (2024), 국가R&D국제공동연구매뉴얼

- '혁신법시행령' 제44조제3항 제3호에 따라 '보안과제를 수행하는 연구기관'은 '외국 공동연구 시 보안관리 방안'을 보안관리규정에 포함시켜야 합니다.

국가연구개발사업혁신법 시행령

제44조(국가연구개발사업 등의 보안대책) ① 관계 중앙행정기관의 장 및 연구기관의 장은 다음 각 호의 연구개발성과에 대하여 법 제21조제1항에 따른 보안대책(이하 "보안대책"이라 한다)을 수립·시행해야 한다.
1. 「산업기술의 유출방지 및 보호에 관한 법률」 제2조제1호에 따른 산업기술과 관련된 비공개 연구개발성과
2. 법 제21조제2항에 따라 보안과제로 분류된 연구개발과제의 연구개발성과

② 중앙행정기관의 장이 수립하는 보안대책에는 다음 각 호의 사항이 포함돼야 한다.〈개정 2022. 12. 6.〉
1. 제1항 각 호에 따른 연구개발성과의 수집·분석·가공·배포 방안
2. 제47조에 따른 보안관리 실태 점검의 구체적 방안

3. 제48조제1항에 따른 보안사고의 예방·대응·조사·재발방지 방안
4. **연구개발과제협약으로 정하는 바에 따라 외국에 소재한 기관·단체 또는 외국인과 공동으로 연구를 수행하는 경우의 보안관리 방안**
5. 보안대책을 총괄하는 담당자 지정 방안
6. 보안교육 실시 방안
7. 제66조에 따른 국가정보원과의 보안에 관한 협력 방안

③ 연구기관의 장이 수립하는 보안대책에는 다음 각 호의 사항이 포함되어야 한다.〈개정 2022. 12. 6.〉

1. 소속 연구자가 준수해야 하는 보안 관련 의무사항
2. 연구시설 및 연구관리시스템에 대한 보안조치 사항
3. 제2항제3호부터 제6호까지에서 규정한 사항
4. 제1호부터 제3호까지에서 규정한 사항이 포함된 보안관리규정 제정·운영 방안

참고 미국 에너지부(DOE) 국제협력 시작 시 협약계약 참고사항

- 국제협력 절차에 대해 미리 파악해 두면 상호 소통이 용이할 수 있습니다.
- 아래는 에너지부(DOE)의 국제협력 관련 규정 입니다.

DOE 규정	상세내용
1 외국기관과의 협력지침 (DOE P 485.1A)	• (협력 검토 사항) 외국 기관과의 협력이 DOE 및 연구소의 미션과 부합하는 지 사전 검토 추진* * 미국 전략적 이익 및 외교정책 일치, 미국 법령 규정 준수, DOE 기술공유에 따른 리스크 평가 • (검토 대상 협력) ①양해각서(MOU) 및 유사 문서 (Statement of Intent 등), ②전략적 파트너십 프로그램(SPP, 구 Work for Others), ③협동연구개발계약(CRADA, Cooperative Research and Development Agreement), ④기술상용화 협정, ⑤기타 외국 기관과의 계약적 법적 문서 등에 적용 • (검토 절차) 모든 MOU 및 계약 문서는 최소 5년마다 본부에서 재검토하여 정책 및 국가안보 기준과 일치 여부를 확인하므로 유의 • (제한 사항) S&T Risk Matrix*에서 제한(Restricted) 기술로 지정된 분야에 대해, 위험국(Countries of Risk)**과의 협력은 사전 면제 절차가 없는 한 금지됨 * DOE는 기존의 수출통제나 분류 체계에 포함되지 않는 신흥기술이라 하더라도, 국가안보 또는 경제안보에 잠재적 위험이 있다고 판단되는 기술을 식별하고 보호하기 위해 S&T Risk Matrix 기술을 구분, 기술등급은 위험도에 따라 'Red, Yellow, Green'으로 분류됨 ** Countries of Risk: 중국·러시아·이란·북한·벨라루스('25.5월 기준)

DOE 규정	상세내용
2 협동연구개발계약(CRADA*) 체결 시 외국기관 참여 요건 (DOE O 483.1B Chg 2) *Cooperative Research and Development Agreement	• (개요) 미국 정부가 국공립연구소, 민간, 대학 등의 협력으로 공동 기술을 개발할 수 있도록 표준화 된 협력 틀을 개발한 것으로 자국 내 협력 뿐 아니라 외국과 연구협력을 위한 계약형식으로도 활용 • (일반적 검토사항) DOE는 외국 기관과의 CRADA 체결 시 해당 요건*에 부합하는지 여부를 사전 검토 * DOE 미션과 일치 필요, 단순 자금 제공 뿐 아니라 기술협력 기여, 미국 내 기술활용 우선조건 충족, '수출통제, 기밀정보, 지식재산권' 관련 조치 명시 필요, 참여기관이 외국 소유 및 지배, 영향을 받는 경우 검토 추가 • (승인 관련 추가 절차) 해당 협력이 위험국(Countries of Risk) 소속 외국 기관과의 협력이거나, S&T Risk Matrix 상의 제한 기술 분야에 해당하는 경우 추가 승인 필요
3 전략적 파트너십 프로그램 (Strategic Partnership Projects)	• (개요) DOE 또는 NNSA(National Nuclear Security Administration, 국립핵안보청) 시설이 외부 기관(미국 내·외 정부, 산업계, 학계 등)의 자금을 받아 연구·기술·서비스를 제공하는 제도로, DOE 예산이 아닌 외부 자금으로 수행되는 연구·기술 프로젝트 ※ 민간에서 수행하기 어려운 특수한 기술/시설 활용 제공, DOE 기술의 산업 이전 및 상업화 촉진, DOE/NNSA 연구소의 기술 기반 강화, 정부기관 간 협력 또는 민간과의 공동 연구 활성화 • (승인 요건) 전략적 파트너십 프로그램 체결 시 충족해야 하는 조건은 다음과 같으므로 주의 필요 * 미국 민간 부문과의 직접적 경쟁을 유발해서는 안됨, DOE 모든 지침 준수, 위험국가 또는 S&T Risk Matrix 상 Red 기술인 경우 승인 필요

02. 보안과제에 외국기관 참여

1 연구보안 위험 포인트

» 보안과제에서 취득한 정보나 지식재산이 국외로 유출되는 경우 국가안보 위협 및 국민경제 손실로 이어질 수 있습니다.

2 권고사항 및 의무

❶ 보안과제 외국기관 참여 시 사전검토

- [법] 국내 연구진의 노력으로 보안과제 목표 달성이 불가한 경우에만 보안과제에 외국기관 참여가 가능합니다. 연구책임자는 보안과제 관련 관계자와 함께 외국기관 없이 보안과제 목표 달성이 가능한지 우선 검토합니다.

• 보안과제에 외국기관 참여가 꼭 필요한 지 전문기관 및 소속기관 연구보안 담당부서와 검토	□Yes □No

- 만약 공모 절차를 거쳐 보안과제에 참여할 외국기관을 선정한다면 연구책임자는 공모 이전에 관련 사항을 과제 담당 중앙행정기관 담당자와 긴밀하게 상의합니다.

❷ 보안과제 외국기관 참여 시 의사결정 절차

- **(연구책임자)** 외국기관의 보안과제 참여 시 연구보안 담당부서에 연구보안심의회의 개최를 요청해야 하며 심의자료 작성을 지원합니다.
- **(연구보안심의회의)** [법] 보안과제에 외국기관이 참여하기 위해서는 주관연구기관의 연구보안심의회의에서 관련 사항을 심의 및 의결하고 기관장은 사전 승인해야 합니다.
  - 연구보안심의회의는 외국 연구기관 등과 공동연구 등을 위한 협약사항, 참여 외국인의 신상 및 과제 참여 범위, 과제 관련 정보 접근 권한의 범위, 보안수단 전반을 논의하고 외국기관 참여를 의결 합니다.
  - 이때 과제가 국가핵심기술 또는 전략물자에 해당하는 경우, 외국기관과 공동개발 또는 기술교류가 발생되기 이전 수출허가를 받아야 합니다.

• 연구기관 연구보안심의회의에서 보안과제 외국기관 참여 심의 및 의결, 기관장의 사전승인	□Yes □No

- **(연구보안 담당부서)** [법] 보안과제 외국기관 참여에 대한 협약 시 과제 담당 중앙행정기관(또는 전문기관)의 사전 승인 공문이 필요합니다. 기관의 연구보안 담당부서는 승인요청 공문을 중앙행정기관장에게 송부합니다.

• 보안과제 외국기관 참여 관련 중앙행정기관 사전 승인 필요	□Yes □No

  - 연구책임자는 협약내용을 검토하고 중앙행정기관-연구보안 담당부서 간의 의사소통을 지원하거나 직접 중앙행정기관 담당자에게 보고할 수 있습니다.

- **(연구보안 담당부서)** [법] 중앙행정기관장 사전 승인 후 1달 이내 연구기관의 연구보안 담당부서는 협약서 및 이에 준하는 구체적인 내용을 중앙행정기관에게 보고하고 국정원장에게 통보하도록 합니다.
- **(연구보안 담당부서)** 보안과제에 참여하는 외국기관의 연구참여 인력들에게 우리나라의 보안과제 관련 연구방침을 안내하도록 합니다. 협약서에 관련 내용을 구체적으로 작성할 수 있습니다.

  – 상호 협의하에 외국기관이 우리나라 법규에 준하는 보안대책을 수립하도록 권고할 수 있습니다.

3 연구보안 모의사례

❶ 보안과제 국제공동연구 수행 사례

가상상황	• 우리나라 정부의 과학분야 협력기조에 따라서 A국의 B대학과 우리나라 출연연 C는 MOU를 추진한 상태이다. 차년도에는 우리나라 국가R&D 중 '보안과제'를 함께 연구하며 긴밀한 협력을 추구하기로 하였다. 연구책임자인 D는 보안과제이면서 국제공동연구인 경우는 처음 겪기에 해당 사항을 연구보안 담당부서에 문의하게 되었다.
연구보안 포인트	✓ 보안과제 국제 공동연구 추진 시 기관의 사전승인, 부처승인/국정원통보(기관승인 후 1월 이내) 절차를 거쳐야 합니다. ✓ 외국과 공동연구를 추진하려는 경우 연구기관은 보안관리 방안을 보안대책에 포함시켜야 합니다.

4 관련 법규 및 매뉴얼

- 국내기관과의 공동·위탁연구개발과제 등으로 보안과제 목표 달성이 불가능한 경우에만 외국기관의 연구 참여가 가능함을 유의해야 하며 외국기관 참여 관련 절차에 주의하도록 합니다.

국가연구개발사업 보안대책

제9조(외국 연구자 등의 보안과제 참여 등) ① 보안과제에의 대한민국 국적을 가지지 아니한 외국인의 참여는 내국인을 통한 목적달성이 어려울 경우 보충적으로 인정하는 것을 원칙으로 한다.

② 연구개발기관의 장은 보안과제에 관하여 외국 정부·기관·단체 등과 공동연구를 수행하려거나 이들에게 연구의 일부를 수행하게 하려는 경우 중앙행정기관의 장의 사전 승인을 얻어야 한다.

③ 연구개발기관의 장은 보안과제에 대한 외국인의 참여를 승인하려할 경우 제6조에 따른 연구보안심의회의 심의를 거쳐야 한다. 이 때 연구보안심의회는 외국인의 보안과제에의 기여 가능성, 기술격차 등을 고려할 때 향후 외국에의 기술 유출 가능성 등을 종합적으로 검토하여야 한다.

④ 연구개발기관의 장은 제2항에 따라 중앙행정기관의 장의 사전승인을 얻었거나 제3항에 따라 보안과제에 외국인을 참여시킨 경우 해당 사항이 발생하고 1월 이내에 해당 보안과제에서 외국 연구개발기관 등과 공동연구 등을 위한 협약사항 또는 이에 준하는 사항, 또한 참여 외국인의 신상 및 과제 참여 범위, 과제 관련 정보 접근 권한의 범위 등의 정보를 중앙행정기관의 장에 보고하고 국가정보원장에게 통보하여야 한다.

- 보안과제에 참여하는 외국 연구기관이 자체 보안대책을 마련하기 어려운 경우 또는 주관연구기관과 외국 연구기관의 보안대책을 통일성 있게 운영할 필요가 있는 경우, 우리나라 연구기관 보안대책을 외국기관이 따르도록 할 수 있습니다.
- 보안과제 뿐 아니라 산업보안, 국방보안 해당 시 다음 규정을 준수해야 하므로 확인 바랍니다.

구분	법령 내용	근거법
국가핵심기술	• 국가핵심기술이 실질적으로 이전·공유되는 외국기업 등과의 연구 시 산업부장관 승인	산업기술보호지침 제17조
방위산업기술	• 외국정부와의 합작·기술제휴 시 기술보호정책 마련 및 계약 체결. 필요 시 국정원 협조	방위산업기술보호지침 제39조

제3절 안전한 국제협력을 추구하고 싶어요!

01. 국외수혜정보 보고 추진 원칙 및 방법

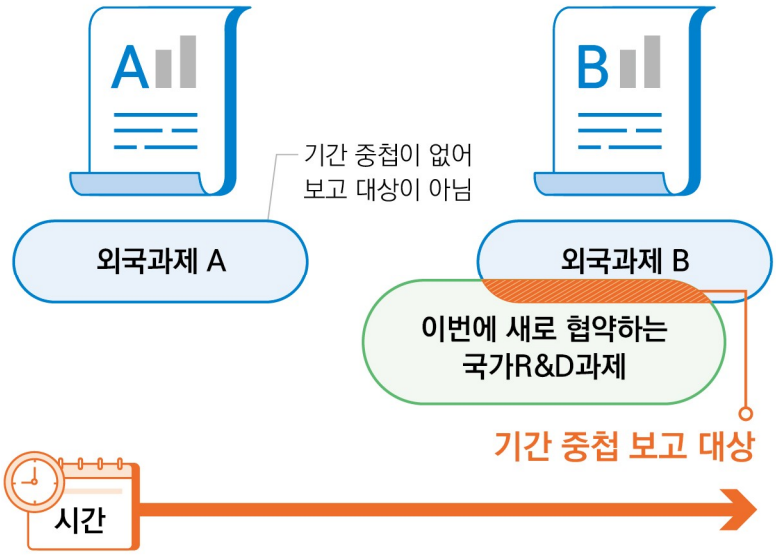
1 연구보안 위험 포인트

» 기술패권 경쟁 속 일부 해외 기관에서 우리 연구자를 유인하여 국가연구자산을 탈취하는 사례가 증가하고 있습니다.

» 국가연구개발사업을 수행하거나 수행하고자 하는 연구책임자라면 국외로부터의 지원 또는 지원예정 사항을 투명하게 공개하여 안전하게 국제협력을 추진할 수 있도록 해야 합니다.

2 권고사항 및 의무

- **(보고 의무 대상자)** [법] 국가연구개발사업을 수행하거나 수행하고자 하는 주관연구기관의 연구책임자 및 공동·위탁연구기관의 책임자입니다.
- **(보고 의무 발생기간)** [법] '국가R&D 수행기간과 중첩' 되는 시기에 대한 보고를 추진합니다.



- **(보고 의무 범위)** [법] 외국의 정부·기관·단체로부터의 ❶재정적·행정적 지원, ❷노무 또는 자문을 제공하고 받는 대가에 대해 보고합니다.

❶ 재정적·행정적 지원: 연구시설·시설, 연구인력, 겸직 등

❷ 노무 또는 자문을 제공하고 받는 대가: 동일 기관으로부터 연간 5,000달러 이상의 금전·유가증권·교통·숙박 등 제공받은 경우 보고의 대상이 됨

• 국가연구개발사업을 수행하거나 수행하고자 하는 연구책임자라면 국외수혜정보 보고 대상, 의무보고 기간, 보고범위, 보고내용 전반에 대한 숙지 필요	□Yes □No

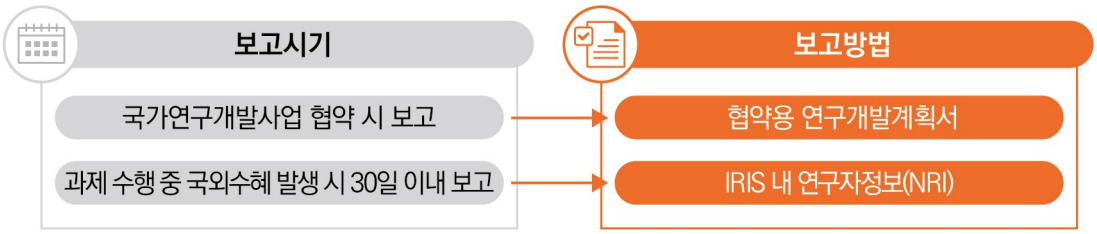
구분	상세예시	보고대상
외국의 연구과제 지원	신청, 선정, 지정, 협약, 계약	O
	단순 문의, 제안, 논의, 지원 종료	X
외국의 학술활동 지원(강의/자문)	동일 기관으로부터 연간 5,000달러 이상 지원	O
	동일 기관으로부터 연간 5,000달러 미만의 지원	X
	대가 없는 자문 수행 및 명예직	X
외국의 연구시설 장비 지원	해외기관이 현저히 낮은 금액 또는 무상으로 장비 증여	O
	정당한 대가 지불 후 해외 연구기관 실험장비 구매	X
	기존 이용료가 높은 해외 연구시설을 무료 이용	O
	기존 이용료가 높은 해외 연구시설을 정당한 대가 지불 후 이용	X
	기존 이용료 무료인 해외 기관 시설장비 단순 공동 활용	X
외국의 연구인력 지원	국가R&D 참여연구원이 아닌 외국인 연구원의 과제 참여	O
	국가R&D 참여연구원인 외국인 연구원의 과제 참여	X

- **(보고시기)** [법] 처음 국외수혜정보 보고를 하게 되는 시기는 국가연구개발사업의 '협약' 단계입니다. 과제를 수행하는 중간에 새로운 국외수혜사항이 생기는 경우 30일 내에 보고하시기를 권고합니다.

• 국가R&D 협약 시 국외수혜정보 보고 필요 사항을 IRIS-NRI 또는 연구개발과제 계획서에 기입	□Yes □No
• 국가R&D 수행 중이라도 국외수혜정보 보고 사항 발생 시 30일 이내 IRIS-NRI에 내용 보고 추진	□Yes □No

- **(보고항목)** [법] 국외수혜정보 보고 항목은 '지원지급 사유, 내용, 기간, 국가' 등입니다.

- **(보고 방법)** [법] 국가연구개발사업의 협약용 연구개발계획서에 기재하거나 IRIS 내의 국가연구자정보 시스템(NRI)에 입력할 수 있습니다.
  - (협약 시기) IRIS 연구자정보(NRI)에 관련 정보를 기재하시면 협약용 연구개발계획서로 연동 됩니다.
  - (과제 중간) IRIS 연구자정보(NRI)에서 내용을 직접 업데이트 하셔야 합니다.



[그림] IRIS 국가연구자정보시스템(NRI)의 국외수혜정보 보고 입력 메뉴 위치

- **(위반처벌)** [법] 고의 또는 과실로 보고를 누락하거나 허위보고 하였을 경우 혁신법 제31조에 따른 '거짓이나 그 밖의 부정한 방법으로 연구개발과제를 수행하는 행위'에 해당되어 제재부가금의 부과 및 국가연구개발활동에 대한 참여제한이 가능합니다.
- **(문의처)** 국외수혜정보 보고 관련 문의가 있을 시에는 소속된 연구기관의 사업관리 담당부서 또는 연구보안 담당부서, 과제 발주 전문기관 담당자, R&D 신문고 등에 문의하실 수 있습니다.

3 연구보안 모의사례

❶ 국외수혜정보 보고 누락 사례

가상상황	• 국가연구개발사업 연구책임자인 공공연구기관의 A박사는 1,000만원 상당의 지분을 수여받는 대가로 해외 B 기업 대상 자문을 추진하였다. A박사의 자문은 국가연구개발사업과 중첩되는 사안이 다수 존재했고 해외 B기업은 A박사의 자문에 힘입어 특허 출원 및 제품 판매를 진행하기까지 했다. • A박사는 국가연구개발사업을 추진 중에 있기 때문에 IRIS NRI(국가연구자정보시스템)에 국외수혜정보 보고를 추진해야 한다는 것을 알고는 있었지만 귀찮기도 하고 왠지 꺼림칙하여 국외수혜정보 보고를 하지 않았다. • 한편, 국가연구개발사업 전문기관 담당자 C씨는 국내 기업체로부터 해외 B기업이 A박사와 경제적으로 밀접한 관계를 맺고 있으며 A박사의 연구결과와 유사한 내용으로 제품 판매를 진행하고 있음을 파악하게 되었다. • 전문기관 담당자 C씨는 A박사에게 사실 관계를 보고하라고 공식적으로 요청 하였으나 A 박사는 해당 사실을 부인하였다. 이에 전문기관 담당자 C씨는 '연구성과 사용에 대한 부정행위 및 국가R&D과제를 거짓으로 수행한 경우'로 A박사를 처분하였다.
연구보안 포인트	✓ 연구책임자는 과제수행 도중에 발생한 국외수혜정보 보고를 IRIS에 신고해야 합니다. ✓ 전문기관 담당자, 연구기관 보안담당자는 소속 연구자의 국외수혜정보 보고에 대한 사항을 안내해야 합니다. ✓ 고의 또는 중과실로 국외수혜정보를 보고하지 않거나 허위 보고한 경우 국가R&D과제를 거짓으로 수행하거나 신청한 경우에 해당되어 제재처분 대상이 될 수 있습니다.

4 관련 법규 및 매뉴얼

- 국가연구개발혁신법 매뉴얼에 국외수혜정보 보고 가이드라인을 제공하고 있으니 참고하시기 바랍니다.
- 국가연구개발혁신법에 따라 국가연구개발사업의 연구책임자·책임자는 협약 시에 연구개발기간 동안 발생할 국외수혜 사항을 연구개발과제계획서에 보고해야 합니다.

국가연구개발혁신법

제9조(연구개발과제 및 연구기관의 공모 절차) ③ 연구개발계획서에는 다음 각 호의 사항이 포함돼야 한다.
8. 연구책임자가 연구개발기간 동안 외국의 정부·기관·단체 등으로부터 받는 행정적·재정적 지원이나 노무 또는 자문 등을 제공하고 받는 대가에 관한 사항

국가연구개발혁신법 시행규칙

별지 제1호서식 연구개발계획서의 연구책임자 등 현황
아. 연구개발기간 동안 외국의 정부·기관·단체 등으로부터 받는 행정적·재정적 지원이나 노무 또는 자문 등을 제공하고 받는 대가에 관한 사항(협약 시에만 제출합니다)

02. 개인 국제협력 및 해외 기관 진출

1 연구보안 위험 포인트

» 국제교류가 활발해 짐에 따라 연구자 개인 자격으로 국제협력을 하거나, 해외기관 파견·취업을 하는 경우도 빈번해지고 있습니다.

» 글로벌 스탠다드에 부합하는 연구보안 원칙을 지켜나갈 때 지속 가능한 국제협력이 가능해지므로 연구자들은 협력 대상 국가의 연구보안 수칙을 사전에 검토해 두어야 합니다.

» 세계 공통적으로 연구자에게는 쉽고 기본적인 연구보안 원칙 준수를 강조하므로 평소 기초적인 연구보안 규칙을 준수해 왔다면 해외의 연구보안 문화에도 쉽게 익숙해질 수 있습니다.

2 권고사항 및 의무

❶ 과제 시작

- **(정보공개)** 미국·EU 국가 공통으로 '정부R&D 연구계획서' 작성 시, 연구자의 투명한 정보공개*를 요구하고 있으므로 연구자는 평소 개인의 연구수혜 이력 등을 관리해두어 국외 펀딩 연구기관의 요구에 대응할 수 있도록 합니다.

  * 외국 기관 자금 및 현물 수혜여부, 자문 역할, 겸임 역할, 외국 인재 채용 프로그램 참여 과거이력, 기타 펀딩 수혜내역 등

  – 일부 대학·연구소 중에는 소속기관 연구자들에게 내부 시스템에 외부 활동, 국제협력 내역을 신고하도록 하는 경우도 있으니 기관 방침에 따르시기 바랍니다.

- **(수출통제)** 미국·EU 국가들 대부분 수출통제 기술에 대한 외국인 접근 제한원칙을 고수하고 있으며 제한적으로만 정부 사전승인을 통하여 외국인 접근을 허가하고 있습니다. 수출통제 기술은 각국의 기밀이므로 연구분야가 해당 기술과 연관되었다면 각국의 규정을 철저하게 준수해야 합니다.

  * 참고: 우리나라의 경우에도 대외무역법 등에 따른 전략물자에 해당하는 사안에 대한 국제공동연구 수행 시, 수출허가를 득하고 과제를 수행해야 함

- **(기관별 안내준수)** 해외 대학, 국공립연구기관은 상위 법령을 정리하여 기관 내부에 독자적인 보안 체계를 만들어 연구자에게 안내하고 있습니다. 기관마다 보안수준이 다를 수 있으므로 기관 안내사항과 교육 제공 내용을 준수해야 합니다.

• 개인의 과제수행, 자문이력, 겸직 등을 미리 정리해 둠	□Yes □No
• 연구자 활동국가의 요구에 따라 정보공개 요구 사항 사전 확인	□Yes □No
• 연구자 활동 국가의 수출통제 기술에 대해 이해	□Yes □No
• 연구자 활동 기관의 연구보안 교육, 안내사항 준수	□Yes □No

❷ 과제 수행

- **(신뢰관계)** 해외 대학, 국공립연구기관은 외국인을 관리하는 현장 책임자(Host)에게 많은 책임과 권한을 부여하고 있습니다. 지속적 협력 연구를 진행하기 위해서는 이들과 두터운 신뢰 관계를 형성해 두어야 합니다.

- **(보안관리 체계)** 미국·EU 등 주요 국가의 국공립연구소는 '기술 및 문서 등급, 연구성격'에 따라 외국인 연구자의 정보 접근권한, 시설출입 통제 등을 제한하고 있습니다. 기관 별 방침이 다를 수 있으나 일반적 주의사항은 아래와 같습니다.
- **(문서데이터 관리)** 기관 별 보안등급 체계에 따라 자료공유 수준, 이메일 송부 절차가 달라질 수 있으므로 이 점에 유의하시기 바랍니다.

  ※ 예를 들어 미국 에너지부(DOE)의 경우 DOE O 471.3에 의거 외부 공개 시 잠재적 국가적, 상업적 피해를 입힐 수 있는 정보를 포함한 문서를 Official Use Only Information으로 지정하고 해당 문서 별 명확히 표기함, 또한 등급 별 '접근권한, 대외공개 정책, 데이터 교환' 정책을 달리하고 있음

- **(시설출입)** 외국인 연구자 '방문가능 지역, 일자' 등 연구보안 계획(Security Plan)에 대해 현지 연구 책임자에게 문의 합니다. 사원증 관리, 내부 사진을 SNS에 업로드하지 않는 등 기초적인 사안에 대한 주의도 필요 합니다.
- **(정보기기)** 반입이 필요한 정보기기에 대해 사전 승인절차가 있는지 확인하고 필요 시 사전승인을 받도록 합니다.
  - **(발표자료 검토)** 기관의 보안등급 체계 별 발표 가능 내용이 달라질 수 있습니다. 각 기관 보안 담당자는 연구자의 외부 발표 내용 중 수출통제 관련 기술이 포함되어 있는 지 여부를 검토할 수 있습니다.
  - **(기관방문)** 연구 목적으로 국방·에너지 시설 방문 시 사전에 심사절차가 존재할 수 있으므로 이를 사전에 알아보고 준비하도록 합니다.
- **(기타)** 미국·EU를 중심으로 개인정보보호, 연구데이터 관리에 대한 교육 및 관리체계가 강화되고 있습니다. 연구자는 소속 해외기관 및 학계의 방침에 따라 해당 내용을 관리하도록 합니다.
  - **(개인정보보호 방침)** 미국·EU의 경우 개인이 사적 이익을 위해 개인정보가 포함된 데이터를 활용하지 못하도록 개인정보 보호, 관리에 대한 교육을 철저히 하고 있습니다.
  - **(연구데이터)** 미국·EU를 중심으로 연구재현성, 연구무결성을 추구하기 위한 연구데이터 공개가 확산되고 있습니다. 연구자는 불이익을 받지 않도록 연구 과정 중 창출된 데이터를 소속 해외기관 방침에 따라 관리하도록 합니다.

❸ 성과공개 및 활용

- **(성과 대외공개)** 해외 기관에서 관리하는 보안등급에 따라 논문발표, 특허출원 관련 보안심의가 있을 수 있으므로 관련 계획이 있다면 현장책임자(host) 등에게 먼저 문의하도록 합니다.
- **(지식재산 활용)** 해외 국가의 지식재산 관련 법률이 우리나라와 상이하여, 연구자가 발명자인 지식재산 일지라도 활용에 어려움을 겪을 수 있으므로 사전에 명확한 계약 조건을 설정하여 불필요한 충돌을 방지하도록 합니다.

  ※ 예를 들어 미국의 경우 공동특허 활용 시, 공동 출원인의 허락없이 실시 가능하나 우리나라법률의 경우 공동 출원인 모두의 허가가 필요[8)]

8) 특허청(법무법인 다래). (2024), 한미 국제공동연구 계약서 작성 안내서

3 연구보안 모의사례

❶ 악의적으로 겸임 및 외국자원 지급여부를 미공개 한 사례[9)]

가상상황	• S대에서 박사학위를 수여받은 한국인 J씨는 미국에서 Post-doc을 하다 미국 H대학에서 5년째 연구 중이다. J씨는 2024년 1월에 NIH 펀드 지원을 획득하여 12개월 간 연구를 진행하게 되었다. 비슷한 시기에 J씨는 모교인 S대로부터 여름, 겨울방학인 4개월 동안 강의 및 연구를 진행할 수 없겠냐는 연락을 받았다. S대학 지원 내용은 급여, 연구개발과제 비용, 집세, 여행비 등이 포함되어 있었고 J씨는 해당 제안을 수락 하였다. J씨는 H대학의 방침에 따라 국제협력 및 외부활동을 보고 했어야 하나 이를 제대로 공개하지 않았다. • 여름방학에 맞춰 한국에 도착한 J씨는 NIH 펀드로 수여받은 과제 내용과 거의 유사한 내용으로 연구계획서를 한국 전문기관에 제출하여 과제를 수주하기까지 했다. • 미국에 돌아간 J씨는 NIH 중간보고(Progress Report)에 "귀하의 개인 연구 활동 관련 외부 지원에 변화가 있습니까?"라는 질의에 "보고 사항 없음"이라고 표시하였다. • J씨의 한국 귀국이 너무 잦아 이를 수상하게 여긴 미국 H대학 관계자는 인터넷 검색을 통해 J씨가 한국에서 유사한 연구개발과제를 수행하고 발표도 하였다는 사실을 알게 되었다. • H대학은 J를 해고하게 되었고 NIH는 자금 지원을 회수 하기로 결정 하였다.
연구보안 포인트	✓ 미국 연방 R&D 과제에 참여하는 모든 연구자는 자국 내외 직위, 겸직, 자문, 명예직, 금전적 대가 등을 연구계획서에 보고해야 합니다. ✓ 소속 기관 방침에 따라서 동일한 내용을 기관에도 보고해야 할 수 있습니다.

4 관련 법규 및 매뉴얼

- 미국 국립과학재단(NSF)의 경우 NSF펀딩 과제에 참여하는 모든 연구자를 대상으로 외국 정부·기관과의 모든 관계(자문·명예직·방문연구 등)를 연구계획서에 공개하도록 하고 있습니다.

  ※ 참고 : NSF PAPPG(Proposal & Award Policies & Procedures Guide): 미국 국립과학재단(NSF)의 제안 및 수상 절차에 관한 지침을 제공하는 문서

- 영국 연구혁신청(UKRI) 또한 연구비 신청자에 한하여 외국기관과의 관계를 포함한 개인적, 영리적 이해관계 신고를 의무화 하였습니다.

  ※ 참고: UKRI, Declaration of Interest ('20)

참고 미국 에너지부(DOE) 국제협력 시작 시 개인의 주의사항

- 미국 에너지부(DOE)는 개인단위의 외국영향을 관리하기 위하여 '위험국가 인재유치 프로그램 참여 금지, 외국인 신원 조사 및 정보접근 제한'에 대한 정책을 펼치고 있습니다. 만약 우리나라 연구자가 DOE 산하 국공립 연구기관에 '파견, 채용, 방문 시' 아래와 같은 사안을 주의하여 준비를 추진하도록 합니다.

  ※ 사업 및 기술기반 관련 사항은 3-2-1.협약·계약 시 연구보안(p.59) 참고

9) NIH. (2023), NIH Foreign Interference: General Principles, Case Studies, Publicly Available Information on Specific Cases, and Oversight Reports. 참고하여 재작성

- 우리나라 연구자가 DOE와 다양한 형태의 국제협력을 고려하고 있다면 연구자 개인의 국내외 연구비 수혜 이력 및 연구자원(연구실 시설, 연구원)의 출처 등을 체계적으로 정리해 둘 필요성이 있습니다.
- 미국 시민권·영주권이 없는 한국인은 모두 DOE 기준의 외국인으로 간주되어 DOE 시설 접근 및 정보 교류 시 사전 승인이 필요하므로 관련 서류에 미비함이 없도록 준비해야 합니다.
- DOE 산하 연구소라도 연구소별 보안수준이 많이 다를 수 있음을 감안하여 세부조치는 파견대상 연구소의 규정과 절차를 반영하고 따를 필요가 있습니다.

〈참고〉 개인 단위의 DOE 산하 국공립연구소 파견, 연구진행 시 참고 사항

DOE 규정명	구분	주요 내용
1 외국정부 연계활동 통제 (DOE O 486.1A)	규정주요 내용	**① 적용대상자 및 목적** • DOE 계약자* 및 직원 등에 대한 위험국가** 관련 활동파악 * CRADA, SPP, ACT 범위 내에서 DOE/NNSA 사이트 또는 임대공간에서 보수 수령 여부와 무관하게 R&D를 수행하는 연구자는 "Contractor Personnel"로 간주되어 본 규정의 적용 대상임 ** Countries of Risk: 중국·러시아·이란·북한·벨라루스('25.5월 기준) **② 주요 요구사항** • '위험국가 인재유치 프로그램*' 참여를 원칙적으로 금지 * 예시: 천인계획, 메가그랜트 프로그램 등 • 사전보고 누락 및 허위 신고 시 협력중단 및 참여제한 가능 ※ CRADA 규정(DOE Order 483.1B)에 관련 정보를 요청하는 절차는 명시되어 있지 않으나, 본 규정에 따라 요청이 가능할 수 있으므로 유의
	우리나라 연구자 상황별 적용 예시*	**① 개인이 DOE와 계약자(Contractor Personnel) 상태인 경우** • 위험국가가 제공하는 '인재유치 프로그램 참여' 금지 **② 정부 양자 간 국제협력으로 DOE 산하기관에 파견가는 경우** • 정부 양자 간 협력 프로젝트인 경우 관련 규정의 면제적용이 가능하나 계약 형태에 따라 다를 수 있으므로 주의가 필요함
2 외국인 신원 조사 및 DOE 자산 등 접근 통제 DOE O 142.3B	규정주요 내용	**① 적용대상자 및 목적** • 비 미국 국적자의 DOE 시설, 정보, 기술 접근 관리 **② 주요 요구사항** • DOE와 협력 또는 방문 시 서류 제출* * Access Request, 이력서, 이민/비자상태, 국가 위험도 평가, 테러, 배경 조사 등 • 외국인 정보를 DOE 담당자가 FACTS(Foreign Access Central Tracking System) 시스템 등록* * 민감국가 국적자가 국가핵안보청(NNSA: National Nuclear Security Administration) 연구소 접근 시 사전 신원조회를 위해 접근 시작일 최소 45일 전까지 FACTS에 입력해야 하므로 빠른 정보제출 필요 • DOE 근무 현장책임자(Host) 지정

	우리나라 연구자 상황별 적용 예시*	**① 미국 시민권·영주권이 없는 개인 자격으로 DOE 산하 기관 방문, 정보 접근 요구가 필요할 때** • DOE 관계자 현장책임자(Host) 지정, FACTS 등록, 서류 제출 등 추진하여 사전 승인 • DOE 관계자는 외국인의 신원, 시설/정보 접근 필요성, 기술 단위 위험성에 따라 접근범위 등 평가하여 승인 허가 • 현장책임자(Host)의 관리감독, 보안계획(Security Plan)에 따라 승인된 정보/시설 접근 가능 **② 국가 단위 국제협력으로 DOE 방문, 파견 가는 경우** • 동일절차 진행 • 다만, DOE가 참여하는 공식 국제협력 프로젝트의 경우 한국 연구자는 양 국가(기관) 간 사전에 합의된 시설/정보에 대한 접근 • 보안계획(Security Plan)에 따라 합의된 정보/시설 접근 • 현장책임자(Host)의 관리감독

* 예시 상황이며 실제 적용 내용은 DOE 산하 국공립연구소의 보안수준과 상세규정, 개별 계약 사안에 따라 달라질 수 있음

03. 보안과제 수행 연구자의 외국과제 수행

1 연구보안 위험 포인트

» 연구과제를 수행할 때, 연구비 제공자가 연구자에게 직·간접적으로 자료의 제공 등을 요구할 경우 이를 거절하기가 쉽지 않습니다.

» 보안과제를 수행중이거나, 수행한지 얼마되지 않은 연구자(종료 후 3년 이내)가 외국으로부터 연구비 지원을 받는 경우 관련 현황을 연구보안 담당부서 등에 알려 시스템적으로 보안과제 관련 내용이 유출되지 않도록 도움을 받아야 합니다.

2 권고사항 및 의무

- [법] '현재 보안과제 수행 중이거나 보안과제 수행 후 3년 이내인 연구자'가 외국으로부터 지원을 받아 연구개발과제*를 수행하고자 하는 경우 해당 사실을 소속 기관의 연구보안 담당부서에 알리고 연구보안 심의회의에 심의를 요청해야 합니다.

  * 외국과의 학술활동(강의, 자문)을 제외한 용역 형태, 공동 및 위탁연구개발과제(예: 해외수탁과제)

  – 연구자가 보행과제 수행 종료 후 3년 이내에 다른 기관에 이직했다면 해당 기관에 심의를 요청해야 하며 퇴직하였다면 마지막 소속기관에 심의를 요청하시면 됩니다.

- [법] 연구자는 연구보안심의회의 심의자료 작성을 지원하며, 이 때 '과제지원 국외국가 및 기관명, 과제 지원 범위 및 기간, 보안과제 관련성, 수혜경위' 등을 보고하고 연구보안심의회의에서 이를 검토할 수 있도록 합니다.

- [법] 연구자의 소속 연구기관의 장은 연구보안심의회의 심의·의결을 거쳐 보안과제 수행 연구자의 외국과제 수행을 승인합니다.

- [법] 연구보안 담당부서는 기관장 승인 후 한달 이내에 보안과제 관련 중앙행정기관의 장에게 관련 내용을 보고하고 국정원에 관련 사실을 통보 합니다.

  – 연구자는 중앙행정기관의 과제 담당자에게 관련 사실을 보고하는 것을 지원할 수 있습니다.

• 보안과제 수행 연구자가 국외 지원 연구과제를 수행할 경우 연구보안심의회 심의·의결 및 연구기관장의 사전 승인 필요	☐Yes ☐No
• 연구기관장의 사전 승인 후 한달 이내 중앙행정기관 장에게 관련 내용 보고 필요	☐Yes ☐No
• 연구기관 장의 사전 승인 후 한달 이내 국정원 장에게 관련 사실을 통보 필요	☐Yes ☐No

3 연구보안 모의사례

❶ 보안과제 수행 후 퇴직자의 연구자산 유출 사례

가상상황	• A출연연에서 은퇴한 B씨는 해외 한 국가에서 이전에 수출한 연구기술과 관련하여 일자리를 제안받았다. B씨 입장에서는 은퇴 후 생계가 막막해지기도 하였고 국가적으로 권장되었던 수출이라 일자리 제안을 받아들이는 데에는 크게 망설임이 없었다. • B씨는 A출연연 퇴사 시에 관련 영업비밀을 유출하지 않기로 서약하였고 데이터도 최대한 활용하지 않기로 교육받았다. 특히 보안과제를 수행하고 3년이 채 되지 않은 시점이라 보안과제 유출 방지를 위한 교육도 추가로 받았다. • 하지만 막상 해외 국가로 이직해 보니 현장의 기술적 요구상황이 긴급하기도 하고 또 머릿속에 이미 지득한 지식이 많아 B씨는 자연스럽게 관련 지식을 해외국가에 전수하게 되었다. 그 중 일부는 보안과제를 수행하며 알게 된 노하우도 있다는 생각도 들었지만 구분하기가 모호하다는 생각도 들었다.
연구보안 포인트	✓ '은퇴자' 일지라도 보안과제 수행 후 3년 이내인 상황이라면 과제관련 외국접촉 시 '외국접촉 보고서'를 제출해야 합니다. ✓ 연구기관은 해당 은퇴자의 동향을 보안과제 3년 이내 시점까지 추적할 것을 권고합니다.

4 관련 법규 및 매뉴얼

- 보안과제 수행 중 또는 수행 후 3년 이내 참여연구원이 외국기관(정부·단체·기관)으로부터 지원을 받아 연구를 수행하게 될 시, 연구기관의 장은 관련 내용을 사전 승인해야 합니다.
- 연구기관의 사전 승인 후에 한달 내에 과제담당 중앙행정기관 장에 대한 보고, 국가정보원 통보가 필요합니다.

국가연구개발사업 보안대책

제8조(외국 정부 등과의 접촉 관리 등) ② 보안과제를 수행하고 있거나 수행한지 3년이 지나지 아니한 연구자가 외국 정부·기관·단체 등의 지원을 받아 연구개발을 수행하는 경우 사전에 연구보안심의회의 심의를 거쳐 현재 연구자가 소속된 연구개발기관의 장(퇴직으로 소속기관이 없거나 법 제2조제3호에 따른 연구개발기관이 아닌 기관으로 이직하는 경우에는 마지막으로 소속되었던 연구개발기관의 장)의 사전 승인을 받아야 한다.
③ 연구개발기관의 장은 제1항에 따라 보고받은 사항, 제2항에 따라 사전 승인한 사항을 보고 및 승인 후 1월 이내에 중앙행정기관의 장에 보고하고 국가정보원장에 통보한다.

제4장 기술사업화 단계의 연구보안

제1절 기술이전 및 창업을 하려 해요!

01. 기술이전, 양도, 해외수출 시 주의사항

1 연구보안 위험 포인트

» 국민 세금으로 창출한 연구개발성과를 실시하여 널리 확산 되도록 하는 것은 바람직한 방향입니다. 하지만 무분별한 성과확산으로 국가 연구자산이 유출되지 않도록 적절한 보호조치가 필요합니다.

» 보안과제에서 창출된 연구개발성과물에 대한 기술실시계약을 체결할 시, 적절한 보안조치를 취하지 않는다면 보안사고가 발생할 수 있기에 면밀한 주의가 필요합니다.

» 특히 해외로의 성과양도 및 수출 시에는 중앙행정기관의 사전승인 등 다양한 이해관계자의 합의가 이뤄져야 합니다.

2 권고사항 및 의무

❶ 일반 기술이전 시 보안 및 지식재산 검토 사항

- 국가연구개발혁신법 상 일반과제의 연구개발성과 기술이전·양도·해외수출에 대해서는 별도의 제약이 존재하지 않습니다.
  - 다만 소중한 연구자산을 보호하기 위하여 연구개발성과 실시를 추진하는 과정 중 아래와 같은 사항에 대한 검토를 추진하는 것이 바람직 합니다.
  - 연구자 단독으로 해당 과정을 해내기 어려우므로 기관의 연구보안 및 기술이전 사업화 담당자, 외부 전문가 그룹 등의 도움을 받으시길 바랍니다.

• (계약 전) 기술이전 희망업체의 신용, 재정상태에 대한 평판 검토	☐Yes ☐No
• (계약 전) 기술이전 희망업체와 상담 시, 상담내용 관련 비밀유지계약 체결	☐Yes ☐No
• (계약 단계) 기술이전 대상 기관의 연구보안 관련 수준이 미비하다고 판단된다면 부가적인 보호대책을 계약서에 기재할 수 있도록 검토	☐Yes ☐No
• (계약 단계) 대상기관의 개량기술 관련 보안조치 및 지식재산권 소유 관련 조항을 검토	☐Yes ☐No
• (계약 단계) 비밀유지계약 위반 시 손해배상 의무가 있음을 계약서에 명시	☐Yes ☐No
• (계약 단계) 기술이전 계약 만료 및 해지 시에도 비밀유지의무를 유효한 것으로 명시	☐Yes ☐No
• (계약 단계) 기술이전 해지 시에 기술자료 반납, 폐기 요청을 계약서에 명시	☐Yes ☐No
• (계약 단계) 대상기관 매출액 실태조사 연계 혹은 별도로 기술이전 보안관리 실태를 조사할 수 있도록 조항 추가	☐Yes ☐No
• (계약 단계) 기술이전 목록, 기술지도·전수 및 완료확인서 징구조항을 계약서에 명시	☐Yes ☐No

❷ 보안과제 관련 소유권 양도, 기술이전, 해외수출

- [법] 보안과제에서 창출된 연구개발성과는 원칙 상 소유권의 양도가 불가합니다.
  - [법] 소유권 양도가 필요한 경우가 발생한다면 소유권을 이전받는 기관이 원 연구개발성과소유기관에서 추진하고 있던 '보안대책(고시)의 제3조~15조'를 지킬 수 있도록 해야 합니다.

• 보안과제 연구개발성과 소유권 양도가 반드시 필요한 것인지 검토	□Yes □No
• 보안과제 연구개발성과 소유권 양도계약 시 소유권을 이전받는 기관이 보안대책 제3조~제15조를 지키도록 계약 체결	□Yes □No

- [법] 보안과제의 연구개발성과를 외국기업 또는 외국으로 수출하고자 할 경우에는 중앙행정기관의 장의 사전 승인을 얻어야 합니다.

• 보안과제 연구개발성과를 외국기업 및 외국 수출 시 중앙행정기관 장 사전 승인	□Yes □No

- [법] 보안과제에서 창출된 연구개발성과를 다른 기관과 실시계약을 체결하려는 경우 '제3자 기술 실시(사용)권 금지협약'을 체결하여야 합니다.

• 성과 소유 기관이 다른 기관과 보안과제 실시 계약 시 제3자 기술실시권 금지협약 체결	□Yes □No

- [법] '대외무역법' 상 전략물자나 '산업기술보호법' 상 국가핵심기술, '방위산업기술'은 수출통제 대상이므로, 해당 법령에 영향을 받는 과제라면 관련 법령 및 절차를 준수해야 하므로 주의가 필요합니다.
  - 만약 대외무역법에 따른 '전략물자'이자 산업기술보호법에 따른' 국가핵심기술'에 해당하는 경우 산업기술보호법에 따른 승인을 받았다면, 대외무역법에 따른 허가를 받은 것으로 봅니다. 단, 반대의 경우는 해당하지 않습니다.
  - 보안과제에도 해당한다면 관련 절차를 모두 준수해야 합니다.

• 전략물자, 국가핵심기술, 방위산업기술 해당여부 검토	□Yes □No

3 연구보안 모의사례

❶ 보안과제에서 해외수출 발생한 건

가상상황	• 대학 기술사업화팀 A책임은 최근 해외 기술이전을 준비하고 있다. 그런데 해당 기술이 국가안보와 연관이 있을 것 같은 생각이 들어 여러 정보를 알아보니 해당 성과를 창출한 과제 중 하나가 '보안과제'라는 것을 확인할 수 있었다. 또한 전략물자관리시스템 판정에 따라 '대외무역법'에 의한 '전략물자'에도 해당한다는 것을 알게 되었다. A책임은 연구보안 담당부서에 보안절차 재확인을 위한 연락을 하게 되었다. • 연구보안 담당부서는 A책임에게 '보안과제'에 대해서는 과제 발주 부처(또는 전문기관)에 해외 기술이전을 승인 받아야 하고 전략물자에 대해서는 산업통상자원부에 수출허가를 받아야 함을 안내하였다. • 기술사업화팀과 연구보안 팀은 이에 따라 '보안과제' 관련 부서인 '과학기술정보통신부'와 '전략물자'를 주관하는 '산업통상자원부' 승인을 모두 준비하게 되었다.
연구보안 포인트	✓ 해외 수출과 관련된 법률(대외무역법, 산업기술보호법 등)을 검토해야 하며 '보안과제' 뿐 아니라 '전략물자, 국가핵심기술 등'에도 해당 된다면 관련 법을 모두 따라야만 합니다.

4 관련 법규 및 매뉴얼

- 보안과제 뿐 아니라 산업보안, 국방보안에 해당 시 다음 규정을 준수해야 하므로 확인 바랍니다.

구분	법령 내용	근거법
국가핵심기술	• 외국기업 등에 국가핵심기술에 해당하는 특허권의 양도·실시권의 설정·영업비밀의 이전을 하고자 하는 경우 산업부 장관 승인 • 매각 및 이전 시 산업부 장관승인	산업기술보호법 제11조, 산업기술보호지침 제4장
전략물자	• 전략물자를 국내에서 국외로 이전(정보통신망·매체·구두 등)하는 경우 산업부장관 및 관계부처 허가필요	대외무역법 제19조의2
	• 전략물자 수출 관련 절차 준수	대외무역법제23조, 전략물자 등 수출통관에 관한 고시
방위산업기술	• 국내기술이전 계약 체결 전 외부망, 출입통제 등에 대한 대책 강구 • 해외수출 이전 보호대책 강구, 방위사업청장에 수출허가 신청	방위산업기술 보호지침제38조

- 보안과제에서 창출된 연구개발성과를 외국에 수출하거나 이전하는 경우에는 관련 절차를 준수하여야 하며 사전에 연구보안 담당부서, 기술이전 관련부서와 협의 하여야 합니다.

국가연구개발사업 보안대책

제15조(보안과제 연구개발성과의 귀속 및 실시) ① 보안과제를 통해 창출된 연구개발성과를 협약에 따라 소유하고 있는 기관은 그 성과의 소유권을 특별한 사정이 없는 한 이전하지 않는 것을 원칙으로 한다.
② 제1항에도 불구하고 보안과제로부터 창출된 연구개발성과의 소유권을 국내의 다른 기관으로 이전할 필요성이 있을 때에는 이전받는 기관이 제3조부터 제15조까지를 적용받도록 계약을 체결하여야 하며, 이 때 제3조부터 제15조의 '연구기관'은 성과를 이전받는 기관으로 본다. 다만 외국으로의 소유권 이전이 불가피할 경우에는 이에 대하여 중앙행정기관의 장의 사전 승인을 얻어야 한다.
③ 보안과제의 연구개발성과에 대하여 다른 기관과 실시계약을 체결하려는 경우 '제3자 기술 실시(사용)권 금지협약'을 체결하여야 하며, 외국기업 또는 외국으로 수출하고자 할 경우에는 중앙행정기관의 장의 사전 승인을 얻어야 한다.

02. 실험실 창업

1 연구보안 위험 포인트

» 대학공공연 보유 기술을 기반으로 한 실험실 창업 기업수가 증가하고 있습니다.

» 해당 기업의 경우, 원 소속기관의 연구보안 관리를 벗어나 스스로 보안을 지켜야 하나 소수 인력이 다양한 업무를 수행하게 되고 외부 개입이 많을 수 밖에 없어 보안관리 전반에 취약점이 있을 수 있습니다.

※ 외부 투자 필요, 후속 공동연구 추진, M&A 등 지속해야 하며 잦은 이직 발생 가능

» 실험실 창업을 위한 휴·겸직 기간 내에 연구자가 창출한 발명이 원 소속기관의 직무발명에 해당되는지 여부 등에 대해 상호 심사숙고하여 판단하므로 연구자-연구기관 간 갈등을 예방하도록 합니다.

2 권고사항 및 의무

❶ 실험실 창업 허가단계

- 연구기관은 필요에 따라 창업 허가 시 직무발명과 지식재산권 보호사항, 연구보안사항을 포함하여 창업자와 표준 협약서/서약서를 작성할 수 있습니다.
  - 실험실 창업 시 창업자와 연구기관 간 직무발명 관련 충돌이 발생하지 않도록 특허 출원 등에 대해 사전 협의를 진행해야 합니다.
  - 연구보안 관련해서 실험실 창업 투자계약, M&A 발생 시 원소속기관과 상의하도록 하거나 보안실태 점검을 포함시키는 등의 특약을 제시할 수 있습니다.
- [법] 보안과제에서 파생된 연구개발성과를 활용한 창업이라면 '소유권 양도, 성과실시'와 관련하여 '4-1-1. 기술이전·양도·해외수출 시 주의사항(p.79)'의 법적 의무를 모두 따라야 합니다.
- 연구원 창업자는 창업기업의 연구수행에 참여한 참여연구자들을 대상으로 한 교육, 보안각서 등을 통해 연구내용이 외부에 유출되지 않도록 책임져야 합니다.

• 실험실 창업 시 연구기관과 보안사항 협의	□Yes □No
• 실험실 창업 시 연구기관과 직무발명 관련 충돌이 발생하지 않도록 특허 출원 등에 사전 협의	□Yes □No

❷ 실험실 창업 투자 주의사항

- 실험실 창업 관련 투자 제안을 받았을 때, 창업자는 해당 기업 혹은 투자자의 연구 보안 사고 이력, 평판을 검토해 보아야 합니다. 투자유치를 위한 기술적 사안을 논의하기에 앞서 NDA를 체결하여 상호 비밀 보장을 유지하도록 합니다.
- 실험실 창업 이후 M&A를 추진하고자 할 경우에 산업핵심기술, 전략물자에 해당하지 않는지 판정 절차를 거친 후에 진행합니다.

• 실험실 창업 투자 시 관련 사항을 소속 기관에 문의	□Yes □No
• 투자기관이 제3국의 외국기관의 지배를 받는 경우인지	□Yes □No
• 해당 투자기관에 문제가 된 연구보안 사고사례가 있었는지	□Yes □No
• 투자기관과 사업계획 구상 시, NDA 체결	□Yes □No
• 실험실 창업 투자 대상 기술(또는 기업 자체)이 국가핵심기술, 전략물자 등에 해당하는지 여부 점검	□Yes □No

3 연구보안 모의사례

❶ 실험실 창업 기업의 M&A 사례

가상상황	• S대의 A교수는 국가연구개발사업의 장기적인 지원으로 기초연구의 상업화 단계에 이르게 되었다. 사업성이 있다고 판단하여 S대 로부터 기술을 양도받고 정부의 지원을 받아 창업도 하게 되었다. 하지만 사업 과정은 연구와 매우 달라 경영이 쉽지 않았고 사업을 진행할수록 끊임없이 돈이 들어 포기하고 싶어졌다. 또한 국내 시장이 예상보다 빠르게 성장하지 않아 미래를 장담하기 어려웠다. • 마침 중국의 C기업이 M&A를 제시해 왔고 A교수는 협상을 진행하기로 마음먹었다. 그 과정에서 정부 및 공공기관 관계자가 찾아와 해당 기술이 보안과제, 국가핵심기술에 해당하는지 판정하게 되었고 판정 결과 해당 사항이 없어 M&A 허가가 떨어졌다. • 국가연구개발사업에서 투자된 기술을 M&A 해도 되는지 마음에 걸렸지만 A교수의 기술은 국내 시장이 형성되지 않은 단계라 선택지가 없다는 결론을 내렸다. A교수는 기술료를 통해 정부에 보답해야겠다고 생각했다.
연구보안 포인트	✓ 연구기관 연구보안심의회의는 실험실 창업 허가 시, 창업 대상기술의 보안과제 해당 여부에 대해 검토해야 합니다. ✓ 연구기관은 보안과제 관련 실험실 창업자에게 '국가연구개발사업 보안대책'에 대한 관리 현황 자료 제출을 요구할 수 있습니다. ✓ 해외수출 시 보안과제·전략물자·국가핵심기술 해당 여부를 확인하고 중앙행정기관장의 허가를 받아야 합니다.

❷ 창업기업 직무발명 미신고 사례

가상상황	• A출연연 소속 김박사는 본인이 발명자인 A출연연의 특허 7건을 가지고 2018.1. 주식회사 G사를 창업하였다. 창업겸직(2018.7~2021.7)중이던 2018.12월에 과거 재직 중 수행한 연구개발 직무분야와 관련성 있는 발명 등 5건을 해당 기업 명의로 특허출원 하였다. • A출연연의 창업 규정 중에는 '창업 중 발생한 지식재산권이 직무발명인 경우 원소속기관으로 귀속된다'는 조항이 존재하였다. 이에 따라 김박사는 기업 명의로 5건의 특허를 출원하기 전에 기관에 신고하여 직무발명 여부를 판단 받아야만 했는데 김박사는 해당 절차를 무시하였다. • A출연연은 직무발명신고 등 절차를 지키라고 김박사에게 요청하였다. 또한 특허심의위원회에서 해당 특허가 직무분야와 관련이 있는 발명인지 검토하게 되었다.
연구보안 포인트	✓ 예비창업기간, 창업휴직 및 겸직기간 중에 발생한 창업자의 원 소속기관 관련 직무발명에 따른 모든 지식재산권은 출원전에 즉시 신고해야 합니다.

4 관련 법규 및 매뉴얼

- 보안과제 뿐 아니라 국가핵심기술, 전략물자, 방위산업기술에 해당 시 다음 규정을 준수해야 하므로 확인 바랍니다.

구분	법령 내용	근거법
국가핵심기술	• 해외 인수·합병, 합작투자 시 장관 승인	산업기술보호법 제11조의2 산업기술보호지침 제26조~제33조
방위산업기술	• 인수·합병 발생 시에도 보호대책 추진	방위산업기술보호지침 제40조

- 출연연의 경우 아래 규정을 준수해야 합니다.

출연(연) 연구원창업 규정 가이드라인(국가과학기술연구회, 2024.8)

제10조(연구개발결과 및 지식재산권 등 사용)

① 창업지원기간 동안 창업대상기술에 대해서는 창업자에게 실시권을 부여할 수 있다.

② 창업자 및 창업참여자는 창업지원기간 이후 발생한 연구개발결과 및 지식재산권 등에 있어서 관련 법령 및 "연구기관"의 규정에 따른다.

③ "연구기관"은 창업기업에게 기술료를 징수할 수 있으며 징수비율, 금액 등은 "위원회"에서 관련 법령 및 "연구기관"의 규정에 따라 결정한다.

④ 예비창업기간, 창업휴직 및 겸직기간 중에 발생한 창업자의 원 소속기관의 직무발명에 따른 모든 지식재산권은 출원전에 즉시 신고해야 하며, 관련 위원회에서 직무발명으로 판단된 연구결과의 소유지분은 "연구기관"과 창업기업의 협의에 따른다.

제2절 품목화 된 기술보호를 위해 어떻게 해야 되나요?

01. 산업보안·국방보안 판정절차 및 주의사항

1 연구보안 위험 포인트

» 연구기술이 보안과제에 해당하는지 여부에 대한 판단과 더불어 산업보안·국방보안에 해당하는 영역이 있는지도 살펴야 합니다.

» 연구보안·산업보안·국방보안을 동시에 지킴으로써 연구자산 유출에 대한 위험요소를 최소화 할 수 있습니다.

2 권고사항 및 의무

- [법] 산업보안, 국방보안 분야에서는 아래와 같은 제도를 운영하여 기술 보호를 추진하고 있습니다.
- [법] 보안과제 수행 연구기관은 국가핵심기술 판정 필요성 및 후속조치, 판정절차, 의무사항 위반 시 불이익 등을 해당 연구자에게 교육하도록 되어 있습니다. 연구자는 해당 교육을 이수하시길 바랍니다.

기술구분	정의	판정내용	판정절차
1.국가핵심기술[10] (산업통상자원부: 산업기술보호법)	• 국내외 시장에서 차지하는 기술적·경제적 가치가 높거나 관련 산업의 성장잠재력이 높아 해외로 유출될 경우에 국가의 안전보장 및 국민경제의 발전에 중대한 악영향을 줄 우려가 있는 기술	• '국가핵심기술 지정 등에 관한 고시'에 따른 국가핵심기술목록 해당 여부 판정	• 기술보유 기관의 판정 신청→산업통상자원부 여부판정 진행→신청 받은 후 15일이내 판정
2. 전략물자기술 (산업통상자원부: 대외무역법)[11]	• 재래식무기 또는 대량파괴무기와 이의 운반수단인 미사일의 제조, 개발, 사용 또는 보관 등에 이용 가능한 물품, SW, 기술 • 국제평화와 안전유지, 국가안보를 위해 수출입에 제한	• '전략물자 수출입고시'에 따른 이중용도품목, 상황허가 대상품목, 군용물자 품목 해당 여부를 판정	• (자가판정) 전략물자관리 시스템에서 온라인 자가 판정이 가능하나 산업부로부터 자격을 부여받은 자율준수무역거래자 AA 등급 이상만 가능 • (전문판정) 개인·기업의 신청→전문판정 기관이 전략물자 해당 여부를 판정→접수일로부터 15일 이내 판정
3. 방위산업기술 (방위사업청: 방위산업기술 보호법)[12]	• 방위산업과 관련한 국방과학기술 중 국가안보 등을 위하여 보호되어야 하는 기술	• '방위산업기술 지정 고시'에 따른 기술 해당 여부 판정	• 기술보유 기관의 판정→신청신청일로부터 15일 이내 방위사업청의 판정

- 연구자는 관련 법률에 따라 자가 판정을 시도해 볼 수 있으며 혼란스러운 경우 소속 기관의 연구보안 담당 부서에 반드시 문의해야 합니다.

• 산업보안, 국방보안 해당 여부가 의심되는 경우 연구보안(산업보안) 담당 부서에 국가핵심기술, 전략물자기술, 방위산업기술 등 여부 판정지원 요청	☐Yes ☐No

- 연구자가 '산업보안, 국방보안' 해당되는 기술을 연구한다면 '외국기관 참여, 외국인 참여, 성과공개, 외국정보 교류' 등에서 많은 주의를 기울어야 합니다. 사전 교육을 필수적으로 수강하시기를 권고하며 '전문기관 및 기관 내 연구보안 담당부서'와 긴밀히 업무에 대해 논의하시길 바랍니다.

3 연구보안 모의사례

❶ 연구자가 해외 학회에서 국가핵심기술이 포함된 연구자료를 발표

가상상황	• 연구자 A는 반도체 공정 관련 연구를 수행하며 해외 학회에서 연구결과를 발표하였다. 그러나 연구자가 발표한 내용 중 국가핵심기술에 해당되는 내용이 있었음에도 불구하고 사전 보안성 검토 과정을 거치지 않았다. 발표 이후, 외국 연구기관에서 해당 내용을 바탕으로 유사한 연구를 진행하는 정황이 포착되었으며, 국가핵심기술 유출 위험이 제기되었다.
연구보안 포인트	✓ 연구자는 해외 학회 발표 전 발표자료가 국가핵심기술 및 전략물자기술 등에 해당되는지 스스로 점검해야 합니다. ✓ 연구자는 연구책임자 및 연구보안/산업보안 담당자에게 발표자료 내용의 국가핵심기술 및 전략물자기술 해당 여부를 확인받아야 합니다.

4 관련 법규 및 매뉴얼

- 국가핵심기술, 전략물자, 방위산업기술에 해당 시 관련 법령을 준수해야하므로 각별한 주의가 필요합니다.

산업기술의 유출방지 및 보호에 관한 법률

제2조(정의) 2. "국가핵심기술"이라 함은 국내외 시장에서 차지하는 기술적·경제적 가치가 높거나 관련 산업의 성장잠재력이 높아 해외로 유출될 경우에 국가의 안전보장 및 국민경제의 발전에 중대한 악영향을 줄 우려가 있는 기술로서 제9조의 규정에 따라 지정된 것을 말한다.

대외무역법

제19조(전략물자) 산업통상자원부장관은 관계 행정기관의 장과 협의하여 국제평화 및 안전유지와 국가안보를 위하여 필요하다고 인정하는 경우에는 대통령령으로 정하는 국제수출통제체제 또는 이에 준하는 다자간 수출통제 공조(이하 "국제수출통제체제등"이라 한다)에 따라 수출허가 등 제한이 필요한 물품등(대통령령으로 정하는 기술을 포함한다. 이하 이 절에서 같다)을 지정·고시하여야 한다.

---

10) 산업보안 행정지원시스템, https://is-support.or.kr/coretech/coretech01
11) 전략물자관리시스템, https://yestrade.go.kr/user/main.do?method=main
12) 방산수출입지원시스템, https://www.d4b.go.kr/index.do

방위산업기술보호법

제2조(정의) "방위산업기술"이란 방위산업과 관련한 국방과학기술 중 국가안보 등을 위하여 보호되어야 하는 기술로서 방위사업청장이 제7조에 따라 지정하고 고시한 것을 말한다.

- 보안과제 수행 연구기관은 국가핵심기술 판정절차, 전략물자 및 국가핵심기술 위무사항 위반 시 불이익 등을 연구자에게 안내해야 합니다.

국가연구개발사업 보안대책

[별표] 연구기관보안대책에 포함되어야 하는 사항(제4조 관련)

1. 보안관리체계
   바. 소속 직원의 보안교육 이수 의무에 관한 사항

※ 연구기관보안대책에 따른 연구자의 의무, 우대사항 및 의무사항 위반시 「산업기술의 유출방지 및 보호에 관한 법률」, 「대외무역법」에 따라 받을 수 있는 불이익에 관한 사항과 연구성과에 대한 「산업기술의 유출방지 및 보호에 관한 법률」상 핵심기술 판정 필요성과 후속조치 등

참고 보안과제 관리 시 함께 검토가 필요한 산업 및 국방보안 조치 및 법령

- 아래는 보안과제 관리 영역 별 함께 주의가 필요한 보안 주의사항을 정리한 것입니다. 아래 보안 조치 이행 전 과제관리 전문기관, 연구보안 담당자와 반드시 상의하셔야 합니다.

과제관리	구분	상황 및 조치	관련 법령
외국기관 연구참여 (p.64 참고)	보안과제	• 보안과제에 외국 연구기관 참여 시 기관장·부처 사전승인·국정원통보	보안대책 제9조 제2~4항
	국가핵심기술	• 국가핵심기술이 실질적으로 이전·공유되는 외국기업 등과의 연구 시 산업부장관 승인 ※ 산업기술보호법 상 수출행위	산업기술보호지침 제17조
	전략물자	• 참여하는 외국기관과 전략물자(기술)를 연구 시 산업부장관 승인 ※ 대외무역법상 상 기술이전행위	대외무역법 시행령 제32조의3
	방위산업기술	• 외국정부와의 합작·기술제휴 시 기술보호정책 마련 및 계약체결. 필요 시 국정원 협조	방위산업기술 보호지침 제39조
외국인참여/관리 (p.52 참고)	보안과제	• 외국인 참여 시 기관장승인·부처보고·국정원 통보	혁신법 시행령 제46조 제3호 및 제4호
		• 외국인 참여범위 제한	보안대책 제9조 제4항
	국가핵심기술	• 국가핵심기술을 인수·합병하려는 외국인의 비밀 유지 의무	산업기술보호법 제34조 제3의2호
	전략물자	• 외국인 고용 시 외국인이 제공받게 되는 정보가 전략물자 인지 확인 필요	대외무역법 시행령 제32조의3
	방위산업기술	• 상시출입 외국인의 출입통제, 기술보호서약, 교육, 출입통제, 정보통신 매체 이용 전반에 대한 계획	방위산업기술 보호지침 제21조

과제관리	구분	상황 및 조치	관련 법령
		• 외국인이 대상기술을 취급할 수 없으나 필요 시 방위사업청장·국가정보원장 신고, 상시출입 외국인의 출입통제, 기술보호서약, 교육, 출입통제, 정보통신 매체 이용 전반에 대한 계획	방위산업기술 보호지침 제22조
		• 상시출입 외부인·외국인을 보호지역에서 근무하게 할 수 없으며 필요 시 범위 설정 필요	방위산업기술 보호지침 제26조
		• 외부인·외국인 방문은 특정목적(단순방문, 견학 제외)이 있을때만 허가, 보호대책 및 출입현황 기록관리 필요	방위산업기술 보호지침 제28조
외국과 정보교류 (외국접촉) (p.25 참고)	**보안과제**	• 보안과제 관련 유의미하고 지속적 접촉 시 기관 보고·부처보고·국정원통보	보안대책 제8조 제2항 및 3항
		• 해외출장 교육 및 보고	보안대책 제4조
	국가핵심기술	• 외국정부·기관에 국가핵심기술 용역자료, 해외 인허가 자료 제공, 클라우드 등 접근허가 시 산업부 장관 승인 ※ 산업기술보호법 상 수출행위	산업기술보호 지침 제17조
	전략물자	• 정보통신망(전화·팩스·이메일), 구두나 행위 (이전·교육·훈련·실연), 정보처리장치(기록매체·컴퓨터)을 통한 기술이전 시 산업부장관 및 관계부처 승인 ※ 대외무역법 상 기술이전 행위	대외무역법 시행령 제32조의3
	방위산업기술	• 방산기술 관련자 해외출장 시에 관련 정보를 저장 및 송신하지 않아야 함	방위산업기술 보호지침 제23조
		• 출장관련 임직원의 정보보안교육, 저장매체 반출 점검, 복귀 후 점검	방위산업기술 보호지침 제23조
연구데이터·자료관리 (p.39 참고)	**보안과제**	• 보안등급 세분화	보안대책 제10조
	국가핵심기술	• 보호등급 부여, 취급인력 권한관리, 암호화, 이력 유지관리, 자료반출 승인	산업기술보호법 제10조 및 시행령 제14조, 산업기술보호지침 제3장
	방위산업기술	• 일반기술과 방위산업 기술을 표시·보관	방위산업기술 보호지침 제14조
성과공개 (p.18, 22, 42 참고)	**보안과제**	• 비공개 필요시 부처 승인	혁신법 제17조 제2항 혁신법 시행령 제35조 제2항 및 제3항
	국가핵심기술	• 공공기관은 국가핵심기술 정보 비공개, 필요 시 장관승인	산업기술보호법 제9조의2
	방위산업기술	• 성과 공개 시 부서장, 기술보호책임자 승인 필요	방위산업기술 보호지침 제16조

과제관리	구분	상황 및 조치	관련 법령
성과실시 (p.79, 82 참고)	보안과제	• 실시계약 체결 시 보안특약, 해외수출 및 소유권 이전시 부처 사전승인	보안대책 제15조
	국가핵심기술	• 외국기업에 국가핵심기술자료전송·양도·기술지도·위탁연구·인력파견 시 산업부장관 승인 ※ 산업기술보호법 상 수출행위	산업기술보호지침 제17조
		• 외국기업 등에 국가핵심기술에 해당하는 특허권의 양도·실시권의 설정·영업비밀의 이전을 하고자 하는 경우 산업부 장관 승인 ※ 산업기술보호법 상 수출행위	산업기술보호지침 제17조
		• 매각 및 이전 시 산업부 장관승인	산업기술보호법 제11조
		• 해외 인수·합병, 합작투자 시 장관 승인	산업기술보호법 제11조의2, 산업기술보호지침 제26조~제33조
	전략물자	• 전략물자를 국내에서 국외로 이전(정보통신망·매체·구두 등)하는 경우 산업부장관 및 관계부처 허가필요	대외무역법 제19조2
		• 전략물자 수출 관련 절차 준수	대외무역법 제23조, 전략물자수출입고시
		• 특허권의 경우 수출허가가 필요하지 않으나 노하우 제공(기술파견, 추가기술정보) 시 수출허가 필요	대외무역법 제19조2 (전략물자 길라잡이 (2023))
	방위산업기술	• 국내기술이전 계약 체결 전 외부망, 출입통제 등에 대한 대책강구	방위산업기술 보호지침 제38조
		• 해외수출 이전 보호대책 강구, 방위사업청장에 수출허가 신청	방위산업기술 보호지침 제38조
		• 인수·합병 발생 시에도 보호대책 추진	방위산업기술 보호지침 제40조

02. 기술임치를 통한 지식재산 보호

1 연구보안 위험 포인트

» 공공연구기관, 중소기업과의 공동연구 시, 폐업 혹은 영업비밀이나 노하우 관리가 제대로 되지 않아 연구성과가 특허출원 전에 유출되는 경우가 있습니다.

» 다양한 규모의 기업이 공동기관으로 연구개발과제에 참여하는 경우 상호 기술탈취를 우려해야 할 수 있습니다.

2 권고사항 및 의무

- 연구자는 함께 업무를 수행하는 기업이 폐업, 파산하거나 영업비밀 등이 잘 관리되지 않는 경우를 대비하여 협의하에 SW 및 기술 임치를 제안할 수 있습니다.
- 중소기업 연구소가 타 기업과 연구를 진행하는 중에 기술탈취가 염려된다면 기술을 임치할 수 있습니다.
- 우리나라의 대표적인 기술임치 기관은 '저작권 위원회 SW 임치제도'와 '대중소기업 농어업협력재단 기술자료임치센터'가 있습니다.

• 공동연구 중인 상용화 단계 기술 탈취, 기업도산이 우려되는 경우 기술임치 고려	☐Yes ☐No

3 연구보안 모의사례

❶ 기술임치를 통한 연구자산 보호[13)]

가상상황	• A연구실의 D박사는 C중소기업와 공동으로 무기체계 관련 SW를 개발한 상태이다. 김박사는 C중소기업이 해당 기술을 다른 공급처에 제공하는 경우나, 또는 기업이 망하여 SW를 못 쓰게 되는 경우를 대비해야 겠다는 생각이 들었다. 이에 D박사는 연구보안 담당부서에 혹시 아이디어가 있는지 문의하였다. • 연구보안 담당부서는 대중소기업 농어업협력재단 기술자료임치센터, 저작권위원회 SW 임치제도를 활용해 다자간 임치협약을 체결한다면 충분한 안전장치가 될 것임을 안내하고 관련 비용을 간접비에서 지원할 수 있다고 하였다.
연구보안 포인트	✓ 연구비 사용 규정에 따라 기술임치 관련 간접비 사용이 가능합니다.

13) 중소벤처기업부, 대중소기업농어업협력재단. (2020), 기술자료 임치제도 우수사례집. (참고하여 사례 작성).

4 관련 법규 및 매뉴얼

- 기술임치비용은 연구보안관리비 비목으로 활용할 수 있습니다.

국가연구개발사업 연구개발비 사용 기준

제16조(연구지원비 사용용도)
6. 연구보안관리비 : 연구개발과제 수행과 관련한 다음 각 목의 비용
   가. 보안장비 구입, 보안교육, 보안취약점 진단, 보안사고 대응 지원 또는 보안컨설팅 등 연구보안 활동 관련 비용
   나. 「대·중소기업 상생협력 촉진에 관한 법률」 제24조의2에 따른 기술자료 임치 관련 비용
   다. 「산업기술의 유출방지 및 보호에 관한 법률」 제10조제1항에 따른 국가핵심기술의 보호조치 관련 비용
   라. 그 밖에 연구개발과제 보안을 위한 비용

- 연구자가 공동으로 연구하는 중소기업 등이 '모방특허를 우려해 특허출원을 꺼려하거나, 보안 인프라가 미비한 경우', 연구자는 보안에 대해 우려할 수 밖에 없습니다. 이 때 기술임치 제도를 적극 활용하여 공동연구성과 유출을 방지할 수 있습니다.

대·중소기업 상생협력 촉진에 관한 법률

제24조의2(기술자료 임치제도) ① 수탁·위탁기업[수탁·위탁기업 외에 단독 또는 공동으로 기술자료를 임치(任置)하고자 하는 기업을 포함한다]은 전문인력과 설비 등을 갖춘 기관으로서 대통령령으로 정하는 기관[이하 "수치인"(受置人)이라 한다]과 서로 합의하여 기술자료를 임치하고자 하는 기업(이하 "임치기업"이라 한다)의 기술자료를 임치할 수 있다.
② 위탁기업은 다음 각 호의 어느 하나에 해당하는 경우에는 수치인에게 수탁기업이 임치한 기술자료를 내줄 것을 요청할 수 있다.
1. 수탁기업이 동의한 경우
2. 수탁기업이 파산선고 또는 해산결의로 그 권리가 소멸되거나 사업장을 폐쇄하여 사업을 할 수 없는 경우 등 위탁기업과 수탁기업이 협의하여 정한 기술자료 교부조건에 부합하는 경우
③ 수치인은 중소벤처기업부장관이 정하는 기술자료 교부조건에 부합하는 경우에 임치기업의 기술자료를 요청한 자에게 이를 교부한다.
④ 정부는 수치인에게 예산의 범위에서 필요한 지원을 할 수 있다.
⑤ 그 밖에 기술자료의 임치 등에 필요한 사항은 대통령령으로 정한다.

저작권법

제101조의7(프로그램의 임치) ① 프로그램의 저작재산권자와 프로그램의 이용허락을 받은 자는 대통령령으로 정하는 자(이하 이 조에서 "수치인"이라 한다)와 서로 합의하여 프로그램의 원시코드 및 기술정보 등을 수치인에게 임치할 수 있다.
② 프로그램의 이용허락을 받은 자는 제1항에 따른 합의에서 정한 사유가 발생한 때에 수치인에게 프로그램의 원시코드 및 기술정보 등의 제공을 요구할 수 있다.

제5장 연구보안 사고 대응

제1절 연구보안 사고가 발생하고 말았어요!

01. 연구보안 사고 대응절차 및 연구자 행동

1 연구보안 위험 포인트

» 연구보안 사고는 불시에 발생하는 경우가 많고, 조기에 체계적으로 대응하지 않는다면 피해규모가 더욱 커질 수 있습니다.

» 연구보안 사고의 주된 목격자가 될 수 있는 연구자가 평소 연구보안 사고에 대해 무관심하다면 쉽사리 자산 유출의 타깃이 될 수 있고 실수로 사고를 발생시킬 수도 있으므로 주의해야 합니다.

» 연구기관 내 일어나는 단순 분실, 출입증 대여 등의 일상적 상황이 연구성과물 절취 및 연구보안 사고로 발전되는 경우도 많기에 평소 경각심을 가져야 합니다.

2 권고사항 및 의무

❶ 연구보안 사고란

- [법] 연구보안 사고란 보안과제 등 중요 연구개발과제 관련 '연구개발성과 및 정보, 해당 성과 및 정보를 유통·관리하는 시스템' 등이 침해·유출·누설·분실·훼손·도난·파손·파괴 되는 경우를 지칭합니다.

〈표 〉 연구보안 사고의 의미와 종류

상세 내용(혁신법 시행령 제48조)
• 제44조제1항 각 호에 해당하는 연구개발성과의 침해·유출·누설·분실·훼손·도난 • 제44조제1항 각 호에 해당하는 연구개발성과를 유통·관리·보존하는 시스템의 유출·파손·파괴 ※ 제44조제1항 각 호에 해당하는 연구개발성과 1) 「산업기술의 유출방지 및 보호에 관한 법률」 제2조제1호에 따른 산업기술과 관련된 비공개 연구개발성과 2) 법 제21조제2항에 따라 보안과제로 분류된 연구개발과제의 연구개발성과

❷ 연구보안 사고 사전 예방

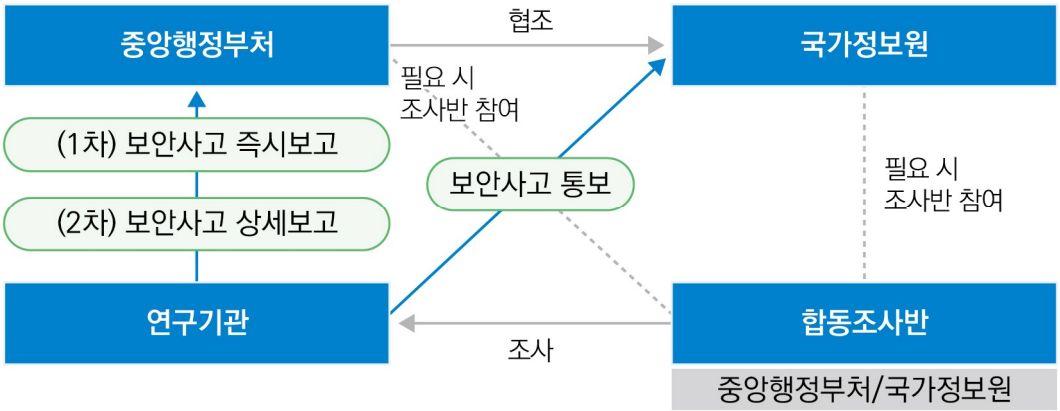
- 연구기관은 보안사고 예방 및 대응 방법 등을 명시한 규정 제정, 담당자 지정 등을 통해 보안사고를 지속적으로 예방하도록 합니다.
  - 연구기관은 연구보안 사고 관련 연구부서 실태점검, 모의 훈련 등을 실시할 수 있으며 연구자는 이에 적극 협조해야 합니다.
- 연구자가 연구보안 사고를 인지하고 예방하기 위해서 사전에 기관으로부터 연구보안 교육을 받도록 합니다.

• 연구 중 데이터 유출, 해킹 등 보안 사고가 발생할 경우에 대비한 비상 대응 계획에 대해 인지하고 있는 지	☐Yes ☐No
• 연구보안 사고의 유형에 대해 인지하고 있는 지	☐Yes ☐No
• 연구보안 사고 발생 시 담당자가 누구인지 인지하고 있는 지	☐Yes ☐No

❸ 연구보안 사고 발생 시 조치

- [법] **(①상황파악·즉시보고)** 연구자가 연구보안 사고가 발생한 사실을 최초로 인지한 경우에 상급자 또는 연구보안 담당부서에 최대한 빠른 시간 내에 이 사실을 알려야 합니다. 연구보안 담당부서는 사고확산 방지조치를 한 후, 사고발생 사실을 담당 중앙행정기관에게 즉각 보고하고, 국가정보원에 통보해야 합니다.
- **(②사실확인)** 연구기관은 관련 법령에 따른 보안 규정 상 하자를 파악하고 보안사고 경위에 대하여 정리합니다.
  - 연구보안, 일반보안, 정보보안 담당자로 구성된 사고대응반을 소집할 수 있으며 필요 시 관계기관에 조사 협조를 요청할 수 있습니다.
- [법] **(③상위기관 상세보고)** 보안사고 발생 사실을 알린 이후, '사고평가와 사실확인'을 거쳐 보안사고 전반에 대한 사항을 파악하여 지체없이 담당 중앙행정기관 장, 과학기술정보통신부에 보고하고 국가정보원에 통보합니다.

  1. 보안사고의 일시·장소
  2. 보안사고를 낸 사람의 인적사항
  3. 보안사고의 세부 내용
- [법] **(④관계기관 조사)** 중앙행정기관과 국가정보원, 관계기관은 필요에 따라 합동조사반을 구성하여 연구보안 사고원인 및 피해규모, 보안사고 대책 준수여부등을 조사할 수 있습니다.
  - 이 때 연구보안 사고 관련 연구자는 최대한 조사에 협조해야 합니다.



❹ 연구보안 사고 발생 후 사후조치

- [법] 연구기관은 연구보안 사고 원인분석, 재발방지 대책, 보안위반자 징계, 상위기관 시정명령 등을 포함한 후속 대책을 수립할 수 있습니다.

3 연구보안 모의사례

❶ 전산장비 관리 불철저

가상상황	• A박사는 5년간 사용하던 올인원 PC 2대를 폐기하기로 결심하였다. 먼저, 자산관리 부서에 연락하는 것이 절차이지만, A박사는 연구실 정리를 위해 일단 해당 PC를 실험실 밖 복도에 두었다. 또한 자산관리 부서에 전화하는 것을 잊어 버리고 별도의 보안조치 없이 PC를 복도에 3일간 방치하였다. • 이 때 연구동 출입이 가능한 협력업체의 직원인 김과장이 복도에 방치된 PC를 절취 하였다. A박사는 이 사실을 알지 못한 채 자산관리 부서에 PC 폐기를 요청 하였다. PC를 수거하러 온 자산관리부서 담당자는 A박사에게 PC가 어디에 있는지 문의였고 A박사는 그제서야 문제를 파악하였다. A박사는 그 즉시 의심 정황을 연구보안 담당부서에 신고하였다. • 관련사항을 신고받은 연구보안 담당부서는 CCTV와 출입기록을 대조하여 협력업체 김과장이 물품을 절취한 것을 발견하였다. 그 즉시 경찰서에 수사를 의뢰하고 보안사고 관련 관계기관에 상황을 보고하게 되었다.
연구보안 포인트	✓ 연구자는 연구보안 사고가 발생하였음을 직감한 즉시 관련 사실을 연구보안 부서에 신고해야 합니다. ✓ 연구자는 정보와 자산 불용처리 절차를 준수하여야 합니다. 불용처리 전 사용책임자 주관하에 하드디스크 저장내용을 삭제(포맷)하고, 자산관리부서에 불용처리 이관 전까지 자산을 관리하여야 합니다.

4 관련 법규 및 매뉴얼

- 혁신법 및 관계규정에서는 연구보안 사고의 종류, 상위 기관 보고 내용 및 절차, 연구기관의 대응 등에 대해 안내하고 있습니다.

국가연구개발혁신법 시행령

제48조(보안사고에 대한 조치) ① 연구개발기관의 장은 다음 각 호의 어느 하나에 해당하는 사고(이하 "보안사고"라 한다)가 발생한 경우에는 그 사고를 알게 된 즉시 필요한 조치를 하고, 중앙행정기관의 장에게 보고해야 한다.

1. 제44조제1항 각 호에 해당하는 연구개발성과의 침해·유출·누설·분실·훼손·도난
2. 제44조제1항 각 호에 해당하는 연구개발성과를 유통·관리·보존하는 시스템의 유출·파손·파괴

② 연구개발기관의 장은 제1항에 따른 보고를 한 후 다음 각 호의 사항을 파악하여 지체 없이 중앙행정기관의 장에게 보고해야 한다.

1. 보안사고의 일시·장소
2. 보안사고를 낸 사람의 인적사항
3. 보안사고의 세부 내용

③ 중앙행정기관의 장은 보안사고를 알게 되거나 제1항에 따른 보고를 받은 경우에는 그 경위를 조사할 수 있다. 이 경우 해당 연구개발기관과 연구책임자는 조사에 성실히 협조해야 한다.

국가연구개발사업 보안대책

제6조(연구보안심의회의 구성 및 운영) ① 연구기관의 장은 다음 각 호의 사항을 심의하기 위하여 연구기관 내에 연구보안심의회를 구성·운영하여야 한다.

6. 보안사고에 대한 조치계획 및 재발방지 대책에 관한 사항

제13조(보안사고에 대한 조치) ① 연구기관의 장은 영 제48조제1항 및 제2항에 따라 중앙행정기관의 장에게 보안사고에 관한 사항을 보고하고 국가정보원장에 통보한다.

② 중앙행정기관의 장은 영 제48조제3항에 따른 보안사고 경위 조사를 국가정보원과 합동으로 실시한다. 이 경우 조사를 실시하기 전에 다음 각 호의 사항을 국가정보원장과 협의한다.

1. 조사방식(서면 또는 현장) 및 조사시기
2. 조사범위 및 조사방법
3. 조사반 구성
4. 그 밖에 조사에 필요한 사항

제2절 연구보안 규정 위반 이후 어떻게 되나요?

01. 연구보안 규정 위반 시 처분

1 연구보안 위험 포인트

» 혁신법은 연구보안 사고 예방에 초점을 두고 있습니다. 연구보안 관리 규정 위반은 연구자의 경력과 명예에 오점이 될 수 있음을 기억해야 합니다.

» 연구보안 사고가 타 법과 연계되어 처분 시에는 징역형, 벌금형을 받을 수 있으므로 연구자는 이를 유념하여 연구보안 관리 규정을 항상 준수하도록 합니다.

2 권고사항 및 의무

- 연구자는 평소 연구보안 관련 규정 위반 사항이 무엇이고 규정 위반 시 어떠한 처벌을 받게 되는지를 숙지하여 규정을 위반하지 않도록 주의해야 합니다.
- 연구책임자는 참여연구원들이 부지불식간에 연구보안 규정을 위반하지 않도록 주의를 주고 참여연구원들을 관리·감독 합니다.

❶ 연구보안 관리규정 위반자의 참여 제한

- [법] 중앙행정기관의 장은 연구보안 관리규정 위반자가 국가연구개발사업에 참여하는 것을 제한 할 수 있습니다.

〈연구개발 참여제한 처분기준(혁신법 시행령 별표6)〉

참여제한 사유		제한기간
보안대책을 위반한 경우		2년
정당한 절차 없이 연구개발 내용을 누설하거나 유출한 경우	① 국내로 누설·유출	2년
	② 해외로 누설·유출	5년

※ 가중사항에 해당하는 경우에는 참여제한 기간의 2분의 1 범위에서 가중할 수 있음
감경사항에 해당하는 경우 참여제한 기간의 2분의 1 범위에서 감경할 수 있음

※ 둘 이상의 위반행위가 서로 다른 연구개발과제에서 발생한 경우, 가중 및 감경기준을 적용하여 산출된 참여제한 기간을 모두 합산해 정함 (합산 시 최대 10년 가능)

- 연구보안 담당부서에서 보안 위반자를 적발하거나 위반자에 대한 신고를 접수한 경우, 자체 조사를 통하여 징계 안건을 인사관리 부서에 통보하고 인사관리부서는 징계 안건을 토대로 그에 합당한 징계 조치를 부여합니다.

❷ 연구보안 관리규정 위반자의 제재부가금 처분기준

- [법] 중앙행정기관의 장은 연구보안 관리규정 위반자에게 제재부가금을 처분하거나 제재처분과 별도로 이미 지급한 정부 연구개발비 중 제재사유와 관련된 연구개발비를 환수할 수 있습니다.

〈연구개발 참여제한 처분기준 혁신법 시행령 별표7〉

제재처분 사유	제재부가금 부과액 (이미 지급한 정부 연구개발비 기준)	
	제재처분 대상이 연구기관인 경우	제재처분 대상이 개인인 경우
보안대책 위반	정부지원연구개발비 전액	정부지원연구개발비 전액의 100분의 20
보안과제로 분류된 연구개발과제의 보안사항을 국내에 누설하거나 유출하는 행위	정부지원연구개발비 전액	정부지원연구개발비 전액의 100분의 20
보안과제로 분류된 연구개발과제의 보안사항을 국외에 누설하거나 유출하는 행위	정부지원연구개발비 전액의 100분의 250	정부지원연구개발비 전액의 100분의 50

※ 가중기준에 해당하는 경우에는 제재부가금의 2분의 1 범위에서 가중할 수 있음
감경사항에 해당하는 경우 제재부가금의 2분의 1 범위에서 감경할 수 있음

※ 둘 이상의 위반행위가 서로 다른 연구개발과제에서 발생한 경우, 가중 및 감경기준을 적용하여 산출된 제재부가금 부과액을 모두 합산하여 정함 (합산 시 기지급 정부연구지원연구개발비의 최대 5배 한도)

③ 기타

- 국가연구개발사업의 연구보안 관리규정 위반으로 참여제한 및 제재부가금 처분을 받았다 할지라도, 타 법령의 보안규정을 위반한 경우 별도의 벌금형과 징역형에 처해질 수 있습니다.
- 연구기관은 연구보안 관리 규정을 위반한 연구자에 대한 징계를 내릴 시, 외부 기관에서 받은 처벌의 중차대함을 따져 징계 수준을 조정할 수 있습니다.

[참고] 타법령 연관 보안사고 발생 시의 처벌사항

구분	상세내용	근거법
군사기밀과 관련된 연구과제 수행 중 보안사고(누설 등) 발생 시의 제재처분	• 업무상 군사기밀을 취급하는 자가 군사기밀 누설시: 3년 이상의 유기징역 • 과실로 인한 누설의 경우: 2년 이하의 징역 또는 2천만원 이하의 벌금 • 외국을 위해 군사기밀 누설시: 형의 2분의 1까지 가중 처벌 관련하여 본인 또는 제3자가 받은 재산이나 이익은 몰수	군사기밀보호법 제13조 내지 제20조의2
방위산업기술과 관련된 연구과제 수행 중 보안사고(누설 등) 발생 시의 제재처분	• 비밀유지의무를 위반하여 비밀을 누설·도용한 경우: 7년 이하의 징역 또는 10년 이하의 자격정지 또는 7천만원 이하의 벌금 • 과실로 인하여 방위산업기술을 취득·사용 또는 공개하는 경우: 5년 이하의 징역 또는 5억원 이하의 벌금 • 관련하여 본인 또는 제3자가 받은 재산이나 이익은 몰수	방위산업기술 보호법 제19조 내지 제21조

구분	상세내용	근거법
국가핵심기술과 관련된 연구과제 수행 중 보안사고(누설 등) 발생 시의 제재처분	• 비밀유지의무를 위반하여 비밀을 누설·도용한 경우: 5년 이하의 징역 또는 10년 이하의 자격정지 또는 5천만원 이하의 벌금 • 과실로 인하여 국가핵심기술을 취득·사용 또는 공개하는 경우: 3년 이하의 징역 또는 3억원 이하의 벌금 • 관련하여 본인이 얻은 재산은 몰수	산업기술의 유출방지 및 보호에 관한 법률 제34조 내지 제36조
전략물자(기술)과 관련된 연구과제 수행 중 허가 없이 이전한 경우	• 수출허가를 받지 아니하고 전략물자를 수출하거나 수출신고한자 등은 고의성 여부에 따라 5년에서 7년 이하의 징역 또는 수출가액의 3배에서 5배이하의 벌금 • 행정기관의 장은 8시간 이내의 교육명령이나 3년 이내의 수출입제한 가능 • 위반자는 자진신고를 할 수 있으며, 이 경우 고의성 등의 여부에 따라 처분시 참작	대외무역법 제30조, 제49조, 제53조 전략물자수출입고시 제97조의2
연구기관의 연구성과에 해당하는 영업비밀을 국외에 유출하였을 경우 처벌	• 영업비밀 국외유출 : 15년 이하 징역 또는 15억원 이하의 벌금	영업비밀보호법 제18조

02. 연구보안 위반행위에 대한 가중처벌 및 감경 요인

1 연구보안 포인트

» 연구보안 사고에 책임이 있는 연구자라 할지라도 위반의 정도, 조사 협조 수준 등을 고려하여 감경 처분이 가능하므로 보안사고 과정에 성실하게 협조해야 합니다.

» 반면, 연구자가 의도적이고 반복적인 위반 행위를 하는 경우 가중 처벌하여 더 이상 피해가 확산되지 않도록 해야 합니다.

2 권고사항 및 의무

- [법] 연구기관의 장은 연구보안 사고의 고의성, 사소한 부주의 여부, 규정위반 정도, 연구기관의 피해 규모 등을 감안하여 위반자를 처벌할 수 있도록 규정을 마련할 수 있습니다. 연구기관은 관련 규정을 게시판 등에 안내해야 하며 연구자는 이를 잘 숙지해야 합니다.
- [법] 연구보안 규정을 위반한 자일지라도, 보안사고 관련 조사에 성실히 협조한다면 감경 요소가 될 수 있습니다.

〈가중 및 감면기준 혁신법 시행령 별표6 및 별표7〉

감경요소 예시	가중요소 예시
• 위반행위에 대해 중앙행정기관의 장이 실시하는 조사에 성실하게 협조 • 사소한 부주의나 오류로 인한 위반행위 • 그 밖에 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 감경할 필요가 있다고 인정되는 경우 • 연구기관의 장이 부정행위를 검증하여 필요한 조치를 한 경우 (기관 부과 참여제한 또는 제재부가금의 경우에 한함)	• 하나의 연구개발과제에서 발생한 위반행위가 둘 이상인 경우 • 그 밖에 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 가중할 필요가 있다고 인정되는 경우 • 참여제한 기간이 종료된 날부터 5년 이내에 같은 위반행위로 참여제한 처분을 받는 경우 (참여제한의 경우에 한함)

3 연구보안 모의사례

① 연구보안 사고 조사에 성실하게 협조

가상상황	• 보안과제 연구책임자인 송박사는 P국 출신의 외국인의 B연구원과 재료 분야 물성에 대해 함께 연구하고 있다. 송박사는 B연구원에게 실험의 일부를 부탁하면서 장비에 대한 접근 권한을 허가 하였다. • B연구원은 이러한 권한을 악용하여 장비 내 다른 실험데이터를 복사하여 본국으로 귀국하였다. • 뒤늦게 이러한 사실을 알아챈 송박사는 해당 사실을 즉각 소속기관 연구보안 부서에게 신고하였다. 또한 연구보안 담당부서가 중앙행정기관에게 보고하는 내용, 중앙행정기관의 조사 절차에 대해 적극적으로 참여 하였다. • 해당 연구기관에서는 보안사고 관련 조사를 마치고 보안사고 발생의 실마리를 제공한 송박사에 대한 징계조치를 심의하게 되었다. 보안사고심의위원회는 '보안사고를 인지하고 바로 소관기관에 신고한 점, 보안사고의 피해가 크지 않은 점, 송박사가 조사에 적극 도움을 준 점, 평소에 송박사가 보안교육을 잘 이수하고 보안사고 예방에 최선을 다한 점' 등을 고려하여 가벼운 수준의 징계형량을 부여하였다.
연구보안 포인트	✓ 연구책임자 혹은 참여연구원이 부득이하게 연구관리 보안규정을 위반한 경우, 상황을 인지한 뒤 즉시 연구책임자 및 소관 중앙행정부처에 상황을 알리고 조사에 성실하게 임해야 합니다.

4 관련 법규 및 매뉴얼

- 혁신법 및 관계규정에서는 국가연구개발사업에서 발생하는 연구보안대책 위반 및 보안사항의 누설·유출에 대한 제재처분을 규정하고 있습니다.

국가연구개발혁신법

제31조(국가연구개발사업 관련 부정행위의 금지) ① 올바른 연구윤리 확보를 위하여 연구자 및 연구기관은 국가연구개발활동을 수행하는 경우 다음 각 호의 국가연구개발사업 관련 부정행위(이하 "부정행위"라 한다)를 하여서는 아니 된다.

4. 제21조제1항에 따른 보안대책을 위반하거나 제21조제2항에 따라 보안과제로 분류된 연구개발과제의 보안사항을 누설하거나 유출하는 행위

제32조(부정행위 등에 대한 제재처분) ① 중앙행정기관의 장은 다음 각 호의 어느 하나에 해당하는 경우에는 해당 연구기관, 연구책임자, 연구자, 연구지원인력 또는 연구기관 소속 임직원에 대하여 10년 이내의 범위에서 국가연구개발활동(연구지원은 제외한다)에 대한 참여를 제한하거나 이미 지급한 정부 연구개발비의 5배의 범위에서 제재부가금을 부과할 수 있다.

1. 제12조제2항에 따른 평가 결과 연구개발과제의 수행과정과 결과가 극히 불량한 경우
2. 연구자 또는 연구개발기관이 이 법 또는 협약에 따른 의무를 고의로 이행하지 아니하여 제15조제1항에 따라 연구개발과제가 변경 또는 중단된 경우
3. 연구자 또는 연구개발기관이 제31조제1항 각 호의 어느 하나에 해당하는 부정행위를 한 경우
4. 연구자 또는 연구개발기관이 정당한 사유 없이 연구개발과제의 수행을 포기한 경우
5. 연구개발기관이 정당한 사유 없이 제18조제2항에 따른 기술료의 일부 또는 수익의 일부를 납부하지 아니한 경우
6. 연구개발기관이 정당한 사유 없이 제13조제7항에 따른 연구개발비 회수 금액을 납부하지 아니한 경우

② 제1항에 따른 참여제한 처분이나 제재부가금 부과처분은 병과할 수 있다.

③ 중앙행정기관의 장은 제1항 및 제2항에 따른 제재처분과 별도로 이미 지급한 정부 연구개발비 중 제재사유와 관련된 연구개발비를 환수할 수 있다.

④ 중앙행정기관의 장은 제재처분을 하거나 연구개발비를 환수하는 때에는 제재사유의 중대성, 위반행위의 고의 유무, 위반 횟수, 연구개발과제의 수행 단계 및 진행 정도 등을 고려하여야 한다.

⑤ 제1항에 따른 제재처분은 그 제재사유가 발생한 연구개발과제의 종료일 또는 그 제재사유가 발생한 국가연구개발활동의 종료일부터 10년이 지나면 할 수 없다.

⑥ 제1항에 따른 제재사유별 참여제한의 기준 및 제재부가금의 부과기준, 제3항에 따른 연구개발비 환수의 기준 및 범위는 대통령령으로 정한다.

제34조(제재처분의 사후관리) ① 소관 중앙행정기관의 장과 제33조제6항에 따라 결정을 통보받은 관계 중앙행정기관의 장은 참여제한 처분을 받은 자에 대하여 지체 없이 모든 국가연구개발활동(연구지원은 제외한다)에 대한 참여를 제한하여야 한다.

② 중앙행정기관의 장은 제32조에 따라 연구개발비 환수처분 및 제재부가금 부과처분을 받은 자가 환수금 또는 제재부가금을 기한까지 납부하지 아니하면 기간을 정하여 독촉을 하고, 그 지정된 기간 내에 환수금 또는 제재부가금을 내지 아니하면 국세 체납처분의 예에 따라 징수한다.

③ 제2항에 따른 독촉의 절차는 대통령령으로 정한다.