연구책임자 · 참여연구원 대상

연구개발과제 보안관리 교육

국가연구개발사업 보안규정 이해와 실천

상명대학교 천안산학협력단

2026

CONTENTS

목차

01 WHY IT MATTERS

연구보안, 왜 지금 중요한가

국가연구개발사업 규모가 커지고 국제협력·기술경쟁이 심화되면서, 연구성과 유출은 개인·기관을 넘어 국가 경쟁력의 문제가 되었습니다. 관련 법령과 점검도 함께 강화되는 추세입니다.

국가연구개발사업 예산 규모

19.6조 → 31.1조

2018년 대비 2023년 약 1.6배 증가 (12대 국가전략기술 중심)

→ 보안관리 대상·책임도 함께 확대

1

법령 강화

국가연구개발혁신법 개정으로 보안지침·보안대책 체계가 정비되는 추세

2

점검 강화

전문기관·정보당국의 연구보안 현장점검이 상시화

3

국제협력 확대

외국기관 공동연구·외국인 참여가 늘며 관리 필요성 증가

02 CONCEPT

연구보안이란?

보호가치가 있는 대상을, 위험요소로부터 지켜 질서와 안녕을 유지하는 연속적인 활동입니다.

1

보호대상

연구데이터, 연구노트, 시제품, 미공개 성과 등 가치있는 연구자산

→

2

위험요소

정보 유출, 해킹, 무단 접촉·반출 등 위협 + 관리 공백(취약점)

→

3

보안대책

분류·점검·서약·교육 등 상명대 규정에 따른 예방·대응 조치

02 LEGAL FRAMEWORK

관련 법령 체계

국가연구개발혁신법 · 시행령 · 시행규칙

「국가연구개발혁신법」 제21조(국가연구개발사업 등의 보안) · 「동법 시행령」 제44~49조

상명대학교 연구개발과제 보안관리 규정

본교 국가연구개발과제 수행 시 준수해야 하는 자체 규정 (제정 2009 · 2차 개정 2024.11.15)

별표 1 보안등급 분류 기준 점검표 · 별표 2 보안서약서

실무에서 실제로 작성·제출하는 서식

※ 본 교육자료는 상명대학교 규정과 서식을 기준으로 구성되었습니다. 세부 의무의 적용 여부는 과제의 유형 및 보안등급에 따라 달라질 수 있습니다.

03 CLASSIFICATION

보안등급 분류: 보안과제 vs 일반과제

보안과제

정의

수행성과가 대외로 유출될 경우 기술적·재산적 가치의 손실이 예상되어 일정 수준의 보안조치가 필요한 과제

적용

규정 제8조에 따른 보안조치 전면 적용 (외국기관 위탁 제한 · 외국인 접촉관리 · 서약서 제출 등)

일반과제

정의

보안과제로 지정되지 아니한 과제

적용

소관기관 요청 또는 심의위원회 위원장이 필요성을 인정하는 경우 보안조치 준용 가능

근거: 상명대학교 연구개발과제 보안관리 규정 제5조(분류기준)

03 CLASSIFICATION

보안과제 분류기준

1. 지식재산권 확보와 관련해 기술유출 가능성이 있는 연구
2. 세계 초일류 기술제품 개발과 관련되는 연구
3. 외국의 기술이전 거부로 국산화 추진 중이거나 보호 필요성이 인정되는 연구
4. 국방·안보 관련 기술로 전용 가능한 연구
5. 국가핵심기술로 지정·고시·공고된 기술과 관련된 연구
6. 「산업기술의 유출방지 및 보호에 관한 법률」상 산업기술 요건 해당 연구
7. 연구결과물이 본교의 중요 경제적 자산이거나, 누설 시 손해를 끼칠 수 있는 연구

※ 위 항목 중 한 가지라도 해당되면 보안과제로 분류됩니다.

03 PROCESS

보안등급 분류 절차

1

연구책임자

과제 신청 시 [별표1] 보안등급 분류
기준 점검표 작성

→

2

산학연구팀

점검표 접수 및
심의위원회 상정

→

3

심의위원회

보안과제 해당 시
적정성 심의

→

4

결과 통보

심의 결과를
연구책임자에게 통보

이의가 있는 경우 연구책임자는 사유를 명시하여 심의위원회에 재검토를 요청할 수 있습니다. (제6조④)

03 COMMITTEE

연구개발과제 보안관리 심의위원회

구성

- 위원장을 포함해 5인 이내 위원으로 구성
- 산학협력단장은 당연직 위원
- 위촉직 위원: 보안과제 수행경력 연구책임자 또는 관련 단과대학장 중 추천·임명
- 위원장은 산학협력단장, 간사 1인을 둘 수 있음

주요 심의사항

1. 보안관리규정의 제·개정에 관한 사항
2. 연구개발과제 보안등급 분류에 대한 적정성
3. 연구개발과제와 관련된 보안사고의 처리
4. 연구대외비의 공개 및 대외제공에 관한 사항
5. 기타 위원장이 필요하다고 인정하는 사항

보안과제에 적용

보안과제 보안조치 사항 ① — 대외·인적 관리

가

외국기업·국외연구기관 위탁 원칙적 제한

불가피한 사유가 있는 경우 보안관리 책임자의 사전승인 필요

나

외국인 참여 원칙적 제한 및 접촉현황 관리

연구책임자는 참여연구원의 외국인 접촉현황을 관리

다

외국인 참여 시 출입지역·열람자료 제한

불가피하게 참여하는 경우에도 접근 범위를 제한

근거: 규정 제8조①1호 가~다목

보안과제 보안조치 사항 ② — 정보·문서 관리

라 **비밀정보 취급 및 시설 노출 방지**

연구 관련 유무형 정보·자료·결과물을 비밀정보로 취급, 연구시설 무단 노출 금지

마 **보안서약서 제출**

협약 후 참여연구원 최초 등록 시 [별표2] 보안서약서를 천안산학협력단장에게 제출

바 **대외 공개·반출 시 사전 승인**

연구내용·결과의 대외 공개·반출 필요 시 승인 여부 판단 후 보안조치 시행

사 **정기·수시 보안점검 및 교육**

본교는 연구원 대상 정기·수시 보안점검과 교육을 실시

근거: 규정 제8조①1호 라~사목

04 AI SECURITY

생성형 AI 활용 시 준수사항

연구보안 및 정보보호를 위한 실무 유의사항

!

연구책임자 및 참여연구원은 생성형 인공지능(AI) 서비스 활용 시, 연구개발과제와 관련된 비공개 정보·연구데이터·연구성과·개인정보 등을 외부에 무단으로 제공·입력·전송해서는 안 됩니다.

금지

미공개 연구데이터·성과·개인정보를 챗봇·AI 서비스에 입력

준수

본교 연구보안 관리지침 및 정보보안 기준 준수

05 PLEDGE

보안서약서 제출 안내

누가 · 언제

대상

연구에 참여하는 모든 연구원
(내·외국인 모두 포함)

제출 시점

**교내·교외 과제 선정·협약 후,
참여연구원 최초 등록 시 제출**

서약 내용 요약

1. 연구과정에서 습득한 연구기밀을 수행 중은 물론 종료 후에도 산학협력단장의 허락 없이 자신 또는 제3자를 위해 사용하지 않는다
2. 연구내용·성과가 적법하게 공개되었더라도 미공개 부문은 동일하게 비밀유지 의무를 부담한다
3. 연구가 완료되거나 수행이 불가능해진 경우, 보유 중인 연구기밀·관련자료를 즉시 반납하고 비밀유지 의무를 부담한다

06 INCIDENT RESPONSE

보안사고 발생 시 처리

1

즉시 보고

정보자료 유출, 정보시스템 해킹 등 보안사고 발생 시 사고일시·장소·사고자 인적사항·사고내용을 심의위원회에 즉시 보고

→

2

필요 조치

연구책임자는 사고 확산 방지를 위한 필요한 조치를 즉시 시행

→

3

비공개 조사

심의위원회 위원장은 조사가 종결될 때까지 관련 내용을 공개하지 않음

→

4

재발방지

사고 수습 후 재발방지 대책을 마련

보고체계: 연구자 → 연구책임자·산학협력단 즉시 보고 → 연구개발기관 조치 및 관계 중앙행정기관 보고 (시행령 제48조)

06 VIOLATION

보안관리 위반 시 조치

연구책임자·참여연구원은 연구개발과제 수행 기간 중은 물론 기간 종료 후에도 보안유지에 최선을 다해야 하며, 위반 시 국가연구개발사업 참여제한 등의 조치를 받을 수 있고 관련 규정에 따라 책임을 지게 됩니다.

보안규정 위반을 인지한 경우, 지체없이 산학협력단장에게 보고해야 합니다.

연구자의 숙지사항: 보안규정 위반 시 즉시 보고 의무는 연구자 전원에게 적용됩니다.

07 CASE AWARENESS

국내외 연구보안 인식 사례

사례

해외 사례

해외 대학 소속 교수가 외국 정부로부터 연구비를 받은 사실을 신고하지 않아 처벌과 함께 교수직을 박탈당한 사례가 보고된 바 있습니다.

사례

해외 사례

빅테크 전직 엔지니어가 슈퍼컴퓨팅·AI 관련 기밀자료를 유출한 혐의로 기소된 사례가 알려졌습니다.

공통적으로 확인되는 점: 신고·보고 의무 소홀, 정보 관리 소홀이 개인의 불이익뿐 아니라 소속기관 전체의 신뢰에도 영향을 미칩니다.

국가연구개발혁신법 개정사항 (2026.8.20. 시행)

「국가연구개발혁신법」 제21조 개정사항이 2026.2.19. 공포되어 2026.8.20.부터 시행됩니다. 하위 시행령·고시 및 본교 규정 반영은 순차적으로 안내될 예정입니다.

1 “민감과제” 분류체계 시행

기존 보안과제 / 일반과제 2단계에서, 중간 수준 관리가 필요한 “민감과제”를 추가한 3단계 분류로 개편됩니다. (2026.8.20. 시행)

2 국외수혜정보 관리 강화

연구책임자가 외국 정부·기관·단체로부터 받는 행정적·재정적 지원 등 “국외수혜정보”에 대한 보고·관리 체계가 강화됩니다. (2026.8.20. 시행)

3 보안과제 성과 소유권 이전 통제

특별한 사정이 있는 경우에 한해 사전승인 절차를 거쳐 소유권 이전이 가능하도록 절차가 구체화됩니다. (2026.8.20. 시행)

4 보안사고 대응체계 강화

보안사고 발생 시 과기정통부장관·국가정보원장 통보 의무 신설 등 참여연구원까지 보고 의무가 확대됩니다. (2026.8.20. 시행)

08 CHECKLIST

연구자 핵심 체크리스트

- ✓ 산학협력단 연구보안 교육을 이수했다
- ✓ 보안과제 수행 시 외국기관·외국인과의 접촉·참여에 필요한 보안관리 절차를 준수한다
- ✓ [별표2] 보안서약서를 제출했다 (협약 후 참여연구원 등록 시)
- ✓ 생성형 AI에 비공개 연구정보를 입력하지 않는다
- ✓ 수행 중인 과제의 보안등급(보안/일반)을 알고 있다
- ✓ 보안규정 위반을 인지하면 즉시 산학협력단장에게 보고한다

CONTACT

문의처

천안캠퍼스

산학연구팀

TEL	041-623-0358
EMAIL	yeon3423@smu.ac.kr
ADDRESS	충남 천안시 동남구 상명대길 31

규정·서식 원문 및 최신 공지는 산학협력단 홈페이지에서 확인하실 수 있습니다.

세 줄 요약

1. 연구보안 교육 이수와 [별표2] 보안서약서 제출은 참여연구원 전원의 의무입니다.
2. 보안등급 분류·조치는 규정 제5~8조를 따르며, 위반 시 참여제한 등 책임이 따릅니다.
3. 생성형 AI에는 비공개 연구정보를 입력하지 않으며, 이상 발생 시 즉시 보고합니다.

감사합니다

상명대학교 천안산학협력단