연구보안관리규정

2024년 10월 31일

연구윤리보안센터

연구보안관리규정

2024.10.31. 제정

제1장 총칙

제1조(목적)

본 규정은 「국가연구개발사업혁신법」에 따라 한양대학교(이하 “대학”이라 한다)가 수행하는 국가연구개발사업의 보안대책을 수립·시행함에 있어 필요한 방법 및 절차를 정함으로써 국가연구개발사업의 보안에 관한 업무를 효율적으로 수행하도록 하는 데 있다.

제2조(용어의 정의)

1. “국가연구개발사업”이란 중앙행정기관이 법령에 근거하여 연구개발과제를 특정하여 그 연구개발비의 전부 또는 일부를 출연하거나 공공기금 등으로 지원하는 과학기술 분야의 연구개발사업을 말한다.
2. “중앙행정기관”은 국가연구개발사업을 추진하는 국가기관을 말한다.
3. “전문기관”은 중앙행정기관의 장이 소관 연구개발사업에 대한 기획·관리·평가 및 활용 등의 업무를 대행하도록 하기 위하여 설립하거나 지정한 기관을 말한다.
4. “주관연구기관”이란 국가연구개발사업의 연구개발과제(이하”연구개발과제”라 한다)를 주관하여 수행하는 기관을 말한다.
5. “협동연구기관”이란 연구개발과제가 2개 이상의 세부과제로 나누어질 경우, 협약으로 정하는 바에 따라 연구개발과제의 세부과제(이하 “세부과제”라 한다)를 주관하여 수행함으로써 주관연구기관과 협동으로 연구개발과제를 수행하는 기관을 말한다.
6. “참여기업”이란 연구개발성과를 실시할 목적으로 해당 연구개발과제에 필요한 연구개발비의 일부를 부담하는 기업, 「산업기술연구조합 육성법」에 따라 설립된 산업기술연구조합, 그 밖에 중앙행정기관의 장이 정하는 기관을 말한다.
7. “연구책임자”란 연구의 절차와 방법에 따라 실제 연구를 진행하고 주관하는 책임자를 말한다.
8. “보안담당부서”란 연구개발과제에 대하여 보안업무를 수행하는 연구윤리보안센터를 말한다.
9. “연구개발성과”라 함은 연구개발성과 중 「특허법」, 「실용신안법」, 「디자인 보호법」, 「상표법」, 「저작권법」 등 법률에 의하여 지식재산으로 보호되는 모든 성과물을 말한다.

제3조(적용범위)

① 본 규정은 대학이 수행하는 국가연구개발사업에 대하여 적용한다.

② 제2조에 따라 대학이 주관연구기관 또는 협동연구기관으로 수행하는 국가연구개발과제에 참여하는 참여기관은 본 규정에 따른다.

제2장 연구보안관리 체계

제4조(연구보안심의회)

① 연구보안심의회(이하 “보안심의회”라 한다)는 당연직으로서 다음 각 호의 자로 구성한다.

1. 위원장: 연구부총장
2. 부위원장: 산학협력단장
3. 위원: 공과대학장, 교무처장, 관리처장, 정보통신처장, 산학협력1부단장, 산학협력2부단장, 산학협력3부단장

② 위원장은 위원회를 통할하며 위원장이 유고 시는 부위원장이 그 직무를 대행한다.

③ 보안심의회는 다음 각 호의 사항을 심의한다.

1. 연구개발과제와 관련된 자체 보안관리 규정의 제·개정
2. 연구개발과제 보안등급 변경에 관한 사항
3. 연구개발과제와 관련된 보안사고의 처리
4. 연구보안 우수자 및 위반자에 대한 조치
5. 그 밖에 보안심의회의 구성과 운영에 관한 사항은 보안심의회 위원장이 정한다.

④ 위의 안건 중 경미한 사항은 서면결의로 처리할 수 있다.

제5조(연구보안관리 업무)

보안심의회에 관한 사항은 보안담당 부서에서 수행하되, 기타 개별 보안관리 사항이 특수 분야의 전문기술을 필요로 하는 경우 또는 타 부서 소관 사항인 경우 해당 부서에서 수행한다.

제3장 보안등급 분류

제6조(보안과제의 분류)

① 연구개발과제의 보안등급은 다음 각 호와 같이 분류한다.

1. 보안과제: 연구개발결과물 등이 외부로 유출될 경우 기술적·재산적 가치에 상당한 손실이 예상되어 보안조치가 필요한 경우로서 다음 각목의 어느 하나에 해당하는 과제
   가. 「방위사업법」 제3조 제1호에 따른 방위력개선사업과 관련된 연구개발과제
   나. 외국에서 기술이전을 거부하여 국산화를 추진 중인 기술
   다. 중앙행정기관의 장이 보호의 필요성이 있다고 인정하는 미래핵심기술
   라. 「산업기술 유출방지 및 보호에 관한 법률」 제2조 제2호에 따른 국가핵심기술
   마. 「대외무역법」 제19조 제1항에 따른 수출허가 등 제한이 필요한 기술
   바. 그 밖에 중앙행정기관의 장이 보안과제로 분류할 필요가 있다고 인정하는 과제
2. 일반과제: 보안과제로 지정되지 아니한 과제

② 연구개발과제 수행과정 중 산출되는 모든 문서에는 제1항에서 규정한 보안등급에 따른 표기하여야 한다.

③ 「국가정보원법 보안업무규정」에 따라 Ⅰ·Ⅱ·Ⅲ급 비밀 또는 대외비로 분류된 과제와 「군사기밀보호법 시행령」에 따라 군사 Ⅰ·Ⅱ·Ⅲ급 비밀 또는 이에 준하는 대외비로 분류된 과제에 대해서는 제1항과 제2항의 규정에도 불구하고 관련 법령에서 정하는 바에 따른다.

제7조(보안등급 분류 절차)

① 국가연구개발과제의 경우 연구책임자가 연구계획서를 작성할 때에는 중앙행정기관의 장이 공고한 연구개발사업의 보안등급을 따라야 한다.

② 연구계약 담당부서는 중앙행정기관 또는 전문기관에서 결정된 보안과제 선정 결과를 연구책임자 및 보안담당부서에 통보하여야 한다.

제8조(보안등급 변경)

① 국가연구개발사업의 연구책임자가 연구개발과제의 보안등급을 변경하고자 하는 때에는 변경내역, 변경사유 등을 명시하여 연구계약 담당부서에 제출한다.

② 연구계약 담당부서는 연구책임자가 제출한 연구개발과제의 보안등급 변경사항을 보안심의회의 심의를 거쳐 산학협력단장의 승인을 받아 변경하며, 국가연구개발과제의 경우 변경사항을 소관 중앙행정기관의 장에게 제출하여야 한다.

③ 연구계약 담당부서는 소관 중앙행정기관에 제출한 보안등급으로 변경된 경우 이와 관련된 기관, 연구책임자 및 관련 부서에 통보하여야 한다. 다만, 일반과제에서 보안과제로 변경된 경우에는 관련 내용을 국가정보원장에게 통보하여야 한다.

④ 연구계약 담당 부서는 소관 중앙행정기관에 제출한 보안등급의 변경을 철회할 것을 소관 중앙행정기관으로부터 통보받을 경우 특별한 사유가 없는 한 이와 관련된 기관, 연구책임자 및 관련 부서에 통보하여야 한다.

제9조(연구개발성과에 대한 보안등급)

① 연구개발성과의 보안등급은 제6조와 제8조에 따라 분류·변경된 연구개발과제 보안등급으로 한다.

② 산학협력단장은 연구개발과제에 대한 최종평가 시 중앙행정기관의 장이 부여한 보안등급 결과를 반영하여 보안등급을 변경하여야 한다.

제4장 보안조치

제10조(보안등급에 따른 조치)

연구책임자 및 참여연구원은 제9조의 보안등급에 따른 보안관리 조치를 이행하여야 하며 그 내용은 **[별지 1]**과 같다.

제11조(보안대책 수립·시행)

대학은 국가연구개발사업 관련 보안관리 담당자를 지정하고 보안관리 지침을 마련하는 등 보안대책을 수립·시행하여야 한다.

제12조(연구개발결과 공개 시 보안조치)

① 연구개발 결과물 반출·대외제공·발표 시 연구책임자의 사전 보안성검토 절차를 이행하여야 하며, 연구책임자는 사전에 전문기관의 장(또는 중앙행정기관의 장) 및 보안담당부서의 장과 협의하여 보안대책을 강구하여야 한다.

② 다음 각 호의 어느 하나에 해당하는 경우에는 다음 각 호의 구분에 따라 연구개발결과를 해당기간 동안 비공개하여야 한다. 다만, 비공개 기간 연장이 필요한 특별한 사유가 있는 경우에는 기간 만료일부터 3개월 이전에 중앙행정기관의 장의 승인을 받아 연장할 수 있다.

1. 중앙행정기관의 장이 제9조제2항에 따른 보안등급을 검토한 결과 보안과제로 분류된 경우: 최대 3년 이내의 범위에서 해당 보안과제에서 정한 기간

2. 주관연구기관의 장이 지식재산권 취득을 위하여 공개 유보를 요청하여 중앙행정기관의 장이 승인한 경우: 1년 6개월 이내

3. 참여기업의 대표가 영업비밀 보호 등의 정당한 사유로 비공개를 요청하여 중앙행정기관의 장이 승인한 경우: 1년 6개월 이내

제13조(연구개발 성과물관리)

① 연구개발 성과물의 특허권, 지식재산권 등의 확보 방안을 수립하여 연구개발 성과물에 대한 보안대책을 수립하여야 한다.

② 보안과제의 연구성과물의 소유권은 특별한 사정이 없는 한 이전하지 않는 것을 원칙으로 하나, 국내의 다른 기관으로 이전할 필요성이 있을 때에는 「국가연구개발사업 보안대책」제15조에 따른 계약을 체결하여야 하며, 외국기업 또는 외국으로 소유권 이전 및 실시계약 등을 할 경우에는 소관 행정기관의 장의 사전 승인을 얻어야 한다.

④ 연구개발 결과 활용 시 계약체결 대상자로는 국내에 있는 자로서 기술 실시 능력이 있는 자를 우선적으로 고려하여야 하며, 연구성과물 기술 실시 또는 사용 계약 시 "제3자 기술 실시(사용)권 금지 협약"을 체결하여야 한다.

제14조(보안관리 실태점검 조치)

중앙행정기관의 장 등 관계기관이 국가연구개발 사업에 대한 보안관리 실태를 점검한 후 개선명령을 받은 경우에는 산학협력단장이 개선명령을 받은 시점부터 6개월 이내 개선조치에 대한 후속조치 결과를 중앙 행정기관의 장 및 국가정보원장에게 보고하여야 한다.

제5장 보안사고 조치 및 포상

제15조(보안사고 발생시 조치)

① 연구개발과제와 관련하여 다음 각 호의 어느 하나에 해당하는 보안사고가 발생하는 경우 그 사고를 인지한 즉시 해당 연구책임자는 사고일시·장소, 사고자 인적사항, 사고내용 등을 기재하여 보안담당부서의 장에게 보고하고 필요한 조치를 취하여야 한다.

1. 연구개발과제와 관련된 정보의 유출, 누설, 분실 또는 도난

2. 연구개발과제와 관련된 정보를 유통·관리·보존하는 시스템의 유출, 파손 또는 파괴

3. 그 밖에 중앙행정기관의 장이 정하는 보안관련 사고

② 보안담당부서의 장은 제1항의 보안사고 관련 내용을 즉시 전문기관의 장 및 소관 중앙행정기관의 장에게 보고하여야 하며, 사고 일시·장소, 사고자 인적사항, 사고내용 등 세부적인 사고 경위를 추가로 제출하는 등 필요한 조치를 취하여야 한다.

③ 사고관련 연구책임자 및 참여연구원, 보안관련 부서담당자는 조사가 종결될 때까지 관련 내용을 제2항에서 명시한 기관 외 공개하지 아니한다.

④ 보안담당부서의 장은 관련 내용을 보안심의회에 보고하여야 하며, 보안심의회에서는 보안사고에 대한 내용을 심의하여 처리방법 및 재발방지 대책을 마련하고 필요한 경우 국가정보원 장에게 보안사고를 예방하기 위한 보안교육 등 관련 대책 지원을 요청할 수 있다.

제16조(보안관리 위반시 조치)

① 연구책임자 및 참여연구원, 대학 내 모든 구성원은 본 규정에서 정하는 사항 및 관련법령을 준수해야 한다.

② 연구보안규정을 위반한 경우, 그 귀책사유를 감안하여 연구참여제한 또는 소속 인사위원회를 통

한 징계요구, 필요한 경우 수사기관에 의뢰하여 위반자를 처벌할 수 있다.

③ 참여연구원 및 연구관련 부서 담당자 등은 연구기간 중은 물론 연구종료 후에도 보안유지에 최선을 다하여야 하며, 위반 시 관계법규에 따라 책임을 진다.

제17조(보안우수자 포상)

대학은 다음 각 호의 기준에 부합하는 연구보안 우수자(또는 연구실) 대하여 보안심의회의 심의를 거쳐 포상할 수 있다.

① 상위기관 연구보안감사, 국가정보원 연구보안평가, 자체적으로 실시한 정기 또는 불시 연구보안관리 점검을 통하여 연구보안 이행 성적이 우수한 자

② 그 밖에 보안심의회 위원장이 포상이 필요하다고 인정하는 경우

제18조(기타)

본 규정에서 규정한 내용 이외의 사항에 대해서는「국가연구개발혁신법」등 관계법령 및 대학 내 보안관련 규정을 따른다.

부 칙

제1조(시행일)

본 규정은 공포한 날부터 시행한다.

[별지 제1호] 보안관리 조치사항

1. 보안관리 체계

해당과제	세부 조치사항	이행대상	
		연구기관	연구책임자
모든과제	1. 연구보안 관계 법령에 따라 연구기관 보안관리 실정을 반영한 자체 보안관리 규정의 제정·개정	◯	
모든과제	2. 연구개발과제 보안관리와 관련한 각종 안건을 심의하기 위한 연구보안심의회 운영	◯	
모든과제	3. 연구과제 보안관리 업무의 종합계획·관리를 담당하는 보안관리책임자 및 보안 업무 전담직원 지정·배치	◯	
모든과제	4. 연구개발과제 보안관리 부서 및 연구 인력에 대한 보안 관련 규정 교육·홍보 실시	◯	
모든과제	5. 자체 보안관리 규정에 보안 우수자 및 규정 위반자에 대한 상벌 조치 명시	◯	
모든과제	6. 보안사고 예방·조치·대응 등 재발 방지책 마련	◯	
모든과제	7. 연구기관 및 연구원에 대한 정기 수시 보안점검 및 교육 실시	◯	
모든과제	8. 화재, 홍수, 재난, 재해 등 비상시 대응계획 수립	◯	
보안과제	9. 외국기업 및 국외연구기관과 공동연구 위탁연구 시 중앙행정기관의 사전 승인 절차 이행	◯	

[별지 제1호] 보안관리 조치사항

2. 참여연구원 관리

해당과제	세부 조치사항	이행 대상	
		연구기관	연구책임자
모든과제	1. 참여연구원(외국인 포함)의 채용·갱신·퇴직 시 고용계약서 및 보안서약서를 받고, 이 경우 연구과제 보안관리 의무 및 그 위반 시의 제재 등을 명시	◯	◯
모든과제	2. 연구과제 수행 연구원의 보안의식을 높이기 위한 보안 관련 교육 이수		◯
모든과제	3. 퇴직(예정)자의 반출(예상)자료에 대한 보안성 검토, 연구성과물 회수, 전산망 접속 차단 등의 조치	◯	
모든과제	4. 외부기관 파견자 등 임시직 및 방문자에 대한 별도 보안조치	◯	◯
모든과제	5. 연구성과 유출 혐의(전력)자가 과제에 참여할 경우 특별 관리조치	◯	
모든과제	6. 참여연구원의 국외 출장 시 사전 보안교육 및 귀국보고(출장기간에 접촉한 사람 및 협의 내용 등을 포함한다) 실시	◯	◯
보안과제	7. 외국인 연구원의 별도 보안조치(영문 보안서약서 작성, 출입지역 제한, 반출·반입 물품 제한, 특이 동향 관리 등)	◯	
보안과제	8. 보안과제 참여연구원이 과제와 관련하여 접촉하는 외국인 현황 관리	◯	◯
보안과제	9. 외국인 연구원이 보안과제 참여 시 소속 기관의 장의 승인 절차 이행		◯

[별지 제1호] 보안관리 조치사항

3. 연구개발 내용 및 성과의 관리

해당과제	세부 조치사항	이행 대상	
		연구기관	연구책임자
모든과제	1. 연구개발과제 수행과정 중 산출되는 모든 문서에 보안등급 표기		○
모든과제	2. 연구수행 단계별 특허권·지식재산권 확보 방안과 주요 연구자료 및 성과물의 무단 유출 방지를 위한 보안책 마련·시행	○	○
모든과제	3. 연구개발 성과의 대외 공개(홈페이지 게재 포함) 및 제공 시, 연구책임자의 사전 보안성 검토 확인절차 이행	○	○
모든과제	4. 연구개발 성과의 해외 기술이전(양도) 추진 시 관계법령 준수	○	
모든과제	5. 연구개발성과 활용 시 국내에 있는 자를 계약체결 대상으로 우선 고려	○	
보안과제	6. 외부 기관과 보안과제의 공동(협동 위탁 포함)연구 협약 시 성과물의 귀속, 자료 제공 및 장비 반납 등에 관한 사전 보안대책 마련 및 적용	○	○
보안과제	7. 연구성과물 기술 실시(사용) 계약 시 “제3자 기술 실시(사용)권 금지협약” 체결	○	

4. 연구시설 관리

해당과제	세부 조치사항	이행 대상	
		연구기관	연구책임자
모든과제	1. 노트북, 외장형 하드디스크 드라이브 등 정보통신매체에 대한 반입·출입 절차 마련 및 이행	○	○
모든과제	2. 외곽, 주요 시설물에 폐쇠회로 텔레비전, 침입감지센서 등 첨단장비의 설치·운용	○	
모든과제	3. 연구개발과제와 관련된 핵심기술 및 정보를 보관하는 전산실 및 중요시설물에 대해서 보호구역 지정 후 특별 보안관리 조치	○	
모든과제	4. 외부 입주기관(벤처기업 포함)의 연구시설 내부 출입통제 조치	○	
보안과제	5. 연구시설 출입자에 대한 개인별 출입권한 차등 부여 및 통제	○	
보안과제	6. 외부방문자 출입 시 보안관리책임자의 사전 허가 후에 담당 직원이 방문자와 함께 방문지역 동행	○	○

[별지 제1호] 보안관리 조치사항

5. 정보통신망 관리

해당과제	세부 조치사항	이행 대상	
		연구기관	연구책임자
모든과제	1. 연구개발과제의 보안을 목적으로 전산망 보호를 위한 방화벽 시스템, 침입탐지시스템 등 각종 장비의 설치·운영	◯	
모든과제	2. 외부에서 내부망 접속 시 사용자 인증으로 정보시스템 접근 제한 조치	◯	
모든과제	3. 컴퓨터에 각종 장비 및 소프트웨어 설치 시, 보안관리책임자의 사전 승인	◯	◯
모든과제	4. 무선통신망 구축 시 비인가 사용자의 차단을 위한 사용자 인증, 암호화 통신, 암호화 키의 주기적 변경 등 보안조치	◯	
모든과제	5. 사전에 소속 기관에서 인가받은 보안 이동형 저장매체 사용	◯	◯
모든과제	6. 보안시스템 안전사고에 대비 데이터 백업시스템 구축·운영 및 원거리 지역 보안시설에 중요 데이터 별도 복사본 보관	◯	
모든과제	7. 비인가 개인용 정보통신매체 반입·출입 통제 및 내부망 연결 제한	◯	◯
모든과제	8. 업무용 컴퓨터 대상 보안 소프트웨어, 보안패치 등 설치 및 업데이트	◯	◯
모든과제	9. 보안사고에 대비하여 정보시스템 사용 기록(최소 6개월 이상)보관 - 보관 권장기간 : 1년	◯	
모든과제	10. 직책, 업무에 따라 각종 전산 자료에 대한 차등적 접근권한 부여	◯	
모든과제	11. 네트워크 자료(시스템 구성, IP현황 등)의 보안관리	◯	
모든과제	12. 전산장비 폐기 및 외부 이관 시, 하드디스크 드라이브 등에 저장된 주요 자료가 불법으로 복구되지 않도록 조치	◯	◯
보안과제	13. 내부망의 연구실별 물리적 또는 논리적(방화벽 등) 분리	◯	◯
보안과제	14. 업무용 컴퓨터 자료를 휴대전화, 이동형 저장매체 등 개인용 정보통신매체에 복사·저장·전송할 경우 보안관리책임자의 사전 승인	◯	◯
보안과제	15. 인터넷을 이용하여 외부로 자료 전송 시, 승인 절차 등 보안대책 마련 및 이행	◯	◯
보안과제	16. 메신저, 인터넷 저장소, 외부 이메일 등 자료 유출 가능 경로 접속차단	◯	