

국가연구개발사업 공통 보안관리 지침

제1장 총칙

제1조(목적) 이 지침의 목적은 「국가연구개발사업의 관리 등에 관한 규정」에 따라 국민대학교(이하 “본교”라 한다)가 수행하는 국가연구개발사업의 보안대책을 수립·시행함에 있어 필요한 방법 및 절차를 정함으로써 국가연구개발사업의 보안에 관한 업무를 효율적으로 수행하도록 하는데 있다. <개정 2018.05.16.>

제2조(용어의 정의) 이 지침에서 사용하는 용어의 정의는 다음 각 호와 같다.

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 연구개발과제를 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 연구개발결과물을 실시할 목적으로 해당 연구개발과제에 필요한 연구개발비 일부를 부담하는 기업, 「산업기술연구조합 육성법」에 따라 설립된 산업기술연구조합, 그 밖에 중앙행정기관의 장이 정하는 기관을 말한다.
7. “위탁연구기관”이란 협약으로 정하는 바에 따라 주관연구기관으로부터 연구개발과제의 일부 또는 세부과제의 일부를 위탁받아 수행하는 기관을 말한다.
8. “연구책임자”란 연구의 절차와 방법에 따라 실제 연구를 진행하고 주관하는 책임자를 말한다.
9. “국제공동연구”란 복수의 연구개발주체가 동일한 연구과제의 수행에 소요되는 연구개발자금·인력·시설·기자재·정보 등 과학기술자원을 공동으로 부담하여 국제적으로 수행하는 연구개발사업을 말한다.
10. “연구개발성과”라 함은 연구개발성과 중 「특허법», 「실용신안법», 「디자인보호법», 「상표법», 「저작권법」 등 법률에 의하여 지식재산으로 보호되는 모든 성과물을 말한다.

<본조신설 2018.05.16.>

제3조(적용범위) ① 이 지침은 본교가 수행하는 국가연구개발사업에 대하여 적용한다. <개정 2018.05.16.>

② 제2조에 따라 본교가 주관연구기관 또는 협동연구기관으로 수행하는 국가연구개발사업에 참여하는 참여기관은 이 지침에 따른다. <신설 2018.05.16.>

제4조(보안대책 수립·시행) 산학협력단장(이하 “단장”이라 한다)은 국가연구개발사업 관련 보안관리 담당자를 지정하고 보안관리 지침을 마련하는 등 보안대책을 수립·시행하여야 한다. <본조 신설 2018.05.16.>

제5조(연구보안심의위원회) ① 보안업무의 효과적인 수행과 운영관리에 관한 사항을 심의하기 위하여 연구보안심의위원회(이하 “위원회”라 한다)를 둔다. <개정 2018.05.16.>

② 위원회의 위원장은 단장으로 하며, 위원은 총무처장, 기획처장, 국제교류처장, 입학처장, 정보통신처장(이하 “당연직 위원”이라 한다)을 포함하여 15인 이내의 위원으로 구성한다. <개정 2018.05.16.>

③ 당연직 위원 이외의 위원은 본교 전임교원 중에서 총장이 임명하며, 그 임기는 2년으로 하되 연임할 수 있다. <신설 2018.05.16.>

④ 위원장은 위원회를 통할하며, 위원장 유고 시는 위원장이 지명하는 위원이 그 직무를 대행한다. <신설 2018.05.16.>

⑤ 위원회의 사무를 처리하기 위하여 간사 1인을 두며, 간사는 연구관리팀장으로 한다. <신설 2018.05.16.>

⑥ 심의안건 중 경미한 사항은 서면결의로 처리할 수 있다. <신설 2018.05.16.>

⑦ 위원회는 다음 각 호의 사항을 심의·의결한다. <개정 2018.05.16.>

1. 국가연구개발사업과 관련된 보안관리 규정의 제·개정
2. 연구개발과제의 보안등급 변경에 관한 사항
3. 국가연구개발사업과 관련된 보안사고의 처리 및 보안 관련 규정 위반자의 처리에 관한 사항
4. 보안업무 세부시행계획 수립에 관한 사항
5. 보안업무 감사·지도·점검에 관한 사항
6. 그 밖에 위원장이 필요하다고 인정하는 사항

제2장 보안등급 분류

제6조(분류기준) ① 연구개발과제의 보안등급은 다음 각호와 같이 분류한다. <개정 2018.05.16.>

1. 보안과제: 연구개발결과물 등이 외부로 유출될 경우 기술적·재산적 가치에 상당한 손실이 예상되어 보안조치가 필요한 경우로서 다음 각 목의 어느 하나에 해당하는 과제
가. 세계 초일류 기술제품의 개발과 관련되는 연구개발과제
나. 외국에서 기술이전을 거부하여 국산화를 추진 중인 기술 또는 미래 핵심 기술로서 보호의 필요성이 인정되는 연구개발과제
다. 「산업기술의 유출방지 및 보호에 관한 법률」 제2조 제2호의 국가핵심기술과 관련된 연구개발과제
라. 「대외무역법」 제19조 제1항 및 동법 시행령 제32조의2에 따른 수출허가 등의 제한이 필요한 기술과 관련된 연구과제
마. 그 밖에 중앙행정기관의 장이 보안과제로 분류되어야 할 사유가 있다고 인정하는 과제

2. 일반과제: 보안과제로 지정되지 아니한 과제

② 연구개발과제 수행 과정 중 산출되는 모든 문서에는 제1항에 따라 분류된 보안등급을 표기하여야 한다. <개정 2018.05.16.>

③ 「보안업무규정」에 따른 I 급비밀·II 급비밀·III 급비밀 또는 이에 준하는 대외비로 분류된 과제와 「군사기밀보호법 시행령」에 따른 군사 I 급비밀·II 급비밀·III 급비밀 또는 이에 준하는 대외비로 분류된 과제에 대해서는 제1항 및 제2항에도 불구하고 관련 법령에서 정하는 바에 따른다. <개정 2018.05.16.>

④ “삭제” <2018.05.16.>

제7조(분류 절차) ① 연구책임자가 연구개발계획서를 작성할 때에는 중앙행정기관의 장이 공고한 연구개발사업의 보안등급을 따라야 한다. <개정 2018.05.16.>

② 연구관리팀은 보안과제 보호를 위해 필요시 연구제목을 가제목으로 부여할 수 있다. <개정 2018.05.16.>

③ 연구관리팀은 중앙행정기관 또는 전문기관에서 결정된 보안과제 선정 결과를 연구책임자 및 보안 관련 부서에 통보하여야 한다. <신설 2018.05.16.>

제8조(보안등급 변경) ① 연구책임자가 연구개발과제의 보안등급을 변경하고자 하는 때에는 변경내역, 변경사유 등을 명시하여 연구관리팀에 제출하여야 한다. <개정 2018.05.16.>

② 연구관리팀은 연구책임자가 제출한 연구개발과제의 보안등급 변경사항을 위원회의 심의를 거쳐 단장의 승인을 받아 소관 중앙행정기관의 장에게 변경 내용, 변경 사유 등을 제출하여야 한다. <개정 2018.05.16.>

③ 연구관리팀은 소관 중앙행정기관에 제출한 보안등급으로 변경된 경우 이와 관련된 기관, 연구책임자 및 보안 관련 부서에 통보하여야 한다. 다만, 일반과제에서 보안과제로 변경된 경우에는 관련 내용을 국가정보원장에게 통보하여야 한다. <개정 2018.05.16.>

④ 연구관리팀은 소관 중앙행정기관에 제출한 보안등급의 변경을 철회할 것을 소관 중앙행정기관으로부터 통보받을 경우 특별한 사유가 없는 한 이와 관련된 기관, 연구책임자 및 보안 관련 부서에 통보하여야 한다. <개정 2018.05.16.>

제9조(연구개발결과의 보안등급) ① 연구개발결과의 보안등급은 제6조에 따라 결정되거나 제8조에 따라 변경된 연구개발과제 보안등급으로 한다.

② 단장은 연구개발과제에 대한 최종평가 시 중앙행정기관의 장이 부여한 보안등급결과를 반영하여 보안등급을 변경하여야 한다.

<본조신설 2018.05.16.>

제3장 보안 조치

제10조(보안등급에 따른 조치) ① 단장은 필요시 연구개발과제의 관리와 관련하여 보안대책을 수립·시행하여야 한다. <개정 2018.05.16.>

② 단장 및 연구책임자는 제9조의 보안등급에 따른 보안관리 조치를 이행하여야 하며,

그 내용은 별표 2와 같다. <개정 2018.05.16.>

③ 단장은 중앙행정기관의 장과 보안과제에 대하여 협약을 체결하는 경우 별표 2의 조치 사항을 이행하여야 함을 협약에 명시하여야 한다. <개정 2018.05.16.>

제11조(참여연구원에 대한 조치) 연구책임자는 첨단기술의 유출 등을 방지하기 위하여 참여 연구원 및 참여기관 등에 대한 보안조치를 다음 각 호 및 별표 2에 따라 조치하고, 그 결과를 연구관리팀에 제출하여야 한다.

1. 연구성과 유출 혐의(전력)자는 연구개발과제 참여를 원칙적으로 제한한다. 단, 불가피한 사유가 있다고 판단되는 경우에는 단장의 사전 승인을 받아야 한다.
2. 보안과제를 수행하는 참여연구원은 비밀취급인가를 받아야 한다.
3. 보안과제를 수행하는 참여연구원이 당해 연구와 관련하여 외국인을 접촉하였을 경우에는 '참여연구원 외국인 접촉보고서'(별표4)를 작성·유지하여야 한다.
4. 연구책임자는 참여연구원이 해외 출장 시 사전보안교육을 실시하고 귀국 시 '출장결과 보고서'를 작성·제출토록 하여야 한다.
5. 연구책임자는 참여연구원이 퇴직(예정) 시는 '퇴직자 보안서약서'(별표 5)를 작성하게 하고, 반출(예상)자료에 대한 보안성 검토 및 연구개발결과물 회수, 전산망 접속차단 등에 대한 조치를 하여야 한다.

<본조신설 2018.05.16.>

제12조(외국기업 및 외국인 등에 대한 보안조치) 보안과제의 첨단기술 유출 등을 방지하기 위하여 외국인 및 외국기업 등에 대한 보안조치를 다음 각 호에 따라 수행하여야 한다.

1. 중앙행정기관의 장 또는 전문기관의 장으로부터 승인받지 아니한 외국기업 또는 국외 연구기관에의 연구개발과제의 공동·위탁연구는 원칙적으로 제한한다. 단, 불가피한 사유가 있다고 판단되는 경우에는 중앙행정기관의 장에게 사전 승인을 받아야 한다.
2. 외국인 연구원의 연구개발과제 참여는 원칙적으로 제한한다. 단, 불가피한 사유가 있다고 판단되는 경우에는 '외국인 연구참여 승인 신청서'(별표 3)를 작성하여 단장에게 사전승인을 받아야 한다.
3. 단장 및 연구책임자는 영문보안서약서 작성, 출입지역 제한, 특이동향 관리 등 외국인 연구원에 대한 별도의 보안조치를 강구하여야 한다.

<본조신설 2018.05.16.>

제13조(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 단장과 협의하여 보안대책을 강구하여야 한다.

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

1. 중앙행정기관의 장이 제10조 제2항에 따른 보안등급을 검토한 결과 보안과제로 분류된 경우: 최대 3년 이내의 범위에서 해당 보안과제에서 정한 기간

2. 단장이 지식재산권의 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
- <본조신설 2018.05.16.>

제14조(통신기기 등의 활용에 대한 보안조치) 단장 및 연구책임자는 휴대용 정보통신기기, 이메일 등 인터넷서비스 활용 등과 관련된 보안 조치로 별표 2에 규정된 사항과 그 밖에 단장이 필요하다고 인정하는 사항을 포함하여 보안대책을 수립·시행하여야 한다.

<본조신설 2018.05.16.>

제15조(연구정보의 국외 유출방지 보안대책) ① 단장은 국가연구개발사업과 관련된 중요한 연구정보의 국외 유출을 방지하기 위하여 별표 2에 규정된 보안관리 조치사항과 그 밖에 단장이 필요하다고 인정하는 사항을 포함하여 자체 보안대책을 수립·시행하여야 한다.

② 단장은 참여연구원이 보안과제와 관련하여 외국정부·기관 또는 단체를 방문하거나 방문을 받을 경우에는 연구과제명, 연구책임자, 방문일시·장소 및 주요 방문내용 등의 사항을 문서로 소관 중앙행정기관의 장 및 국가정보원장에게 해당 방문일 5일 전까지 통보하여야 한다. 다만, 방문이 사전에 알린 내용과 다르게 이루어진 경우에는 방문 후에 해당 사항을 추가로 알려야 하며, 방문이 긴급한 경우 등 사전에 알리지 못한 경우에는 방문이 끝난 후에 통보하여야 한다.

<본조신설 2018.05.16.>

제16조(국제공동연구 시 보안조치) ① 보안과제의 연구책임자는 외국기업 및 국외 연구기관과 공동연구를 수행할 경우에는 소관 중앙행정기관의 사전 승인절차를 이행하여야 한다.

② 국제공동연구를 진행할 경우 협약서에 포함되어야 하는 사항은 다음 각 호와 같다.

1. 국제 공동연구를 위해서 제공한 본교의 특허나 노하우 처리
2. 정보 등 제공과 비밀유지 의무
3. 연구의 역할분담 또는 비용분담 중지의 경우 처리
4. 연구개발기간의 설정
5. 연구개발 성과물의 귀속
6. 특허권의 출현 등의 처리
7. 특허권의 실시(제3자에 대한 실시 허락)
8. 공동연구 종료 후 이용특허권의 처리 등

③ 국제공동연구에 제공되거나 그 결과로서 발생하는 중요 정보에 대해서는 적절한 보안대책을 강구하여야 한다.

<본조신설 2018.05.16.>

제17조(해외 기술이전 시 보안조치) 연구개발결과 해외 기술이전(양도) 추진 시는 「산업기술의 유출방지 및 보호에 관한 법률」 제11조(국가핵심기술의 수출 등) 및 제11조의 2(국가핵심기술을 보유하는 대상기관의 해외인수·합병 등), 「기술촉진법」 제13조(전략기술 수

출의 승인 등)를 준수하여야 한다.

<본조신설 2018.05.16.>

제18조(연구개발 성과물관리) ① 연구개발 성과물의 특허권, 지식재산권 등의 확보 방안을 수립하여 연구개발 성과물에 대한 보안대책을 수립하여야 한다.

② 주관연구기관·협동연구기관 및 참여기관의 장은 국가연구개발사업에 따른 연구개발결과로서 지식재산권을 출원하거나 등록하는 경우에는 다음 각 호의 조치를 하여야 한다.

1. 국내 또는 국외에서 출원하거나 등록하는 지식재산권의 경우에는 지식재산권 출원서 또는 등록신청서와 그 사실을 증명할 수 있는 서류를 출원 또는 등록 후 6개월 이내에 관계 중앙행정기관의 장에게 제출하여야 한다.

2. 국외에서 등록된 지식재산권의 경우에는 등록공보 발간 후 3개월 이내에 등록공보의 사본을 관계 중앙행정기관의 장에게 제출하여야 한다.

③ 연구성과물 기술 실시 또는 사용 계약 시 “제3자 기술 실시(사용)권 금지협약”을 체결하여야 한다.

④ 연구개발 결과 활용 시 계약체결 대상자로는 국내에 있는 자로서 기술 실시 능력이 있는 자를 우선적으로 고려하여야 한다.

<본조신설 2018.05.16.>

제19조(연구개발과제 보안관리 현황 보고) 단장은 연구과제의 보안관리 현황을 매년 전문기관의 장에게 보고하여야 한다. 전문기관의 장이 없는 경우 중앙행정기관의 보안관리심의회에 직접 보고하여야 한다. <개정 2018.05.16.>

제20조(보안관리 실태점검 조치) 중앙행정기관의 장 등 관계기관이 국가연구개발사업에 대한 보안관리 실태를 점검한 후 개선명령을 받은 경우에는 단장이 개선명령을 받은 시점부터 6개월 이내 개선조치에 대한 후속조치 결과를 중앙행정기관의 장 및 국가정보원장에게 보고하여야 한다.

<본조신설 2018.05.16.>

제4장 보안사고 처리

제21조(보안사고 발생 시 처리) ① 연구개발과제와 관련하여 다음 각호의 어느 하나에 해당하는 보안사고가 발생하는 경우 그 사고를 인지한 즉시 해당 연구책임자는 사고일시·장소, 사고자 인적사항, 사고내용 등을 기재하여 단장에게 보고하고 필요한 조치를 취하여야 한다. <개정 2018.05.16.>

1. 연구개발과제와 관련된 정보의 유출, 누설, 분실 또는 도난

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

3. 그 밖에 중앙행정기관의 장이 정하는 보안관련 사고

② 단장은 제1항의 보안사고 관련 내용을 즉시 전문기관의 장 및 소관 중앙행정기관의 장에게 보고하여야 하며, 사고 일시·장소, 사고자 인적사항, 사고내용 등 세부적인 사고

경위를 보고일 부터 5일 이내에 추가로 제출하는 등 필요한 조치를 취하여야 한다.

<개정 2018.05.16.>

③ 해당 연구책임자 및 참여연구원, 보안관련 부서담당자는 조사가 종결될 때까지 관련 내용을 제2항에 명시한 기관 외에 공개하지 아니한다. <개정 2018.05.16.>

④ 단장은 보안사고 관련 내용을 위원회에 보고하여야 하며, 위원회에서는 보안사고에 대한 내용을 심의하여 처리방법 및 재발방지 대책을 마련하고 필요한 경우 국가정보원의 장에게 보안사고를 예방하기 위한 보안교육 등 관련 대책 지원을 요청할 수 있다.

<개정 2018.05.16.>

⑤ 단장, 연구책임자, 보안관련 부서는 중앙행정기관과 국가정보원 등 관계기관이 합동으로 보안사고 관련 경위를 조사할 경우 조사에 성실히 협조하여야 한다.

<개정 2018.05.16.>

제22조(보안관리 위반 시 조치) ① 단장, 연구책임자, 참여연구원 등은 이 지침에서 정하는 사항 및 관련 국가연구개발사업 보안관리규정을 준수하여야 한다. <개정 2018.05.16.>

② 단장은 제10조 제2항에 따른 보안관리 조치 및 제21조 제1항에 따른 보고 등을 정당한 사유 없이 이행하지 않은 자에 대하여 관계법규 또는 본교 규정 등에 따라 인사상 불리한 조치를 취할 수 있다. <개정 2018.05.16.>

③ 참여연구원 및 연구 관련 부서 담당자 등은 연구기간 중은 물론 연구종료 후에도 보안유지에 최선을 다하여야 하며, 위반 시 관계 법규에 따라 책임을 진다. <개정 2018.05.16.>

제5장 기타

제23조(기타) 이 지침에 규정한 내용 이외의 사항에 대해서는 「국가연구개발사업의 관리 등에 관한 규정」 등 관계법령에 따른다.

<본조 신설 2018.05.16.>

부 칙

① **(시행일)** 이 지침은 2007년 6월 22일부터 시행한다.

② **(경과조치)** 이 지침의 시행 전에 보안등급을 확정하여 관리되고 있는 계속과제의 경우 이 지침에서 정하는 분류절차를 생략할 수 있다.

부 칙

이 지침은 2018년 5월 16일부터 시행한다.

보안서약서

소 속 :

직위 / 직급 :

성 명 :

생년월일 :

상기 본인은 “ _____ ” 연구과제의 연구원으로
참여하면서 다음사항을 준수할 것을 서약합니다.

1. 연구보안관리 규정에 따라 과제 이행 시 책임과 의무를 다하여 보안을 준수한다.
2. 본 연구개발과제를 수행하는 과정에서 알 수 있었던 연구기밀에 대해 연구과제 수행중은 물론이고 종료 후에도 국민대학교 산학협력단장의 허락 없이 자신 또는 제3자를 위하여 사용하지 않는다.
3. 본 연구개발과제 추진성고가 적법하게 공개된 경우라고 하여도 미공개 부문에 대해서는 앞서와 같이 비밀유지 의무를 부담한다.
4. 본 연구개발과제가 완료되거나 연구개발과제를 수행할 수 없게 된 경우, 그 시점에서 본인이 보유하고 있는 연구기밀을 포함한 관련 자료를 즉시 연구개발 책임자에게 반납하며 앞서와 같이 비밀유지 의무를 부담한다.
5. 위 사항을 위반할 시에는 동기여하를 막론하고 제 법규에 의거 엄중한 처벌을 받을 것을 서약하며 어떠한 조치에도 이의를 제기하지 아니한다.

년 월 일

서약인

(인)

국민대학교 산학협력단장 귀하

국가연구개발사업 보안관리 조치사항

1. 보안관리 체계

해당 과제	세부 조치사항	이행 대상	
		산학 협력단	연구 책임자
모든 과제	1. 이 지침 또는 관계 법령에 따라 연구기관 보안관리 실정을 반영한 자체 보안관리 규정의 제정·개정	○	
	2. 연구개발과제 보안관리와 관련한 각종 안건을 심의하기 위한 연구보안심의위원회 운영	○	
	3. 연구과제 보안관리 업무의 종합계획·관리를 담당하는 보안관리 책임자 및 보안 업무 전담직원 지정·배치	○	
	4. 국가연구개발사업 보안관리 부서 및 연구 인력에 대한 보안 관련 규정 교육·홍보 실시	○	
	5. 자체 보안관리 규정에 보안 우수자 및 규정 위반자에 대한 상벌 조치 명시	○	
	6. 보안사고 예방·조치·대응 등 재발 방지책 마련	○	
	7. 연구기관 및 연구원에 대한 정기·수시 보안점검 및 보안교육 실시	○	
	8. 화재, 홍수, 재난, 재해 등 비상시 대응계획 수립	○	
보안 과제	9. 외국기업 및 국외 연구기관과 공동연구·위탁연구 시 중앙행정기관의 사전 승인 절차 이행	○	

2. 참여연구원 관리

해당 과제	세부 조치사항	이행 대상	
		산학 협력단	연구 책임자
모든 과제	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	○	○
	2. 연구과제 수행 연구원의 보안의식을 높이기 위한 보안 관련 교육 이수		○
	3. 퇴직(예정)자의 반출(예상)자료에 대한 보안성 검토, 연구성과물 회수, 전산망 접속 차단 등의 제때 조치	○	
	4. 외부기관 파견자 등 임시직 및 방문자에 대한 별도 보안조치	○	○
	5. 연구성과 유출 혐의(진력)자가 과제에 참여할 경우 특별 관리조치	○	
	6. 참여연구원의 국외 출장 시 사전 보안교육 및 귀국보고 실시 -출장기간에 접촉한 사람 및 협의 내용 등을 포함	○	○
보안 과제	7. 외국인 연구원의 별도 보안조치(영문 보안서약서 작성, 출입지역 제한, 반출·반입 물품 제한, 특이 동향 관리 등)	○	
	8. 보안과제 참여연구원이 과제와 관련하여 접촉하는 외국인 현황 관리	○	○
	9. 외국인 연구원의 보안과제 참여 시 소속 기관의 장의 승인절차 이행		○

3. 연구개발내용 및 결과의 관리

해당 과제	세부 조치사항	이행 대상	
		산학 협력단	연구 책임자
모든 과제	1. 연구개발과제 수행과정 중 산출되는 모든 문서에 보안등급 표기		○
	2. 연구수행 단계별 특허권·지식재산권 확보 방안과 주요 연구자료 및 성과물의 무단 유출 방지를 위한 보안책 마련·시행	○	○
	3. 연구개발 성과의 대외 공개(홈페이지 게재 포함) 및 제공 시, 연구책임자의 사전 보안성 검토 확인절차 이행	○	○
	4. 연구개발 결과의 해외 기술이전(양도) 추진 시 관계 법령 준수 -「산업기술의 유출방지 및 보호에 관한 법률」 제11조(국가핵심기술의 수출 등) -「대외무역법」 제13조(전략기술 수출의 승인 등)	○	
	5. 연구개발 결과 활용 시 국내에 있는 자를 계약체결 대상으로 우선 고려	○	
보안 과제	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	○	○
	7. 연구성과물 기술 실시(사용) 계약 시 “제3자 기술 실시(사용)권 금지협약” 체결	○	

4. 연구시설 관리

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

5. 정보통신망 관리

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

퇴직자 보안서약서

(보안과제 수행 연구원이 퇴직한 경우에 한함)

본인은 “국민대학교(또는 국민대학교 산학협력단)”을 퇴직함에 있어 다음 사항을 숙지하고 이를 이행하지 않을 경우 관계법령에 의거 처벌받을 것은 물론 “국민대학교(또는 국민대학교 산학협력단)”에 손해를 입힐 경우에는 그 손해액을 지체없이 변상할 것을 엄숙히 서약합니다.

1. “국민대학교(또는 국민대학교 산학협력단)”에 근무 중 취득한 국가보안 등에 관한 제반 비밀과 직무상 취득한 과학기술정보 관련 제반 비밀사항 및 중요 기술비밀을 관련 법령, 국민대학교 규정 및 지침에 따라 일체 누설하거나 도용하지 않는다.
2. “국민대학교(또는 국민대학교 산학협력단)”에 근무 중의 모든 발명, 고안, 창작 및 발견 등에 대하여 “국민대학교(또는 국민대학교 산학협력단)” 또는 그 지정인에게 이를 공개, 양도할 것에 동의하고 그 절차에 적극 협력한다.
3. “국민대학교(또는 국민대학교 산학협력단)”에 근무 중의 모든 연구자료 및 연구결과 보고서, 설계서, 청사진 등과 보조기억장치 등에 대하여 누락 없이 “국민대학교(또는 국민대학교 산학협력단)” 또는 그 지정인에게 인계하고 이를 소지하거나 유출하지 않는다.
4. 퇴직 후 2년간 “국민대학교(또는 국민대학교 산학협력단)”의 사전승인 없이 “국민대학교(또는 국민대학교 산학협력단)”의 연구자료, 연구결과 등과 직무발명, 고안, 창작 및 발견사항 등의 지적재산권을 이용하여 자신 또는 제3자를 위하여 창업하거나, 기업체에 전직, 동업 또는 자문하지 않는다.
5. 위 사항을 위반하는 경우에는 관련 법규(국가보안법, 형법, 부정경쟁방지 및 영업비밀보호에 관한 법률)에 따른 어떠한 처벌도 감수한다.

년 월 일

서약인 주소 :

주민등록번호 :

성 명 :

(인)

국민대학교 산학협력단장 귀하