국가연구개발사업 보안관리 표준 매뉴얼

Manual of security management
on national research development project

미래창조과학부
Ministry of Science, ICT and
Future Planning

국가연구개발사업 보안관리 표준 매뉴얼

Manual of security management
on national research development project

미래창조과학부
Ministry of Science, ICT and
Future Planning

목 차

1. 서론

1. 「국가연구개발사업의 관리 등에 관한 규정」 도식화 ····· 2
2. 국가연구개발사업보안관리 조치사항 지침과 매뉴얼 항목의 관계 ····· 7
3. 용어정의 ····· 13

2. 제 1장 보안관리체계

1.1 보안관리규정 ····· 16
1.2 연구보안심의회 운영 ····· 22
1.3 보안관리자 지정 ····· 24
1.4 보안관리 규정 교육 및 홍보 ····· 27
1.5 보안 우수자 및 위반자에 대한 조치 ····· 32
1.6 보안사고관리 ····· 39
1.7 보안점검 및 보안교육 실시 ····· 47
1.8 비상시 대응계획 수립 ····· 52
1.9 공동 및 위탁 연구 시 사전승인 절차 이행 ····· 55

3. 재 2장 참여 연구원 관리

1절. 참여 연구원 관리

2.1 채용 시 인원관리 ····· 60
2.2 재직 중 인원관리 ····· 64
2.3 계약 갱신 시 인원관리 ····· 66
2.4 퇴직자 관리 ····· 67
2.5 국외 출장자 관리 ····· 69
2.6 연구성과 유출 혐의자 관리 ····· 72
2.7 보안교육 ····· 74
2.8 접촉외국인 관리 ····· 78

2절. 외국인 관리

2.9. 외국인 연구원 관리 ····· 80

3절. 외부인 관리

2.10 상시 출입자 및 파견자 관리 ····· 85
2.11 일시 출입자 관리 ····· 88

4. 제 3장 연구개발 결과 및 내용의 관리

1절. 연구개발 정보 관리

3.1 연구결과물 관리 ····· 92
3.2 주요문서 관리 ····· 104

2절. 연구개발 결과 활용

3.3 연구개발 성과의 대외 공개 ····· 114
3.4 국외기술 이전 ····· 117

5. 제 4장 연구시설 관리

1절. 정보통신매체관리

4.1 외부 정보통신매체 반출입 통제 ····· 122

2절. 시설접근통제

4.2 주요시설물 관리 ····· 124
4.3 보호구역 별도 관리 ····· 131
4.4 외부 입주기관 통제 ····· 134

3절. 인적 접근 통제

4.5 연구시설 출입자 통제 ····· 135
4.6 외부방문자 출입 통제 ····· 138

6. 제 5장 정보통신망 관리

1절. 시스템 관리

5.1 업무용 컴퓨터 관리 ····· 142
5.2 저장매체 관리 ····· 146
5.3 정보시스템 사용 관리 ····· 150
5.4 전산장비의 폐기 ····· 151

2절. 데이터 관리

5.5 데이터 전송 ····· 153
5.6 데이터 유출 제한 ····· 157
5.7 데이터 백업 ····· 169

3절. 네트워크 보호

5.8 전산망 보호 설비 ····· 176
5.9 접근 제한 ····· 178
5.10 네트워크 자료 관리 ····· 183

7. 부록

연구보안관리규정 예시 ····· 186
국가연구개발사업 보안관리 조치사항(제 10조 관련) ····· 198
각종 양식 ····· 203
연구보안관리 우수·미흡사례 ····· 226

01

서 론

미래창조과학부
Ministry of Science, ICT and Future Planning

1. 「국가연구개발사업의 관리 등에 관한 규정」 도식화

「**국가연구개발사업의 관리 등에 관한 규정**」 은 제1장 총칙, 제2장 국가연구개발사업의 기획·관리·평가, 제3장 연구개발결과의 귀속 및 활용 촉진, 제4장 기술료의 징수 및 사용, 제5장 국가연구개발사업의 보안 및 정보관리, 제6장 국가연구개발사업 참여제한 및 사업비환수, 제7장 보칙으로 구성되어 있다. 그 중 제2장, 제3장, 제4장, 제5장에 대한 내용을 요약하여 연구개발과제의 생성 시 부터 집행까지의 과정을 도식화하였다.

먼저 각 장별로 상세한 내용으로 다루기 이전에 2장부터 5장까지 내용을 간략히 나타내면 다음과 같다.

제2장 국가연구개발사업의 기획·관리·평가

- 1절 : 국가연구개발사업의 기획 및 공고
- 2절 : 연구개발과제의 선정
- 3절 : 협약
- 4절 : 연구개발비의 지급 및 관리
- 5절 : 연구개발결과의 보고 및 평가
- 6절 : 연구개발비 정산

제3장 연구개발결과의 귀속 및 활용 촉진

- 연구결과물의 소유
- 연구개발결과의 활용 촉진

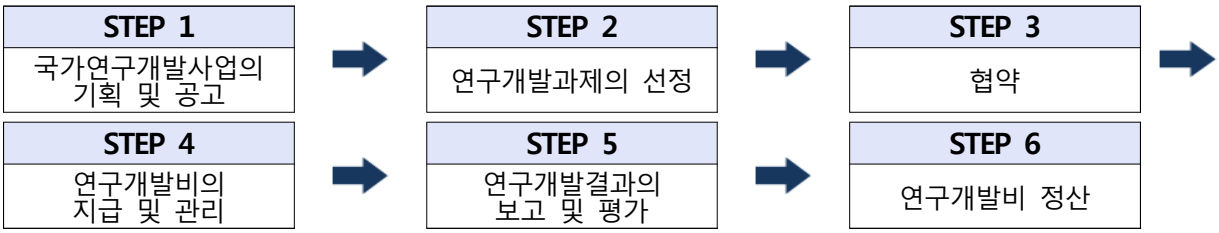
제4장 기술료의 징수 및 사용

- 기술료의 징수
- 기술료의 사용

제5장 국가연구개발사업의 보안 및 정보관리

- 국가연구개발사업의 보안
- 보안관리심의회
- 연구기관 보안관리심의회
- 보안과제와 일반과제의 분류기준
- 분류절차
- 보안등급 변경
- 보안등급에 따른 조치
- 연구개발결과의 보안등급
- 연구개발과제 보안관리 현황 보고
- 보안관리 위반 시 조치

가. 제2장 국가연구개발사업의 기획·관리·평가



1절 국가연구개발사업 기획 및 공고

· 중앙행정기관의 장은 국가연구개발사업을 추진하려는 경우에는 그 사업의 경제적 타당성 등에 대한 사전조사 또는 기획연구를 수행하여야 한다.
√ 중앙행정기관의 장은 국가연구개발사업을 수행하려는 연구책임자에게 연구보안에 대한 사항을 사전에 검토하고 포함할 것을 요구하도록 한다.

2절 연구개발과제의 선정

· 중앙행정기관의 장은 연구개발 선정 시 연구개발과제 평가단을 구성하여야 한다.
√ 연구개발과제 평가단은 과제 선정 시 해당 과제의 연구보안 조치사항에 대한 검토를 수행한다.
· 중앙행정기관의 장은 평가단의 명단과 종합 평가의견을 연구개발과제 신청자에 통보하여야 한다.
· 주관 연구기관의 장은 연구개발과제 선정 통보일로부터 15일 이내에 연구개발 계획서를 중앙행정기관의 장 또는 전문기관의 장에게 제출하여야 한다.
√ 연구개발계획서에는 해당 과제의 연구보안과 관련되는 위험요소와 이에 대한 예방 대책을 포함한다.

3절 협약

· 선정과제에 대하여 통보 받은 일로부터 1개월 이내에 주관연구기관의 장은 협약을 체결해야 한다.
√ 중앙행정기관은 과제의 연구보안 조치에 대한 계획을 검토 후 보안기준이 충족되었을 때에 주관연구기관과의 협약 체결을 진행한다.

4절 연구개발비의 지급

① **연구개발비의 지급**
· 중앙행정기관의 장은 연구개발비의 전부 또는 일부를 출연할 수 있다.
② **연구개발비의 사용**
· 주관연구기관의 장은 연구개발비 관리를 위한 별도의 계정을 설정하고 계정과 연결된 신용카드를 발급받아 관리하여야 한다.
· 단, 연구개발계획서 상의 연구개발비 사용계획에 맞게 사용하도록 노력하여야 하며 증명자료를 갖추어야 한다.

5절 연구개발결과의 보고 및 평가

① **연구개발결과의 보고**
· 주관연구기관의 장은 연구개발의 종료 시 연구개발 최종 보고서, 요약서, 주관연구기관 자체평가 의견서와 그 전자문서를 중앙행정기관의 장에게 제출하여야 한다.
√ 연구개발 최종보고서의 내용에는 연구개발결과물에 대한 사후 보안조치 계획을 포함한다.
② **연구개발결과의 평가**
· 중앙행정기관의 장은 연구개발결과와 연구 성과 활용 계획, 실적에 대한 중간평가 및 최종평가를 하고, 연구개발결과의 활용을 위한 추적평가를 할 수 있다.
③ **연구개발결과의 공개**
· 중앙행정기관의 장은 제출 받은 연구개발 최종보고서 및 요약서의 데이터 베이스를 구축하여 관련 연구기관 산업계 및 학계 등에서 활용할 수 있도록 널리 공개해야 한다.
√ 보안과제의 경우 최대 3년 내의 비공개 기간 동안 개발결과의 최종보고서 및 요약서를 적극적으로 공개하거나 활용하는 규정을 적용하지 아니할 수 있다.

6절 연구개발비 정산

· 주관 연구기관의 장은 협약기간 종료 후 3개월 이내에 다음 문서 또는 전자문서로 연구개발비의 사용실적을 중앙행정기관의 장 또는 전문기관의 장에게 보고해야 한다.
- 연구개발계획과 집행실적의 대비표
- 연구개발과제를 수행하는 연구기관의 자체 회계감사 의견서

나. 제3장 연구개발결과의 귀속 및 활용 촉진

연구결과물의 소유

· 국가연구개발사업의 수행 과정에서 얻어지는 연구기자재, 연구시설 및 장비, 시작품 및 연구노트 등 유형적 결과물은 협약으로 정하는 바에 따라 주관연구기관의 소유로 한다.
√ 보안과제의 경우, 무형적 결과물은 주관연구기관의 단독소유를 원칙으로 하며, 공동연구기관이 자체개발 또는 주도적으로 개발한 경우에는 주관연구기관과의 협상에 의해 공동으로 소유할 수 있다. 단, 이 경우에는 소속 중앙행정기관과 국가정보원장의 사전승인 심사를 거쳐야 한다.

연구개발결과의 활용 촉진

· 연구개발결과물 소유기관의 장 또는 전문기관의 장은 연구개발결과가 널리 활용 될 수 있도록 출원 중인 지식재산권을 포함한 연구개발 결과물을 대상으로 기술실시계약을 체결하는 등 연구개발 결과를 활용하는 데에 필요한 조치를 하여야 한다.
√ 보안과제의 경우, 연구성과물 기술실시 계약 시 '제 3자 기술 실시(사용)권 금지 협약'을 체결한다.

다. 제4장 기술료의 징수 및 사용

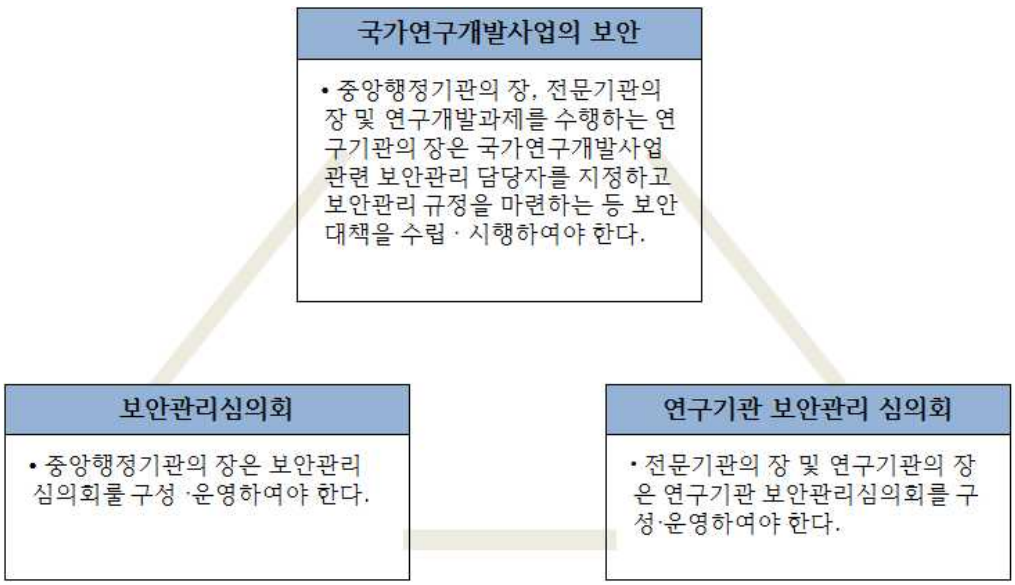
기술료의 징수

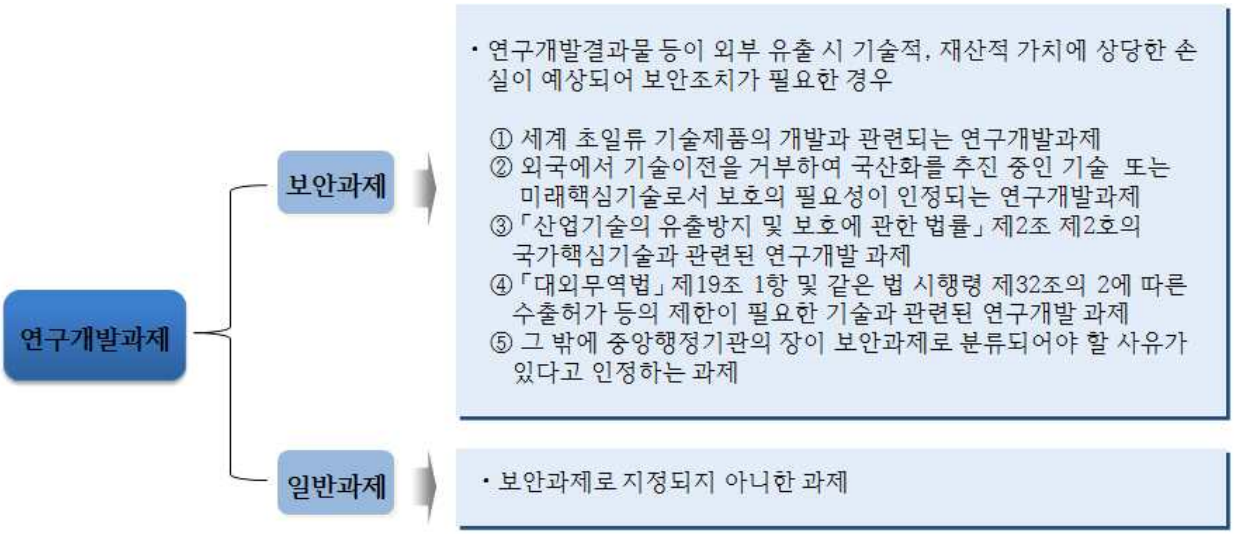
· 실시권의 내용 기술료 및 기술료 납부방법 등은 연구개발결과물 소유기관의 장이 연구개발결과물을 실시하려는 자와 합의하여 정한다.

기술료의 사용

· 연구개발결과물 소유기관의 장이 비영리법인, 영리법인일 경우 각각 징수한 기술료를 법령에 기술된 호와 같이 사용하여야 한다.

라. 제5장 국가연구개발사업의 보안 및 정보관리





☞ 연구개발과제 수행 과정 중 산출되는 모든 문서에는 분류기준에 따라 분류된 보안등급을 표기하여야 한다.

분류절차

▪ 중앙행정기관의 장은 연구개발과제 평가단으로 하여금 보안등급 분류의 적정성을 검토하게 하고 그 결과를 반영하여 보안등급을 결정한다.

보안등급 변경

▪ 연구개발과제의 보안등급 변경 시 자체 보안관리 규정의 절차에 따라 연구보안심의회의 심의를 거쳐 변경할 수 있으며 변경 시 소관 중앙행정기관장에게 변경내용과 사유를 제출하여야 한다.

보안등급에 따른 조치

▪ 연구기관의 장 및 연구책임자는 분류한 보안등급에 따른 보안관리 조치를 하여야 하며 그 내용은 별표2의 3과 같다.

본 매뉴얼은 별표 2의 3의 지침을 기준으로 하였음

연구개발결과의 보안등급

▪ 연구개발결과의 보안등급은 연구과제의 보안등급에 따라 결정되거나 변경된 연구개발과제 보안등급으로 한다.

연구개발과제 보안관리 현황 보고

▪ 전문기관의 장은 연구기관의 국가연구개발사업 보안관리 현황을 미래창조과학부령으로 정하는 서식에 따라 조사할 수 있다.

보안관리 위반 시 조치

▪ 전문기관, 연구기관, 연구책임자 및 참여연구원 등은 이 영에서 정하는 사항 및 관련 국가연구개발사업 보안관리규정을 지켜야 한다.

2. 국가연구개발사업보안관리 세부 조치사항과 매뉴얼 항목간의 관계

1. 보안관리 체계

세부 조치사항	메뉴얼의 항목
1. 이 규칙 또는 관계 법령에 따라 연구기관 보안관리 실정을 반영한 자체 보안관리규정의 제정 · 개정	1.1 보안관리규정
2. 연구개발과제 보안관리와 관련한 각종 안건을 심의하기 위한 연구보안심의회 운영	1.2 연구보안심의회 운영
3. 연구과제 보안관리 업무의 종합계획 · 관리를 담당하는 보안관리책임자 및 보안 업무 전담직원 지정 · 배치	1.3 보안관리자 지정
4. 국가연구개발사업 보안관리 부서 및 연구 인력에 대한 보안 관련 규정 교육 · 홍보 실시	1.4 보안관리 규정 교육 및 홍보
5. 자체 보안관리 규정에 보안 우수자 및 규정 위반자에 대한 상벌 조치 명시	1.5 보안 우수자 및 위반자에 대한 조치
6. 보안사고 예방 · 조치 · 대응 등 재발 방지책 마련	1.6 보안사고관리
7. 연구기관 및 연구원에 대한 정기 · 수시 보안점검 및 보안교육 실시	1.7 보안점검 및 보안교육 실시
8. 화재, 홍수, 재난, 재해 등 비상시 대응계획 수립	1.8 비상시 대응계획 수립
9. 외국기업 및 국외연구기관과 공동연구 · 위탁연구 시 중앙행정기관의 사전 승인 절차 이행	1.9 공동 및 위탁 연구 시 사전승인 절차 이행

2. 참여연구원 관리

세부 조치사항	메뉴얼의 항목
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	2.1.1 신입채용 시 인원관리 2.2.1 재직 중 인원관리 2.3.1 계약 갱신 시 인원관리 2.4.1 퇴직자 관리
2. 연구과제 수행 연구원의 보안의식을 높이기 위한 보안 관련 교육 이수	2.7.1 보안교육
3. 퇴직(예정)자의 반출(예상)자료에 대한 보안성 검토, 연구성과물 회수, 전산망 접속 차단 등을 제 때 조치	2.4.1 퇴직자 관리
4. 외부기관 파견자 등 임시직 및 방문자에 대한 별도 보안조치	2.10.1 상시 출입자 및 파견자 관리 2.11.1 일시 출입자 관리
5. 연구성과 유출 혐의(전력)자가 과제에 참여할 경우 특별 관리조치	2.6.1 연구성과 유출 혐의자 관리
6. 참여연구원의 해외 출장 시 사전 보안교육 및 귀국보고 실시	2.5.1 국외 출장 시 고려사항
7. 외국인 연구원의 별도 보안조치(영문 보안서약서 작성, 출입지역 제한, 반출 · 반입 물품 제한, 특이 동향 관리 등)	2.9.1 외국인 연구원 관리
8. 보안과제 참여연구원이 과제와 관련하여 접촉하는 외국인 현황 관리	2.8.1 연구원의 접촉외국인 관리
9. 외국인 연구원의 보안과제 참여 시 소속 기관장의 승인 절차 이행	2.9.2 보안과제 참여 시 관리

3. 연구개발 결과 및 내용의 관리

세부 조치사항	메뉴얼의 항목
1. 연구개발과제 수행과정 중 산출되는 모든 문서에 보안등급 표기	3.1.2 연구성과물의 보안등급 부여
2. 연구수행 단계별 특허권 · 지식재산권 확보 방안과 주요 연구자료 및 성과물의 무단 유출 방지를 위한 보안책 마련 · 시행	3.1.1 연구개발 성과물의 권리 확보
3. 연구개발 성과의 대외 공개(홈페이지 게재 포함) 및 제공 시, 연구책임자의 사전 보안성 검토 확인절차 이행	3.3.1 연구개발 성과의 대외 공개 시 관리
4. 연구개발결과의 해외 기술이전(양도) 추진 시 관계법령 준수 - 「산업기술의 유출방지 및 보호에 관한 법률」 제11조 (국가핵심기술의 수출 등) - 「대외무역법」 제13조(전략기술 수출의 승인 등)	3.4.1 국외기술 이전 시 관리
5. 연구개발 결과 활용 시 국내에 있는 자를 계약체결 대상으로 우선 고려	3.1.4 연구개발 성과물의 활용
6. 외부 기관과 보안과제의 공동(협동 · 위탁 포함)연구협약 시 성과물의 귀속, 자료 제공 및 장비 반납 등에 관한 사전 보안대책 마련 및 적용	3.1.3 외부기관과 공동 협약 시 연구 결과물의 관리
7. 연구성과물 기술 실시(사용) 계약 시 “제3자 기술 실시(사용)권 금지협약” 체결	3.1.4 연구개발 성과물의 활용
※ 지침의 조치사항 외 추가 항목	3.2 주요 문서 관리 3.2.1 문서 생성 3.2.2 문서 활용 3.2.3 문서 보관 3.2.4 문서 폐기

4. 연구시설 관리

세부 조치사항	메뉴얼의 항목
1. 노트북, 외장형 하드디스크 드라이브 등 정보통신 매체에 대한 반입 · 출입 절차 마련 및 이행	4.1.1 외부 정부통신매체 반·출입 통제
2. 외곽, 주요 시설물에 폐쇄회로 텔레비전, 침입감지 센서 등 첨단장비를 설치 · 운용	4.2.1 감시 장치 설치
3. 연구개발과제와 관련된 핵심기술 및 정보를 보관하는 전산실 및 중요시설물에 대해서 보호구역 지정 후 특별 보안관리 조치	4.3.1 보호구역의 지정 4.3.2 보호구역 통제 수단 4.3.3 보호구역 내 업무
4. 외부 입주기관(벤처기업 포함)의 연구시설 내부 출입 통제 조치	4.4.1 외부 입주기관 통제 및 관리
5. 연구시설 출입자에 대한 개인별 출입권한 차등 부여 및 통제	4.5.1 연구시설 출입자 통제 및 관리
6. 외부방문자 출입 시 보안관리책임자의 사전 허가 후에 담당 직원이 방문자와 함께 방문지역 동행	4.6.1 외부 방문자 출입 통제 및 관리

5. 정보통신망 관리

세부 조치사항	메뉴얼의 항목
1. 연구개발과제의 보안을 목적으로 전산망 보호를 위한 방화벽 시스템, 침입탐지시스템 등 각종 장비의 설치·운영	5.8.1 전산망 보호 설비 마련
2. 외부에서 내부망 접속 시 사용자 인증으로 정보시스템 접근 제한 조치	5.9.1 내부망 연결 제한
3. 컴퓨터에 각종 장비 및 소프트웨어 설치 시, 보안 관리 책임자의 사전 승인	5.1.2 소프트웨어 설치
4. 무선통신망 구축 시 비인가 사용자의 차단을 위한 사용자 인증, 암호화 통신, 암호화 키의 주기적 변경 등 보안조치	5.9.2 무선통신망 관리
5. 사전에 소속 기관에서 인가받은 보안 이동형 저장매체 사용	5.2.2 이동형 매체 관리
6. 보안시스템 안전사고에 대비 데이터 백업시스템 구축·운영 및 원거리 지역 보안시설에 중요 데이터 별도 복사본 보관	5.7.1 사내 백업 시스템 5.7.2 원격지 백업
7. 비인가 개인용 정보통신매체 반입·출입 통제 및 내부망 연결 제한	5.2.1 하드웨어 관리
8. 업무용 컴퓨터 대상 보안 소프트웨어, 보안패치 등 설치 및 업데이트	5.1.1 PC 보안관리
9. 보안사고에 대비하여 정보시스템 사용 기록 (최소 6개월 이상) 보관 - 보관 권장기간 : 1년	5.3.1 정보시스템 사용 기록 관리
10. 직책, 업무에 따라 각종 전산 자료에 대한 차등적 접근권한 부여	5.6.2 전산자료에 대한 접근 통제
11. 네트워크 자료(시스템 구성, IP 현황 등)의 대외 보안 관리	5.10.1 네트워크 자료 관리

세부 조치사항	메뉴얼의 항목
12. 전산장비 폐기 및 외부 이관 시, 하드디스크 드라이브 등에 저장된 주요 자료가 불법으로 복구되지 않도록 조치	5.4.1 전산장비의 처분 및 재사용
13. 내부망의 연구실별 물리적 또는 논리적(방화벽 등) 분리	5.9.1 내부망 연결 제한
14. 업무용 컴퓨터 자료를 휴대전화, 이동형 저장매체 등 개인용 정보통신매체에 복사 · 저장 · 전송할 경우 보안관리책임자의 사전 승인	5.5.1 개인용 저장매체에 전송
15. 인터넷을 이용하여 외부로 자료 전송 시, 승인 절차 등 보안대책 마련 및 이행	5.5.2 외부로의 전송
16. 메신저, 인터넷 저장소, 외부 이메일 등 자료 유출 가능 경로 접속차단	5.6.1 데이터 유출가능 경로 관리

3. 용어정의

1. 국가연구개발사업이란 중앙행정기관이 법령에 근거하여 연구개발과제를 특정하여 그 연구개발비의 전부 또는 일부를 출연하거나 공공기금 등으로 지원하는 과학기술 분야의 연구개발사업을 말한다.
2. 보안과제란 연구개발결과물 등이 외부로 유출될 경우 기술적·재산적 가치에 상당한 손실이 예상되어 보안조치가 필요한 과제를 말한다.
3. 연구보안사고란 연구개발사업과 관련된 중요한 정보 및 성과물이 외부로 유출되거나 누설, 분실 또는 도난을 당하거나 연구개발사업과 관련된 정보를 유통하고 관리, 보존하는 시스템이 외부로 유출, 손괴 또는 파괴된 경우를 말하며 그 밖에 중앙행정기관의 장이 정하는 보안 관련 사고를 말한다.
4. 보안총괄책임자란 연구기관의 시설보안, 정보보안, 연구보안을 총괄적으로 관리하는 책임자를 말한다.
5. 연구보안관리자란 중요한 연구개발정보를 보호하기 위하여 연구보안 규정 제·개정 및 계획수립, 감독, 지도 등 일련의 보호활동을 하는 연구보안책임자 및 담당자를 말한다.
6. 분임연구보안관리자란 연구보안관리자의 연구보안 임무 및 활동을 보조하기 위하여 각 연구과제별(또는 부서별)로 연구개발정보에 대한 보호활동을 하는 연구책임자(또는 부서장) 및 연구원(또는 부서원)을 말한다.
7. 국제공동연구란 복수의 연구개발주체가 동일한 연구과제의 수행에 소요되는 연구개발자금·인력·시설·기자재·정보 등 연구 자원을 공동으로 부담하여 국제적으로 수행하는 연구개발을 말한다.
8. 국제위탁연구란 의뢰기관이 수행하는 연구의 일부를 해외 전문가 또는 해외 연구기관에게 위탁하여 수행하게 하는 연구를 말한다.
9. 연구성과 유출혐의자란 과거에 연구개발 관련 기밀자료나 연구개발 성과물을 고의적 또는 실수로 외부에 유출한 경험이 있는 자를 말한다.
10. 지식재산권은 문화, 예술, 과학작품, 산업활동 등 인간의 지적 창작 활동의 결과로 생기는 모든 무형의 소산물에 대한 권리를 말한다.
11. 특허권이란 발명, 발견에 의한 신제품 또는 신제법을 일정기간 독점적으로 제작하거나, 사용·판매할 수 있는 권리를 말한다. 선출원주의에 따라 특허를 먼저 출원한 사람이 특허권을 얻는다.
12. 특허 출원이란 새로운 발명, 발견을 한 사람이 국가에 대하여 그 특허를 요구하는 행위를 말한다.
13. 영업비밀이란 공공연히 알려져 있지 않으며, 독립된 경제적 가치를 가지고 있고, 상당한

노력에 의해 비밀로 유지된 생산방법, 판매방법 기타 영업활동에 유용한 기술상 또는 경영상의 정보를 말한다.

14. 공동협약이란 복수의 연구개발주체가 동일한 연구개발과제를 수행하기 위해 소요되는 연구개발비·인력·기자재·정보 등 연구 자원을 공동으로 부담하여 수행하는 것을 목적으로 계약 체결하는 것을 말한다.
15. 연구개발 성과물이란 연구개발을 통하여 창출되는 특허·논문 등 과학기술적 성과와 유·무형의 경제·사회·문화적 성과를 말한다.
16. 기술실시계약이란 연구기관이 소유하고 있거나 그 사용 권리를 보유하고 있는 연구결과 또는 기술(지적재산권 포함)에 대해 교육지도 또는 현장지도를 통하거나 기술자료를 제공하여 실시자에게 실시권을 허여하는 계약을 말한다.
17. 기술이전이란 국가연구개발사업으로 개발한 결과물(기술, 지식, 정보)이 양도실시권 허여·기술지도 등의 방법을 통하여 기술보유자로부터 그 외의 자에게 이전되는 것을 말한다.
18. 국가핵심기술이란 국내외 시장에서 차지하는 기술적·경제적 가치가 높거나 관련 산업의 성장잠재력이 높아 해외로 유출될 경우에 국가의 안전보장 및 국민경제의 발전에 중대한 악영향을 줄 우려가 있는 기술을 말한다.
19. 공용구역이란 보안상 차별화된 통제가 필요하지 않은 지역으로 연구기관의 임직원이나 외부인 등 모든 사람에게 공개된 구역을 말한다.
20. 일반구역이란 보안상 차별화된 통제가 필요하지 않은 지역으로 임직원이나 출입이 허가된 정기 방문자, 임시 방문자에 한하여 출입이 가능한 구역을 말한다.
21. 제한구역이란 보안상 비인가자의 접근을 방지하기 위하여 사전에 보안총괄책임자로부터 허가를 득한 자만이 출입 가능한 지역으로 연구기관의 중요한 설비가 위치하고 있는 구역을 말한다.
22. 통제구역이란 침해사고 또는 유출사고 발생 시 연구기관에 치명적인 영향을 미치는 보안상 극히 중요한 시설로서 사전에 보안총괄책임자로부터 허가를 득한 자만이 출입 가능한 지역으로 퇴실 시까지 직원의 동행이 필요하며 외부방문객의 출입이 엄격하게 제한된 구역을 말한다.
23. 임시방문자란 필요에 의해 일시적으로 연구기관을 방문자하는 자를 말한다.
24. 정기방문자란 필요에 의해 정기적으로 연구기관을 출입하는 방문자를 말하며 연구개발용역업체 직원 또는 연구시설 및 장비유지보수업체 직원, 청소용역 직원 등이 이에 해당된다.

02

제 1 장
보안관리체계

1.1 보안관리규정
1.2 연구보안심의회 운영
1.3 보안관리자 지정
1.4 보안관리 규정 교육 및 홍보
1.5 보안 우수자 및 위반자에 대한 조치
1.6 보안사고관리
1.7 보안점검 및 보안교육 실시
1.8 비상시 대응계획 수립
1.9 공동 및 위탁 연구 시 사전승인 절차 이행

미래창조과학부
Ministry of Science, ICT and Future Planning

1.1 보안관리규정

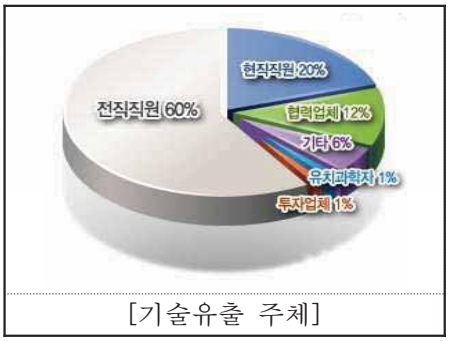
해당과제	
모든과제	보안과제
○	

이행대상		
연구기관	연구책임자	참여연구원
◎		

1.1.1 보안관리규정

최근 국가연구개발사업과 민간부문의 연구개발사업으로 개발된 첨단 기술이 해외로 유출되었다가 적발된 건수가 점차 증가하고 있는 추세를 보이고 있으며 전·현직 직원 또는 협력업체로 인해 발생하는 연구보안사고가 거의 92%를 차지하고 있는 실정이다.

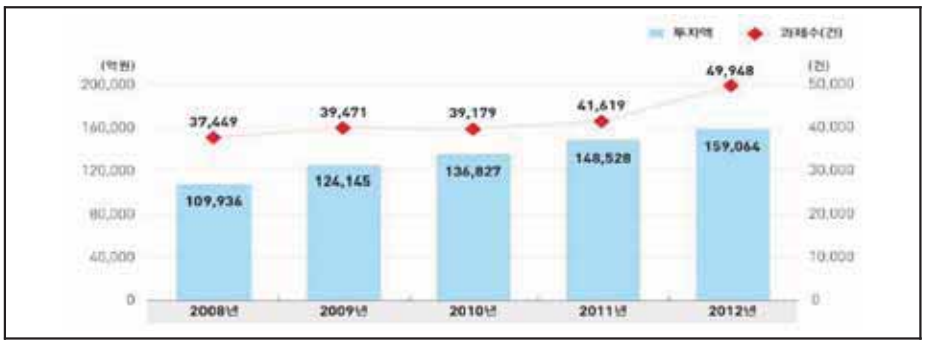
[연도별 기술유출 사고 건 수]



[기술유출 주체]

출처: 산업기밀보호센터 기술유출 통계(2012)

또한, 전 세계적으로 과학기술경쟁력이 국가경쟁력의 중요한 요소로 인식됨에 따라 글로벌 차원의 과학기술 경쟁이 심화되면서 우리나라는 연구개발에 대한 투자가 날로 증가하고 그에 따른 최첨단 연구개발 성과물도 더불어 늘어가고 있는 실정이다.



[국가연구개발사업 투자액 및 과제수 추이 (2008∽2012)]

출처: 2012년도 국가연구개발사업 조사·분석보고서(KISTEP)

[우리나라 국내 특허출원 및 등록 건수 추이 (2003∽2012)]

출처: 우리나라와 주요국의 특허성과 현황(KISTEP)

따라서 이러한 연구개발 성과물을 보호하고 연구보안 사고를 사전에 예방하기 위한 가장 기본적인 조치 사항으로 연구기관의 환경에 적합한 체계적인 연구보안관리 규정을 제정하여 이를 모든 임직원이 준수할 수 있도록 시행하여야 한다.

내용

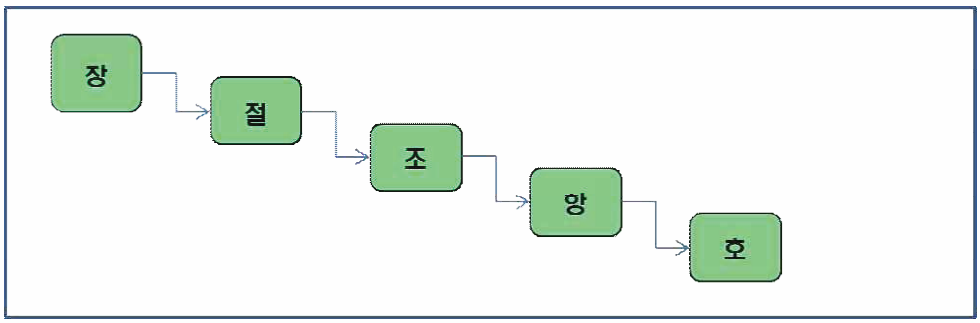
· 연구보안관리 규정은 이해하기 쉽고 표현이 정확해야하며 구체적이면서 연구기관의 실정에 적용 가능해야 한다.

정확성	- 평이한 문장으로 정확하게 표현 - 필요한 내용 누락되지 않도록 주의
이해성	- 추상적인 표현은 배제하고 세밀하고 구체적으로 표현 - 이해하기 쉬운 단어로 간결하게 작성
통일성	- 문장 또는 내용이 서로 모순되지 않도록 통일성 유지 - 용어, 문체, 형식 등 통일성 유지
실행 가능성	- 모든 임직원이 준수 가능한 규정 마련 - 각 기관의 실정에 맞는 규정 마련
적법성	- 상위법에 위배되지 않도록 작성 - 기관 내 다른 규정과 적법한 범위 내에서 작성

[규정 작성 시 고려 사항]

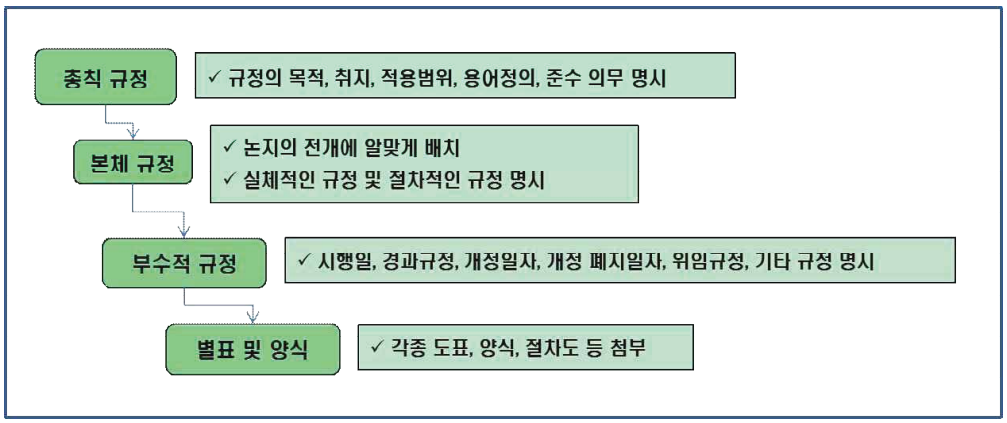
내용

- 연구보안관리 규정의 제목을 정할 때는 전체 내용에 맞게 간결해야 되는데 기본 규정인 경우에는 OO규정 또는 OO규칙이라 붙이고 위임규정인 경우에는 OO지침, OO요령이라고 붙인다.
- 또한, 연구보안관리 규정의 이해와 규정열람의 편의성을 도모하기 위하여 규정을 장, 절, 조, 항, 호로 그 내용에 따라 분류한다.



[연구보안관리 규정 형식 체계도]

- 연구보안관리 규정은 이해하기 쉽게 논리적으로 전개가 되도록 배열하는 것이 일반적이며 총칙 규정, 본체 규정, 부속 규정 등으로 구성된다. 총칙 규정에는 규정의 목적, 취지, 적용범위 등 준수의무 사항들을 명시하고 본체 규정에는 논지의 전개에 알맞게 배치하되, 이해하기 쉬운 표현방법을 사용하면서 실체적인 규정 및 절차적인 규정을 명시한다. 부수적 규정에서는 시행일, 경과규정, 개정일자, 위임규정 등을 명시하면 된다. 그리고 마지막으로 규정의 이해를 돕고자 각종 도표나 양식 등을 첨부한다.

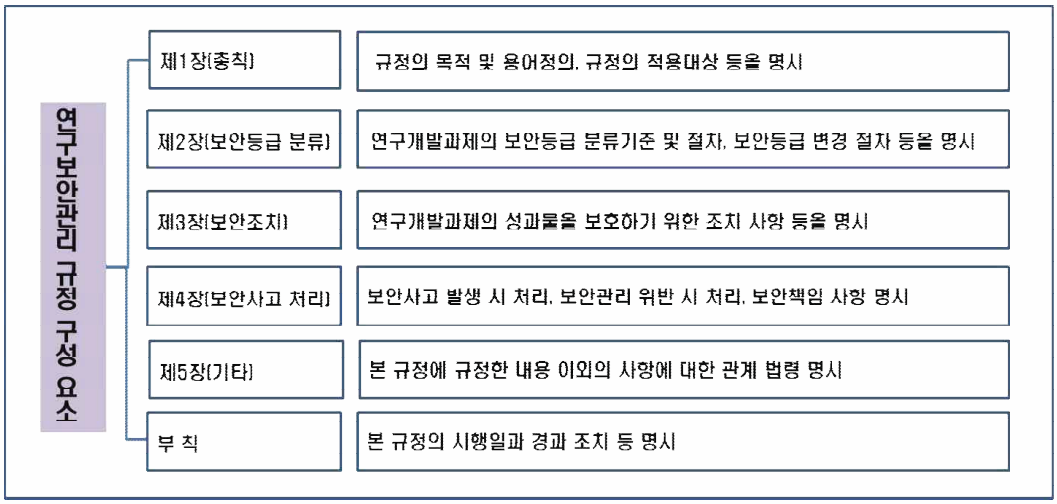


[연구보안관리 규정 구성도]

- 연구보안관리 규정의 일반적인 구성은 제1장에 총칙으로 규정의 목적 및 적용 대상 등을 명시한다. 제2장에서는 보안등급 분류 기준 및 보안등급 변경절차 등을 명시하고 제3장에서는 연구개발과제의 성과물을 보호하기 위한 조치사항들을 명시한다. [별첨 1.1.1 참조]

내용

제4장에서는 보안사고 발생 시 처리 사항과 보안관리 위반 시 처리사항에 관한 내용을 명시하면 된다. 그리고 제 5장 기타에서는 본 규정에서 규정한 내용 이외의 사항에 대한 관계 법령을 명시하고 마지막에 부칙으로 본 규정의 시행일과 경과 조치 등을 명시하면 된다.

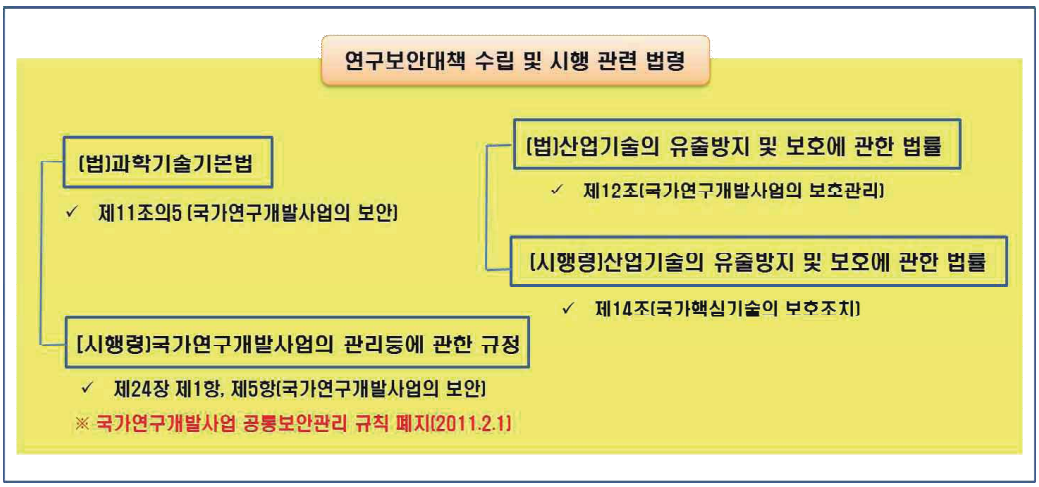


[연구보안관리 규정의 일반적인 구성 요소]

실행지침

1. 연구보안관리 규정 제정

· 「과학기술기본법」 및 「국가연구개발사업의 관리 등에 관한 규정」등 상위법을 준수하여 작성하여야 한다.



[연구보안 관련 법률 및 규정 체계]

실행지침

- 연구보안관리를 전담하는 부서와 담당자를 지정하고 연구보안관리의 중요한 사항들을 심의하는 연구보안심의회를 구성하는 절차를 마련해야 한다. 또한, 위원장을 포함하여 위원들의 임기와 위원회에서 다루어야 하는 주요 심의 내용 등을 구체적으로 명시해야 한다.
- 연구개발과제의 보안등급을 분류하는 기준과 절차를 명시하고 보안등급의 변경이 필요하다고 판단될 때 이를 변경하는 절차도 기술해야 한다. 또한, 연구개발 결과물에 대한 보안등급을 부여하는 절차와 변경 절차도 마련해야 하며 그 결과를 관련 기관 및 해당 연구책임자에게 통보하는 절차도 수립해야 한다.
- 연구개발과제의 산출물 및 성과물을 보호하기 위하여 보안등급에 따른 보안 조치사항과 더불어 참여연구원, 외국기업 및 외국인, 연구개발결과 공개, 통신기기 활용, 국제공동연구, 해외 기술이전, 연구개발 성과물관리 등을 위한 보안 조치 사항을 기술해야 한다.
- 연구개발과제 보안관리 현황을 전문기관의 장에게 보고하는 절차와 보안관리 실태 점검결과에 따른 개선조치 시한과 보고대상 범위를 규정해야 한다.
- 보안사고의 유형 및 정의를 구체화하고 보안사고 발생 시 처리방안과 절차를 명시해야 하며 보안관리 준수 의무사항과 보안관리 위반사항에 따른 처리내용을 명시해야 한다.
- 연구 시제품 제작 및 연구과제 재위탁, 해외유치과학자 등에 관한 보안대책을 명시해야 한다.
- 연구기관의 고유한 기능과 환경을 고려하여 실제로 적용이 필요하고 가능한 내용 위주로 연구보안관리 규정을 작성해야 한다.

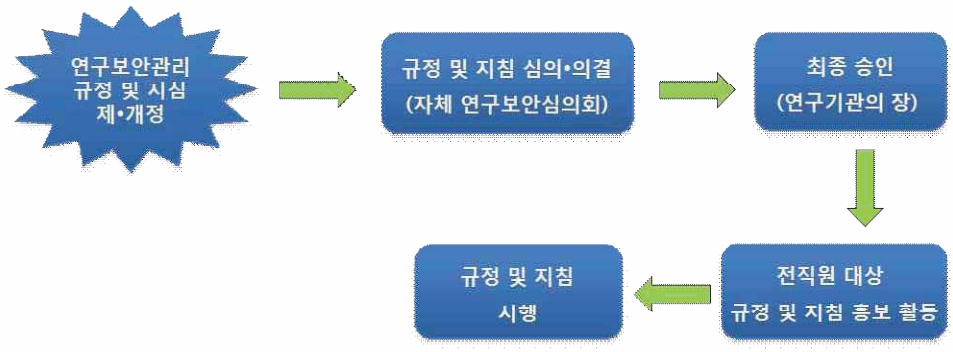
2. 연구보안관리 규정 개정

- 핵심 기술과 관련된 중요한 연구 정보 및 성과물을 외부로 유출하기 위한 수법은 나날이 발전하고 있기 때문에 연구보안 사고를 미연에 방지하기 위해서는 현실에 맞게 연구보안 관리 규정을 수시로 보완하여 개정해야 한다.
- 연구보안 사고의 재발방지를 위하여 연구보안관리 실태점검에서 발견된 취약점에 대한 개선책과 연구보안 사고 발생 시 마련한 보안대책 등을 반영하여 규정 및 지침을 개정해야 한다.
- 연구보안 관련 상위법이 개정되면 그 즉시 자체 연구보안관리 규정 및 지침도 상위법에 위배되지 않도록 개정해야 한다.

실행지침

3. 연구보안관리 규정 제·개정 승인 절차 이행 및 시행

- 연구보안관리 책임자가 연구보안관리 규정을 제·개정하고자 하는 경우 자체 연구보안심의회의 심의를 거쳐 연구기관의 장으로부터 승인을 받아야 한다.
- 연구보안관리 책임자는 제·개정된 연구보안관리 규정 및 지침에 관한 내용을 전 직원이 준수할 수 있도록 자체 게시판 또는 이메일, 홍보 책자 등을 통해 널리 알리고 이를 즉시 시행하여야 한다.



[연구보안관리 규정 및 지침의 승인 및 시행 절차]

1.2 연구보안심의회 운영

해당과제	
모든과제	보안과제
○	

이행대상		
연구기관	연구책임자	참여연구원
◎		

1.2.1 구성 및 운영방법

연구보안 환경의 변화에 따라 적절하게 대응하고 연구보안 사고를 사전에 예방하며 보안사고 발생 시 신속하게 처리하는 등 연구보안 관리의 효율적인 업무 수행을 위하여 필요한 중요한 사항을 심의하기 위하여 자체적으로 가칭 연구보안심의회를 구성하여 운영하여야 하며 이를 효율적으로 운영하기 위한 방법도 세부적으로 마련할 필요가 있다.

내용

연구기관의 장은 연구보안심의회의 주요 역할 및 기능들을 정립하고 이를 구성하기 위한 방법과 절차 등을 수립하여야 한다. 또한, 연구보안심의회의 조직 체계를 포함하여 이를 개최하기 위한 절차와 운영 방법 등에 관한 세부적인 사항들을 마련해야 한다. 그리고 연구보안심의회에서 심의하고 의결해야 하는 주요 사항들을 구체적으로 명시하여야 한다.

실행지침

1. 연구보안심의회 구성 시기 및 방법

- 연구기관의 장은 정기적(1년 또는 2년 주기)으로 연구보안심의회의 위원장과 위원들을 내부 임직원들 중에서 공식적인 절차를 거쳐 임명해야 한다.

실행지침

2. 연구보안심의회 위원 구성

- 위원장 1인을 포함하여 가급적 5인 이상 10인 이내의 위원으로 구성한다.
- 위원장은 임원중에서 임명하되, 연구관리 총괄부서장을 위원장으로 선임할 수 있다.

3. 연구보안심의회 심의 내용

- 국가연구개발사업(또는 자체 연구개발사업)과 관련된 자체 보안관리 규정의 제정 및 개정
- 국가연구개발과제(또는 자체 연구개발과제) 보안등급 분류에 대한 적정성
- 국가연구개발사업(또는 자체 연구개발과제)과 관련된 보안사고의 처리
- 연구보안 관련 포상자 추천
- 그 밖에 위원장이 필요하다고 인정하는 사항

4. 연구보안심의회 개최 및 운영 방법

- 위원회의 서무를 처리하기 위하여 간사 1인을 두어야 하며 연구보안담당 부서장 또는 연구관리담당 부서장이 간사 역할을 수행한다.
- 연구기관의 장 또는 위원장의 필요에 의해 위원회를 개최한다. 단 재적위원의 3분의 2이상 출석과 출석위원의 과반수이상의 찬성으로 의결하되, 가부동수인 경우 심의회 위원장이 결정한다.
- 심의회 위원장이 필요하다고 인정할 때에는 관계자를 출석시켜 의견을 진술하도록 할 수 있다.
- 심의 안건중 경미한 사항은 서면결의로 처리할 수 있다.
- 심의회 위원장은 연구보안 관련 포상 및 처벌을 인사위원회 안건으로 상정할 수 있다.
- 심의회 위원장 유고 시 위원장이 지명하는 위원이 그 직무를 대행할 수 있다.
- 연구보안심의회는 연구기관의 규모 및 사정에 따라 연구심의회(가칭)에서 그 기능을 수행할 수도 있다.

1.3 보안관리자 지정

해당과제	
모든과제	보안과제
○	

이행대상		
연구기관	연구책임자	참여연구원
◎		

1.3.1 보안관리자 지정

연구기관의 연구개발 보안업무를 철저하게 수행하고 지속적으로 관리하기 위하여 연구기관의 장은 연구보안관리 업무를 전담해서 처리할 수 있는 연구보안 관리자(연구보안 책임자 및 담당자)를 지정하여 임명하여야 한다. 이를 통해, 연구보안관리 업무가 평상시에 체계적으로 관리되고 위급한 비상사태 발생 시 신속하게 대응하고 처리할 수 있도록 하여야 한다.

내용

- 연구보안관리자는 연구보안 관리를 위한 종합계획을 수립하고 이를 효율적으로 운영하기 위해 지도 감사 및 교육을 진행하여야 한다.
- 또한, 연구보안 관리와 관련된 전반적인 보안조치를 수행하고 연구보안 사고를 사전에 예방하기 위하여 정기적으로 연구보안실태 점검을 실시하여 미진한 사항은 보완책을 마련하여 보안사고 재발방지를 위한 절차를 수립하여야 한다.
- 이와 더불어 연구보안 업무를 효율적이고 체계적으로 수행하기 위하여 연구보안심의회를 운영하고 관리하는 임무를 수행한다.
- 이와 별도로 연구보안책임자는 각 연구개발과제에 대한 연구보안 규정 준수를 강화하기 위하여 분임연구보안 책임자와 분임연구보안 담당자를 지정하여 운영할 수도 있다.

실행지침

1. 연구보안 관리자(연구보안 책임자 및 담당자) 선정 절차 수립

- 연구보안 책임자와 담당자는 연구기관의 장이 임명하되, 연구보안 담당자가 연구보안관리 업무를 충실히 수행할 수 있는 여건을 마련하여야 한다.
- 연구보안 책임자는 연구보안 업무를 효율적으로 수행하기 위하여 각 연구과제별로(또는 부서별로) 연구책임자(또는 부서장)를 분임연구보안 책임자로 임명할 수 있으며 참여연구원(또는 부서원)중에서 분임연구보안 담당자를 임명할 수 있다.

2. 연구보안 관리자 자격 기준 마련

- 연구관리 업무 또는 그에 합당한 업무 경험이 있는 자로서 외부에서 실시하는 연구보안 관련 교육을 이수한 자이어야 한다.
- 연구보안 업무를 수행하는데 결격 사유가 없는 자이어야 한다.

3. 연구보안 관리자 임무 지정

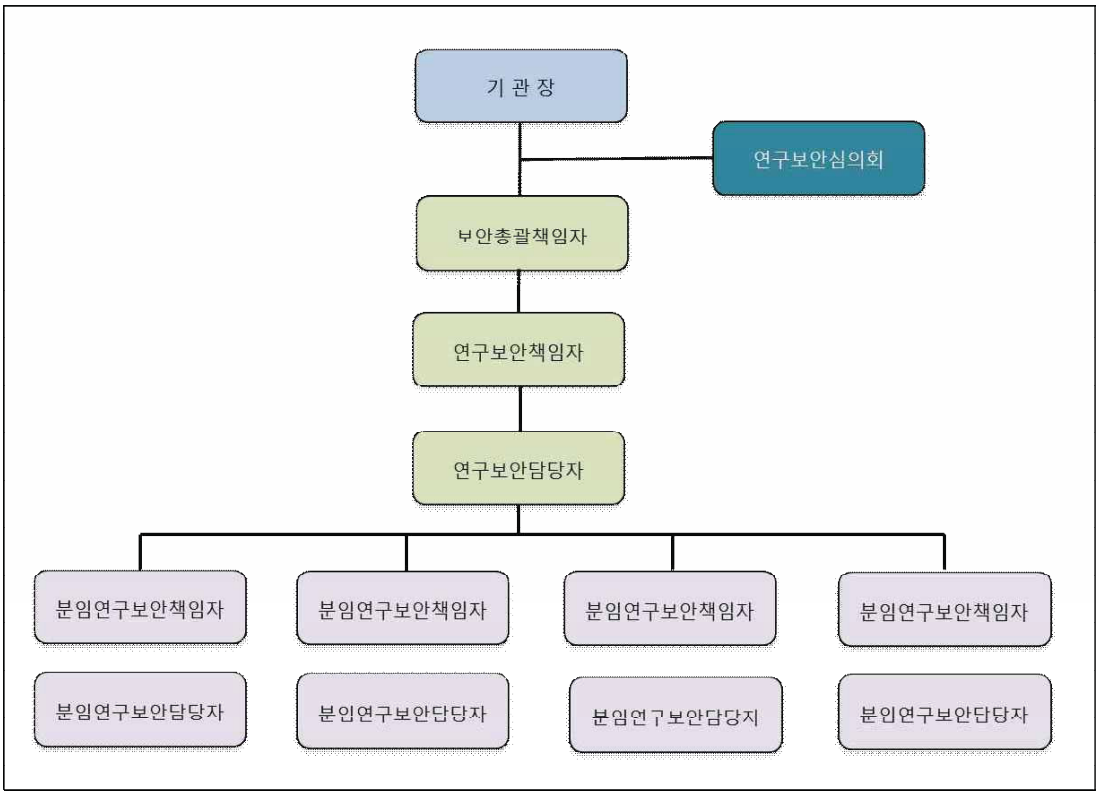
- 연구보안 관련 규정의 제정 및 개정
- 연구보안관리 업무수행에 관한 계획 수립과 조정 및 감독
- 연구보안심의회 운영 및 간사 임무
- 연구개발 비밀취급인가자 소요파악 및 비밀취급인가증 발급의뢰
- 연구책임자 및 참여연구원에 대한 보안서약서 징구
- 정기적인 연구보안 교육 및 지도
- 연구보안관리 실태 점검 및 개선책 마련
- 연구개발 보안과제 현황 파악 및 관리
- 연구보안사고 보고 및 조치 후 사고 방지책 마련
- 연구개발 비밀문서 관리 및 운용, 감독
- 기타 연구보안과 관련된 제반 업무 수행

4. 분임연구보안 책임자와 담당자 임무 지정

- 참여연구원의 연구보안 관리실태 점검
- 연구보안 책임자 및 담당자가 지시하는 사항 처리
- 연구개발 비밀문서의 보관 및 관리
- 연구개발 비밀문서 소각 및 파기 확인
- 연구개발 비밀관리기록부의 기록유지 및 확인
- 비상시 연구개발 비밀문서의 안전기출 및 파기

실행지침

- 연구개발 비밀의 누설, 도난, 분실 및 손상 방지를 위한 조치
- 기타 연구보안과 관련된 사항 처리



[연구보안 조직도]

1.4 보안관리규정 교육 및 홍보

해당과제	
모든과제	보안과제
○	

이행대상		
연구기관	연구책임자	참여연구원
◎		

1.4.1 보안 교육

연구개발 정보의 유출 기법은 나날이 발전하고 있으며 이와 더불어 핵심기술이 외부에 유출되는 연구보안 사고도 매년 증가하고 있는 추세이다. 이처럼 연구보안 사고가 줄어들지 않는 가장 주된 이유는 임직원들이 연구보안에 대한 의식이 부족하여 연구보안관리 규정을 제대로 숙지하지 않기 때문이다. 따라서 연구보안 사고를 미연에 방지하거나 연구보안 사고가 발생한 경우 경제적 피해를 최소화하기 위해서는 전 직원을 대상으로 연구보안관리 교육을 정기적 또는 수시로 실시하여 임직원들이 규정을 제대로 숙지하고 실천할 수 있도록 하여야 한다.

내용

- 연구보안관리 교육의 효율성을 극대화하기 위해서는 정해진 시점에 전 직원을 대상으로 동시에 교육을 실시하여야 한다. 따라서 매년 연구보안관리 교육 시행 계획과 연구보안 교육 내용을 구체적으로 수립하여 이행하여야 한다.
- 또한, 연구보안과 관련된 전문적인 내용을 교육하고자 하는 경우에는 외부 전문가나 전문기관에 의뢰하여 교육을 실시하는 것도 좋은 방법이라고 할 수 있다.
- 연구보안관리 규정은 제정된 후에도 연구보안 환경이 변하거나 연구보안 사고 원인분석 결과에 따른 개선책을 반영하기 위하여 수시로 개정된다. 이러한 경우에도 빠른 시간 내에 연구보안 교육을 실시하여 전 직원이 개정된 규정을 숙지하고 업무에 적용할 수 있도록 조치해야 한다.
- 연구기관의 교육 시행 환경과 상황에 따라 연구보안 책임자는 집합교육 또는 온라인 교육, 유인물 배포 등 적절한 교육 방법을 선택하여 시행할 수 있다.

내용

교육 방법	장점	단점
집합교육	·학습자의 성실성과 참여도 관리가 용이 ·교습자와 학습자간 상호작용 가능 ·온라인교육 대비 시스템 구축을 위한 초기 비용 불필요 ·체험적 요소가 중요한 학습과정에는 적절	·교육 시간, 공간, 이동에 따른 제약사항 발생 ·교육장소, 교육 부대비용 증가 ·일회성 교육으로 학습 효과 저조
온라인교육	·교육 시간과 공간 제약 없이 교육 대상자들이 편리한 방식으로 교육 수강 ·자료 공유가 쉽고 최신 정보 제공 ·학습자의 심리적 부담 최소화 ·지속적인 반복학습이 가능하여 학습효과 증대	·학습자의 성실성과 참여도 관리의 어려움 ·교습자와 교육 대상자간 상호작용 부족 ·시스템 구축에 따른 과다한 초기비용 발생 ·교재개발, 시스템 운영 등 지속적인 투자 필요 ·체험적 요소가 중요한 학습과정에는 부적절
유인물 배포	·교육 시간, 장소, 이동에 따른 제약 없이 교육 가능 ·교육 비용이 가장 저렴 ·수시 반복 학습 가능 ·학습자의 심리적 부담 최소화	·학습자의 성실성과 참여도 관리의 어려움으로 학습효과가 가장 저조 ·교습자와 교육 대상자간 상호작용 부족 ·체험적 요소가 중요한 학습과정에는 부적절

[보안교육 유형]

- 연구보안 교육의 질적 향상을 도모하기 위하여 교육이 완료된 후에는 참석자 대상으로 설문조사를 실시하여 미비한 점은 개선책을 마련하여 교육계획 수립 시 반영해야 한다.

실행지침

1. 연구보안관리 교육 계획 수립

- 연구보안관리자는 연구기관의 환경과 상황을 고려하여 연구보안관리 교육 시기와 실시 횟수, 교육 내용 및 교육 방법 등에 관한 사항 등을 포함하여 연구보안교육 계획을 매년 초에 수립하여야 한다.
- 연구보안관리 교육 시행 계획(안)은 연구보안심의회의 의결을 거쳐 연구기관의 장에게 보고하여 최종 승인을 받아야 한다.

실행지침

2. 연구보안관리 교육 실시 횟수

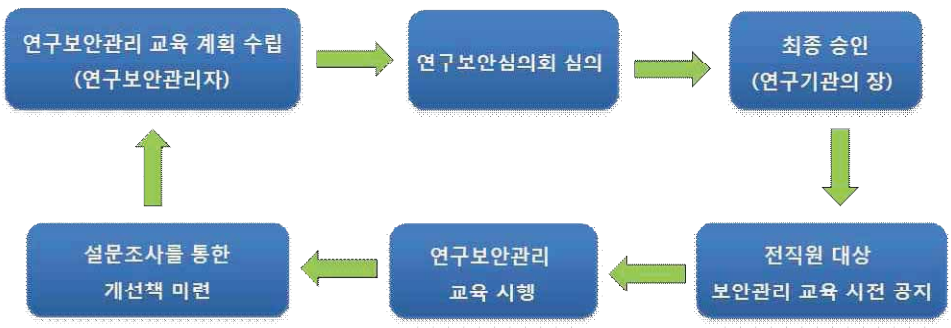
- (정기 교육)연구보안관리 교육은 시행 계획에서 정한 바에 따라 매년 정해진 시점에 정기교육을 실시하되, 최소한 매년 1회 이상 시행하여야 한다.
- (수시 교육)신입 및 경력 직원이 입사한 경우 또는 연구보안관리 규정이 개정된 경우와 연구보안 사고가 발생한 경우를 포함하여 연구기관의 장 또는 연구보안관리자가 연구보안관리 교육이 필요하다고 인정한 경우에는 해당자들 대상으로 수시로 교육을 실시하여야 한다.

3. 연구보안관리 교육 시행 방법

- 연구보안관리 교육을 실시하는 방법은 집합교육, 온라인교육, 유인물 배포 등 교육 시기와 연구기관의 교육 여건에 따라 연구보안관리자가 효율적인 보안교육 방법을 선택하여 실시하여야 한다.
- 연구보안관리 교육을 실시하기 전에 전 직원을 대상으로 교육 실시 관련 내용을 사전에 공지해야 한다.

4. 연구보안관리 교육 사후관리

- 연구보안관리 교육은 모든 임직원이 참석하는 것을 원칙으로 하여야 한다.
- 부득이한 사유로 교육에 참석하지 못한 임직원은 차후에 별도 교육을 실시하거나 유인물 배포, 전자메일로 유인물 발송 등 교육내용을 숙지할 수 있도록 조치해야 한다.
- 교육대상자들로부터 설문조사를 실시한 후 미비한 사항에 대한 개선책을 마련하여 다음 교육계획 수립 시 반영해야 한다.



[연구보안교육 실시 체계도]

1.4 보안관리규정 교육 및 홍보

해당과제	
모든과제	보안과제
○	

이행대상		
연구기관	연구책임자	참여연구원
◎		

1.4.2 홍보

연구자들이 연구보안관리 규정 및 지침 등과 같은 연구보안 관련 내용을 언제든지 학습하여 실생활에 바로 적용할 수 있도록 적극적인 홍보 활동을 강화해야 한다. 연구보안 사고는 앞서 언급한 바와 같이 연구보안관리 규정을 제대로 숙지하지 못한 상태에서 무의식적으로 실수 또는 과실에 의해 발생하는 경우도 많다. 이에, 연구원들이 연구보안에 대해 지속적으로 경각심을 유지하고 연구보안 관련 사항들을 수시로 학습할 수 있도록 홍보 계획 및 방법을 구체적으로 마련하여 시행하여야 한다.

내용

- 연구보안관리와 관련된 내용을 널리 홍보할 수 있는 방법으로는 장소와 시간에 구애받지 않고 학습이 가능한 동영상을 활용한 홍보와 온라인을 활용한 홍보, 모바일을 활용한 홍보가 있으며 매뉴얼 또는 책자를 통해 학습이 가능한 간행물을 활용한 홍보 등이 있다.
- 교육 홍보의 주요 점검사항으로 먼저 홍보 주체 및 대상을 선정해야 되는데 누가 홍보를 주도하고 홍보 대상은 누구인지를 파악해야 한다. 그리고 홍보하고자 하는 내용의 핵심 메시지는 무엇인지 파악해야 하며 어떤 방식으로 홍보할 건지에 대한 홍보매체(동영상, 온라인, 모발일, 간행물 등)를 정해야 된다. 이와 더불어, 홍보는 언제 시작할 건지와 얼마동안 진행할 건지에 대한 홍보시점과 기간을 정해야 되며 이에 따른 홍보비용이 얼마나 소요되는지 사전에 파악해야 한다. 또한, 홍보에 대한 효과를 측정하기 위한 방안도 마련하여 그 결과를 토대로 향후 홍보계획 수립 시 반영해야 한다.
- 홍보의 효율성을 극대화하기 위해서는 수요자 맞춤형 테마 위주로 일관된 메시지를 전달하고 전문용어를 순화하여 이해하기 쉽고 실천 가능한 내용으로 제작하고 배포하여야 한다.

내용

· 연구보안관리 교육과 관련된 주요 홍보 테마에 대한 예시는 다음과 같다.

- 연구보안 관련 규정 및 지침
- 연구보안 사고 최근 동향
- 연구보안 사고 발생 시 대처 방법
- 연구보안 사고 예방법
- 연구보안 사고 사례 및 대처 방안
- 연구보안 생활 수칙 등

실행지침

1. 홍보 계획 수립

· 매년 홍보해야 되는 테마들을 선정하여 홍보 방법과 기간, 소요 예산 등을 사전에 수립하여야 한다.

· 홍보 효과를 측정하는 방안을 마련하고 이에 대한 대응 전략을 수립하여야 한다.

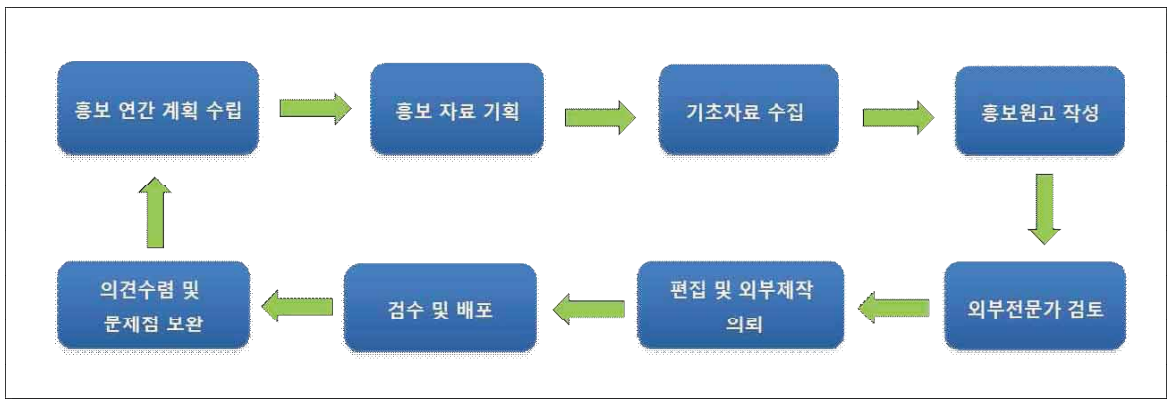
· 연구보안 홍보 시행 계획(안)은 연구보안심의회의 의결을 거쳐 연구기관의 장에게 보고하여 최종 승인을 받아야 한다.

2. 홍보 시행 방법

· 홍보 효과를 극대화하기 위하여 홍보 매체의 특성을 상호 보완적으로 적절히 활용하여 시행하여야 한다.

3. 홍보 사후 관리

· 대상자들로부터 의견 수렴을 실시한 후 미비한 사항에 대한 개선책을 마련하여 다음 홍보 계획 수립 시 반영해야 한다.



[홍보물 발간 업무 흐름도]

1.5 보안우수자 및 위반자에 대한 조치

해당과제	
모든과제	보안과제
○	

이행대상		
연구기관	연구책임자	참여연구원
◎		

1.5.1 보안우수자

연구보안 사고를 예방하기 위해서는 정기적인 보안교육도 중요하지만 임직원들이 이러한 교육내용을 몸소 실천하는 것이 더 중요하다. 따라서 정기 또는 불시 보안점검을 실시하여 연구원들의 사기진작 및 공로를 치하하기 위하여 연구보안 우수자들에게 포상을 실시하여야 한다. 이를 통해 임직원들의 적극적인 참여를 유도하고 임직원들의 보안 의식을 제고할 수 있다.

내용

- 연구보안 우수자에 대한 객관성과 공정성을 확보하기 위하여 포상 선정 평가기준을 마련하여야 한다. 특히, 재직 중 징계 및 경고 처분을 받은 자 또는 각종 비위, 부조리 등으로 물의를 일으켜 포상대상자로 합당하지 않다고 판단되거나 기타 법규상 결격사유가 있는 자는 제외하여야 한다.
- 포상추천 대상자에 대하여는 반드시 연구보안관리자의 책임 하에 공적조서, 경력 확인 등을 실시하고 결격사유 해당 유무를 철저히 조사하여 포상적격자를 엄선 추천해야 한다.[별첨 1.5.1 참조]
- 포상추천 대상자의 공적사항 기록 시 반드시 추천기준에 의한 구체적이고 세밀한 공적사항을 기록하여 공적 내용을 분명하게 파악할 수 있도록 작성하여야 한다. [별첨 1.5.1 참조]
- 연구보안 우수자는 중복포상을 방지하기 위하여 포상추천 대상자에서 일정기간 배제하여야 한다.
- 연구보안 우수자를 선정하기 위한 공식적인 절차를 수립하고 그에 합당한 포상금 및 인사 상 가점을 부여하는 규정 및 지침을 마련하여 시행하여야 한다.

실행지침

1. 연구보안 우수자 선정 및 포상 기준 마련

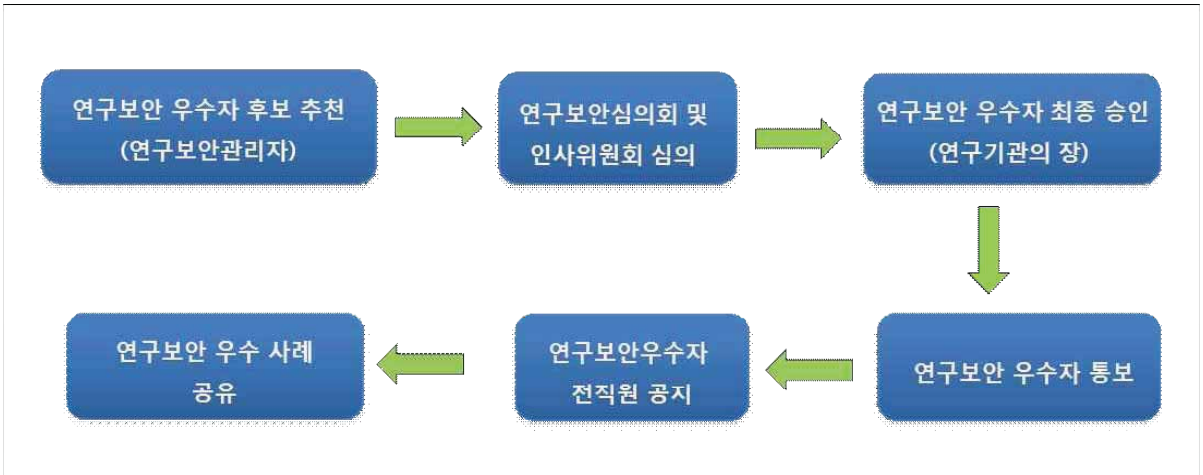
- 자체 규정에 연구보안 우수자 선정 및 포상 기준을 수립해야 한다.
- 선정 기준은 상위기관 연구보안감사, 국가정보원 연구보안평가, 자체적으로 실시한 정기 또는 불시 연구보안관리 점검을 통하여 연구보안 이행 성적이 우수한 임직원을 선정해야 한다.
- 연구보안 우수자에 대한 인사고과, 승진, 포상, 교육훈련 등 모든 임직원이 관심을 가질 수 있는 파격적인 포상 기준을 마련해야 한다.

2. 연구보안 우수자 선정 절차 수립

- 연구보안 우수자는 자체 연구보안심의회 또는 인사위원회 등의 심의를 거쳐 선정하여야 한다.
- 연구보안관리자는 심의에서 최종 확정된 보안우수자 후보를 연구기관의 장에게 보고하여 최종 승인을 받아야 한다.

3. 연구보안 우수 사례 확산

- 연구보안 우수자는 내부 게시판을 통하여 전 직원들에게 공지하고 우수 사례를 임직원들이 공유할 수 있도록 게시판 또는 유인물을 제작·배포하여 보안의식 수준을 제고하여야 한다.



[연구보안 우수자 선정 절차]

1.5 보안우수자 및 위반자에 대한 조치

해당과제	
모든과제	보안과제
○	

이행대상		
연구기관	연구책임자	참여연구원
◎		

1.5.2 보안위반자

연구보안관리 규정을 위반하여 중요한 연구 정보 및 성과물이 무단으로 외부에 유출되는 보안사고를 일으킨 위반자는 그에 상응하는 처벌을 받아야 한다. 이를 통해 연구보안 사고의 재발을 방지하거나 최소화할 수 있을 뿐 만 아니라 임직원들에게 연구보안 사고에 대한 경각심을 불러일으키는 효과를 기대할 수 있다.

내용

- 비밀을 필요로 하는 중요한 연구 산출물 및 성과물을 무단으로 외부에 유출하는 동기로 개인의 영리 목적이 68%로 전체 중에서 가장 많은 영역을 차지하고 있으며 그 다음으로 금전 유혹이 15%를 차지하고 있다. 나머지 동기는 인사 불만이 7%, 처우 불만은 6%, 기타 3%, 비리 1%를 나타내고 있다.
- 기술 유출 유형으로는 무단보관이 47%로 가장 많은 부분을 차지하고 있으며 내부 공모에 의한 유출이 26%를 차지하고 있다. 또한, 직원 매수에 의한 유출은 20%를 차지하고 공동연구, 위장합작, 기타가 8%를 차지하고 있다.
- 연구보안 사고는 위에서 언급한 바와 같이 어떠한 동기에 의하여 사전 계획을 통해 의도적으로 중요한 연구 정보 및 성과물을 외부로 유출하는 경우도 있지만 본인의 부주의 및 과실로 인하여 본인 의사와 상관없이 연구보안 사고가 발생하는 경우도 있다.
- 따라서 처벌의 공정성과 중립성을 유지하기 위하여 연구보안 사고를 철저하게 조사하여 그 결과에 따라 자체 규정을 근거로 위반자를 처벌하는 절차를 수립하고 시행하여야 한다.

※ 보안위반자 기준

① 연구정보 및 비밀정보 유출

1. 연구정보 누설
   - 개인의 목적(영리·비영리)을 위하여 고의로 핵심 연구 산출물 및 성과물 등을 외부로 유출한 경우
   - 핵심 연구 산출물 및 성과물 등을 외부로 유출하는데 가담한 경우
2. 연구정보 분실
   - 보안과제 또는 대외비에 해당하는 연구 산출물 및 성과물을 분실한 경우
   - 분실 신고 등을 제대로 이행하지 않는 등 적절한 조치를 취하지 않은 경우
3. 연구보안사고 발생 사실 노출
   - 연구보안사고에 대한 조사가 완료되기 전에 관련 정보를 외부로 유출한 경우

② 연구개발정보 관리 위반

1. 연구개발정보 보안등급 관리 위반
   - 연구 산출물 및 성과물에 대한 보안등급을 부여하지 않은 경우
   - 연구 산출물 및 성과물의 보안등급을 과소 또는 과대 분류한 경우
2. 연구 산출물 관리 위반
   - 연구 산출물 및 성과물을 방치하거나 비밀보관함에 보관하지 않은 경우
   - 연구 산출물 및 저장매체를 복구할 수 없도록 완전하게 폐기하지 않은 경우
   - 보안과제 및 대외비의 연구 결과물(보고서 등)을 제한 없이 외부로 배포한 경우
   - 승인받지 않은 비밀자료 및 대외비 문서를 열람하거나 복사하는 경우
3. 연구개발 성과물권리 확보 소홀
   - 보안과제 및 핵심기술에 대한 성과물의 영업비밀 또는 특허권, 지식재산권 확보를 등한시하여 기술적·경제적 손실이 발생한 경우

③ 출입통제 위반

1. 인가되지 않은 제한구역 또는 통제구역을 출입한 경우
2. 노트북, 외장형 디스크, USB 등 저장매체를 사전 허가 없이 반·출입한 경우
3. 촬영제한구역에서 사전 허가 없이 사진을 찍거나 동영상을 촬영한 경우
4. 정기적 출입자로부터 보안서약서를 받지 않은 경우
5. 보안과제와 관련하여 외부방문자 출입 시 직원이 방문자와 함께 동행하지 않은 경우

④ 사전 승인절차 위반

1. 연구 성과 대외공개 사전검토 미 이행
   - 보안과제 및 대외비에 해당하는 연구 성과를 대외로 발표하는 경우 사전 보안성 검토를 이행하지 않은 경우
   - 보안과제 및 대외비 자료를 대외로 공개하는 경우 사전에 보안성 검토를 이행하지 않은 경우
2. 보안과제와 관련하여 외부방문자 출입 시 연구보안관리 책임자의 사전 허가를 받지 않은 경우
3. 보안과제 연구책임자가 해외기업 또는 연구기관과 공동연구(위탁연구 포함)를 수행하기 전에 사전 승인절차를 이행하지 않은 경우
4. 보안과제를 수행하고 있는 연구책임자 또는 참여연구원이 외국 정부나 기관 방문 시 중앙행정기관의 장 또는 국정원장에게 통보하지 않은 경우
5. 보안과제 참여연구원이 외국인과 접촉 시 연구책임자의 사전 승인절차를 이행하지 않은 경우
6. 보안과제에 외국인이 참여하는 경우 연구기관의 장으로부터 사전 승인을 받지 않은 경우
7. 보안과제와 관련하여 외국 정부·기관 또는 단체가 방문하는 경우 사전에 소관 중앙행정기관의 장 또는 국가정보원장에게 보고하지 않은 경우(단, 긴급한 사유로 인해 사후보고가 타당하다고 인정되는 경우에는 제외)

⑤ 사후조치 위반

1. 연구보안사고 발생 시 사고발생 사실을 즉시 상위 부서장 또는 보안관리담당부서에 보고하지 않은 경우
2. 보안과제 또는 대외비에 해당하는 연구 산출물 및 성과물을 분실한 경우 상위부서장 또는 보안관리담당부서에 분실 신고 등 적절한 조치를 이행하지 않은 경우
3. 보안과제 참여연구원이 외국인과 접촉한 후 2일 이내에 그 결과를 상위 부서장에게 보고하지 않은 경우

실행지침

1. 연구보안관리 위반자 처벌 규정 마련

- 연구보안 사고의 고의성 여부, 규정위반 사항, 연구기관의 피해 규모 등을 감안하여 위반자를 처벌할 수 있도록 처벌 절차 및 수위를 결정할 수 있는 규정을 마련하여야 한다.[별첨 제1.5.2호]
- 연구보안 규정 및 지침을 준수하지 않거나 본인의 부주의 및 과실로 인하여 보안사고가 발생한 경우 연구기관의 장은 그 귀책사유를 감안하여 위반자에게 연구개발사업의 참여를 제한하여야 한다.
- 위반자 처벌규정은 연구보안심의회 또는 인사위원회(또는 징계위원회) 등 관련 위원회의 심의를 거친 후 연구기관 장의 최종 승인을 받는 적법한 절차를 거쳐야 한다.
- 확정된 처벌규정은 모든 임직원이 숙지할 수 있도록 게시판 또는 다른 매체를 통해 공지하여야 한다.

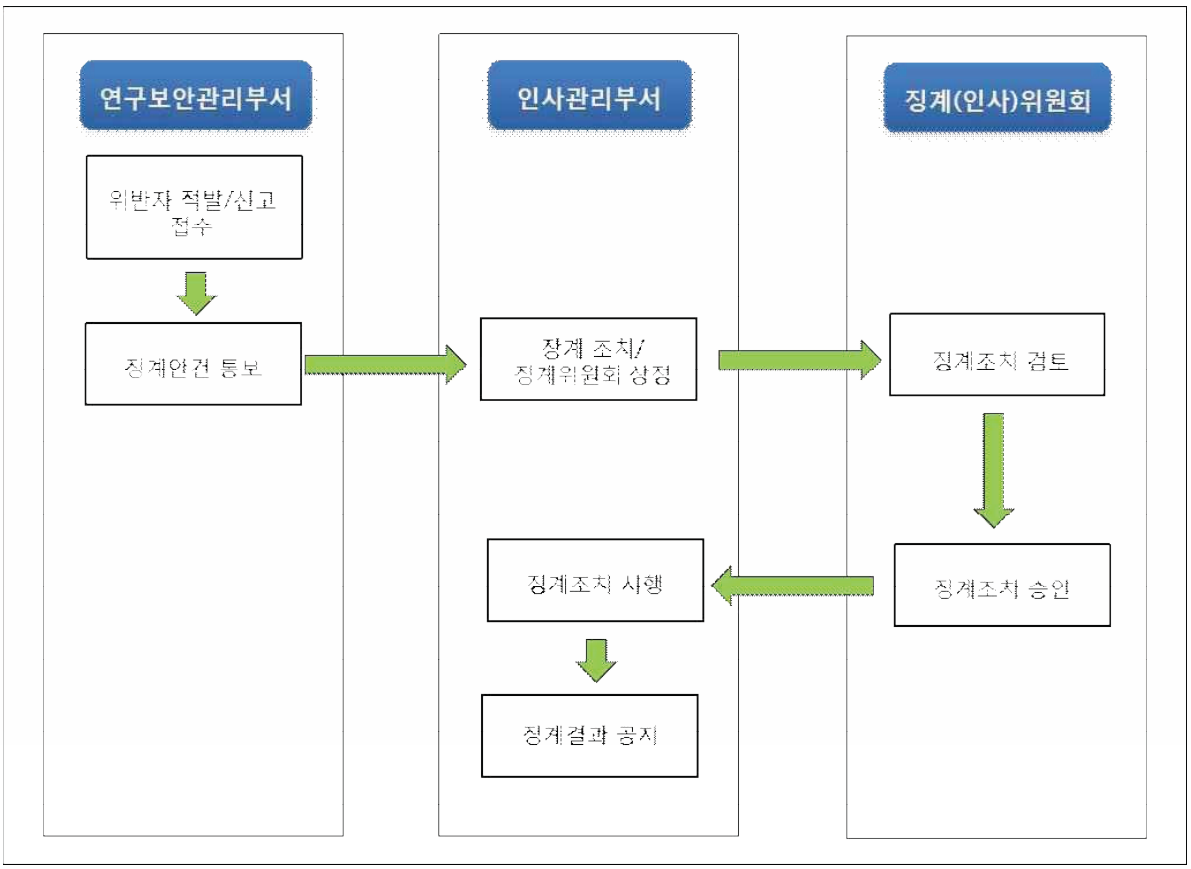
2. 연구보안관리 위반자 징계 절차 이행

- 연구보안관리 부서에서 보안 위반자를 적발하거나 신고가 접수된 경우 자체 조사를 통하여 징계 안건을 인사관리 부서에 통보하여야 한다.
- 인사관리 부서는 징계 안건을 토대로 그에 합당한 징계 조치를 부여하고 인사(징계) 위원회에 안건을 상정하여야 한다.
- 인사(징계)위원회는 보안 위반자에 대한 징계 조치를 검토한 후 징계 조치 결과를 인사관리 부서에 통보하여야 한다.
- 인사관리 부서는 징계 조치 결과를 위반자에게 통보하여 시행하고 전 직원들에게 이러한 사실을 공지하여야 한다.
- 국가연구개발사업의 보안사고 또는 연구보안사고의 심각성으로 인하여 외부 기관으로부터 처벌을 받은 자는 징계 시 그 결과를 반영하여야 한다.

3. 연구보안관리 위반자 사후 관리

- 연구기관의 장은 위반자가 보안을 필요로 하는 자체 연구개발과제 또는 국가연구개발사업에 참여하는 것을 제한하여야 한다.
- 연구보안관리자는 연구보안관리 위반자에 대한 현황을 지속적으로 관리하고 유지해야 한다.

실행지침



[연구보안 위반자 징계 절차 예시]

1.6 보안사고 관리

해당과제	
모든과제	보안과제
○	

이행대상		
연구기관	연구책임자	참여연구원
◎		

1.6.1 사전 조치

연구보안 사고는 사전에 예방하는 것이 경제적으로나 시간적으로 피해를 줄일 수 있는 가장 좋은 보안대책이다. 따라서 연구보안 사고를 예방하고 대응하기 위한 일련의 조치사항들을 사전에 수립하는 것은 아주 중요하며 반드시 이행하여야 한다.

내용

연구보안 사고의 사전 예방 조치로는 연구보안 사고 예방 및 대응 방법 등을 명시한 규정을 자체적으로 마련하여 임직원을 대상으로 보안교육을 정기적 또는 수시로 실시하여 임직원의 보안의식 수준을 제고해야 한다. 그리고 임직원이 연구보안 규정 및 수칙들을 제대로 업무에 적용하고 있는지 정기적으로 연구보안실태 점검을 실시하고 그 과정에서 취약점이 발견되면 수정·보완해나가는 절차를 지속적으로 이행하여야 한다.

실행지침

1. 연구보안사고 예방 및 대응 수칙 수립

- 연구보안 사고를 예방하고 신속하게 대응하기 위하여 연구보안사고 예방 및 대응 절차와 방법 등을 명시한 규정 또는 지침을 사전에 수립하여야 한다.
- 연구보안사고를 예방하기 위한 조치사항과 더불어 보안사고 발생 시 단계별 대응방법과 상황 보고체계, 비상연락 체계 등을 구체적으로 명시하여야 한다.

실행지침

2. 연구보안 조직 및 시설보안, 정보보안 조직과의 협업체계 구축

- 연구보안 사고는 불시에 발생하는 경향을 지니고 있으므로 연구기관의 장은 연구보안 관리자를 임명하여 지속적으로 연구보안관리 업무를 전담할 수 있도록 배치하여야 한다.
- 또한, 연구보안 사고는 다양한 유출 경로와 기법을 통해 발생하는 특성을 지니고 있기 때문에 연구보안관리 부서는 시설보안 및 정보보안 부서와 협업할 수 있는 체계를 마련하여 보안사고 발생 시 신속하게 조치하고 대응할 수 있는 공동 대응기반을 마련하여야 한다.

3. 연구보안 사고 예방 및 대응 요령에 관한 교육 실시

- 임직원 대상으로 연구보안 사고 예방 및 사고 발생 시 신속한 보고 체계와 행동 요령 등을 숙지할 수 있도록 정기적인 교육을 실시하여야 한다. 이를 통해 임직원들이 연구보안 사고를 사전에 예방하거나 보안사고 발생 시 신속하게 대응할 수 있어야 한다.

4. 연구보안 사고 대응 모의 훈련 실시

- 연구보안 사고 발생 시 신속하고 정확하게 대응하는 역량을 강화하기 위하여 모의 훈련 시나리오를 만들어 정기적으로 연구보안 사고 대응 훈련을 실시해야 한다.
- 모의훈련 결과를 평가하고 분석하여 발견된 취약점에 대한 보완책은 반드시 관련 규정과 연구보안 교육에 반영하여 차후에 적절하게 대응할 수 있도록 전 직원을 대상으로 교육을 실시하여야 한다.

5. 연구보안 실태 점검 실시

- 연구보안관리 실태 점검 및 조사계획에 따라 매년 임직원들의 연구보안관리 준수 여부를 점검하여야 한다.
- 연구보안관리 실태 점검에서 발견된 취약점에 대한 보완책은 반드시 관련 규정과 연구보안 교육에 반영하여 차후에 적절하게 대응할 수 있도록 전 직원을 대상으로 교육을 실시하여야 한다.

1.6 보안사고 관리

해당과제	
모든과제	보안과제
○	

이행대상		
연구기관	연구책임자	참여연구원
◎		

1.6.2 대응 조치

국가연구개발사업과 관련된 중요한 정보나 자료가 외부로 유출되거나 누설 또는 분실 등 연구보안 사고가 발생한 경우 피해를 최소화하고 빠른 복구 통해 업무의 연속성을 보장하기 위하여 연구보안 사고 발생 시 신속하고 체계적으로 대응할 수 있는 방안을 마련하여 보안사고 발생 초기에 적절하게 대응하는 것이 아주 중요하다.

내용

- 연구보안 사고는 연구개발사업과 관련된 정보 및 성과물이 외부로 유출되거나 누설, 분실 또는 도난을 당하거나 연구개발사업과 관련된 정보를 유통하고 관리, 보존하는 시스템이 외부로 유출, 손괴 또는 파괴된 경우를 말하며 그 밖에 중앙행정기관의 장이 정하는 보안 관련 사고를 의미한다.
- 연구보안 사고 단계별 대응 절차는 다음과 같이 6단계로 구분된다.

① 사고 탐지

연구보안관리자가 직접 연구보안 사고 발생 사실을 감지하거나 내부 직원 또는 외부인에 의한 신고 접수로 사고발생을 탐지할 수 있다.

② 초기 대응

연구보안관리자는 초기에 대응할 수 있는 조치사항을 수행하고 침해 사고 관련부서에 통지한다. 그리고 연구보안사고 대응팀이 구성되면 초기 조치 사항들을 인계하고 이후의 조치는 연구보안사고 대응팀과 함께 공조한다. 원활한 인수인계 및 조치사항들을 검토하기 위해 각 단계에서 수행되는 모든 세부사항들은 문서화를 통해 그 기록을 유지하고 관리하여야 한다.

내용

③ 대응전략 체계화

초기 대응체계가 마무리되면 실제로 사고가 발생했는지, 보안사고의 유형은 무엇인지 그리고 보안사고로 인한 잠재적인 업무 영향은 어떤지 등을 알 수가 있다. 이렇게 적절한 정보가 준비되면 이를 판단근거로 하여 현재 사고를 어떻게 처리할 것인지를 결정할 수가 있다. 보안사고의 유형에 따라 가장 적절한 대응전략을 수립하기 위해서는 정책, 기술, 법, 업무 등 사고와 관련된 요인들을 전체적으로 고려해야 한다. 즉, 외부에 유출된 정보 또는 성과물이 얼마나 중요하고 민감한지와 사건이 외부에 알려졌는지, 유출자는 누구인지, 경제적 피해 규모는 얼마인지, 외부기관에 협조를 요청해야 되는지 등을 고려하여 최적의 대응전략을 결정한 후 의사결정자의 최종 승인을 받고 최대한 빠른 시간 내에 대응 조치를 수행하여야 한다. 또한, 사고 대응과정에서 수사기관에 신고하여 법적인 대응을 할 것인지 아닌지를 결정하여야 하며 사고의 내용이 법적인 제제가 필요한 사항이 아니라 내부에서 처리해야 할 사항이라면 보안사고 대응조치가 마무리된 이후에 처리한다.

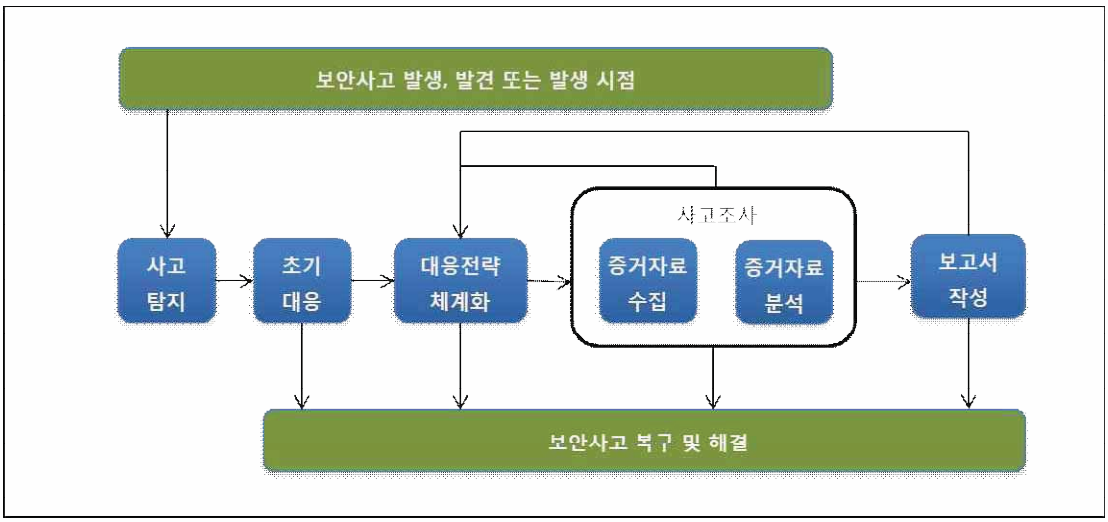
④ 사고 조사

조사의 핵심은 보안 사고를 유발한 행위자와 보안사고의 대상이 무엇인지 알아내는 것이 중요하다. 이를 확인하기 위해 사고 조사과정은 증거자료 수집과 분석단계로 나눌 수 있다. 증거자료 수집은 보안사고 분석을 위해 살펴보아야 할 범행들과 단서들을 수집하는 과정이다. 특히, 법적 소송을 염두에 두고 있다면 수집하는 증거자료는 무결성과 적법성을 유지하여야 한다. 그 다음으로 사고와 관련하여 누가, 무엇을, 언제, 어디서, 어떻게 그리고 왜와 같은 정보들을 알아내기 위하여 수집된 증거자료를 분석하여야 한다.

⑤ 보고서작성

보고서는 보안 사고를 분석한 내용을 육하원칙에 의거하여 작성하고 원인분석에 따른 대응 방안도 작성하여야 한다. 보고서를 접하게 되는 상급자 또는 의사결정권자는 연구보안에 대한 기본지식이 부족한 경우가 많기 때문에 누구나 알기 쉬운 형태로 작성하여야 한다.

내용

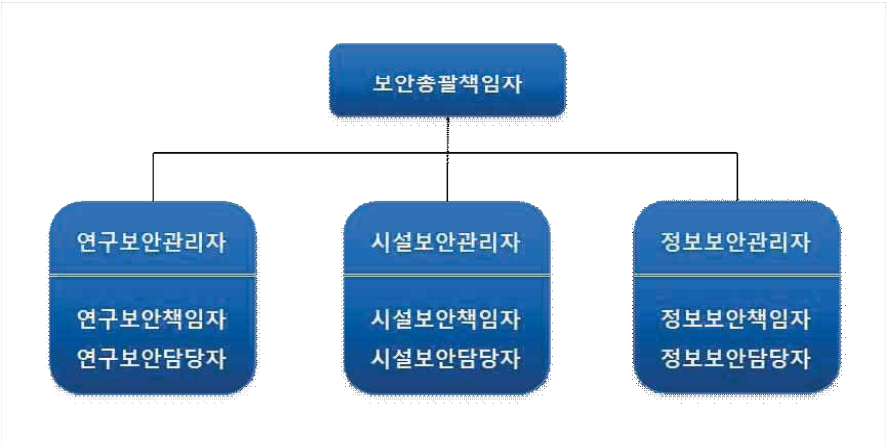


[보안사고 대응 절차]

실행지침

1. 보안사고 대응 절차 수립

- 연구보안 사고가 발생한 사실을 최초로 인지한 임직원은 상급자 또는 연구보안관리자에게 최대한 빠른 시간 내에 이 사실을 알려야 한다.
- 연구보안관리자는 이 사실을 보안총괄책임자에게 즉시 구두로 통보한 후 피해가 더 이상 확산되지 않도록 초기 대응 조치를 수행하여야 한다.
- 사고 발생을 보고받은 보안총괄책임자는 연구기관의 장에게 즉시 보고하고 연구기관의 장은 중앙행정기관의 장에게 즉시 보고하여야 한다.



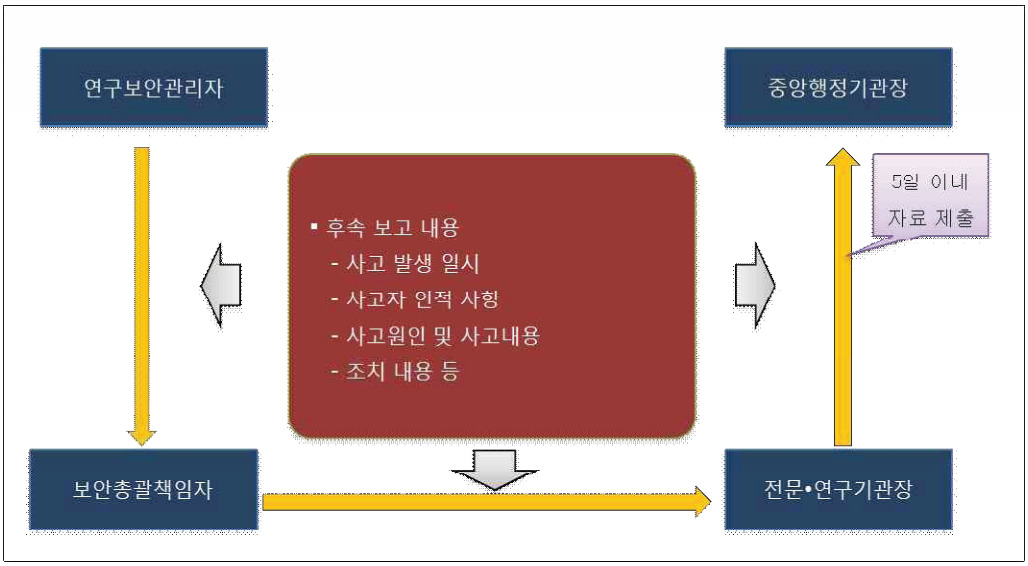
[보안조직 구성도(예시)]

실행지침

- 보안총괄책임자는 연구보안사고 대응팀을 즉시 소집하여야 하며 대응전략을 수립하여 신속하게 대응 조치하여야 한다.
- 연구보안 사고는 조사가 완료될 때까지 연구기관의 장, 중앙행정기관의 장은 관련 내용을 비공개로 진행하여야 한다.

2. 후속 대응절차 마련

- 연구보안관리자 및 보안총괄책임자는 연구보안 사고에 대한 세부 내용을 조속히 파악하여 연구기관의 장에게 보고하고 연구기관의 장은 연구보안 사고 발생일로부터 5일 이내에 세부 내용을 중앙행정기관의 장에게 추가로 제출해야 한다. 세부 내용은 다음과 같다.
  - 연구보안사고 발생 일시와 발생 장소
  - 사고자의 인적사항과 사고 발생원인 및 내용
  - 사고 발생 시 조치 사항 등



[보안사고 보고 절차]

3. 연구보안 사고 조사 및 보고서 작성

- 연구보안 사고를 보고받은 중앙행정기관의 장은 필요에 따라 국가정보원 등 관계기관의 장과 협의하여 필요하다고 판단되면 합동으로 경위를 조사할 수 있다.
- 중앙행정기관과 국가정보원, 관계기관은 합동조사반을 구성하여 데이터를 수집·분석하여 연구보안 사고원인 및 피해규모, 보안사고 대책 등을 조사한다.
- 조사가 완료되면 합동조사반은 사고발생 원인, 피해 규모, 보안 조치사항 등의 완료 보고서를 작성한다.

1.6 보안사고 관리

해당과제	
모든과제	보안과제
○	

이행대상		
연구기관	연구책임자	참여연구원
◎		

1.6.3 사후 조치

향후 동일한 연구보안 사고가 발생하지 않도록 조치를 취하는 사후 조치는 아주 중요한 업무에 해당된다. 따라서 연구보안 사고에 대한 수습이 마무리되면 사고 원인 분석에 의한 보안대책을 근거로 반드시 관련 규정이나 지침, 보안교육 자료, 연구보안 실태점검 계획, 모의훈련 시행 계획 등에 반영하여야 한다.

내용

연구보안 사고가 마무리되면 이에 대한 사후 조치로 사고 원인에 따른 재발방지책을 마련하여 관련 규정 및 지침이나 보안교육 자료, 모의훈련계획, 연구보안점검 실태 계획 등에 반영하여야 한다. 또한, 필요시 외부 전문기관에 보안교육 등 관련 대책을 지원 요청하여 임직원들의 보안의식 수준을 강화해야 하며 보안위반자는 자체 규정에 따라 처벌하여 다른 임직원들에게 연구보안의 중요성과 경각심을 일깨워 주는 계기를 마련해야 한다.

실행지침

1. 연구보안사고 재발방지 대책 수립

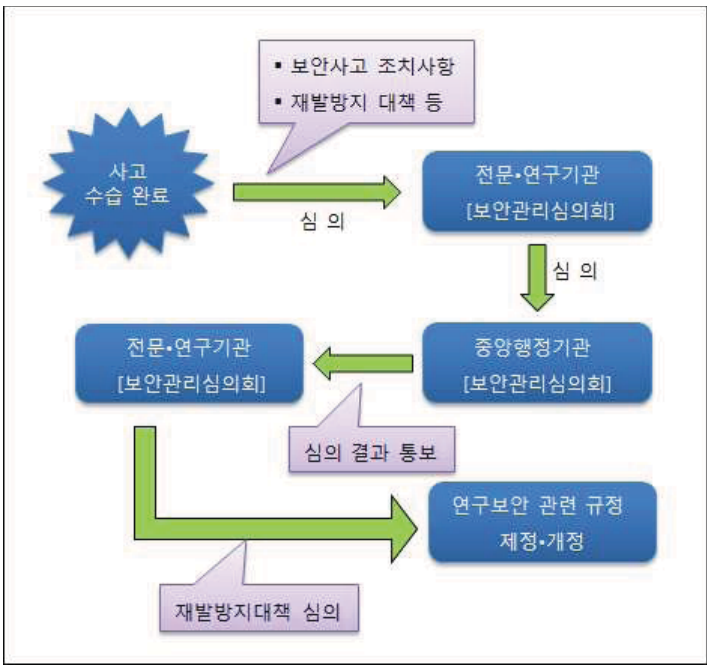
- 연구보안관리자는 연구보안사고 보고서를 근거로 향후 보안사고 재발방지 대책을 수립하여야 한다.
- 자체 연구보안심의회를 개최하여 연구보안 사고조치 사항 및 재발방지 대책과 관련된 전반적인 사항을 심의하여 그 결과를 연구기관의 장에게 보고한다.

실행지침

- 연구기관의 장은 조치결과 및 향후 재발방지 대책 등을 소관 중앙행정기관의 장에게 보고하여 심의 결과를 통보받는다.
- 연구기관의 장은 연구보안 사고 예방을 위한 대책을 마련하기 위하여 외부 전문기관 또는 전문가의 도움이 필요하다고 판단되면 협조를 요청할 수도 있다.

2. 보안사고 원인 분석에 의한 규정 및 지침 개정

- 중앙행정기관의 장으로부터 심의 결과를 통보받은 연구기관의 장은 자체 연구보안심의회 심의를 거쳐 재발방지를 위한 개선책을 연구보안 관련 규정 및 지침, 보안교육 자료 등에 반영해야 한다.



[연구보안사고 사후처리 방법]

3. 연구보안 사고 관련자 처벌

- 연구기관의 장은 연구보안심의회 또는 징계위원회(또는 인사위원회)를 개최하여 내부규정에 따라 그 귀책사유를 감안하여 징계 여부 및 수위를 결정하여 연구보안 사고 관련자들을 처벌하여야 한다.
- 연구기관의 장은 연구보안 위반자들이 보안을 필요로 하는 국가연구개발사업 또는 자체 연구개발사업에 참여하는 것을 제한하여야 한다.

1.7 보안점검 및 보안교육 실시

해당과제	
모든과제	보안과제
○	

이행대상		
연구기관	연구책임자	참여연구원
◎		

1.7.1 보안점검 실시

연구보안 사고를 예방하고 그로 인한 피해를 최소화하기 위하여 임직원들이 연구보안 규정을 제대로 준수하고 있는지 확인하기 위해 보안점검을 정기적으로 실시해야 한다. 또한, 보안점검 과정에서 보안관리의 취약점이 발견되면 개선책을 마련하여 연구보안 관리를 한층 더 강화할 수 있는 계기가 된다.

내용

- 연구보안관리자는 매년 보안점검 계획을 수립하여 최종 결정권자의 승인을 받은 후에 전 직원을 대상으로 보안점검을 시행하여야 한다.
- 출장, 휴가 등으로 연구보안 점검을 받지 못한 임직원은 별도로 재점검 일정을 마련하여 시행하여야 보안점검의 효과를 극대화할 수 있다.
- 연구보안 점검을 시행하기에 앞서 보안점검 항목을 만들어야 한다. 보안 점검의 신뢰성을 확보하기 위하여 점검영역과 점검항목으로 구분하여 세밀한 영역까지 보안점검이 가능하도록 설계하여야 한다. 점검 영역에서 점검해야 할 주요 사항은 보안관리 체계가 제대로 이루어지고 있는지와 참여연구원과 연구개발 내용 및 결과는 잘 관리되고 있는지 점검해야 한다. 또한, 연구시설과 정보통신망 관리도 규정을 잘 준수하고 있는지와 연구개발과제 보안관리 현황도 제대로 관리하고 있는지 점검해야 한다.[별첨 1.1.1의 첨부 2참조]
- 시간이 지남에 따라 연구보안 환경이 변하거나 연구보안 관련 규정 또는 지침이 변경되기 마련이다. 이때, 연구보안 점검영역 및 점검항목도 변경된 연구보안 환경 또는 규정이나 지침 등을 반영하여 수정하거나 보완하여야 한다.
- 연구보안 점검은 연구보안관리 부서와 시설관리 부서, 정보시스템관리 부서와 합동으로 실시하되, 부서 고유기능에 맞게 역할을 분담하여 시행하면 효율적으로 점검할 수도 있다.

실행지침

1. 연구보안 점검 계획 수립

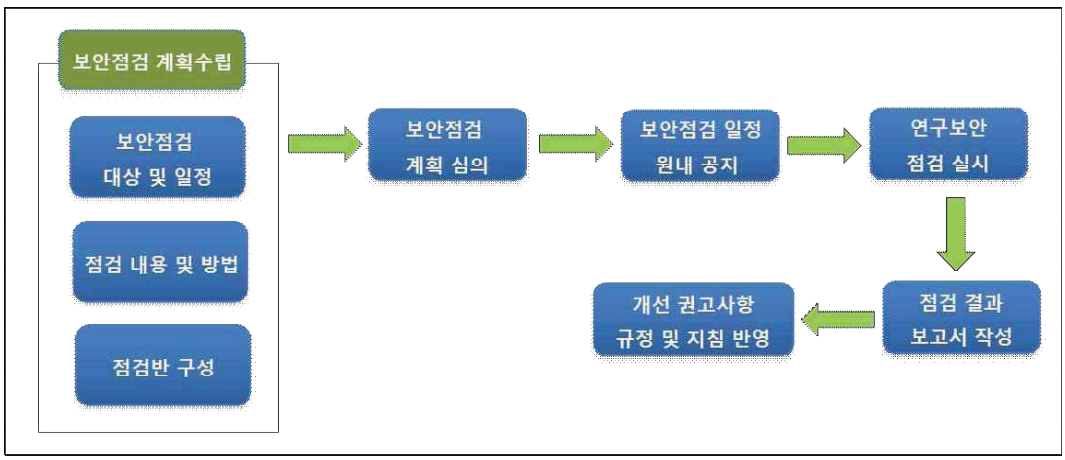
- 연구보안관리자는 매년 초에 연구보안 점검 계획을 수립하여야 하며 계획 수립 단계에서 보안 점검 대상 및 시기, 점검 내용 및 방법을 명시하고 점검반 구성 방법 등을 작성하여야 한다.
- 연구보안 점검 계획은 자체 연구보안심의회의 심의를 거쳐 연구기관의 장으로부터 최종 승인을 받은 후에 시행하여야 한다.

2. 연구보안 점검 실시

- 보안점검 계획에 따라 연구보안 점검을 실시하기 전에 전 직원에게 점검 대상, 점검 내용 및 방법, 점검 일시 등을 사전에 공지해야 한다.
- 연구보안 점검은 사전에 작성된 점검표에 의해 실시하되, 휴가, 출장 등으로 자리를 비운 직원은 향후에라도 보안점검을 실시하거나 그에 준하는 조치를 이행하여야 한다.

3. 점검 결과보고서 작성 및 사후 조치 이행

- 연구보안관리자는 연구보안관리 실태 점검 과정에서 발견된 취약점을 비롯하여 조치사항 및 개선사항들을 포함한 점검결과보고서를 작성해야 한다.
- 점검결과보고서는 연구보안심의회 승인을 거친 후 연구기관의 장에게 보고하여 최종 승인을 받아야 한다.
- 점검 결과 발견된 취약점에 대한 개선 권고 사항들은 반드시 연구보안 규정이나 지침, 보안교육 자료 등에 반영하여야 한다.
- 새로이 개정된 연구보안관리 규정이나 지침은 전 직원이 새로운 보안수칙을 준수할 수 있도록 가급적 빠른 시일 내에 공지해야 한다.



[연구보안관리 점검 절차]

1.7 보안점검 및 보안교육 실시

해당과제	
모든과제	보안과제
○	

이행대상		
연구기관	연구책임자	참여연구원
◎		

1.7.2 보안교육 실시

연구보안관리 교육은 보안 사고를 사전에 예방할 수 있는 최선의 방법이다. 따라서 매년 보안교육 계획을 수립하여 그 계획에 따라 차질 없이 보안교육을 실시하여야 하며 모든 연구자들이 보안교육을 이수할 수 있도록 철저하게 관리하여야 한다.

내용

- 연구보안관리 규정을 통해 연구보안관리 교육과 관련된 정책을 명문화하고 매년 보안관리 교육 계획에 따라 정기적으로 또는 필요에 따라 수시로 시행하여야 한다.
- 보안관리 교육 계획 수립 시 교육 시기 및 교육 내용, 교육 방법 등을 구체적으로 명시하여야 하며 교육 대상별 차별화된 보안교육을 제시하여야 한다.

  - 보안교육 제도의 예

  ① 계층에 따른 분류: 임원, 보직자, 연구원 대상 정기/비정기 교육

  임원의 경우는 외부 초빙강사를 초빙해 간담회 등을 통한 교육을 실시하고 최근 보안 동향 및 이슈사항을 공감하는 형태로 비정기적으로 진행하는 것이 가장 효과적이다. 특히 사고사례를 통해 연구보안이 연구기관에 미치는 영향 등을 교육시키도록 하여야 한다.

  보직자의 경우에는 부서 내 보안관리자의 역할을 교육하고 정기적·비정기적으로 연구원들에게 어떠한 보안교육을 시행해야 하는지를 추가적으로 교육하여야 한다. 일반연구원은 원내 보안준수 사항 및 연구보안 관련 공지사항을 통하여 보안의 중요성에 대해 강조하고 위반 시 본인에게 어떠한 불이익이 따르는지 대한 내용도 명확하게 전달하여야 한다.

내용

② 채용형태에 따른 분류: 경력직원, 신입직원 등 채용 시 이루어지는 보안교육
경력직원의 경우 타 연구기관에서의 경험이 있으므로 원내 보안규정의 특징 및 원내 보안 중요성을 주지시켜 연구기관의 보안정책 이해에 중점을 두어야 한다. 반면에 신입직원의 경우에는 기본적인 보안 마인드 및 원내 보안 중요성 등 보안정책 이해에 중점을 두고 교육을 실시해야 한다.

③ 테마별 대상자에 따른 분류: 보안 위반자, 특별 프로젝트 참여연구원, 업무직군에 따라 이루어지는 비정기적 테마 교육

· 또한, 교육의 성과를 높이기 위하여 교육 이수자로부터 보안교육과 관련된 의견을 수렴하여 개선사항은 차년도 보안관리 교육 계획 수립 시 반영하여야 한다.

실행지침

1. 연구보안관리 교육 정책 명문화

· 연구보안관리 규정 또는 지침에 보안교육과 관련된 정책을 명문화하고 다음 사항을 준수하도록 명시하여야 한다.

① 모든 임직원은 입사 시 연구보안 교육과정을 이수하여야 한다.

② 승격자는 승격교육에 포함된 보안교육과정을 이수하여야 한다.

③ 모든 임직원은 연간 1회 이상 보안교육과정을 이수하여야 한다.

④ 보안전담조직 및 유관조직의 담당자는 정기적으로 연구보안 관련 과정을 이수하도록 해야 한다.

2. 연구보안관리 교육 계획 수립

· 매년 연구보안관리 교육 계획은 구체적으로 수립해야 하며 다음 내용이 명시되어 있어야 한다.

- 교육 시기: 최소한 반기별로 실시하되, 필요에 따라 수시로 교육을 실시할 수도 있다.
- 교육 대상: 일반적인 보안교육은 전 직원 대상으로 실시하고 심화교육은 해당되는 연구원들을 대상으로 실시하여야 한다.

실행지침

- 교육 내용: 연구보안관리 관련 규정 및 지침, 연구보안 사고 예방법, 연구보안 사고 최근 동향, 연구보안 사고 대응 방법, 연구보안관리 생활 수칙 등 연구기관에서 필요로 하는 내용으로 교육을 실시해야 한다.
- 교육 방법: 교육 내용 및 교육 여건에 따라 집합교육 또는 온라인 교육을 실시하여야 한다.
- 교육 강사: 연구보안관리자가 자체적으로 교육을 실시하되, 필요 시 외부 보안전문기관 또는 전문 외부강사에게 교육을 의뢰할 수 있다.

3. 연구보안관리 교육 계획 승인 절차 이행

· 연구보안관리 교육 계획은 연구보안심의회의 승인을 거쳐 연구기관의 장에게 보고한 후 게시판을 통해 전 직원에게 알려야 한다.

3. 연구보안관리 교육 실시

· 연구보안관리 교육에 모든 대상자들이 참석할 수 있도록 사전에 공지하여야 한다.
· 부득이한 사정으로 교육에 참석하지 못한 임직원들은 교육 내용을 인지할 수 있도록 재교육 또는 별도의 교육방법을 강구하여 시행하여야 한다.

4. 연구보안관리 교육 사후관리

· 연구보안관리 교육을 이수한 임직원들로부터 설문조사를 실시하여 교육내용, 교육방법, 교육시기 등에 관한 불편사항 또는 개선사항 등의 의견을 수렴하여 차년도 연구보안관리 교육 계획 수립 시 반드시 반영하여야 한다.

1.8 비상시 대응계획 수립

해당과제	
모든과제	보안과제
○	

이행대상		
연구기관	연구책임자	참여연구원
◎		

1.8.1 비상시 대응계획 수립

화재, 홍수, 재난, 재해 등으로 불시에 비상사태가 발생했을 경우 신속하고 정확하게 대응하기 위하여 비상시 대응계획을 수립하여야 한다. 이러한 사전 준비와 계획으로 비상사태 발생 시 능동적으로 대응할 수 있으며 이를 통해 각종 재난으로 인한 피해 규모를 최소화하고 빠른 시일 내에 정상적인 업무 복구가 가능하다.

내용

자연재난 또는 인적재난 등에 관한 비상사태 발생 시 대응계획은 규정이나 지침보다 더 구체적으로 상세하게 대응계획 및 복구계획을 명시하여야 하며 비상사태 발생을 인지한 시점부터 비상사태 종료 시 까지 일련의 대응 과정을 명시하여야 한다. 즉, 대응 조직 및 임무, 비상연락 체계도, 비상사태 발생 시 행동요령, 대피 방법, 복구 및 사후처리 계획 등을 전략적으로 수립해야 한다.

- 화재발생 시 행동요령

① 화재 상황 전파 및 119 신고

화재 발생 시 경보기의 벨을 눌러 다른 사람에게 화재사실을 알리면서 초기 소화가 불가능하다고 판단되면 119에 신고하여야 한다.

② 초기 소화

소화기나 물을 이용하여 불을 끌 수 있을 때까지 노력해야 하며 전기화재인 경우에는 전기스위치를 내리고 물을 사용하면 안 된다.

③ 대피 유도 및 긴급 피난

모포와 수건을 적셔 얼굴을 가리고 불이 난 반대쪽의 비상구, 비상계단을 찾아 1층 또는 옥상 중 가까운 곳으로 이동하며 엘리베이터를 이용하면 안 된다. 이 때 자세를 최대한 낮추고 행동을 최소화하여 산소 소모를 줄여야 하며 닫힌 문을 통과할 때는 반드시 문짝이나 손잡이가 뜨거우면 문을 열지 말고 다른 방향으로 찾아야 한다. 특히, 고립되었을 경우에는 문틈이나 창문으로 연기가 들어오지 못하도록 문틈을 막고 물을 뿌려야 하며 각종 수단을 동원하여 자기가 있는 곳을 외부에 알려야 한다.

내용

- 지진발생 시 행동요령
  ① 머리와 몸을 보호하기 위하여 책상 밑에 들어간다.
  ② 전기를 차단한다.
  ③ 서둘러 나가지 말고 문을 열어 피난 경로를 확보하여야 한다.
- 홍수발생 시 행동요령
  ① 홍수가 발생하면 전원을 차단한다.
  ② 최대한 높은 곳으로 빨리 대피한다.
  ③ 지정된 대피소에 도착하면 통제에 따라 행동한다.

실행지침

1. 비상사태 발생 시 대응 계획 수립

- (대응조직 및 임무) 비상사태 발생 시 효율적으로 대응하기 위한 조직을 구성하고 담당자와 이를 총괄하는 총괄책임자를 임명하여 그에 따른 역할과 임무를 구체적으로 명시해야 한다.
- (비상연락망) 비상사태 발생 시 신속한 대응을 위하여 비상사태 대응 조직원과 외부 기관(소방서, 경찰서, 병원 등)의 연락처 등을 포함한 비상연락망을 작성해야 한다.
- (대응절차) 신속하고 효율적인 대응을 위하여 다음과 같이 대응 절차를 수립하여야 한다.

① 비상사태 인지

비상사태를 인지함과 동시에 신속하게 상황을 전파하고 비상사태 대응팀을 가동하여야 한다. 그리고 재난관리기관, 긴급구조기관(소방서, 경찰서 등) 등 외부 기관에 신고하는 절차도 수립해야 한다.

② 인명 대피 및 구조계획

비상사태 유형별로 대피 요령을 마련하고 대피 장소를 미리 확보하여 대피소까지 안전하게 이동할 수 있는 이동경로를 명시해야 한다. 또한, 부상자 발생 또는 발견 시 응급조치를 포함하여 신속하게 구조하는 방안도 수립해야 한다.

③ 초기 대응 계획

화재, 홍수, 지진 등 비상사태 유형에 따라 초기에 대응할 수 있는 효율적인 방안을 수립해야 한다.

④ 중요 자산 대피 계획

자산의 중요도에 따른 우선순위를 정하여 비상사태 발생 시 가급적 중요한 자산도 안전한 장소로 이동시킬 수 있는 대피 계획도 수립해야 한다.

실행지침

⑤ 긴급 복구 계획

재난 피해 규모를 파악하여 빠른 시일 내에 복구가 가능하도록 재난 복구 계획을 수립하여야 한다. 이 때 외부 전문기관의 협조 체계도 마련하여야 한다.

⑥ 사후 처리

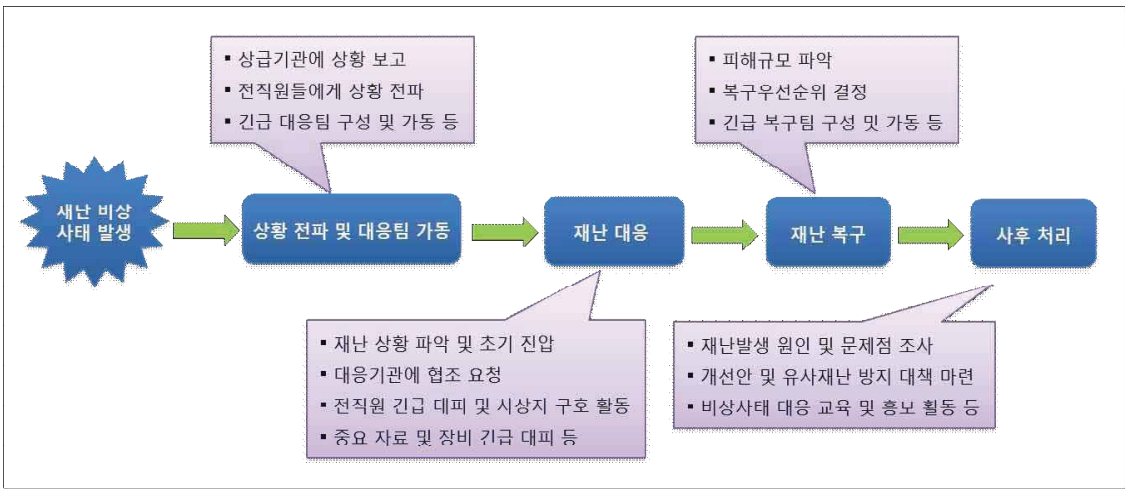
비상사태 대응 및 처리 과정에서 발견된 문제점에 대한 개선사항 또는 보완책은 비상사태 발생 시 대응계획에 반영하고 재발방지를 위하여 모든 임직원들을 대상으로 교육 및 홍보를 시행하여야 한다.

2. 비상 대응 계획 승인 절차 이행

· 비상사태 발생 시 대응 계획을 수립하거나 개선사항을 반영하여 수정·보완 작업이 이루어진 경우에는 반드시 자체 비상대책위원회의 심의를 거쳐 심의결과를 연구기관의 장에게 보고한 후 전 직원들에게 이러한 내용을 공지하여야 한다.

3. 훈련 및 교육

· 비상사태 발생 시 모든 임직원이 당황하지 않고 신속하게 대응하기 위하여 전 직원을 대상으로 매년 1회 이상 모의훈련을 실시하고 이와 더불어 교육 및 홍보 활동을 지속적으로 이행하여야 한다.



[그림] 비상사태 대응 체계도

1.9 공동 및 위탁 연구시 사전승인절차 이행

해당과제	
모든과제	보안과제
	○

이행대상		
연구기관	연구책임자	참여연구원
◎	○	

1.9.1 승인 절차

보안과제를 수행하는 연구책임자가 외국기업 또는 해외에 있는 연구기관과 공동연구 및 위탁연구를 수행하고자 하는 경우에는 연구 내용이 무단으로 외국에 유출되는 사고를 예방하기 위하여 협약 전에 연구기관의 장 및 소관 중앙행정기관의 장으로부터 사전 승인절차를 반드시 이행하여야 한다.

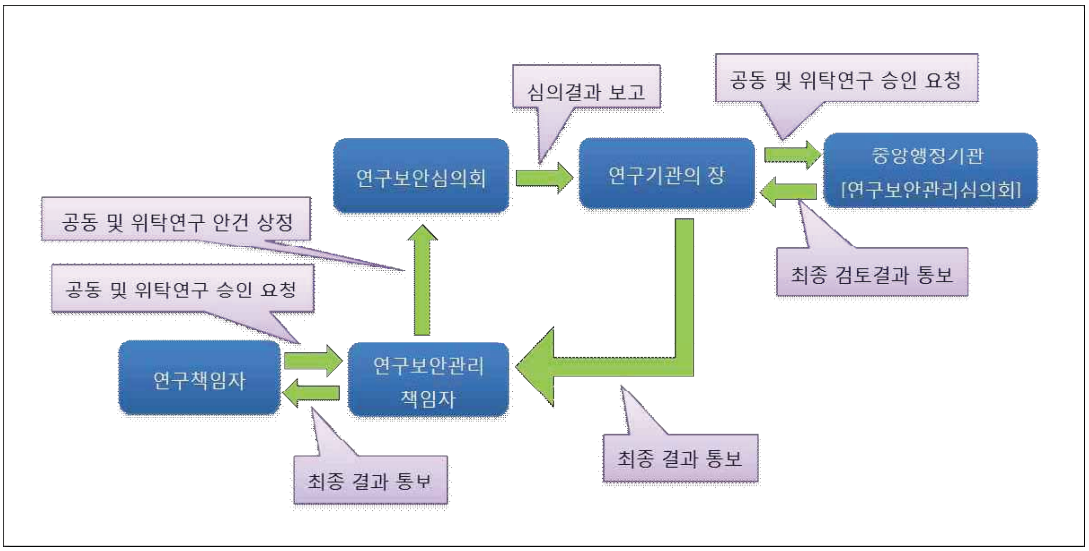
내용

- 국제공동연구란 복수의 연구개발주체가 동일한 연구과제의 수행에 소요되는 연구개발자금·인력·시설·기자재·정보 등 연구 자원을 공동으로 부담하여 국제적으로 수행하는 연구개발을 의미한다.
- 국제위탁연구란 의뢰기관이 수행하는 연구의 일부를 해외 전문가 또는 해외 연구기관에게 위탁하여 수행하게 하는 연구를 의미한다.
- 보안과제란 연구개발결과물 등이 외부로 유출될 경우 기술적·재산적 가치에 상당한 손실이 예상되어 보안조치가 필요한 과제를 의미한다.
- 보안과제가 국제 공동연구 또는 위탁연구로 인한 기술유출 사고를 사전에 예방하고 국제 공동연구 또는 위탁연구의 타당성을 심의받기 위해 연구책임자는 연구기관의 장 및 중앙행정기관의 장으로부터 협약 전에 사전 승인 절차를 이행하여야 한다.
- 보안과제를 수행하는 연구책임자는 중앙행정기관의 장으로부터 사전 승인을 받은 후에야 외국기업 또는 해외 연구기관과 공동연구 또는 위탁연구를 위한 협약을 진행할 수 있다.

실행지침

1. 사전 승인 절차

- 국제 공동연구 또는 위탁연구를 진행하고자 하는 보안과제 책임자는 연구보안관리 자에게 이러한 사실을 문서로 제출하고 연구보안관리자는 이 안건을 연구보안심의회에 상정하여 심의를 받아야 한다.
- 연구보안관리자는 심의결과를 연구기관의 장에게 보고하여 최종 승인을 받아야 한다.
- 심의가 통과된 보안과제의 공동연구 또는 위탁연구에 대한 협약 건은 연구기관의 장이 중앙행정기관의 장에게 승인을 요청하여야 한다.
- 중앙행정기관의 장은 기술보호를 위한 보안대책 및 공동연구 또는 위탁연구의 타당성을 검토한 후 그 결과를 연구기관의 장에게 통보하여야 한다.
- 중앙행정기관의 장으로부터 통보받은 심의결과는 연구보안관리자가 보안과제 책임자에게 그 사실을 통보하여야 한다.
- 중앙행정기관의 장으로부터 사전 승인을 받은 보안과제 책임자만이 국제 공동연구 또는 위탁연구를 위해 외국 해당기관에 계약을 요청할 수 있다.



[공동 및 위탁연구 시 사전승인 절차]

1.9 공동 및 위탁 연구시 사전승인절차 이행

해당과제	
모든과제	보안과제
	○

이행대상		
연구기관	연구책임자	참여연구원
◎	○	

1.9.2 협약 내용

보안과제는 연구 정보나 성과물이 해외로 무단 유출되는 경우 국가적으로 엄청난 손실이 초래할 가능성이 아주 높다. 따라서 외국기업 및 해외 연구기관과 공동연구 또는 위탁연구를 수행하고자 하는 경우에는 중요한 연구 정보나 성과물이 외국으로 무단 유출되지 않도록 대비책을 강구하여야 하며 협약서 작성 시 연구보안과 관련된 중요한 내용이 누락되지 않도록 협약서 내용에 특별히 보호대책을 명시하여야 한다.

내용

- 보안과제를 수행하는 연구책임자가 외국기업 또는 해외 연구소와 공동연구 또는 위탁연구를 위해 협약을 체결하는 경우 적절한 보호대책을 마련하지 못하게 되면 중요한 연구 정보가 유출되더라도 외교나 국가 간 법률 차이 등의 문제로 법적으로 대응하거나 피해 보상을 받는데 어려움을 겪을 수 있다.
- 국제 공동연구 또는 위탁연구 시 제공하는 연구개발 정보의 범위와 서로 간의 연구개발 영역을 설정하고 연구 성과물의 귀속 및 특허권 이용 등에 관한 사항들을 명확하고 구체적으로 명시하여야 한다.
- 또한, 협약서에는 참여자의 신원확인, 보안준수의무 고지, 서약서 집행 등 보안조치를 강구하고 연구보안관리자를 지정하여 연구수행 과정의 보안감독 업무를 수행하도록 하는 등의 보호대책을 마련한 후에 협약 체결을 진행하여야 한다.

실행지침

1. 보안과제의 국제 공동연구 협약서 보안대책 강구

・보안과제가 국제 공동연구 또는 위탁연구를 진행하고자 하는 경우 연구협약서에 필히 다음과 같은 내용이 포함되어야 한다.

① 국제 공동연구 및 위탁연구를 위해 제공하는 특허나 노하우의 보호대책에 관한 사항
② 연구개발 또는 성과물과 관련된 정보의 비밀유지 의무 및 보안조치 사항
③ 연구개발 범위 및 역할분담, 비용분담 등에 관한 사항
④ 연구개발 중단 사태 발생 시 처리에 관한 사항
⑤ 연구개발 기간에 관한 사항
⑥ 연구개발 성과물 귀속에 관한 사항
⑦ 연구개발 장비의 소유권에 관한 사항
⑧ 특허권 출현 등의 처리 및 소유권에 관한 사항
⑨ 특허권 실시(제3자에 대한 실시 허락)에 관한 사항
⑩ 공동연구 또는 위탁연구 종료 후 이용특허권 처리에 관한 사항
⑪ 계약 위반 시 법적 대응 및 처리에 관한 사항
⑫ 보안감독업무를 수행하는 보안관리자 지정에 관한 사항 등

03

제 2 장
참여 연구원 관리

1절. 참여 연구원 관리

2.1 채용 시 인원관리
2.2 재직 중 인원관리
2.3 계약 갱신 시 인원관리
2.4 퇴직자 관리
2.5 국외 출장자 관리
2.6 연구성과 유출 혐의자 관리
2.7 보안교육
2.8 접촉외국인 관리

2절. 외국인 관리

2.9. 외국인 연구원 관리

3절. 외부인 관리

2.10 상시 출입자 및 파견자 관리
2.11 일시 출입자 관리

미래창조과학부
Ministry of Science, ICT and Future Planning

2.1 채용 시 인원관리

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	연구원
◎	◎	O

2.1.1 신입채용 시 고려사항

연구보안 사고는 대부분 내부직원 또는 퇴직자에 의해 발생하는 경우가 많다. 이러한 측면에서 신입직원 채용은 아주 중요하며 신중하게 결정해야 할 사항이다. 중요한 비밀을 보호할 수 있는 도덕적인 자질과 신원에 대해 면밀히 검토하고, 채용 시에는 서약서 작성 등을 통해 연구보안에 대한 인식을 확실히 하도록 한다. 또한, 신입직원 채용 시 개인의 능력만을 고려하기 보다는 채용단계에서부터 연구보안을 함께 고려하는 것이 추후 내부직원에 의한 연구정보유출사고를 예방하는데 큰 도움이 될 것이다.

내용

- 신입직원 채용이란 연구원의 일시적 혹은 지속적인 고용을 포함한다.
- 연구정보보안 측면에서 신입 채용 시 관리 절차는 고용 전과 고용 후로 구분할 수 있다.
- 고용 전 지원자에 대한 검증 사항으로 다음과 같은 내용을 포함하여야 한다.
  - 신원확인
  - 신용 혹은 범죄 사실 여부 확인
  - 서술된 학력과 전문자격 확인
  - 충성도, 성실성 및 태도 확인
  - 인격적 결함 여부 확인

- 고용 후에는 채용된 연구원에게 연구정보보호의 책임의식을 상기시키도록 한다.

실행지침

1. 고용 전 고려사항

- 신입직원 채용 전 지원자를 검증하는 기본적 수단으로 이력서, 연구기관 지원서 양식, 면접이 있다.
- 이력서와 지원서 양식에 따라 기입한 내용을 근거로 지원자의 신원확인 및 관련된 추가 정보를 확인해야 한다.
- 면접을 통하여 해당 연구기관의 요구 조건에 부합하는 정도와 능력을 확인함과 동시에 연구보안문제에 영향을 끼칠 수 있는 성실성, 충성심과 같은 인성에 대한 검증도 수행한다.
- 특히, 보안과제의 경우 연구책임자도 함께 면접에 참여하여 지원자에 대한 면밀한 검토가 이루어지도록 해야 한다.

2. 고용 후 고려사항

- 위와 같은 절차를 거쳐 채용 된 신입직원에게는 고용계약서 외에 보안 서약서를 추가적으로 징구하여 연구기관의 보안지침을 준수하겠다는 서약을 받아냄과 동시에 연구보안에 대한 중요성을 각인시키도록 한다.
- 채용된 신입직원에게 연구보안 내부규정과 기타 사항 등에 대한 전반적인 교육을 실시하여 연구보안 준수사항을 인지할 수 있도록 한다.

2.1 채용 시 인원관리

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	연구원
◎	◎	

2.1.2 경력직원 채용 시 고려사항

연구기관에서는 우수한 인재를 확보하기 위해 해당분야에 경험이 많은 경력자를 채용하는 경우가 빈번하다. 하지만 연구정보를 유출하기 의도적으로 위장취업을 하는 사례도 있으므로 경력직원 채용 시 보다 세심한 절차가 필요하다.

내용

- 경력직원 채용이란 타 연구기관에서 일정기간 연구원으로 소속되었던 자의 채용을 일컫는다.
- 경력직원 채용 시 검증사항으로 다음과 내용을 포함하여야 한다.
  - 신원확인
  - 신용 혹은 범죄 사실 여부의 확인
  - 서술된 학력과 전문자격의 확인
  - 충성도, 성실성 및 태도의 확인
  - 인격적 결함 여부
  - 전 직에서의 보안 준수현황 파악
  - 위장 취업, 단기간 개인 목적의 취업 여부 확인

실행지침

•고용 전

- 경력직원 채용 전 지원자를 검증하는 기본적 수단으로 이력서, 연구기관 지원서 양식, 면접이 있다.
- 지원자가 작성한 이력서와 지원서에 근거하여 지원자의 신원을 확인하고 이와 더불어 경력 사실 증명을 위한 경력증명서를 제출토록 하여 확인한다.
- 신입직원 채용 시와 마찬가지로 면접을 통하여 제출한 서류에 대한 사실성 검토 및 해당 연구기관의 요구 조건에 부합하는 정도와 능력을 확인함과 동시에 연구보안 관련 문제에 영향을 끼칠 수 있는 성실성, 충성심, 인격적 결함여부의 유무를 판단한다. 또한, 정보를 유출하기 위한 위장취업의 가능성을 배제할 수 없으므로 세심한 주의를 기울일 필요가 있다.
- 인성검사의 개별적 실시를 통해 지원자의 인격적 결함 여부를 판단한다.
- 이전에 소속되었던 기관에서의 보안준수현황을 채용 여부에 반영하기 위하여 이전 기관에서의 보안관련 징계사항의 확인, 인터넷 검색이나 평판도를 통해 지원자에 대한 파악이 이루어져야한다.

•고용 후

- 일련의 과정을 거쳐 채용 된 연구원에게는 고용계약서 및 보안 서약서를 추가적으로 징구하여 연구기관의 보안지침을 준수하겠다는 서약을 받음과 동시에 연구보안에 대한 중요성을 각인시키도록 한다.
- 채용된 연구원에게 해당 연구기관의 연구보안 내부규정 및 주의사항에 대한 전반적인 교육을 실시하여 연구보안의식을 고취시킨다.

2.2 재직 중 인원관리

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	연구원
◎	◎	O

2.2.1 재직 중 인원관리

재직 중인 연구원은 연구를 수행하는 과정에서 연구정보와 직접적으로 접촉하며 연구정보 보호의 책임과 의무가 있는 주체이다. 따라서 재직 중인 연구원들이 연구보안에 관한 책임과 의무를 인지하고 보안의식을 고취시킬 수 있도록 관리할 필요가 있다. 재직 중인 인원들을 관리함으로써 내부에 의한 연구정보유출 사고의 발생을 억제할 수 있다.

내용

· 재직 중인 인원이란 연구기관에 의해 일시적 혹은 지속적으로 고용되어 과제에 참여중인 모든 자를 포함한다.

· 재직 중인 인원을 관리할 때에는 다음과 같은 사항을 포함하여야 한다.
  - 모든 임·직원에게 연구기관 내부 보안관리규정의 준수 의무화
  - 보안서약서의 작성 및 보관
  - 부서 및 직무 변경 시 연구정보관련 인수인계 절차 마련

실행지침

- 취급하는 연구성과물의 보안등급이 높고 낮음에 관계없이 재직 중인 모든 연구원들은 보안관리 규정 준수의 의무화와 보안의식의 각인을 위하여 비밀유지서약서를 작성한다.

- 국내 연구정보의 해외유출에 따른 국가적 손실의 발생을 방지하기 위하여 외국인 연구원의 고용은 원칙적으로 제한하는 것이 권고되지만, 필요에 의해 고용된 외국인 연구원이 있다면 영문으로 보안서약서를 받도록 한다. (2.9.1 참고)

- 작성된 비밀유지 서약서는 법적 분쟁 발생 시 증거자료로 활용 될 수 있으므로 연구보안관리자의 책임 하에 연구기관 내 물리적으로 안전한 곳에 필요 시 용이하게 찾아볼 수 있는 형태로 보관하도록 한다.

- 재직 중인 연구원의 부서 및 직무변경 등 인력의 고용조건에 변화가 발생한 경우 변경 이전에 습득한 연구정보가 누출되지 않도록 이전에 사용된 정보자산의 반납, 접근권한의 변경 및 회수조치가 보안 관리자의 책임 하에 신속히 이루어져야 하며, 변경내용에 대하여 항상 기록을 유지하고 해당 부서와 보안관리부서 등에 변경내용이 공유되어야 한다.

- 재직 중인 연구원이 새로운 프로젝트에 참여할 시에 추가적으로 보안서약서를 징구하여 보안지침사항을 환기시키도록 한다.

2.3 계약 갱신 시 인원관리

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	연구원
◎	◎	O

2.3.1 계약 갱신 시 인원관리

해당 연구기관에 연구원으로 소속되어있는 기간이 길수록 접촉하는 연구정보의 양은 많아지므로 재계약시 성과뿐 만 아니라 연구정보보안의 측면에서 평가한 사항을 재계약시 적극 반영할 필요가 있다.

내용

- 계약 갱신 인원관리의 해당 대상은 재직 중인 인원 중 계약기간이 만료되어 재계약이 필요한 인원으로 한정함.
- 계약 갱신을 결정할 때는 다음과 같은 사항을 확인해야 한다.
  - 이전 계약기간 동안에 해당 인원의 보안규정 준수여부
  - 기밀 유출 시도 여부

실행지침

- 이전 계약기간 동안의 보안규정 준수여부를 평가하기 위하여 해당 연구원은 소속된 부서의 연구책임자로부터 평가에 대한 확인증을 서면으로 받는다.
- 연구책임자로부터 받은 확인증을 연구기관에 제출하여 최종 승인이 완료되면 재계약을 체결하도록 하고, 연구책임자로부터 규정을 잘 준수하였다는 확인증을 받지 못했거나 확인증을 받았더라도 연구기관으로부터 승인을 받지 못한 경우에는 계약을 갱신하지 않도록 한다.

2.4 퇴직자 관리

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	연구원
◎	◎	O

2.4.1 퇴직자 관리

퇴직자가 연구수행 중에 습득한 중요한 연구정보를 외부에 누설하는 것을 방지하기 위하여 퇴직 시에 반드시 보안관리규정의 절차를 준수하도록 한다. 실제로, 연구기관 또는 중소기업에서 재직 시 불만을 가졌거나 기타 갈등으로 퇴직한 경우 악의적 감정을 가지고 연구정보 또는 중요 기밀을 경쟁관계에 있는 기관에 유출하는 경우가 빈번하게 발생하였다. 따라서 연구원이 퇴직하고자 하는 경우에는 퇴직사유, 퇴직절차 및 퇴직 후 관리의 모든 과정에 대하여 연구기관에서 관리를 할 필요가 있으며 이러한 관리는 퇴직자에 의한 연구정보유출을 막는 좋은 예방책이 될 것이다.
승진실패 등을 비롯한 각종 인사처분 및 기타 사항에 대해 불만이 있었던 퇴직직원에 대해서는 인권침해가 되지 않는 조건 하에서 사후관리를 더욱 철저하게 하는 것이 보안사고 예방에 큰 도움이 될 것이다.

내용

- 연구보안의 측면에서 퇴직자 관리는 크게 퇴직 전 - 퇴직승인- 퇴직 후로 구분할 수 있다.
- 퇴직 전에는 해당 연구원이 퇴직을 선언하는 시점에서 갑작스런 근무태도의 변화, 행동의 변화는 없는지 확인해야 한다. 평상시와 달리 이상한 행동을 보인다면 연구정보유출을 계획하고 있지는 않는지 의심해볼만 하다. 또한, 퇴직자에 의하여 연구정보가 외부로 유출되지 않도록 여러 가지 사항을 점검해야 한다.
- 이미 퇴직한 연구원은 퇴직 후 일정기간 동안 관심을 가지고 지켜보는 것이 연구정보유출을 확실히 예방하는 길이다.

실행지침

1. 퇴직 전

- 퇴직예정자의 연구정보유출을 의심해볼 만한 특별한 행동의 사례는 다음과 같다.
  (예 : 연구 활동보다 성과물 확보에 집착, 주요부서 연구원의 갑작스러운 사직요구, 연구기관에 대한 부정적 태도로 돌변, 퇴직자와 관련 없는 정보의 보유, 정보의 외부유출 흔적, 눈에 띄게 외부메일을 사용한 흔적 등)
- 퇴직 예정자는 업무 인수인계 및 연구개발 관련 서류, 연구기관의 모든 자산을 일체 반환도록 하며 연구정보 및 시설 접근권한 또한 제한해야 한다.
- 퇴직 예정자에 대한 전반적인 보안점검이 이루어진 후에는 퇴직자가 연구정보를 누설하거나 오용하지 않을 의무와 위반 시 그에 대한 처벌이 따른다는 사항이 명시된 보안서약서를 징구하여야 한다. 추후 퇴직 연구원에게 법적 책임을 묻게 되는 상황이 발생할 시 중요한 증거자료가 될 수 있으므로 보안서약서를 반드시 받아두어야 한다.

2. 퇴직승인

- 연구원의 퇴직을 최종 승인하기 전에 모든 보안 절차의 준수 여부를 확인하여야 하며 업무 인수인계가 명확하고 완전하게 완료되었고 다른 누락된 사항이 없다고 판단되면 연구원의 퇴직을 승인한다.

3. 퇴직 후 보안조치 사항

- 퇴직자가 모든 퇴직 준비를 마치고 개인물품을 외부로 보낼 때 연구내용과 관련된 중요한 정보가 포함되어 있는지 검토하여야 한다.
- 퇴직 이후에도 연구정보보호와 관련된 사항에 대해서는 상호 협의할 수 있는 체계를 구축해 두는 것이 필요하다.
- 퇴직한 연구원이 새로운 연구기관 또는 회사에 고용될 경우, 해당 기관에 연구정보 보호에 관한 관련 내용을 알리는 서한을 보냄으로써 퇴직 연구원을 이전 연구기관의 연구정보 공개가 불가피한 프로젝트나 업무에 투입하지 않도록 하여야 한다.

2.5 국외출장자 관리

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	참여연구원
◎	◎	O

2.5.1 국외 출장 시 고려사항

최근에 국제 학회나 세미나 또는 연구 자료 수집, 공동연구 등으로 연구원이 해외로 출장 가는 빈도가 점차 증가하고 있는 추세이다. 해외 출장 중에 연구보안관리 규정 준수 미비로 연구보안 사고가 발생할 수도 있으므로 이를 예방하기 위한 조치 방안을 수립하여야 한다.

내용

- 연구원이 연구개발과 관련하여 해외로 출장을 가는 경우 생소한 환경에 적응하느라 정신이 없어 중요한 물품을 분실하는 경우도 많고 긴장감이 풀려서 연구보안관리 규정을 허술하게 다루는 경우도 있다.
- 해외 출장 중에 중요한 자료나 물품을 분실 또는 도난을 당하게 되면 되찾을 수 있는 방법이 거의 없기 때문에 출국 전에 보안상으로 완벽하게 준비하는 것이 가장 중요하다.
- 해외 출장 중에 연구보안 사고를 예방하기 위하여 고려해야 할 사항들은 출장 전 보안조치 사항, 출장 중 보안조치 사항, 출장 후 보안조치 사항으로 구분할 수 있다.
- 출장 전에는 방문할 국가의 정보를 수집하고 꼭 필요한 자료나 정보가 아니면 가져가지 아니하도록 한다. 또한, 출장 중에는 업무와 무관한 외부인과의 접촉을 자제하고 중요한 정보나 자료가 분실 또는 도난을 당하지 않도록 각별히 주의하여야 하며 출장 후에는 귀국보고서를 작성하여 연구기관의 장에게 제출하여야 한다.

실행지침

1. 해외 출장 전 보안조치 사항

- 방문할 국가의 치안문제, 범죄 취약지역, 최근 발생범죄 유형과 대사관, 경찰서, 지인 등 긴급한 상황 발생 시 도움을 받을 수 있는 정보를 확인하여야 한다.
- 꼭 필요한 경우가 아니라면 연구기관 로고가 들어가 있는 옷 또는 가방, 전산장비나 중요한 자료 등은 가지고 가지 않아야 한다.
- 전산장비에는 강력한 비밀번호를 설정하고 중요한 모든 정보는 암호화하여야 한다. 또한, 전산장비에 있는 프로그램은 최신 업데이트를 실시하여야 한다.
- 연구보안관리자는 해외 출장을 앞두고 있는 연구원들을 대상으로 연구보안관리 교육을 실시해야 한다.
- 보안과제를 수행하고 있는 연구원이 외국 정부나 기관 등을 방문하고자 하는 경우에는 방문 목적 및 관련 내용을 반드시 사전에 상위 중앙행정기관의 장과 국가정보원의 장에게 통보해야 한다.
- 해외출장 중에 발표하거나 공개해야 할 연구개발 자료는 사전에 연구책임자 또는 연구보안관리 책임자로부터 보안성 검토를 필히 받아야 한다.

2. 해외 출장 중 보안조치 사항

- 해외 출장 중에 여행사, 호텔 관계자 등 외부인에게 소속 기관, 체류목적 등 출장과 관련된 정보 노출을 최소화하여야 한다.
- 업무와 무관한 사람에게 기관 내 직책, 경력, 담당업무 등 관련 정보를 언급하지 않아야 한다.
- 대중교통 등 공공장소에서는 연구과제와 관련된 민감한 정보에 대해 얘기하지 않아야 한다.
- 접근 의도가 불분명한 질문 또는 추궁하는 듯한 질문을 하는 사람은 무시하고 명확하지 않은 대답으로 일관한다.
- 연구과제와 관련된 민감한 정보를 발설해야 할 경우에는 자체 연구보안관리 규정 또는 지침에 따라야 한다.
- 해외 출장 중에 숙소에서 외부로 외출하고자 하는 경우에는 중요한 정보가 저장된 노트북이나 이동매체는 도난이나 복제를 방지하기 위하여 항상 휴대하고 다녀야 한다.

실행지침

- 보안을 요구하는 중요한 자료를 국내로 전송하고자 하는 경우에는 호텔이나 학회 또는 세미나 측에서 제공하는 컴퓨터나 팩스의 이용을 자제해야 한다. 본인의 노트북으로 전송하고자 하는 내용을 암호화하여 메일로 전송하여야 한다.
- 의심되는 특이한 상황이 발생한 경우에는 한국공관 또는 연구기관 등에 문의하여야 한다.

3. 해외 출장 후 보안조치 사항

- 귀국 후에는 가능한 빠른 시일 내에 전산장비의 패스워드를 반드시 변경하여야 한다.
- 출장 중에 소지한 전산장비는 연구기관의 정보보안부서에 의뢰하여 악성프로그램이 설치되어 있는지 반드시 점검을 받아야 한다.
- 해외에서 연구기관으로 귀국하면 출장 중에 접촉한 인물과 협의한 내용 등을 구체적으로 작성한 귀국보고서를 연구기관의 장에게 제출해야 한다. [별첨 2.5.1 참조]

2.6 연구성과 유출 혐의자 관리

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	참여연구원
○		

2.6.1 연구 성과 유출 혐의자 관리

중요한 연구개발 관련 정보 및 성과물을 유출한 혐의가 있는 자는 연구보안 사고 재발을 방지하기 위한 차원에서 유출 혐의자를 특별 관리하기 위한 대책을 마련하여 지속적으로 유지하고 관리하여야 한다.

내용

- 유출 혐의자는 과거에 연구개발 관련 기밀자료나 연구개발 성과물을 고의적 또는 실수로 외부에 유출한 경험이 있는 자를 의미한다.
- 유출 혐의자를 특별 관리하기 위한 대책으로 보안사고가 발생하면 기술적, 경제적 손해가 심각한 보안과제 참여를 원천적으로 차단하고 일반과제 참여 시에도 중요한 정보에 접근하는 것을 원천적으로 차단하는 방안을 수립하여야 한다. 또한, 업무와 무관한 지역에 출입하는 것을 제한하고 외부로 반출 또는 반입하는 물품에 대해서도 통제하는 등 보다 강한 보안대책을 강구하여야 한다.

실행지침

1. 연구 성과 유출 혐의자의 특별 관리 대책 수립

- 연구기관의 장은 연구 성과 유출 혐의자의 보안과제 참여를 원천적으로 제한하여야 한다.
- 일반과제 참여 시에도 연구보안심의회에서 과제 참여의 타당성을 심의하여 연구 성과 유출 혐의자의 참여를 제한할 수 있다.

실행지침

- 연구 성과 유출 혐의자의 업무와 무관한 연구기관의 시설 또는 지역의 출입을 제한하여야 한다.
- 연구 성과 유출 혐의자가 외부로 반출 또는 내부로 반입하는 품목에 대해서도 철저하게 통제하여야 한다.
- 연구개발과 관련된 민감한 정보 또는 자료가 저장되어 있는 정보시스템의 접근 권한을 차단하여야 한다.
- 연구 성과 유출 혐의자가 해외출장 신청 시 연구기관의 장은 방문국가 및 출장목적, 출장기간 등을 면밀하게 검토한 후 승인여부를 결정하여야 한다.

2. 연구 성과 유출 혐의자 현황 관리

- 연구 성과 유출 혐의자를 특별 관리하기 위한 관리대장을 만들어 지속적으로 현황을 관리하고 유지하여야 한다.

2.7 보안교육

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	연구원
◎	◎	O

2.7.1 보안교육

대부분의 연구정보유출은 정보시스템의 취약점을 이용한 해킹에 의한 유출보다는 내부 직원에 의한 연구보안 사고가 많은 부분을 차지하고 있다. 따라서 연구원들에게 연구보안교육을 정기적으로 실시하여 연구 보안 사고를 사전에 예방하는 것이 최선의 방법이다.

내용

- 보안교육에는 크게 정기교육과 수시교육이 있다. 정기교육은 연구기관 내 모든 연구원을 대상으로 연 1회 이상 내부 규정에 의해 수행하며 수시교육은 규정 변경, 신규직원 채용 등 연구보안관리자가 필요하다고 여겨질 때 이루어진다.
- 보안교육 대상에는 재직 중인 전 연구원이 포함되며, 해당 연구기관의 소속이 아니 지만 국가연구개발과제를 함께 수행중인 외부인도 교육 대상에 해당된다.
- 보안교육 기간은 유출사고의 효과적 예방을 위해 재직 연구원의 경우 입사 시 부터 퇴직 시까지 지속적으로 이루어져야 하며 외부 연구원 또한 연구 참여기간동안 지속적으로 교육에 참여하여야 한다.
- 보안교육의 내용에는 기본적으로 정보보호 및 정보보호 관리체계 개요, 연구기관 내 부 규정 및 절차, 규정위반 시 법적 책임, 보안사고 사례, 정보보호 관련 법률, 등의 내용이 포함되어야 한다.
- 보안교육을 수행하는 방법은 교육의 시기와 상황에 따라 연구기관에서 유연하게 선택하여 수행해야한다. *(예 : 집합교육, 온라인 교육, 전달 교육, 유인물 배부 등)*

실행지침

1. 계획수립

· 보안교육 계획은 매년 초에 수립해야 한다. 계획단계에서 교육대상, 교육시기, 교육내용, 교육장소, 교육방법등에 관한 사항들이 결정되어야 한다.

① 정기교육

· 정기교육은 내부규정에 명시된 사항을 준수하여 전 직원이 참여 가능한 교육 시기, 교육 내용, 교육 장소 등을 계획단계에서 고려하여야 한다.

② 수시교육

· 신입직원 또는 경력직원이 새로이 채용되거나 보안관련 규정이 변경 또는 연구보안 관리자의 필요에 의해 수시로 진행되어야 한다.

· 연구책임자 및 부서장은 직원들이 수시 교육에 참여할 수 있도록 적극 독려하여야 한다.

2. 교육 기간 및 시기

① 정기교육

· 재직 중인 연구원 및 연구과제 참여 중인 외부인에 대하여 연구기관의 판단 하에 연 1회 이상 분기별 혹은 반기별로 실시하도록 한다.

② 수시교육

· 연구기관 또는 연구책임자의 판단 하에 추가적으로 보안교육의 필요성을 느낄 때 수시로 실시하도록 한다. 수시교육을 필요로 하는 상황의 예는 다음과 같다.

  - 신입직원 또는 경력직원 채용 시
  - 보안과제 또는 신기술 개발 시
  - 내부 인사이동이 있을 시
  - 정보보호 관련 법률 및 규정 변경 발생 시
  - 연구기관 내 보안사고가 발생 시
  - 타 기관에서 보안사고 발생 시 유사 사고의 발생 예방 시

· 교육 기간의 경우, 재직 연구원은 입사 시 부터 퇴직 시까지 정기교육에 참여해야 하고 국가연구개발사업 과제에 참여 중인 내부연구원 및 외부연구원도 해당 연구기관의 과제에 참여하는 기간 동안 이루어지는 수시 교육에 참여하여야 한다.

3. 교육 대상

- 정기교육의 경우 연구기관의 모든 연구원이 포함되며, 연구정보자산이 위치한 장소 에 직·간접적으로 접근할 수 있는 기타 인력 또한 포함될 수 있다.
- 수시교육의 경우 보안교육 내용에 따라 모든 연구원이 참여할 수도 있고 특정 관련자만 참여할 수도 있다.

4. 보안교육 내용

- 보안교육 내용은 위에서 언급한 내용이 포함될 수 있도록 하며 상황에 따라 연구기관의 장 및 연구보안관리자가 자율적으로 조정하도록 한다.

5. 승인절차

- 교육 시행 계획은 연구보안심의회의 승인을 거쳐 연구기관의 장으로부터 최종 승인을 득한 후 시행한다.

6. 결과보고

- 보안교육을 수행 한 뒤에는 교육 만족도에 대한 설문조사 등을 통하여 교육내용의 적절성과 효과성을 평가하여 연구기관의 장에게 보고하고 미흡한 부분은 개선하여 차후 교육계획 수립 시 반영하여야 한다.

· 기타

- 출장, 휴가 등의 이유로 보안교육을 이수하지 못한 직원은 추가적인 교육 방안을 마련하여 전 연구원이 빠짐없이 참여할 수 있도록 한다.*(예 : 유인물 전달, 전자메일로 교육 내용 발송, 미 참여 인원 개별 소집 등)*
- 보안교육의 참여를 활성화하기 위하여 특별한 이유 없이 교육에 불참한 직원에게 패널티를 부과하여야 한다.

교육계획 수립

· 매년 초 수립, 교육내용 및 대상, 시기, 장소 등으로 계획

↓

승인 절차

· 연구보안심의회 의결을 거쳐 연구기관장이 최종 승인

↓

교육 시행

· 정기교육, 수시교육 및 미 참여자 재교육 시행

↓

사후 관리

· 교육시행 결과보고
· 설문지 조사를 통한 의견수렴
· 의견수렴 결과를 교육계획 수립에 반영

2.8 접촉외국인 관리

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	참여연구원
◎	◎	O

2.8.1 연구원의 접촉 외국인 관리

보안과제를 수행하는 연구책임자는 외국인 접촉 시 우려되는 연구기밀 정보 유출을 사전에 방지하기 위하여 참여연구원이 과제와 관련하여 접촉하는 외국인의 현황을 관리대장에 기록하고 지속적으로 관리하여야 한다.

내용

산업기밀보호 센터에 의하면 2005년부터 2012년간 국내 첨단기술이 해외로 불법 유출되었거나 유출을 기도한 사건으로 총 294건을 적발했다고 밝혔다. 특히, 보안과제인 경우 연구개발 관련 정보 및 성과물 등이 외국에 무단으로 유출되면 기술적·경제적 피해가 심각하게 된다. 이 때문에 연구보안관리자 및 연구책임자는 보안사고 예방 활동을 성실하게 수행하여야 한다. 특히, 과제에 참여하는 연구원 관리에 만전을 기하여야 하며 그 일환으로 참여연구원이 보안과제와 관련하여 외국인과 접촉하는 경우에는 외국인 접촉 현황을 관리대장에 반드시 기록하고 연구책임자가 관리하여야 한다.

실행지침

1. 외국인 접촉 절차 및 방법 수립

- 보안과제 참여연구원은 외국인과 접촉 시 1일전까지 ‘외국인접촉 신청서’(별표 2.9.1)를 작성하여 연구책임자의 승인을 득한 후에 접촉하여야 한다.
- 보안과제 참여연구원은 외국인과 접촉한 후 2일 이내에 ‘외국인접촉 결과서’(별표 2.9.1)를 작성하여 연구책임자에게 보고하여야 한다.
- 외국인 접촉 결과 특이한 사항이 발생하면 연구책임자나 연구보안관리자에게 구두 로 보고하고 이후 서면 결과서를 제출하여야하며 연구책임자는 이러한 사실을 인지 한 즉시 연구보안관리 담당부서에 통보하여야 한다.

2. 외국인 접촉 현황 관리

- 연구책임자는 보안과제와 관련하여 참여연구원이 접촉한 외국인 현황을 관리하기 위하여 관리대장을 만들어야 한다.
- 연구책임자가 관리대장에 기록할 항목은 참여연구원 이름, 접촉대상 이름 및 국적, 접촉일시, 접촉사유 등이다.

[외국인 접촉현황 관리대장]

참여연구원	외국인 (접촉대상/국적)	접촉일시	접촉사유	연구책임자 (서명)
홍길동				

3. 접촉 외국인 관리대장 관리 방법

- 참여연구원이 외국인의 접촉 현황을 관리대장에 기록하면 연구책임자가 사실 여부를 확인한 후 서명하여야 한다.
- 외국인 접촉현황 관리대장은 연구책임자가 유지 관리하고 보관해야 한다.

2.9 외국인 연구원 관리

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	참여연구원
◎	◎	

2.9.1 외국인 연구원 관리

외국인 유치 과학자가 연구개발에 참여할 경우에는 외국인 연구원에 의해 중요한 연구개발 관련 정보 또는 성과물이 국외로 유출될 가능성을 배제할 수 없다. 따라서 연구개발과제에 외국인 및 외국기업 등이 참여하는 것을 원칙적으로 제한할 필요가 있다. 하지만 부득이한 경우가 발생하여 외국인 연구원의 참여가 필요한 경우에는 이와 관련된 별도의 보안대책을 마련하여 연구보안관리를 강화할 필요가 있다.

내용

외국인 참여연구원 관리는 고용 계약하기 전에 준수해야 할 보안사항과 연구수행 중에 준수해야 할 보안사항 그리고 연구계약 만료 후에 준수해야 할 보안사항으로 구분할 수 있다. 먼저 연구기관의 장은 유치과학자와의 활용 계약 전에 보안준수 의무사항이 명시된 서약서[별표 2.10.1]를 징구하고 자체 보안교육을 실시한 후 계약을 체결해야 한다. 또한, 연구책임자는 외국인 참여연구원이 연구수행 중에 연구개발과 무관한 중요한 자료를 수집하거나 핵심 연구시설의 출입을 시도하는 등 특이한 동향을 수시로 관찰하는 연구보안 활동을 게을리 해서는 안 된다.

연구계약 만료 시에는 연구보안관리 책임자와 연구책임자가 반출되는 자료의 보안성을 검토하고 연구기관의 장은 연구개발 활동 중에 취득한 기밀내용에 대한 보안을 유지한다는 서약서를 징구하는 등 관련 부서들이 협조하여 연구보안사고가 발생하지 않도록 조치해야 한다.

실행지침

1. 외국인 연구원 활용 계약 전 보안대책

- 연구기관의 장은 고용 계약서상에 보안준수 의무를 명시하고 연구보안관리 규정을 준수한다는 내용이 명시된 영문보안서약서를 징구해야 한다.[별표 2.10.1 참조]
- 연구기관의 장은 외국인 연구원과 고용 계약을 체결하기 전에 연구보안 교육을 먼저 실시하여야 한다.
- 연구책임자는 연구보안관리자의 승인을 거쳐 출입 가능한 지역만 출입할 수 있는 출입증을 해당부서에 발급 신청하여야 한다.

2. 외국인 연구원의 연구수행 중 보안대책

- 연구보안관리자는 외국인 참여연구원이 소속된 연구책임자를 분임연구보안관리 책임자로 지정하여 연구책임자로 하여금 수시로 보안교육을 실시하고 보안관리 상태에 대한 점검을 실시하도록 하여야 한다.
- 연구보안관리자 및 연구책임자는 유치 과학자가 중요한 연구자료 대출 및 열람하는 것을 제한하여야 한다. 단, 연구 활동 상 대출 및 열람이 불가피한 경우에는 연구책임자가 연구보안관리자에게 보안성 검토를 의뢰하여야 한다.
- 연구보안관리자 및 연구책임자는 유치과학자가 타 분야의 연구시설에 접근하는 것을 원천적으로 차단하고 중요 시설을 무단으로 출입하는 것과 사전에 허락 없이 연구시설을 사진 촬영하는 것을 제한하는 등 보안조치를 취하여야 한다.
- 연구책임자는 외국인 참여연구원이 불필요한 야근을 많이 하거나 공휴일에도 연구실에 출근하는 것을 자제하도록 조치하여야 한다.
- 외국인 참여연구원이 중요한 연구 정보를 무단으로 복사하거나 이동매체 또는 개인 전산장비에 저장하는 것을 차단하여야 한다.

3. 외국인 연구원의 연구계약 만료 시 보안대책

- 외국인 참여연구원의 연구계약기간 만료 시 연구보안관리자와 연구책임자는 연구수행 중 취득한 기밀내용이 누설되지 않도록 각종 연구자료, 성과물 및 연구노트 등을 회수하여야 한다.
- 연구보안관리자 및 연구책임자는 외국인 참여연구원이 연구수행 중에 인지한 연구기밀에 대한 보안유지 의무를 고지하여야 하며 위법 행위 시 처벌 등이 명시된 영문보안서약서를 징구하여야 한다.

실행지침

- 연구보안관리자와 연구책임자는 외국인 참여연구원이 외부로 반출하는 자료 및 장비는 보안성 검토를 실시한 후 반출하게 하는 등 보안대책을 강구하여야 한다.
- 연구책임자는 외국인 참여연구원으로 하여금 출입증을 반납하게 하고 해당부서에 출입증을 반납하여야 한다.

2.9 외국인 연구원 관리

해당과제	
모든과제	보안과제
	○

이행대상		
연구기관	연구책임자	참여연구원
◎	◎	

2.9.2 보안과제 참여 시 관리

보안과제에 한하여 중요한 연구개발 정보 및 성과물이 해외로 무단 유출되는 보안 사고를 미연에 방지하기 위하여 외국인 연구원 또는 외국기업 참여를 엄격하게 제한하고 있다. 하지만 연구개발 성과를 성공적으로 도출하기 위하여 해외의 우수 연구 인력을 연구과제에 참여시켜야 하는 경우도 발생할 수 있다. 따라서 보안과제에 외국인 연구 인력을 참여시키고자 하는 경우에는 별도의 보안 대책을 강구하여야 한다.

내용

외국인 연구원을 보안과제에 참여시키고자 하는 경우에는 일반과제에서 다루는 외국인 연구원 보안관리 사항을 포함하여 더욱 엄격한 보안관리 체계를 마련하여야 한다. 이를 위해, 보안과제 연구책임자는 외국인 연구원을 과제에 참여시키기 전에 연구기관장의 최종 승인을 받아야 하며 중요한 연구시설 또는 자료나 정보시스템의 접근 권한을 최소한으로 부여하는 등 극도로 제한적인 보안 조치를 수립하고 이행하여야 한다.

실행지침

1. 보안과제 참여 시 사전 승인절차 이행

- 외국인 연구원을 보안과제에 참여시키고자 하는 경우에는 사전에 연구책임자가 연구보안관리자에게 통보하고 연구보안심의회의 심의를 요청하여야 한다.
- 연구보안관리자는 연구보안심의회를 개최하여 심의 결과를 연구기관의 장에 보고하여 최종 승인을 받아야 한다.
- 연구보안관리자는 심의결과를 연구책임자에게 통보하고 연구책임자는 심의결과를 수용하여 외국인 연구원의 보안과제 참여 여부를 결정하여야 한다.

2. 보안과제 참여 외국인 연구원의 추가 보안 조치

- 연구기관의 장은 영문으로 작성된 고용계약서와 보안서약서, 퇴직서약서를 징구해야 하며 서약서에 보안관리 의무와 이를 위반할 경우에 부과되는 징계 및 제재 조치 사항 등을 명시하여야 한다.
- 출입증관리부서는 연구보안관리자와 연구책임자의 사전 승인 후에 연구개발과 직접적인 관련이 있는 시설 또는 지역만 출입할 수 있는 제한적인 출입증을 발급하여야 한다.
- 연구책임자는 외국인 연구원이 연구개발과 무관한 민감한 정보가 저장된 정보시스템 또는 연구 장비로의 접근을 통제하여야 한다.
- 연구보안관리자는 개인용 노트북 또는 휴대용 저장매체, 카메라 등 반입 또는 반출하는 물품을 제한해야 한다.
- 연구책임자는 외국인 연구원에 대하여 다음 사항을 수시로 파악하여 연구보안관리부서에 보고하여야 한다.
  - 연구개발과 무관한 중요시설 출입 및 기술자료 입수 기도 동향
  - 혼자 자주 야근을 하거나 휴일에 자주 출근하는 출퇴근 동향
  - 연구개발과 무관한 국내 과학자 및 외부인사와의 통신연락 또는 접촉 동향
  - 타 기관 방문, 허가된 지역이외의 여행, 출국 예정사항 등 국내체류 동향
  - 기타 보안과제에 해당하는 정보수집 등 연구보안에 위배되는 특이 동향 등

2.10 상시 출입자 및 파견자 관리

해당과제	
모든과제	보안과제
○	

이행대상		
연구기관	연구책임자	연구원
◎	◎	O

2.10.1 상시출입자의 구분 및 관리

건물 내에 주기적으로 출입하지만 임·직원이 아닐 경우 외부인으로 분류하며 연구기관에 상시적으로 출입하는 자와 일시적으로 출입하는 자로 구분된다. 상시적으로 출입하는 인원의 경우 연구정보와 접촉할 기회가 많은 반면 연구기관의 소속이 아니므로 소속감이나 연구정보에 대한 책임의식을 기대하기 힘들다. 따라서 일시적인 출입자와는 구분하여 출입 빈도와 목적에 따라 상시 출입자를 구분하고 관리할 필요가 있다.

내용

- 상시출입자는 재직 중 임·직원 외에 연구기관의 연구과제 수행 또는 기타활동을 하는데 있어서 필요에 의하여 상시적으로 출입하는 자이다.
- 상시출입자의 예는 다음과 같다.
  - 연구개발 용역업체의 임직원
  - 경비 및 청소원
  - 연구시설 및 장비 A/S 업체
  - 운송업체
- 단, 연구개발 용역업체의 임직원은 연구정보와 직접적으로 접촉하게 되므로 기타 상시출입자(경비 및 청소원, 연구시설 및 장비 A/S 업체, 운송업체)와 별도로 구분하여 실행지침을 따르도록 한다.
- 상시출입자를 관리하기 위한 방법으로는 크게 보안지역의 접근을 통제하는 물리적인 통제와 출입 시 연구기관의 승인을 얻는 과정을 거치는 내부규정의 절차에 의한 통제가 있다.

실행지침

· 외부자에 대한 구체적 통제를 가하기 이전에 용역업체, 기타 상시출입자에게 내부규정의 ‘상시출입자 관리’ 항목을 제시하여 연구정보보안의 중요성을 상기시킨다.

1. 연구개발 용역업체 임·직원

① 업체

· 연구기관은 연구개발 용역 업체와 비밀유지 계약 체결을 통하여 출입 인력의 관리와 비밀유지의 책임을 지키도록 한다. 비밀유지 계약서에 포함되는 내용은 다음과 같다.
  - 기관명
  - 출입 인원 수
  - 출입인원에 대한 신원확인 및 관리
  - 비밀의 대상과 범위
  - 비밀유지 의무기간
  - 비밀침해에 대한 법적책임

② 용역업체 인력(개인별)

· 업체와의 계약체결이 완료되면 출입 인원의 각 개인에게 보안서약서를 작성하게 하여 연구보안의 준수 사항을 확실히 주지시킨다.

· 보안서약서에 포함되는 내용은 다음과 같다.
  - 출입시간
  - 출입목적
  - 연구보안에 대한 서약

· 해당부서는 출입증 발급부서에 출입증을 신청하여 용역업체 임·직원에게 이를 발급한다. 상시 출입자의 출입증은 일시 출입증과 구분되도록 하며, 연구기관 외부로 나갈 때에는 기관에 반납하도록 하여 개인이 소지하지 못하도록 한다.

· 사전에 허가된 출입가능지역 외 지역에 접근할 필요가 있을 때는 담당직원과 반드 시 동행하도록 한다.

· 출입 시 출입대장에 출입하는 시간, 목적, 만나는 대상을 직접 기록하도록 하거나 시스템에 의하여 자동으로 연구기관 내에 기록되게 한다. 연구기관은 기록된 사항이 비밀유지계약서 및 비밀유지서약서에 작성된 출입 시간, 인원 수 등의 항목과 일치하는지 확인하도록 하고 위반 시에는 출입을 통제하도록 한다.

· 용역업체가 작성한 비밀유지계약서, 출입대장은 연구기관에서 별도로 보관하여 비밀유지 의무사항을 위반하였을 시 법적 증거 자료로 활용하도록 한다.

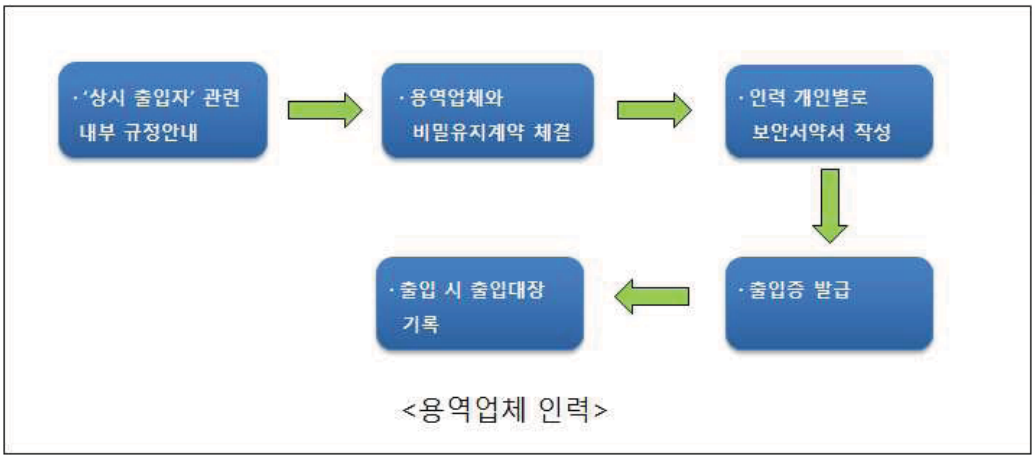
· 연구책임자는 연구과제 수행에 참여하는 용역업체 인원을 파악하여 공동 연구수행 시 연구보안에 각별히 주의하도록 한다.

2. 기타 상시출입자

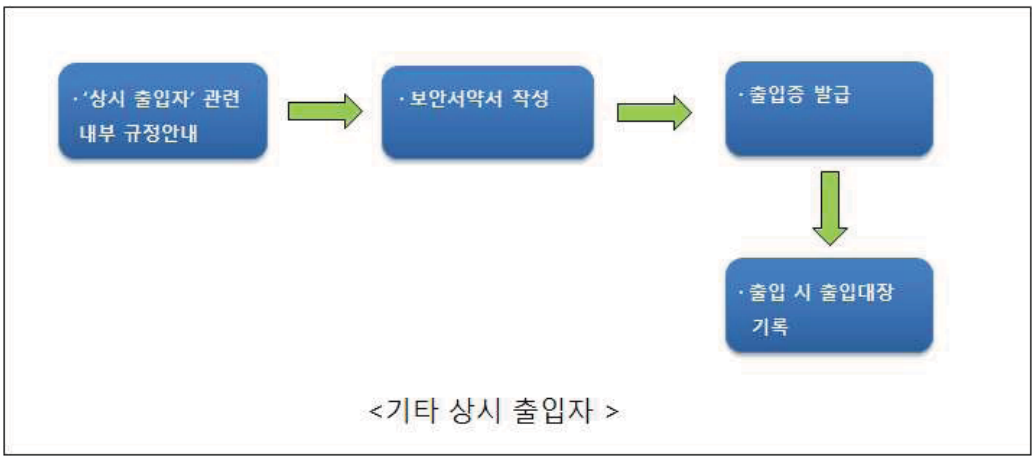
· 개인단위로 수시로 출입하는 자는 고용된 업체의 인력으로써 상시 출입하는 자와 같 이 업체와 계약을 체결하기는 어려우므로 계약서 대신 개별적으로 보안 서약서를 받도록 한다.

· 보안 서약서의 내용에는 출입시간, 출입목적, 비밀대상과 범위, 위반 시 법적 책임을 명시하여야 한다.

· 출입증을 발급하면 반납의 형태로 개인이 소지하는 것을 금지하되 출입 시 출입대장을 작성하도록 한다.



<용역업체 인력>



<기타 상시 출입자 >

2.11 일시 출입자 관리

해당과제	
모든과제	보안과제
○	

이행대상		
연구기관	연구책임자	연구원
◎	◎	O

2.12.1 일시 출입자의 구분 및 관리

출입 빈도와 목적에 따라 일시 출입자를 정의하고 구분한다. 출입이 한시적이라 하더라도 이를 통해 연구정보가 유출될 수 있는 가능성이 있으므로 출입 시 적절한 제한을 가할 필요가 있다

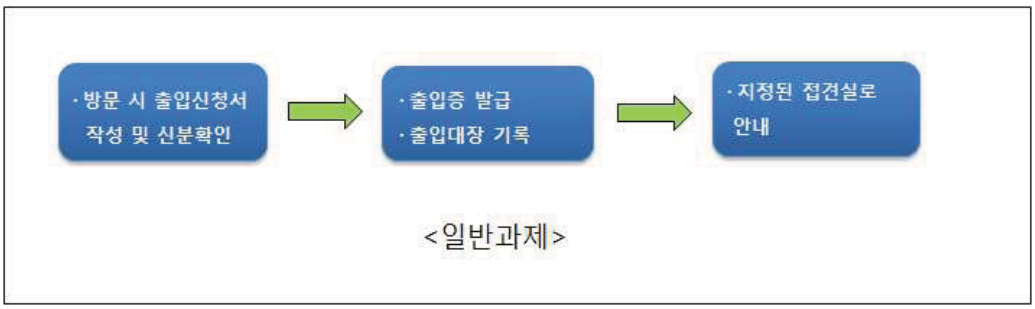
내용

- 일시출입자는 업무적으로 방문하거나 임·직원의 사적인 일로 방문하는 등 연구기관에 일시적으로 방문하는 자를 말한다.
- 상시출입자는 정기적으로 연구기관을 출입하는 반면 일시적인 출입자는 비정기적으 로 방문하기 때문에 출입 시 마다 실행지침의 절차를 따르도록 한다.
- 일시출입자에 의한 연구보안 수단으로 지정 구역만 방문하도록 하는 물리적 통제방법, 출입 시 마다 일련의 과정을 거치도록 하는 절차적 통제방법이 있다.

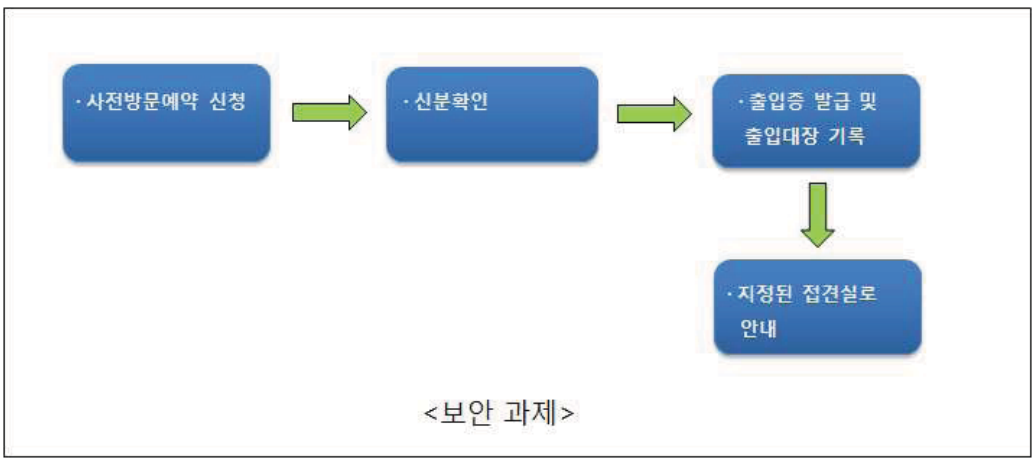
실행지침

- 보안과제와 관련하여 일시출입자가 연구기관에 출입하기 위해서는 사전에 연구기관에 방문 예약을 신청하고 승인을 받을 수 있게 하며 일반과제의 경우 이 절차는 생략하도록 한다.
- 일시출입자가 연구기관을 방문하면 신분을 확인해야 한다. 이 때 신분증이 아닌 명함이나 구두로 신분을 확인하는 것은 신분 위장의 우려가 있으므로 반드시 신분증을 확인하도록 한다. 단, 개인이 아닌 단체로 방문할 경우에는 사전에 방문자의 인적사항을 공문으로 받아 번거로움을 최소화하도록 한다.
- 신분, 방문자 확인이 완료되면 출입자에게 출입증을 발급하며 출입대장에 방문목적, 만나는 임·직원, 그와의 관계, 소속을 등을 기록하도록 한다.

- 모든 승인 절차가 끝난 후 출입 시 휴대폰, 카메라, USB 등 연구정보가 유출될 가능성이 있는 전자기기는 소지할 수 없도록 보안검색을 철저하게 시행해야 한다. 만약 출입자가 반입 금지 품목을 소유했을 경우 기관에서 물품을 접견시간동안 보관하도록 한다.
- 일시출입자는 가능한 한 별도로 마련된 접견실에서만 만나 업무를 처리하도록 한다. *(*해당 연구원은 일시 출입자가 접견실 이외의 연구실이나 실험실 출입이 필요한 경우에는 퇴실 시 까지 동행하도록 하며, 보호구역에는 접근하지 못하도록 통제한다.)*



<일반과제>



<보안 과제>

04

제 3 장
연구개발 결과 및 내용의 관리

1절. 연구개발 정보 관리
3.1 연구결과물 관리
3.2 주요문서 관리

2절. 연구개발 결과 활용
2.3 연구개발 성과의 대외 공개
2.4 국외기술 이전

미래창조과학부
Ministry of Science, ICT and Future Planning

3.1 연구결과물 관리

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	참여연구원
◎	◎	

3.1.1 연구개발 성과물의 권리확보

연구개발 과정에서 창출된 연구개발 성과물은 어떻게 관리하느냐에 따라 기술적·경제적 가치가 크게 달라진다. 즉, 연구개발 성과물을 공개할 경우에는 영업비밀로 보호받지 못함은 물론, 특허 출원 전에 공개하는 경우에는 자신의 연구개발 성과물임에도 불구하고 공지 기술이 되어 특허를 받을 수 없는 예기치 못한 상황이 발생한다. 따라서 연구개발 성과물의 권리를 확보하기 위해서는 특허권, 지식재산권 등의 확보 방안을 수립하여 연구개발 성과물에 대한 보호대책을 수립하여야 한다.

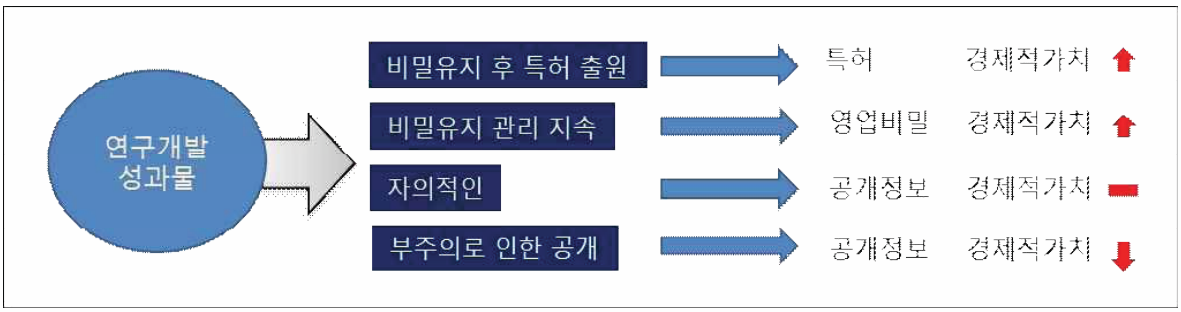
내용

- 연구개발 성과물은 영업비밀로서 철저히 관리되거나, 특허 출원하여 권리를 확보하여야 한다. 특허는 연구개발 결과물을 공개함으로써 독점적 권리를 부여하지만, 영업비밀로 관리하고자 하는 경우에는 연구결과가 공개되면 더 이상 보호를 받을 수 없다.
- 연구기관에서 비밀 정보로 관리하여 외부로 유출 또는 공개될 우려가 없거나, 특허로서 보호의 실익이 크지 않다고 판단되는 경우에는 영업비밀로서 관리하는 것이 유리할 수도 있다.
- 연구개발 성과물의 보호조치 중에는 성과물의 지식재산권 등에 출원하거나 등록하는 방안도 있다. 지식재산권은 문화, 예술, 과학 작품, 산업 활동 등 인간의 지적 창작 활동의 결과로 생기는 모든 무형의 소산물에 대한 권리를 총칭하는 용어로서 두루 IP(Interllectual Property)라는 용어로 통용되고 있다.
- 연구개발 성과물은 지식재산권 등에 출원·등록함으로써 독점권 권리를 인정받을 수 있다. 지식재산권을 확보하게 되면 높은 가격으로 매매하거나 실시료 수입이 가능하기 때문에 그 경제적 가치가 매우 크며, 성과물 보호가 더욱 용이하게 된다.
- 따라서 연구개발 성과물을 어떤 방식으로 보호하는 것이 타당한지에 대하여 특허 관련 전담부서(또는 연구관리부서)와 반드시 사전에 협의하여 가장 적합한 권리 확보 방법 및 보호대책을 결정하여야 한다.

실행지침

1. 연구개발 성과물의 권리 확보 절차 수립

- 연구개발 성과물의 권리를 보호하는 방법(영업비밀, 특허권, 지식재산권 등)을 결정하기 위한 절차를 수립하여야 한다.
- 특허 출원 시 연구개발 성과물은 먼저 연구기관에 신고하고 특허 관련 부서(또는 연구관리부서)에 특허 출원을 의뢰하는 절차를 수립하여야 한다.



- 지식재산권을 출원하거나 등록하고자 하는 경우 연구책임자는 국내 또는 국외에서 출원이나 등록 후 6개월 이내에 지식재산권 출원서 또는 등록신청서와 그 사실을 증명할 수 있는 서류를 연구기관의 장에게 제출하여야 한다. 이때 연구책임자는 참여연구원 등 개인 명의로 출원되지 않도록 유의하여야 한다.
- 국외에서 지식재산권이 등록된 경우에는 등록공보 발간 후 3개월 이내에 등록공보의 사본을 연구기관의 장에게 제출하여야 한다.

2. 연구개발 성과물 관리 전담 부서 설치

- 영업비밀 또는 특허권, 지식재산권 출원·등록으로 연구성과물의 권리를 확보하기 위한 업무를 처리하고 이를 효율적으로 관리하는 지식재산 전담부서를 설치하여야 한다.
- 지식재산 전담부서를 설치할 수 있는 여건이 여의치 않으면 연구관리부서에 지식재산 관리전담 직원을 배치하여야 한다.

3. 연구개발 성과물의 보호 대책 마련

- 영업비밀로 관리되는 연구개발 성과물을 보호하기 위해서는 비밀정보관리 규정이 마련되어야 하며 이를 토대로 비밀유출 방지를 위한 인력 통제와 영업비밀 요건 충족을 위한 문서관리 보호대책을 마련하여야 한다.

실행지침

- 인력 통제는 임직원 입사 시 고용계약서에 비밀유지 의무를 포함하여 서명을 받고 연구과제 수행 전에 비밀유지 양식에 서명을 받아야 한다. 퇴직 시에도 퇴직서약서에 비밀유지 의무를 포함하여 서명을 받아야 하며 제 3자에게 정보를 공개하는 경우에는 비밀유지 협약서를 받아야 한다.
- 연구개발 성과물이 연구보고서로서 비밀 또는 대외비로 분류하여 발간하고자 할 때에는 사전에 배포처를 면밀히 검토하여 그 발간 부수를 최소한으로 하며 연구기관 내에서는 배포하지 아니하고 주관부서에 보관된 것을 열람하도록 조치하여야 한다.

3.1 연구결과물 관리

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	참여연구원
◎		

3.1.2 연구성과물의 보안등급 부여

연구개발과제 선정평가 시 연구개발 선정평가단에서 연구개발 성과물에 대한 기술적·경제적 가치를 미리 평가하여 그에 합당한 보안등급을 부여한다. 하지만 연구개발이 종료된 후 연구개발 성과물의 실질적인 기술적·경제적 가치가 변할 수 있기 때문에 선정평가 시 부여된 보안등급을 연구개발 결과평가단이 재검토하여 그에 적절한 보안등급을 부여하여야 한다.

내용

- 연구개발 성과물에 대한 보안등급을 부여하기 위해서는 먼저 보안등급을 정한 후에 그에 합당한 분류기준을 수립하여야 한다.
- 보안등급과 분류기준이 확정되면 연구개발 성과물에 대한 보안등급을 부여하는 절차를 마련하여야 한다.
- 연구개발 성과물에 대한 보안등급을 부여하는 절차로는 연구개발과제 최종평가 시 연구개발 최종평가단이 성과물에 대한 보안등급을 부여한다.
- 최종평가단은 연구개발 성과물의 보안등급을 선정평가 시에 부여된 보안등급을 부여하거나 연구개발 중에 연구책임자의 요청에 의해 변경된 보안등급을 부여할 수도 있다. 하지만 연구개발 최종평가단이 연구개발 성과물의 기술적·경제적 가치가 변경되었다고 판단되면 보안등급을 재조정하여 부여하여야 한다.
- 연구개발 성과물에 대한 보안등급이 최종 확정되면 그에 합당한 보안조치 사항을 수립하고 지속적으로 관리하여야 한다.

실행지침

1. 연구개발 성과물의 보안등급 분류 기준 수립

· (자체 연구개발과제) 보호조치가 필요한 연구성과물은 자체 「보안업무규정」에 따라 Ⅰ급, Ⅱ급, Ⅲ급 또는 대외비로 보안등급을 정하고 다음과 같이 분류 기준을 수립할 수 있다.

* Ⅰ급 비밀
  누설 시 국가안전보장 및 국가 방위상 위협을 초래하거나 과학기술개발을 위태롭게 하는 등의 우려가 있다고 판단되는 비밀
* Ⅱ급 비밀
  누설 시 국가안전보장 및 연구기관 경영에 막대한 지장을 초래할 우려가 있거나 과학기술개발에 막대한 지장을 초래할 우려가 있는 비밀
* Ⅲ급 비밀
  누설 시 국익에 손해를 끼칠 우려가 있거나 연구기관 경영 및 연구사업 수행에 상당한 손실을 끼칠 우려가 있는 비밀
* 연구대외비
  연구 비밀에 속하지 않으나 누설될 경우 연구기관에 손해 또는 불이익을 끼칠 우려가 있는 사항

· (국가연구개발과제) 연구성과물은 「국가연구개발사업의관리등에관한규정」 제24조의5(분류절차)에 의거하여 보안과제와 일반과제로 보안등급을 정하고 그에 따른 분류 기준은 다음과 같이 적용하여야 한다.

[보안과제 및 일반과제 분류 기준]

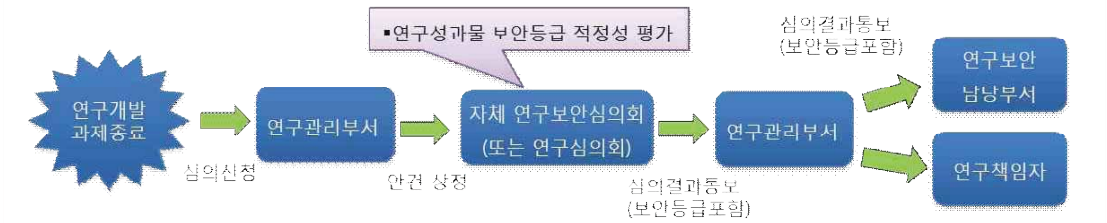
* 보안과제: 연구개발결과물 등이 외부로 유출될 경우 기술적·재산적 가치에 상당한 손실이 예상되어 보안조치가 필요한 경우로서 다음 항목에 해당하는 과제
  - 세계 초일류 기술제품의 개발과 관련되는 연구개발과제
  - 외국에서 기술이전을 거부하여 국산화를 추진 중인 기술 또는 미래핵심기술로서 보호의 필요성이 인정되는 연구개발과제
  - 「산업기술의 유출방지 및 보호에 관한 법률」 제2조제2호의 국가핵심기술과 관련된 연구개발과제
  - 「대외무역법」 제19조제1항 및 같은 법 시행령 제32조의2에 따른 수출허가 등의 제한이 필요한 기술과 관련된 연구개발과제
* 일반과제: 보안과제로 지정되지 아니한 과제

실행지침

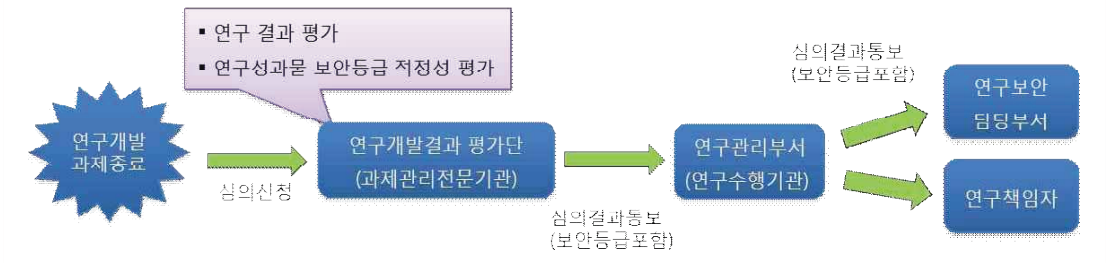
2. 연구성과물의 보안등급 부여 절차 수립

- (자체 연구개발과제) 연구성과물의 보안등급은 연구개발과제 선정 시 자체 「연구심의회」에서 부여한 보안등급 또는 개발 중에 변경된 보안등급을 부여하는 것을 원칙으로 한다.
- (자체 연구개발과제) 연구개발과제 최종평가 시 「연구심의회」에서 연구개발 성과물에 대한 기존 보안등급의 적정성을 검토하여야 하며 기존 보안등급이 적합하지 않다고 판단되는 경우에는 보안등급을 변경할 수 있다.
- (국가연구개발과제) 연구성과물의 보안등급은 연구개발과제 선정 시 「연구개발선정평가단」에서 부여한 보안등급 또는 개발 중에 변경된 보안등급을 특별한 사항이 없는 경우에 기존 등급을 부여한다.
- (국가연구개발과제) 연구개발과제 최종평가 시 「연구개발결과 평가단」이 연구개발 성과물에 대한 기존 보안등급의 적정성을 검토하여야 하며 기존 보안등급이 적합하지 않다고 판단되는 경우에는 보안등급을 변경할 수 있다.

※「국가연구개발사업관리등에관한규정」 제24조의8(연구개발결과의 보안등급) 절차 준수



[자체 연구개발과제 성과물 보안등급 부여 절차]



[국가연구개발과제 성과물 보안등급 부여 절차]

실행지침

3. 보안등급별 보안 대책 수립

- (자체 연구개발과제) 연구성과물의 보안등급에 따른 보안대책은 연구기관 자체에서 규정한 「연구보안관리규정」에 명시하여야 한다.
- (국가연구개발과제) 연구성과물의 보안등급에 따른 보안대책은 「국가연구개발사업의 관리 등에 관한 규정」을 준수하여 수립하여야 한다.
  ① 연구수행 단계별 특허권, 지식재산권 확보 방안과 주요 연구자료 및 성과물의 무단 유출방지를 위한 보안대책을 마련하고 시행하여야 한다.
  ② 연구기관의 장은 보안과제의 연구성과물에 대한 기술 실시 계약 또는 사용 계약 시 “제 3자 기술 실시권 또는 사용권 금지 협약”을 체결하여야 한다.

3.1 연구결과물 관리

해당과제	
모든과제	보안과제
	O

이행대상		
연구기관	연구책임자	참여연구원
◎	◎	

3.1.3 외부기관과 공동협약 시 연구결과물의 관리

보안과제 연구책임자는 연구개발 결과의 목표를 달성하고 연구성과물의 완성도를 높이기 위하여 외부 기관 또는 연구소와 공동연구를 진행해야 하는 경우가 발생할 수 있다. 이 때 보안과제 연구책임자는 공동연구를 위한 협약 체결 전에 연구결과물의 귀속 및 관리에 관한 사전 보안대책을 마련한 후에 협약을 체결하여야 한다.

내용

- 공동협약이란 복수의 연구개발주체가 동일한 연구개발과제를 수행하기 위해 소요되는 연구개발비·인력·기자재·정보 등 연구 자원을 공동으로 부담하여 수행하는 것을 목적으로 계약 체결하는 것을 의미한다.
- 연구 결과물은 유형적 결과물(시제품, 기자재 등)과 무형적 결과물(특허, 영업비밀 등)으로 구분할 수 있으며 이에 따라 소유 기준을 명확하게 수립해야 한다.
- 보안과제의 공동연구에 의한 결과물은 유형적 결과물(시제품, 기자재 등)과 무형적 결과물(특허, 영업비밀 등)로 구분하여 이에 대한 소유 기준을 구체적으로 명확하게 수립하여 협약 시 반영해야 한다. 이를 통해, 연구결과물이 보안과제 책임자의 의사와 관계없이 오·남용되는 사태를 미연에 방지하고 향후 법적인 문제가 발생하더라도 증거자료로 활용할 수 있다.

실행지침

1. 보안과제 연구결과물의 소유 기준 정립

- 유형적 결과물(시제품, 기자재 등)
  - 주관연구기관의 소유로 하되, 공동연구기관이 소유의 조건으로 부담한 것은 공동연구기관의 소유로 할 수 있다.
- 무형적 결과물(특허권, 지식재산권, 영업비밀 등)
  - 주관연구기관 단독 소유를 원칙으로 한다.
  - 공동 연구기관이 자체개발 또는 주도적으로 개발한 경우에는 주관연구기관과의 협상에 의해 공동으로 소유할 수도 있다. 단, 이 경우에는 소속 중앙행정기관의 장과 국가정보원장의 사전 승인 심사를 거쳐야 한다.
- 다음 사항에 해당하는 경우 협약에서 정하는 바에 따라 국가에서 소유할 수도 있다.
  - 국가 안보상 필요한 경우
  - 공익적 목적에 활용하기 위해 필요한 경우
  - 연구결과물을 소유하게 될 기관이 외국에 있는 경우
  - 기타 주관연구기관 또는 공동연구기관이 소유하기에 부적합하다고 판단되는 경우

2. 보안과제 연구결과물의 관리 기준 수립

- 국가연구개발사업으로 수행한 연구결과물에 대한 특허권은 연구책임자 또는 참여연구원 등 개인 명의로 출원·등록해서는 안 되며 주관연구기관명으로 등록하여야 한다.
- 연구결과물 기술 실시(사용) 계약 시 제3자 기술 실시(사용권)를 금지하여야 한다.
- 공동연구기관은 연구개발 관련 정보 및 성과물에 대한 비밀을 유지하여야 한다.
- 연구개발 중단 시 모든 연구개발 산출물은 주관연구기관의 소유로 하여야 한다.
- 공동연구기관이 계약을 위반한 사실을 인지한 경우에 민·형사상 책임과 더불어 손해배상을 청구하여야 한다.

3.1 연구결과물 관리

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	참여연구원
◎		

3.1.4 연구개발 성과물의 활용

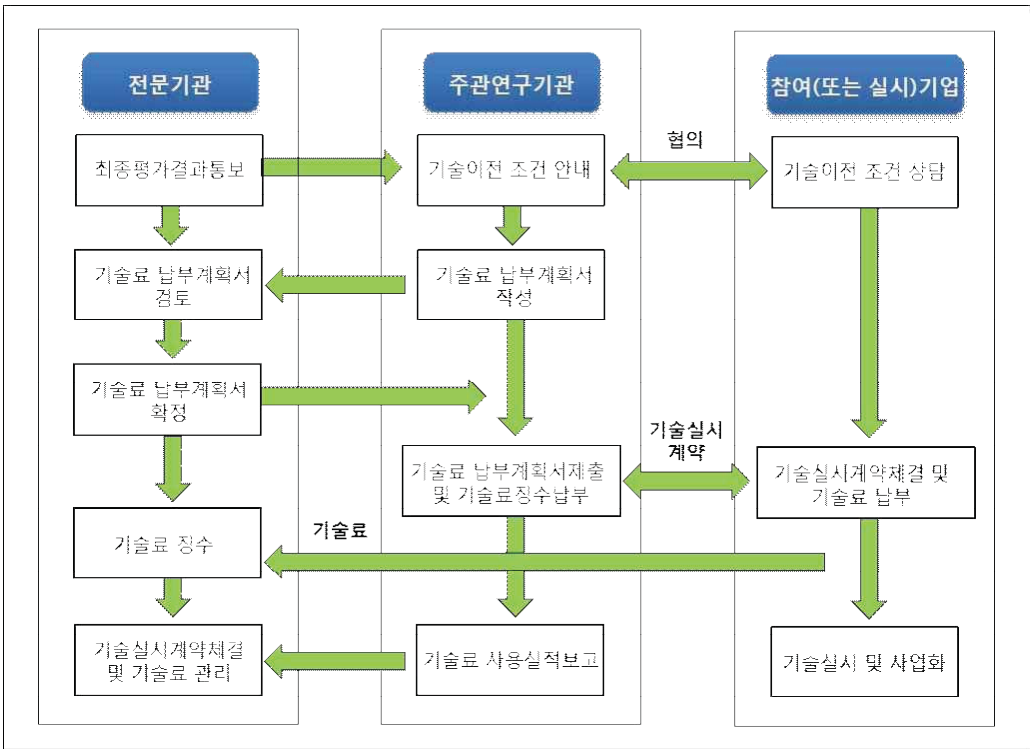
연구개발 성과물 소유기관의 장 또는 전문기관의 장은 연구개발 성과가 널리 활용될 수 있도록 실시권자와 기술실시계약을 체결하는 등 연구개발 성과물을 활용하는데 필요한 조치를 취해야 한다. 다만, 기술실시계약을 체결하는 경우 연구보안사고에 따른 피해를 방지하기 위하여 보안조치 사항이 누락되지 않도록 성과물 활용기준을 마련해야 하며 계약체결 대상자도 신중하게 고려하여야 한다.

내용

- 연구개발 성과물이란 연구개발을 통하여 창출되는 특허·논문 등 과학기술적 성과와 유·무형의 경제·사회·문화적 성과를 총칭한다.
- 기술실시계약이란 연구기관이 소유하고 있거나 그 사용 권리를 보유하고 있는 연구결과 또는 기술(지적재산권 포함)에 대해 교육지도 또는 현장지도를 통하거나 기술자료를 제공하여 실시자에게 실시권을 허여하는 계약을 말한다.
- 기술실시계약을 체결하는 절차와 보안조치 사항은 다음과 같다.
  - (사전협의) 연구기관의 기술에 대해 외부의 제3자(이하 ‘실시예정자’라 함)가 사용, 활용 및 기업화 요청이 있을 경우 연구관리담당부서는 당해 연구책임자 또는 당해 기술 관련자와 함께 실시예정자와 접촉하여 실용화 가능성에 대해 조사·검토하고 의견을 청취한다.
  - (계약의뢰) 연구책임자 및 연구관리부서장은 사전협의 시 실시예정자와 기술의 수준과 단계, 제품의 시장 및 경제성, 활용의 난이성, 기술실시 및 훈련의 범위, 적정 기술실시료(이하 “실시료”라 한다) 수준 등을 협의하고, 실시예정자의 사업 및 경영능력, 의욕 등을 판단하여 성공적인 실용화가 가능하다고 판단되는 경우에만 기술실시계약 체결을 연구관리담당부서에 의뢰한다.

내용

- (계약검토) 연구관리담당부서는 접수된 기술실시계약 체결 요청서를 검토한 후 정부, 출연기관 또는 해당 지적재산권의 공유지분을 갖는 기관(이하 “관계기관” 이라 한다)과 사전 협의 또는 동의가 필요한 경우에는 관계기관의 동의를 받아 계약을 추진한다. 연구관리담당부서는 실시예정자와 계약조건을 협의하는 것을 원칙으로 하되 특별한 사항이 있을 경우 원장의 승인을 받아 확정한다. 실시예정자가 다수일 경우에는 국내 법인을 우선 실시 대상자로 하고 대상 업체의 경영능력(기술능력, 재무능력)을 평가하여 연구책임자의 의견 또는 연구심의회의 심의를 거쳐 실시자를 확정한다.
- (계약체결) 연구관리담당부서는 실시자와 연구 성과 활용을 위한 기술실시계약 및 기술료 납부에 대한 협의를 추진하고 기술실시계약서 및 기술료 납부계획서를 작성하여 연구기관장의 승인을 득한 후 전문기관의 장에게 제출한다. 또한, 보안사고 및 오·남용을 미연에 방지하기 위하여 기술실시 계약서[별첨 3.1.4 참조]에 계약체결 대상자를 비롯하여 기술실시 사용권에 제한을 두어야 한다.
- (체결통보) 연구관리담당부서장은 실시자와 기술실시 계약이 체결되면 이러한 사실을 관련 부서에 통보하여야 한다. 또한, 관련 과제에 따라 전문기관 또는 소속 중앙행정기관 등에 보고가 필요한 경우에는 해당기관에도 통보해야 한다.



[기술실시 계약 체결 절차]

실행지침

1. 기술실시계약 대상자 선정 기준 마련

- 출원 중인 지식재산권을 포함한 연구개발 결과물을 대상으로 기술실시계약을 체결하고자 하는 경우 참여기업 외의 자와 기술실시계약을 하려는 때에는 국내의 기술실시 능력이 있는 중소기업을 우선적으로 고려하여야 한다.
- 참여기업이 있는 경우 연구개발 성과물에 대해서는 참여기업이 실시하는 것을 원칙으로 한다. 다만, 다음과 같은 경우에는 참여기업이외 다른 기업이 실시할 수 있다.
  ① 연구개발 성과물이 일반에 공개하여 활용할 목적으로 개발된 경우
  ② 다른 기업이 실시하는 것을 참여기업이 동의한 경우
  ③ 참여기업이 연구개발과제 종료 후 1년 이내 실시계약을 체결하지 않는 경우
  ④ 참여기업이 약정한 기술료를 1년 이상 납부하지 아니한 경우
  ⑤ 참여기업이 기술실시계약 체결 후 성과물을 활용하는 사업을 정당한 이유 없이 1년 이내에 시작하지 아니하거나 그 사업을 1년 이상 쉬는 경우
  ⑥ 그 밖에 중앙행정기관의 장이 참여기업 외의 자가 실시할 필요가 있다고 인정한 경우

2. 연구개발 성과물의 양도

- 연구개발 성과물 소유기관의 장 또는 전문기관의 장은 등록된 지식재산권에 대하여 기술실시계약이 체결되지 않을 것이라고 판단되는 사유가 있는 경우에는 전문기관의 장 또는 중앙행정기관의 장의 승인을 받아 등록된 지식재산권을 적정한 기관에 양도할 수 있다.

3. 보안과제 성과물의 기술실시 계약

- 보안과제인 경우에는 연구성과물 기술실시(사용) 계약 시 “제3자 기술 실시(사용)권 금지 협약”을 체결해야 한다.

4. 계약 해지 시 보안조치

- 기술실시 계약 해지 시 기술실시 계약과 관련하여 해지 시까지 취득한 제반 자료를 회수하고 사후 연구결과 비밀누설방지 등 보안조치를 철저히 이행하여야 한다.
- 기술실시 계약 해지 이후 실시자는 그 승계인 또는 연구기관의 허락 없이 동 기술을 사용하지 않도록 조치하여야 한다.

3.2 주요문서관리

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	연구원
O	◎	

3.2.1 문서생성

연구를 수행하는 과정에서 많은 문서가 생성되며 여기에는 연구와 관련된 중요한 정보들이 다량 포함되어있는 경우가 허다하다. 따라서 문서 형태로 연구정보 외부로 유출되는 사고도 종종 발생하기 때문에 이러한 중요한 문서가 외부에 누설, 유출, 훼손되는 것을 방지하고 원래의 목적대로 사용할 수 있도록 초기 문서생성단계부터 관리를 강화할 필요가 있다.

내용

- 문서란 의사소통을 위해 고안된 정보를 물리적으로 묶어 놓은 것으로 일반적으로 종이류를 일컫는다. 하지만 정보를 기록하는 매개체의 기술적인 발전에 따라서 다양한 형태로 정보를 기록할 수 있게 되었다. 따라서 연구원들이 작성한 연구결과 및 연구 관련 정보가 기록된 것이라면 종이뿐 만이 아닌 물리적이고 전자적인 형태의 정보자산 또한 포함하는 것이 필요하다. 그 예는 다음과 같다.
  - 출력물
  - 녹음/ 녹화 테이프
  - 차트, 메모
  - 도면, 그림 및 사진
  - 파일

단, 여기서의 문서는 연구 성과물을 제외한 연구노트, 회의록 등 연구정보와 관련된 자료들로 한정한다.

•문서의 생성
- 문서는 연구정보 관련 내용을 형상화, 가시화하는 것까지를 포함하는 것으로 정의 한다.

•보안등급 기준
- 주요문서에 한해서 등급을 결정
- Ⅰ급 비밀(극비), Ⅱ급 비밀, 연구대외비, 일반문서 (3.1.2 연구성과물의 보안등급 부여 참고)

•보안등급의 표시
- 보안 등급의 표시는 분류된 비밀을 외견상 식별할 수 있도록 표시하는 것을 말한다. 표시 목적은 정보를 관리 또는 사용하는 자에게 사용보호와 취급방법을 쉽고 명확하게 소통하기 위함에 있다.
- 이를 통해, 중요한 정보는 신중하게 취급하고 비인가자에게는 경고하여 접근을 통제할 수 있다. 따라서 보안등급은 연구기관 내에서 뿐만 아니라 사업관계가 있는 외부 기업, 협력업체 등과도 원활하고 명확한 소통이 가능하도록 표시방법을 결정하여야 한다.

실행지침

- 중요한 연구 관련 내용이 포함된 문서를 과잉 생산할 경우, 유출될 가능성이 높아지므로 현재 필요한 최소한의 양만 생산하여야 한다.
- 연구기관 내에서 산출되는 모든 문서에는 보안등급을 부여하여야 한다.
- 연구 책임자의 판단 하에 연구핵심 내용과 관련되어있어 보호가 필요하다고 판단되는 모든 문서는 외부로 유출되지 않도록 특별 관리하여야 한다.
- 보안등급은 내용의 가치에 따라 적정하게 분류하되 과대평가나 과소평가를 하여서는 아니 된다. 과대 분류는 과다한 보호로 업무가 가중되거나 필요 없는 제한으로 업무의 지장을 초래하고, 과소분류는 연구정보 보호의 관리소홀로 정보가 유출될 우려가 있다.
- 보안등급 부여 시 관련문서와 연관 지어 추정 분류하여서는 아니 되며 각 문서에 포함된 연구정보의 내용과 가치에 따라 독립적으로 분류해야 한다.

1. 보안문서의 등급분류 기준 수립

* Ⅰ급 비밀(극비)
  - 국외 유출 또는 누설될 경우 국가이익에 심각한 손실을 초래할 수 있는 문건(국내외 미공개 기술정보, 국가 산업경쟁력에 절대적 영향을 미치는 정보, 국외 동종업계에 절대적 우위를 확보할 수 있는 정보 등)

* Ⅱ급 비밀
  - 국외로 유출 또는 누설 될 경우 국가의 기술발전에 지장을 초래하거나 경제적 손실을 가져올 수 있는 문건(국외 동종업계에 상대적 우위를 확보할 수 있는 정보, 장기전략에 관한 주요 정보, 주요 분석 자료 등)

* 대외비
  - 연구 비밀에 속하지 않으나 누설될 경우 간접적으로 손실을 초래할 수 있는 문건(1,2급 비밀 이외 주요 정보, 관련자 이외 공개가 제한되는 정보 등)

* 일반 문서
  - 일반문서의 공개범위는 과제참여 최소단위, 연구과제 전체 참여인원, 기관내부 전체로 구분된다.

2. 보안등급의 지정

- Ⅰ급 비밀 지정 시 연구책임자가 비밀등급을 신청하면 연구보안담당부서에서 연구보안심의회에 심의 요청한 후 그 결과를 연구기관의 장에게 보고한 후 승인을 받아 보안등급을 지정한다.
- Ⅰ급 비밀 외의 등급은 연구책임자의 판단 하에 자율적으로 지정하도록 한다.

3. 보안문서의 등급 표시

- 문서의 등급 표기는 문서를 보호하기 위한 취급 수준을 결정하는 것이므로 모든 문서는 보안등급을 쉽게 식별할 수 있도록 표기해야 한다.
- 외부기관과도 원활하고 명확한 소통이 가능하도록 표준화된 라벨을 사용하여야 한다. 문서의 형태에 따라 연구기관에서는 다음과 같은 방법으로 표기하여야 한다.
  - 비밀문서 보관 봉투
  - 도장 또는 스탬프
  - 문서작성기의 머리글/바닥글 기능
  - 전자문서 출력/다운로드 시 워터마크 기능 활용
  - 비밀등급을 알리는 내용 녹음

3.2 주요문서관리

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	연구원
O	◎	

3.2.2 문서 활용

연구개발과정에서 생성되는 문서를 활용하는 과정에서 필요에 의해 열람되거나 외부로 배포 또는 발송되는 등의 행위가 이루어진다. 중요한 연구정보가 보안성을 검토하는 절차 없이 외부에 공개되면 심각한 문제를 초래할 수 있으므로 각 상황에 적절한 절차를 마련하고 이행하여야 한다.

내용

· 연구기관 내 문서를 활용하는 방법에는 문서의 열람, 문서의 복제· 복사, 문서의 인수인계 등이 있다.
  - 열람 : 비밀문서를 취급하는 방법으로써 구체적인 비밀의 내용을 보고, 듣고 읽는 행위 등이 포함
  - 복제 및 복사 : 비밀의 일부 또는 전부를 재현하는 행위
  - 인수인계 : 비밀문서 담당자의 인사이동으로 인한 문서의 인수인계
  - 전자문서의 2차적 활용

실행지침

1. 열람

· 문서보관책임자는 자신이 보관하고 있는 비밀문서를 업무상 열람시키는 경우 비밀관리기록부에 열람자를 기록한 후 열람하게 하여야한다.

· 비밀문서에 접근권한이 있는 모든 임직원은 어떠한 방법으로 열람하든 “비밀열람기록부”에 본인의 서명을 해야 되고, 이 기록은 해당 비밀이 파기된 후라도 상당기간 보존할 필요가 있다.

- 비밀열람기록부는 각 비밀에 대한 열람자 범위를 파악하기 위하여 각 비밀문서 뒷면에 첨부한다.
- 보관책임자는 자신이 보관하고 있는 비밀을 업무상 열람시키는 경우 비밀관리 기록부에 열람지를 기록한 후 열람하게 하여야한다.
- 비밀열람기록부는 비밀을 생산(작성)한 부서(팀)에서 작성하여 첨부하여야 한다.
- 비밀열람기록부는 그 비밀을 파기하는 경우에는 그 비밀문서에서 분리하여 별도로 보관하여야 한다.

2. 복제 및 복사

- 문서의 복제 및 복사는 실무에서 비밀이 누설되는 가장 흔한 방법이므로 비밀문서는 가능한 한 보관책임자의 철저한 통제 하에 일반 취급자들이 비밀문서를 복사하는 것을 제한하는 것이 중요하다.
- 비밀문서에 접근 권한이 있는 임직원이라고 하더라도 필요에 의해 비밀문서를 복사하고자 하는 경우에는 보관책임자의 승인 하에 이러한 사실을 열람기록부에 기록한 후 복사할 수 있도록 허용하여야 한다.

3. 인수인계

- 부서(팀)내 비밀문서를 담당하는 관리책임자의 전보 또는 퇴직 등으로 인한 인사이동이 발생할 경우에는 부서(팀)내 후임자에게 인수인계하고 보안문서를 생성한 부서(팀)가 해체되는 경우에는 인수부서(팀)에 비밀문서를 인계하여야 한다.
- 보안문서를 인수할 부서(팀)가 없거나 불분명할 때에는 비밀문서는 모두 파기하여야 한다.

4. 전자파일 활용 시

전자파일 형태로 연구 관련 정보가 업무용 PC나 전자기기에 저장되어 있는 경우 파일의 2차적 활용 제한 여부를 표기해야 한다.

- 인쇄 금지 여부
- 인쇄 후 파기 여부
- 인쇄 후 삭제 여부
- 파일의 전자적 송수신 가능 여부

3.2 주요문서관리

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	연구원
O	◎	

3.2.3 문서 보관

주요문서를 보관한다는 것은 기밀을 보호하는 데 있어서 중요한 수단중의 하나로 화재, 도난 또는 파괴로부터 보호하고 비인가자의 접근을 방지해야 한다.

내용

•보관과 보존

- 보관이라 함은 문서의 처리 완결 후부터 보존되기 전까지의 관리를 의미하며 보통 문서가 생성된 연도의 말일까지 문서를 관리하는 것을 말한다.
- 보존이라 함은 보관이 끝난 문서를 소정의 보존 기간에 따라 관리하는 것을 의미한다.

•보관 주체

- 문서의 보관 주체는 문서가 생성된 부서가 보관하는 방법과 연구기관에서 보관하는 방법으로 구분된다.

•보관 장소 및 보호 장치

- 주요 문서가 보관되는 장소는 외부 노출이 잦지 않은 곳이어야 하며 유출, 도난 등을 방지할 수 있는 보호 장치가 별도로 마련되어야 한다.

•보존 기한

- 주요 문서를 보존할 때는 그 기한을 정하여 중요도가 높고 장기간 보존되어야 할 문서가 파기되어버리거나, 중요도가 낮고 장기간 필요하지 않은 문서가 지속적으로 보존되어 업무의 효율성이 떨어지는 일이 발생하는 것을 방지해야 한다. 내부 상황을 고려하여 문서 보존 기한은 자율적으로 정하되 기한은 반드시 명시하도록 한다.

• 문서보존기간 변경

· 문서관리책임자는 매년 규정에 의하여 보존기간이 정하여진 문서를 검토하고 정세 및 환경의 변화로 인하여 문서 보존 기간을 연장 또는 단축할 필요가 발생할 수도 있다. 이때에는 연구기관 장의 승인을 받아 그 기간을 연장 또는 단축할 수 있도록 한다.

•문서관리 기록부

· 문서관리기록부는 문서의 작성, 접수, 보안등급, 이관 등 연구기관이 보관하고 있는 일체의 문서 현황을 관리하고 유지하는 문서관리대장이다.

실행지침

1. 문서 보관 주체

· 문서보관 주체는 문서를 생성한 해당 부서에서 보관하는 방법과 연구기관에서 통합적으로 보관하는 방법이 있다. 이 기준은 문서의 보안등급과 포함하고 있는 연구핵심내용의 양에 따라 결정되어야 한다.

① 연구기관 보관 (통합 보관)

· 연구기관에서 보관하는 경우 지정된 보관관리책임자가 존재하고 보호 장비가 설치 된 안전한 장소에서 보관되므로 부서에서 보관하는 것보다 정보의 유출 위험이 상대적으로 감소하는 장점이 있다.

· 또한, 문서관리기록부에 의해 문서보관 현황을 쉽게 파악할 수 있으므로 중요도가 높은 문서의 보관 방법에 적합하다.

· 모든 주요 문서를 연구기관의 관리 하에 보관하는 것은 활용 시 절차가 복잡하여 업무의 효율성이 떨어지므로 연구기관에서 보관해야 하는 문서 대상은 Ⅰ급, Ⅱ급 비밀의 등급을 판정받은 문서로 한정하는 것이 적합하다.

② 부서(개인) 보관

· Ⅰ,Ⅱ급 비밀 등급을 제외한 대외비, 내부공유 등급의 문서들은 관련 부서 내에서 연구책임자 혹은 문서를 생성한 개인이 보관하도록 한다.

2. 보관 장소 및 보호 장치

① 연구기관 보관 (통합 보관)

- 연구기관에서 보관해야 하는 문서는 Ⅰ,Ⅱ급의 중요도가 높은 문서들로 보관의 장소의 선택이 아주 중요하다. 외부에 많이 노출되는 장소는 피하고 가급적 연구기관 내 비인가자외 출입이 통제된 보호구역에 보관해야 한다.
- 보호구역에 보관하는 것 외에 보안장치를 별도로 설치하여 비밀문서를 보다 안전하게 보관할 수도 있다.(예: 카드리더기, 지문인식기, 홍채인식기. CCTV 등) 단, 보안문서의 중요도를 고려하여 유연하게 보안장치를 설치하여 불필요한 번거로움을 줄여야 한다.

② 부서 보관

대외비를 포함하여 일반문서는 문서를 생성한 부서 또는 개인이 보관할 수 있도록 조치해야 하며 특히, 대외비인 경우에는 허술한 관리로 인한 정보 유출 사고가 발생하지 않도록 이중 시건장치가 있는 보관함에 보관하여야 한다.

3. 문서 관리 기록부

- 생성된 주요 문서들을 보관할 때는 연구기관에서 문서관리 기록부를 별도 마련하여 문서보관 현황을 파악하여야 한다.
- 문서관리 기록부에 기재할 항목은 관리번호, 문서번호, 보안등급, 문서형태, 보관장소, 보존기한, 파기여부, 파기날짜 등을 포함하여 문서 현황을 한눈에 파악할 수 있도록 해야 한다.

문서번호	보안등급	문서형태	보관장소	보존기한	파기여부	파기날짜

3.2 주요문서관리

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	연구원
O	◎	

3.2.3 문서 파기

보존 기한이 초과되었거나 보존할 가치가 없는 문서들을 파기할 때에도 정보유출의 가능성을 염두에 두어야 한다. 문서가 제대로 파기되지 않은 채 외부로 유출될 경우 외부인이 문서에 포함된 중요한 정보를 습득할 수 있기 때문이다. 따라서 문서를 파기할 때에도 세부 규정과 절차를 마련하여 이를 이행하여야 한다.

내용

- **문서 파기**
  - 문서 보존 시 명시된 기한에 따라 파기 예고일이 도래하였을 때 문서의 파기를 결정한다. 단, 업무상 계속 참조할 필요가 있는 문서는 파기 시기가 도래한 경우라도 재분류하여 파기 일을 연장하여야 한다.
  - 파기 예고일 이전이라도 정기적인 점검을 통하여 보존 가치가 없는 문서는 파기하여야 한다. 그 예는 다음과 같다
    - 보안문서가 등급분류 시의 중요도에 비해 현저히 저하되어 현 시점에서 더 이상 보존할 가치가 없거나 이미 보편화된 기술 정보인 경우
    - 보안문서가 합법 또는 불법적으로 외부에 유출되었거나 유사기술 또는 비밀이 타사에 의해 공개되어 가치가 저하된 경우
    - 해당 문서에 포함된 연구정보가 특허로 등록되어 외부에 공개된 경우

실행지침

1. 파기방법

① 종이류 문서 (출력물, 메모, 사진, 도면 등)

- 종이 문서들은 보안상 안전한 곳에 지정된 폐기함에 모아 담당자가 주기적으로 세단기를 이용하여 파쇄하거나 소각하여 문서의 복구가 불가능하도록 조치하여야 한다.
- 전문 폐기업체에 문서 파기를 의뢰하는 경우 담당자가 문서를 파기하는 과정을 참관하여야 한다.
- 개인적으로 보관하고 있는 문서는 세절기를 이용하여 완전히 파쇄하도록 한다.

② 녹음, 녹화테이프

- 정보를 삭제 또는 복구가 불가능하도록 포맷을 하거나 물리적으로 파괴하여 정보를 복구할 수 없도록 조치하여야 한다.

③ 파일

- 전자 문서인 경우 여러 차례의 포맷 또는 영구삭제 프로그램을 이용하여 복원이 불가하도록 삭제하여야 한다.

2. 파기 절차

① 연구기관 보존 문서

- 파기 예고일이 도래한 비밀문서는 도래 시점에 파기를 검토한다.
- 파기가 결정된 문서는 담당자(또는 기관)가 위에 명시된 파기 방법대로 문서를 폐기하여야 한다.
- 파기가 완료된 문서에 대하여 문서관리 기록부에 파기여부를 체크하고 현황을 관리하여야 한다.

② 부서(개인) 보존 문서

- 부서 보존 문서도 내부규정에 따라 보존 기한을 지켜야 하며 문서 파기 시점이 도래하면 부서장은 부서 담당자에게 통보하여 위에 명시된 파기 방법대로 문서를 폐기하여야 한다.

3.3 연구개발 성과의 대외공개

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	참여연구원
O	◎	○

3.3.1 연구개발 성과물의 대외공개 시 관리

연구개발 성과물을 대외적으로 공개하고자 하는 경우에는 공개하는 정보나 외부에 제공하는 자료가 보안상 문제가 없는지 내부적으로 확인하기 위한 검증절차를 수립하고 그 결과에 따라 연구개발 성과물의 공개여부를 결정하여야 한다.

내용

· 연구개발과제에 참여하고 있는 연구원들은 연구개발 성과를 어떠한 보안성 검증도 없이 세미나 또는 학회에 발표하는 사례가 너무나 많이 발생하고 있는 실정이다, 또한, 홈페이지와 게시판 등에 연구개발 성과물을 게재할 때도 별도의 보안성 검토 절차를 무시하는 경우도 허다하다. 이와 같이 보안성 검토를 거치지 않고 연구개발 성과물을 외부에 공개하는 행위는 연구개발 정보를 외부에 무단으로 유출하는 행위와 흡사하다고 할 수 있으며 이 또한 엄밀하게 얘기하면 연구보안 사고에 해당된다고 말할 수 있다. 따라서 연구개발 성과물을 보유하고 있는 연구기관의 장은 연구성과물을 대외로 공개하기 전에 연구개발 성과물에 대한 보안성 검토를 진행하는 절차를 수립하여 자체 연구보안관리 규정에 반영하여야 한다. 이를 통해 연구개발 성과물을 보유하고 있는 해당 부서나 참여연구원은 대외적으로 연구개발 성과물을 공개하거나 외부 기관에 자료를 제공하기 전에 반드시 연구개발 성과물을 외부에 공개하여도 기술적·경제적으로 심각한 손해를 초래하지는 않는지에 대한 여부를 검증하는 절차가 필요하다. 이와 더불어 대외에 공개해서는 안 되는 비공개 정보는 무엇인지 사전에 기준을 수립하고 그에 따라 비공개 기간은 얼마동안 설정하여야 되는지를 연구보안관리 규정 또는 지침에 명확하게 명시하여야 한다.

실행지침

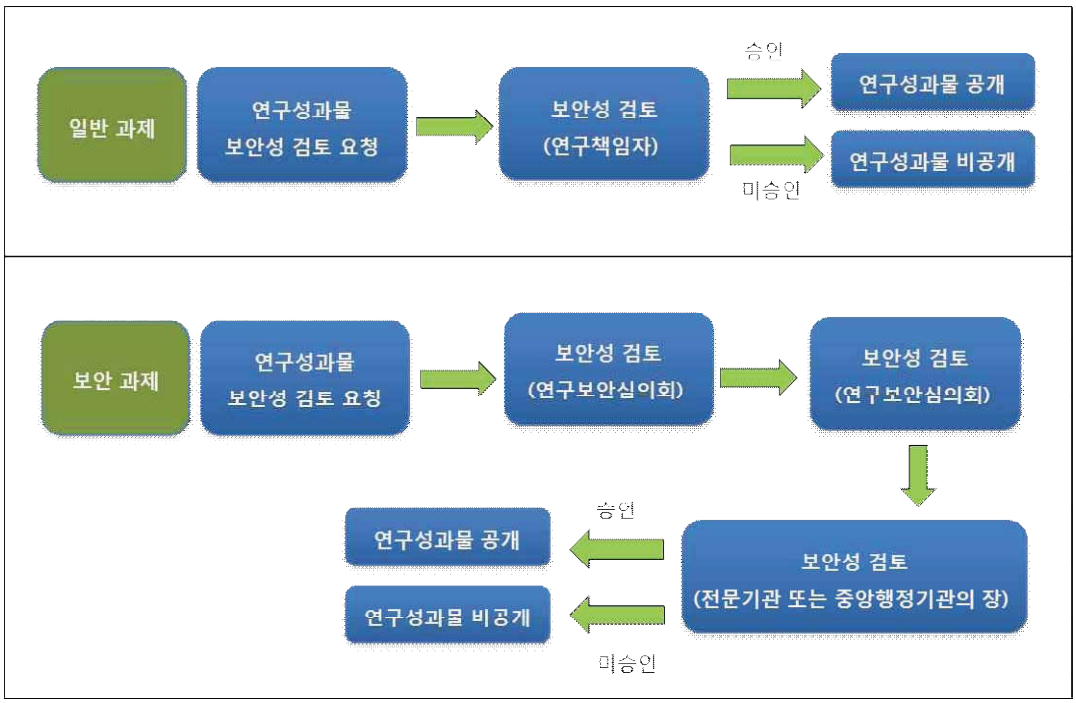
1. 연구개발 성과 대외공개 절차 수립

· 연구개발 성과와 관련된 정보를 외부에 공개하거나 자료를 제공하고자 하는 경우에는 연구책임자로부터 사전에 보안성 검토를 받아야 한다. 즉, 연구개발 성과물을 공개하고자 하는 자는 사전에 연구책임자에게 공식적인 문서로 보안성 검토를 요청하여 연구책임자의 승인을 득한 후에 연구 성과 정보 및 자료를 대외적으로 공개하여야 한다.

[보안등급에 따른 성과물 공개 기준]

구분	연구보고서	기술문서	논문/특허 등
보안과제	비공개 원칙 (필요시 공개)	비공개 원칙 (협약기관 연구결과 평가 등으로 필요한 경우 제한적으로 공개 가능)	공개 원칙 (필요시 비공개)
일반과제	공개 원칙 (필요시 비공개)		공개 원칙

· 보안과제를 수행하는 연구책임자가 연구개발 성과를 대외로 공개하거나 제공하고자 하는 경우에는 보안승인요청서를 작성하여 연구보안관리자와 연구기관장의 승인을 득한 후에 전문기관의 장 또는 중앙행정기관의 장에게 사전 승인을 받아야 한다.



[연구개발 성과물 대외공개 승인 절차]

실행지침

2. 대외 비공개 정보 분류 기준 및 비공개 기간 수립

- 대외적으로 공개할 수 없는 정보 대상을 분류하고 분류 대상에 따라 비공개 기간을 설정하여 명시하여야 한다.
  - 보안등급으로 분류된 과제는 최대 3년 이내의 범위에서 해당 보안과제에서 정한 기간을 비공개할 수 있다.
  - 지식재산권의 취득을 위하여 공개 유보를 요청하여 중앙행정기관의 장이 승인한 경우에는 1년 6개월 이내로 비공개할 수 있다.
  - 참여기업의 대표가 영업비밀 보호 등의 정당한 사유로 비공개를 요청하여 중앙행정기관의 장이 승인한 경우에는 1년 6개월 이내로 비공개 할 수 있다.

3.4 국외기술 이전

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	참여연구원
◎	○	

3.4.1 국외기술 이전 시 관리

연구기관이 보유하고 있는 첨단기술을 해외 기업 또는 연구소로 이전하고자 하는 경우에는 핵심기술 또는 중요한 연구개발 관련 정보가 해외로 유출되지 않도록 적절한 보호대책을 사전에 마련하고 관리하여야 한다.

내용

- 기술이전이란 국가연구개발사업으로 개발한 결과물(기술, 지식, 정보)이 양도실시권 허용·기술지도 등의 방법을 통하여 기술보유자로부터 그 외의 자에게 이전되는 것”을 말한다.
- 기술이전은 기술이전 이전 단계(상담단계)와 기술이전 이후 단계, 계약 해지 및 이후 단계로 구분할 수 있으며 각 단계마다 연구 정보 및 개발 기술이 유출될 가능성이 있으므로 단계별 보안대책을 명확하게 수립하여야 한다.
- 일반적으로 기술이전은 정부출연연구소나 산·학·연협동연구 또는 국가연구개발사업으로 개발한 성과를 민간으로 이전 시 체결하게 되는데 개발 기술이 해외업체 등으로 유출될 소지를 없애기 위해 ‘제3자 기술이전 금지협약’을 체결하여야 한다.
- 해외로 기술이전 시 이전할 기술과 보호할 기술을 명확히 정의하고 이에 따른 보호대책을 강구하여야 한다. 또한, 중요한 개발 기술을 이전해야 하는 경우에는 기술 이전을 받는 대상 국가가 이전 기술에 대한 권리보호가 취약한 경우도 있을 수 있으므로 별도의 대응책 마련이 필요하다.
- 특히, 지식재산권 제도가 미흡한 국가에 진출할 때는 사전에 특허를 출원하여 권리화를 완료한 후에 이전하는 방안도 마련하여야 한다.

실행지침

1. 해외 기술이전(양도) 시 보안대책 수립

· 해외로 기술이전 시 기술이전 이전 단계(또는 상담단계)와 기술이전 이후 단계, 기술이전 해제 또는 해지 이후 단계로 구분하여 보안대책을 수립하여야 한다.

① 기술이전 이전 단계에서의 정보유출 대책

- 기술이전 희망업체와 상담할 때에 기술이전 성사여부와 관계없이 상담단계에서 습득한 기술정보를 기술이전 희망자가 유출할 가능성을 배제하기 위하여 반드시 비밀유지협약[별첨 3.4.1 참조]을 체결하여야 한다.
- 기술이전 대상국가의 기술 및 정보보호 수준을 파악하여 미비하다고 판단되는 경우에는 별도의 보호대책을 마련해야 한다.
- 개발기술이 해외로 유출될 소지를 없애기 위하여 기술이전 대상기관과 제3자 기술이전 금지협약을 체결하여야 한다.
- 이전받은 기술의 보호를 위한 해당 기관 직원의 보안교육 실시는 물론 기술이전과 관련된 핵심자료의 비밀관리, 기밀취급자의 인사관리, 출입제한구역 설정, 관련자와 비밀준수의무 계약체결 등의 보호조치를 이행하도록 계약서에 명기하여야 하며 기술의 제3자 유출 시 손해배상 등을 계약서에 명확하게 기술하여야 한다.

② 기술이전 이후 단계에서의 정보유출 대책

비밀 유지의무를 위반하는 경우에는 계약을 해지할 수 있고 손해 발생 시 민사상 손해배상의무가 있음을 계약서에 명시하여야 한다.

③ 기술이전 해제 또는 해지이후 단계에서의 정보유출 대책

기술이전이 해제되거나 해지된 경우에도 비밀보장의무는 유효한 것으로 명시하고 계약 해지 시에는 기술 자료를 모두 반납하여야 한다는 사실을 계약서에 명시하여야 한다.

· 국가로부터 연구개발비를 지원받아 개발한 국가핵심기술인 경우에는 “산업기술 유출방지 및 보호에 관한 법률” 제11조(국가핵심기술의 수출 등) 규정을 준수하여야 한다.

① 국가로부터 연구개발비를 지원받아 개발한 국가핵심기술을 보유한 대상기관이 해당 국가핵심기술을 외국기업 등에 매각 또는 이전 등의 방법으로 수출(이하 “국가핵심기술의 수출“이라 한다)하고자 하는 경우에는 산업통상자원부장관의 승인을 받아야 한다.

실행지침

② 위에서 언급한 승인대상 외의 국가핵심기술을 보유·관리하고 있는 대상기관이 국가핵심기술의 수출을 하고자 하는 경우에는 산업통상자원부장관에게 사전 신고를 하여야 한다.

③ 신고대상 국가핵심기술을 수출하고자 하는 자는 해당 국가핵심기술이 국가안보와 관련되는지 여부에 대하여 산업통상자원부장관에게 사전검토를 신청할 수 있다.

④ 국가핵심기술을 보유한 대상기관이 국가핵심기술을 수출하기 전에 승인을 얻지 아니하거나 부정한 방법으로 승인을 얻어 국가핵심기술을 수출한 경우 또는 신고대상 국가핵심기술을 신고하지 아니하거나 허위로 신고하고 국가핵심기술을 수출한 경우에는 산업통상자원부장관은 정보수사기관의 장에게 조사를 의뢰하고, 조사결과를 위원회에 보고한 후 위원회의 심의를 거쳐 해당 국가핵심기술의 수출중지·수출금지·원상회복 등의 조치를 명령할 수 있다.

05

제 4 장
연구시설 관리

1절. 정보통신매체관리
- 4.1 외부 정보통신매체 반출입 통제

2절. 시설접근통제
- 4.2 주요시설물 관리
- 4.3 보호구역 별도 관리
- 4.4 외부 입주기관 통제

3절. 인적 접근 통제
- 4.5 연구시설 출입자 통제
- 4.6 외부방문자 출입 통제

미래창조과학부
Ministry of Science, ICT and Future Planning

4.1 외부 정보통신 매체 반출입 통제

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	연구원
◎	◎	O

4.1.1 외부 정보통신매체 반출입 통제

외부에서 내부로 또는 내부에서 외부로 반출입되는 저장매체를 통해 중요한 연구정보가 유출되는 사례가 많이 발생하고 있다. 또한, 외부로부터 유입된 악성코드 감염으로 인해 내부 시스템의 보안취약점이 발생하여 중요한 정보가 유출될 수도 있다. 따라서 정보통신매체의 반출입에 대한 통제절차를 마련하여 연구정보를 보호해야 한다.

내용

- 연구 관련 정보를 불법적으로 복사하여 외부로 유출하는 것을 차단하기 위한 반출입 제한 대상 품목은 다음과 같다.
  - 저장매체 (CD, 테이프 등)
  - 모바일 기기(노트북, 탭, 패드)
  - 카메라
  - USB
  - 스마트 폰 등

실행지침

1. 반입 시 보안조치

- 연구기관 출입 시 승인되지 않은 정보통신매체의 반입은 원칙적으로 금지해야 한다. 단, 불가피하게 반입이 필요한 경우에는 연구보안관리자와 연구책임자로부터 사전 승인을 득한 제품에 한해 반입이 허용되도록 한다.
- 반입 시에는 연구정보 유출, 내부망 악성코드 감염 등의 보안사고를 예방하는 차원에서 다음과 같은 사항을 고려하여야 한다.
  - 안티바이러스 S/W 통한 악성코드 감염여부 점검
  - 장착된 카메라 렌즈 봉인
  - 반입 시 무결성 검사를 위한 소프트웨어 설치
- 사전 승인을 득하지 않은 정보통신매체는 출입 시 연구기관에서 보관한 후 퇴실할 때 본인에게 반환하여야 한다.

2. 반출 시 보안조치

- 정보통신매체를 반출하는 자는 상위 부서장 또는 연구책임자로부터 사전 승인을 받고 비밀유지서약서에 서명해야 한다.
- 정보통신매체를 파일을 저장하지 않고 단순히 지닌 채 반출입 하는 경우, 설치했던 무결성 검사를 위한 소프트웨어를 검토하여 허가되지 않은 연구정보나 기타 기밀 사항의 포함여부를 조사한다.

3. 반출입 관리대장

- 정보보안관리자는 정보통신매체 반출입 관리대장을 별도로 마련하여 반출입 일시, 품명 및 수량, 이름, 사유, 관리부서 확인 및 서명 등의 내용을 기입하고 주기적으로 관리대장 내용에 대한 적정성을 확인해야 한다.

4.2 주요시설물 관리

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	연구원
◎		

4.2.1 감시장치 설치

주요시설 내에 중요한 연구정보 및 민감한 자료들을 외부로 유출할 목적으로 불법적으로 침입을 시도하는 경우가 있다. 이에, 주요 시설물 주변에는 별도의 감시장치를 설치하여 지속적인 모니터링을 통하여 관계자 외 출입을 통제하여야 한다.

내용

1. 감시 장치 종류

가. CCTV (Closed Circuit Television)

- 폐쇄회로 텔레비전이란 용어로 불리는 CCTV는 '영상감시를 목적으로 제한된 지역에서 독립적인 텔레비전 회로를 구축한 것'으로 정의할 수 있으며 특정인만이 영상을 볼 수 있도록 한 텔레비전 전송시스템이다.

① 촬상부

- 촬상부는 피사체를 촬영한 영상신호를 전기신호로 전환하는 역할을 하며, 카메라와 렌즈가 주요 기능을 수행한다. 카메라는 피사체로부터 받은 빛을 전기적 신호로 변환하여 영상을 모니터에서 볼 수 있게 하는 역할을 하며, 렌즈는 카메라 앞에 장착되어 피사체로부터 빛을 모아 촬상소자로 보내는 역할을 하는데, 사람 눈의 수정체에 해당하는 역할을 한다. 감시목적에 따라 선택해야 할 카메라, 렌즈, 필터의 종류등이 결정되며 카메라를 고정 설치하기 위한 브라켓, 하우징 등이 필요하다. 이와 같이 촬상부는 단순히 카메라 본체 뿐 만 아니라 피사체를 정확히 촬상하기 위한 관점으로 카메라의 주변기기까지 포함한다.

② 전송부

· 전송부는 촬상부에서 촬영한 영상을 수상부에 전송하는 역할을 하는데 영상신호 전송을 위해 여러 형태의 통신매체를 이용하게 된다. 영상신호 전송매체로는 유선망이 주로 사용되고 있으며, 그중에서 동축케이블이 많이 사용되고, 광케이블, 전화망, 인터넷 등을 사용하기도 한다. 무선 영상전송을 위해 VHF·UHF, 마이크로 웨이브, 이동통신, 적외선 등을 이용할 수 있다.

③ 수상부

· 수상부는 촬상부에서 전송된 전기신호를 영상신호로 재생하여 사람이 영상을 볼 수 있게 하는 역할을 할 뿐 만 아니라 각종제어, 녹화 등 여러 형태의 시스템으로 구성된다.

나. DVR (Digital Video Recorder)

· 아날로그 영상 감시 장비인 CCTV를 대체하는 디지털 방식의 영상 감시 장비이다. 영상이 고화질로 저장이 되며, 컴퓨터의 하드디스크를 저장 매체로 사용하기 때문에 녹화테이프를 교체할 필요가 없고, 보다 깨끗한 영상을 얻을 수 있다. 이러한 장점 외에 녹화된 영상을 시간대별 또는 카메라별, 검색어 입력으로 쉽게 검색할 수 있으며, 별도의 장치 없이 여러 채널의 영상을 한 개의 모니터에서 분할된 화면으로 볼 수 있게 한다. 또한, 인터넷을 통한 실시간 영상 전송 및 원격지 감시기능이 있어 네트워크로 통합화하고 있는 정부 및 기관, 기업체들에게 가장 적절한 영상 감시 시스템으로 평가받고 있다

다. 지능형 감시 시스템 (Intelligent Surveillance System)

· 지능형 감시 시스템은 감시 및 저장은 기본이며 침입물체 감지 시 자동으로 추적한다. 원격제어는 물론, 네트워크를 통한 영상전송과 중앙컨트롤 서버에서 침입자 정보나 이벤트 정보 등 각종 전용 디스플레이를 통해 감시할 수 있는 시스템이다. 기존 감시 시스템은 단순 저장/검색 수준에 머물렀으나 출입통제 시스템과 각종 카메라를 통한 자동 트래킹 및 데이터베이스와 연동이 된다는 점에서 매우 효과적인 신개념 솔루션이다. 다음과 같은 경우에 적용 가능하다.

- 지정된 영역 진입/탈출 물체
- 지정된 영역에서 갑자기 멈추는 물체, 일정한 기간 이상 머문 물체
- 금지된 방향으로 움직이는 물체
- 버려지거나 사라진 물체
- 갑작스러운 장면 변화에 대한 감지

실행지침

1. 감시장치는 다음과 같은 목적으로 설치·운영할 수 있다.
   - 원거리 관찰
   - 보이지 않는 영역 관찰
   - 중요도가 높은 구역의 집중적 감시
   - 보안적으로 취약한 장소의 관찰
2. 감시장치를 설치해야 하는 장소는 다음과 같다.
   - 전산실, 통신실과 같이 제한구역 및 통제구역으로 지정된 장소 (4.3.1 참고) 에 감시장치가 필수적으로 설치되어야 한다.
   - 보호구역외에도 감시장치가 필요하다고 판단되는 지역에는 추가 설치하도록 한다.
3. 감시장치 설계 시 주의해야 할 사항은 다음과 같다.
   - 감시 목적, 감시 대상, 감시 범위를 충분히 고려하여 장소를 택하고 설치한다.
   - 카메라 선정 시 컬러 및 흑백여부, 룩스(Lux), 화소, 해상도 등의 적합성과 역광의 영향유무, 햇빛의 영향 등을 고려하여 선택해야 한다. 빛이 없으면 촬영할 수가 없는 것이 카메라인데, 어느 정도의 빛으로 촬영할 수 있는가를 나타내는 수치가 감도이다. 감도는 대게 룩스(Lux)로 표시하고 카메라를 평가하는데 사용한다. 수치가 적을수록 감도가 좋아지지만 대부분은 사용목적에 맞추어 선택하는 것이 바람직하다.(칼라 카메라: 1Lux, 흑백카메라: 0.1Lux, 적외선 카메라: IR 0.11Lux)
   - 특히 어두운 곳에 설치하거나, 야간 감시가 필요한 경우 촬영되는 물체가 식별 가능한지 반드시 확인하도록 한다. (Color mode 이상 넘어가게 될 경우 흑백모드로 전환되어 어두운 곳에서도 선명한 화질 구현, IR-cut Filter 사용 시에 0.0001lux 이하의 어두운 곳에서 적외선 촬영으로 선명한 화질 구현)
4. 감시장치를 운영하는 지침을 수립해야 한다.
   - CCTV 감시책임자를 지정하여 허가되지 않은 인원이 함부로 CCTV 작동 및 녹화 영상 열람에 관여할 수 없도록 한다.
   - 감시 장치의 데이터 저장 공간을 충분히 확보하고 정기적인 데이터 백업 주기를 설정하여 일정기간 동안 보관해야 한다. 보관 데이터는 연구정보유출, 도난 사고 발생 등 비상시에 열람할 수 있도록 해야 한다.
   - 감시장치가 항상 정상적으로 작동할 수 있도록 정기적인 유지보수를 통해 관리하도록 한다.

4.2 주요시설물 관리

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	연구원
◎		

4.2.2 출입 통제 시스템

중요한 연구정보나 성과물들을 보호하기 위하여 비인가자의 출입을 통제할 필요가 있다. 따라서 물리적 환경 요소나 건물 유형, 이용 형태에 따라 다양한 출입통제 시스템을 설치하여 인가자만을 출입할 수 있도록 조치해야 한다.

내용

1. 출입통제시스템

중요한 연구 자산이나 시설물을 보호하기 위한 수단으로 물리적 환경 요소나 건물 유형, 이용 형태에 따라 출입 시 인가자만 출입을 허용하는 시스템이다. 출입통제 시스템은 인가된 사람을 식별하는 인식장치와 인식장치를 통제하고 문의 개폐를 결정하는 제어장치, 그리고 문의 열림을 통제하는 문 잠금장치로 구성되며, 출입 상황의 관리, 조회, 통제 등을 위하여 관리 서버를 운용할 수 있다. 출입통제장치의 인식장치에서 출입자를 인식하여 출입을 허용할 것인가를 자동으로 결정하여 출입문 잠금장치로 알려주며, 출입문 잠금장치는 제어장치가 결정한 출입허용 또는 출입 거절을 시행하기 위해 문의 잠금을 해제하여 인가된 사람이 들어오게 하거나 문의 잠금 상태를 유지시켜 사람의 출입을 거절한다.

2. 인식방법

출입통제를 위한 인가자의 인식방법은 크게 세 가지 형태로 행해질 수 있다. 첫번째는 인식 카드와 같이 인가된 사람에게만 주어진 증표에 의한 방법이고, 두 번째는 지문이나 얼굴, 홍채, 음성 등과 같이 사람의 신체적 특징을 이용하는 방법이며, 세 번 째는 비밀번호를 사용하는 방법이다. 보안을 강화하기 위하여 두 가지 이상의

인식방법을 함께 이용하는 방법을 다중인식이라고 불린다.
일반적으로 인식의 안전성 확보를 위해 인식장치와 키보드를 같이 사용하게 되는데, 키보드는 숫자가 적힌 버튼에 여러 개의 마이크로 스위치를 연결한 전자·기계식 장치가 주로 사용되고 있다. 키보드 사용 시 우려되는 것은 인가된 사람이 사용할 때, 다른 사람이 그 암호를 알아내어 사용할 수 있다는 점이며, 키보드 번호판을 마개로 가려서 이러한 단점을 보완할 수 있다.

① 기계장치

출입자를 인식하기 위해 사용되는 인식표 중 가장 잘 알려진 것이 키이며, 키를 대신하여 비교적 쉽게 사용할 수 있는 것이 간단한 숫자나 기호가 표시된 버튼 누름 장치이다. 키나 버튼 누름 장치를 이용하는 인식방법은 직접적이고 기계적인 방법을 사용하는 것이며, 최근에 사용이 증가하고 있는 '디지털 도어락' 이라 불리는 장치는 전자·기계적 방법을 사용하는 일체형 출입통제장치로 출입통제장치의 구성요소가 하나의 장치에 갖추어진 것이라 할 수 있다.

② 플라스틱 카드

플라스틱 카드는 출입통제시스템 인식 증표의 한 형태로 널리 사용되고 있으며, 개인의 신분확인 기능을 이용하여 금융거래, 출퇴근관리, 식수관리 등과 같이 다양한 목적으로 사용되고 있다.
카드는 카드리더와의 통신을 통하여 필요한 정보를 교류하게 되는데 ① 카드를 카드리더에 수직 또는 수평으로 형성된 얕은 홈 안으로 삽입하거나 완전히 통과시키는 방식, ② 카드를 카드리더에 접촉하는 방식, ③ 카드를 카드리더기 가까이에 노출시켜 무선 주파수를 통한 통신이 이루어지는 비접촉식 방식으로 사용된다.
마그네틱 카드(자기카드)는 플라스틱 카드의 후면에 정보가 기록된 마그네틱 띠를 부착하고 마그네틱 띠가 카드리더기를 지나면서 정보를 인식하는 방법으로 제조비용이 저렴하여 많이 사용된다. 그러나 마그네틱 카드는 입력이 가능한 정보의 양이 제한적이고 데이터를 손실할 위험이 있으며, 비교적 위·변조가 용이하다는 단점이 있다.
이에 비해 플라스틱 카드에 CPU와 메모리가 내장된 IC칩이 삽입된 스마트 카드는 보안, 금융, 의료, 통신 등 다양한 용도로 사용된다. 스마트 카드는 많은 양의 정보를 저장할 수 있고, 보안성이 향상되어 한 개의 카드로 여러 기능을 수행할 수 있으며, 기능 향상과 응용 분야의 확장에 따라 사용이 증가하고 있다.

③ 생체인식

인식표의 위조 또는 복제로부터 보호하기 위해 개인별 차이가 있는 신체적 특징을 인식방법으로 이용하고 있다. 출입통제 시스템의 인식을 위해 사용될 수 있는 신체 특징에는 지문, 얼굴, 홍채, 정맥, 손가락길이, 음성, 필체 등 다양하다. 생체인식은 바이오 인식이라고 불리며, 향후 인간의 편의성 향상과 첨단화로 인해 적용 범위가 확대될 것으로 전망된다.

지문은 모양이 개인마다 다르고, 태어날 때 모습 그대로 평생 변하지 않는 특성이 있어 생체인식을 위한 수단으로 널리 사용되고 있다. 지문인식장치는 다양한 형태로 적용할 수 있고, 사용자의 편의성이 뛰어나며 다른 생체인식장치에 비해 비용이 저렴하고 구조가 간단하다는 장점이 있어 가장 많이 사용되고 있으나 사용자에게 거부감을 줄 수 있고, 여러 사람이 같이 장치에 접촉하여 사용함에 따른 위생상의 문제가 있다는 단점이 있다.

얼굴인식은 카메라로부터 얼굴 정보를 입력받아 필터링 과정을 거쳐 추출 및 표준화해서 인식하게 된다. 얼굴인식은 비접촉으로 자연스럽게 확인할 수 있다는 장점이 있으며, 사용자는 자신이 현재 인식당하고 있다는 사실을 전혀 눈치채지 못하고 있는 중에 인식과정이 수행된다. 그러나 얼굴인식은 얼굴의 각도, 표정, 조명, 포즈, 표정 등에 취약하다는 단점이 있다. 기존의 얼굴인식 방법과 매우 다른 3D 얼굴 인식기술은 얼굴표면의 3차원 이미지를 캡쳐 해 얼굴의 뚜렷한 특징을 이용하는데, 여러 각도에서 조명할 수 있고 전체 얼굴을 커버하는 새로운 방법으로 정확도가 높고 처리가 빠르며 사용이 편리하다.

사람의 홍채는 태어난 후 약 18개월 내에 모양이 생성되고 일생 동안 모양이 쉽게 변하지 않는 특징이 있어서 생체인식 수단 중 가장 완벽한 식별 수단으로 평가된다. 홍채인식은 눈에 적외선을 조사하여 검은 동공과 흰자위 사이에 존재하는 링 형태의 홍채 무늬 패턴을 코드화해서 사용자를 인식하게 된다.

손 모양 인식은 인간의 특성 중 하나인 손가락 길이와 손바닥의 차이를 분석하여 인식하는 방법이다. 출입허용을 위해 사용하는 지문확인 방법은 범죄를 연상시키는 별로 좋지 않은 인식 때문에 일반인들이 지문확인 방법의 사용을 꺼리지만 이러한 단점을 개선하는 효과를 위해 달리 선택할 수 있는 인식방법이다.

이 밖에도 인가된 사람의 음성을 사전에 녹음시켜 놓았다가 출입할 때 마다 인식장치 앞에서 소리를 내어 녹음된 목소리와 대조하여 출입허용을 결정하는 음성인식 방법이나 자신의 이름을 사인할 때, 그 압력과 속도를 측정하여 인가된 출입자를 확인하는 필체인식 방법도 사용된다.

④ RFID

RFID는 실리콘 반도체칩을 내장한 태그, 카드 등에 저장된 데이터로 무선주파수를 이용하여 리더에서 자동으로 인식하는 기술을 말하며, RFID 태그가 달린 물체는 언제 어디서나 무선으로 인식 및 추적이 가능하므로 출입통제시스템의 인식장치로 유용하게 적용할 수 있다.

RFID를 이용하여 사람 및 차량의 출입을 구역별로 통제할 수 있고, 출입문마다 직책이나 업무 등에 따라 차별화된 출입통제를 할 수 있다. 그리고 RFID 시스템이 지닌 인식·추적 기능을 이용하여 방문자의 등록과 신분확인 뿐 만 아니라 방문자가 불필요한 지역에 진입하는 것을 통제할 수 있다, 특히 노트북, 소형 저장장치, 문서 등에 RFID 태그를 부착하여 반입과 반출을 효과적으로 감시·통제할 수 있어 출입통제시스템의 효과를 한층 더 높일 수 있다.

⑤ 출입게이트

건물 로비나 출입구 등 보안이 필요한 곳에 효과적인 접근 통제가 가능한 동시에 융통성있게 출입통제가 가능한 게이트이다.

실행지침

1. 출입관리시스템을 관리하고 운영하는 담당자를 지정하여야 한다.
   - 관리자는 출입시스템을 통하여 자동으로 기록된 출입자 자료를 주기적으로 점검하여 출입현황을 실시간으로 관리하고 유지하여야 한다.
   - 관리자는 내부규정에 의해 분류된 출입자 통제 등급 자료를 소지하고 있어야 하며 출입자의 등급 변경과 같은 출입 사유 변경이 발생한 경우 이를 즉각 반영하여 출입통제시스템에서 번호를 삭제하거나 카드를 반납 받아야 한다.
   - 임직원으로 부터 카드분실을 보고받은 즉시 출입시스템에서 해당 번호를 삭제하거나 해당 카드의 사용을 중지시켜야 한다.
2. 출입문의 개폐를 효율적으로 관리하여야 한다.
   - 시간대, 그룹별, 공간별로 출입통제를 실시하여야 한다.
   - 상황에 따라 출입문의 부분 또는 일괄적으로 개폐하여야 있다.
   - 출입문의 현 상태 (개폐)를 실시간으로 관리하여야 한다.

4.3 보호구역 별도 관리

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	연구원
◎		

4.3.1 보호구역의 지정 및 관리

연구시설에는 많은 건물과 구역들이 있지만 모든 건물 및 구역마다 동일하게 보안조치를 적용하는 것은 비효율적이며 적합하지 않다. 따라서 보안과제를 연구하는 실험실 또는 연구실과 전산실, 전기실 등과 같은 연구기관 내 주요 시설물들은 다른 시설물과 별도로 분류하여 관리해야 한다.

내용

• 다른 지역에 비해 보안상 관리가 필요한 곳을 보호구역으로 지정하여야 하며 보호구역은 제한구역과 통제구역으로 나뉜다. 보호구역은 실험실과 연구실 혹은 건물 전체, 구역별로 지정할 수 있다.

- 제한 구역

• 외부인의 출입이 통제되는 중요한 지역
• 필요한 경우에 한해 외부인의 출입이 어느 정도 허락
• 비인가된 접근을 방지하기 위하여 별도의 출입통제 장치 및 감시시스템이 설치된 장소로 출입 시 직원카드와 같은 출입증이 필요한 장소
(*예:부서별 사무실, 연구실 등*)

- 통제 구역

• 비인가자의 출입이 제한되는 중요한 지역
• 제한구역과 달리 외부인의 출입이 금지되며 해당 연구원만 출입 가능
• 제한구역의 통제항목을 모두 포함하고 출입자들은 최소 인원으로 유지되며 출입을 위하여 추가적인 보안절차가 필요한 장소*(예 : 전산실, 통신장비실, 비밀보관실 등)*

실행지침

1. 보호구역에 대한 출입통제관리 정책을 마련하여야 한다.
   - 비인가자의 출입을 통제하기 위하여 별도의 출입통제 장치 및 감시시스템 등을 설치하여 운영한다.
   - 통제구역은 실질적으로 필요한 최소한의 인원에게만 출입을 허용하고 사전에 연구보안관리자로부터 사전 승인을 받아야 한다.
   - 출입통제시스템을 통해 출입자와 출입시간 등이 자동으로 기록되도록 하며 그렇지 않은 경우에는 출입관리대장을 마련하여 기록하도록 한다.
   - 외부 방문객이 보호구역을 출입하고자 하는 경우에는 연구보안관리자로부터 사전 승인을 받아야 하며 담당 직원의 인솔 하에 출입하여야 한다.
   - 보호구역을 출입하는 임직원 및 외부 방문객은 반드시 출입증을 패용하여야 한다.
   - 비인가된 출입자의 접근을 차단하기 위하여 보호구역임을 알리는 문구를 잘 보이는 곳에 부착하여야 한다.

2. 재난, 재해, 외부침입으로부터 보호구역을 보호할 수 있는 방안을 마련해야 한다.
   - 화재, 수해, 정전 등으로부터 보호구역을 보호하기 위하여 다음과 같은 설비를 갖추어야 한다.
     - 화재감지 및 소화설비
     - 누수감지기
     - UPS(무정전 전원장치), 비상발전기, 전압유지기
     - 이중전원선
   - 외부 침입자로부터 보호구역을 보호하기 위하여 다음과 같은 보안장치들을 갖추어야 한다.
     - CCTV,
     - 외부침입감지 및 경보,
     - 출입통제시스템

4.3 보호구역 별도 관리

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	연구원
◎	○	

4.3.2 보호구역 내 업무

보호구역 내에서 연구와 관련된 고유한 업무 외에 이를 지원하기 위한 부수적인 작업을 해야 하는 경우도 발생할 수 있다. 이러한 경우에도 연구보안 사고를 미연에 방지하기 위하여 규정 내 세부 절차를 마련하고 이행하여야 한다.

내용

- '보호구역 내 업무' 라 함은 연구원에 의해 수행되는 본래 업무를 제외한 추가적 작업을 의미한다.

(예: 정보시스템이 위치한 보호구역(전산실 등) 에서 정보시스템 도입 및 폐기, 유지 보수 (정기점검 포함) 등)

실행지침

- 출입권한이 없는 임직원 및 외부인이 보호구역내에서 작업을 수행하고자 하는 경우 작업신청 및 승인, 작업일지 작성, 모바일 기기 반출입 통제 등의 절차를 마련하고 그 기록을 정기적으로 검토하여야 한다.
  - 연구책임자는 작업 전에 보안관리자로부터 사전 승인을 받아야 한다.
  - 연구책임자는 사전에 작업 업체로부터 보안서약서를 징구하고 보호구역 출입 시 준수 의무사항을 주지시켜야 한다.
  - 작업 수행을 위해 모바일 기기의 반출입이 필요한 경우 모바일 기기 안전성 확보 절차(백신 설치 등)를 수행하여야 한다.
  - 보호구역내 작업이 완료되면 작업일지를 기록하도록 해야 한다. 기록항목은 작업일자, 작업시간, 작업내용, 작업업체 및 담당자명, 검토 승인자 등이 포함되어야 한다.

작업일자	작업시간	작업목적	작업내용	작업업체	검토자 승인

4.4 외부 입주기관 통제 및 관리

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	연구원
◎		

4.4.1 외부 입주기관 통제 및 관리

입주 여건에 따라 동일한 건물 내에 연구기관 외의 외부 기관이 함께 입주해 있는 경우가 있을 수도 있다. 이 경우 외부 입주기관 인원이 연구기관 내부에 접근하는 것을 방지할 수 있는 방안과 절차를 수립하고 이를 이행하여야 한다.

내용

입주기관 통제 및 관리를 위해서는 입주기관 임직원들이 허용된 구역만 출입 가능한 출입증 발급을 통한 출입통제와 네트워크의 물리적 망 분리, 또는 출입구의 물리적 분리 등을 통하여 외부기관의 임직원들이 내부 시설 또는 연구 관련 정보에 접근하는 것을 통제하여야 한다,

실행지침

- 가급적이면 출입구를 물리적으로 분리하여 연구기관내 출입을 통제하여야 한다.
- 전산망도 물리적으로 분리하여 연구기관 내부망에 불법적으로 접근하는 것을 차단하여야 한다.
- 한 건물을 공동으로 사용하는 경우에는 외부기관 임직원들이 허용된 구역 이외의 장소에 출입하는 것을 엄격하게 통제하여야 한다.

4.5 연구시설 출입자 통제

해당과제	
모든과제	보안과제
	○

이행대상		
연구기관	연구책임자	참여연구원
◎	○	○

4.5.1 연구시설 출입자 통제 및 관리

보안과제와 관련된 중요한 연구실 또는 실험실은 사전에 허가를 받은 업무와 관련된 자만이 출입 가능하도록 엄격하게 통제하여야 한다. 따라서 보안과제와 관련된 중요한 실험장비 및 연구개발 관련 정보를 보호하기 위하여 내부 임직원이라 하더라도 보안과제와 관련이 없으면 엄격하게 출입을 제한하여야 한다. 이와 같이, 중요한 연구시설의 출입 권한을 통제하고 관리하기 위한 절차를 반드시 수립하고 이행하여야 한다.

내용

- 최근 5년간 국내에서 발생한 해외 기술유출 사건의 주체로 전직 직원과 현직 직원에 의한 기술 유출이 거의 80%를 차지하고 있으며 협력업체에 의한 기술 유출도 12%를 차지하고 있다.[1] 이처럼 연구보안 사고는 대부분 연구기관의 내부 사정을 잘 알고 있는 임직원 또는 협력업체 직원에 의해 발생되는 경향을 보이고 있다.
- 따라서 중요한 연구시설에 대한 출입통제만 엄격하게 관리하더라도 연구보안 사고를 상당 부분 사전에 방지할 수 있으므로 출입통제의 중요성을 아무리 강조해도 지나치지 않다.
- 연구시설에 대한 출입통제를 시행하기에 앞서 중요한 연구시설은 인가된 자만 출입 가능하도록 특별관리 구역으로 지정하여 보호해야 한다. 연구기관 내 모든 시설은 중요도에 따라 공용구역, 일반구역, 제한구역, 통제구역으로 분류할 수 있으며 그에 따라 차별적으로 출입을 통제할 수 있는 방안을 강구하여야 한다.

1) 출처: 산업기밀보호센터

내용

- 공용구역: 보안상 차별화된 통제가 필요하지 않은 지역으로 연구기관의 임직원이나 외부인 등 모든 사람에게 공개된 구역
- 일반구역: 보안상 차별화된 통제가 필요하지 않은 지역으로 임직원이나 출입이 허가된 정기 방문자, 임시 방문자에 한하여 출입이 가능한 구역
- 제한구역: 보안상 비인가자의 접근을 방지하기 위하여 사전에 보안총괄책임자로부터 허가를 득한 자만이 출입 가능한 지역으로 연구기관의 중요한 설비가 위치하고 있는 구역
- 통제구역: 침해사고 또는 유출사고 발생 시 연구기관에 치명적인 영향을 미치는 보안상 극히 중요한 시설로서 사전에 보안총괄책임자로부터 허가를 득한 자만이 출입 가능한 지역으로 퇴실 시까지 직원의 동행이 필요하며 외부방문객의 출입이 엄격하게 제한된 구역

・보안과제와 관련된 연구실 또는 실험실은 통제구역으로 지정하여 내・외부 출입자의 출입을 엄격하게 통제하고 관리하여야 한다. 따라서 통제구역을 출입할 수 있는 출입증 발급 절차를 마련하고 출입증 발급대장[별첨 4.5.1 참조]을 구비하여야 한다. 이를 통해 발급현황을 수시로 점검하여 오・남용되는 사례가 발생하지 않도록 각별히 주의하여야 한다.

・보안과제와 관련된 연구실 또는 실험실의 출입통제를 엄격하게 관리하고 보안사고 발생 시 신속한 대응과 증적자료로 활용하기 위하여 연구책임자는 출입관리대장[별표 4.5.1 참조]을 구비하여 관리하여야 한다.

실행지침

1. 보안과제 관련 연구시설의 통제구역 지정

・연구책임자는 시설보안책임자로부터 보안과제를 수행하는 연구실 및 실험실을 통제구역으로 지정받은 후 모든 내・외부인이 인식하기 쉬운 장소와 출입문에 통제구역이라고 표시하여야 한다.

・구책임자는 통제구역의 관리책임자 및 관리담당자를 지정하여 시설보안담당부서에 통보하여야 한다. 대부분 해당 부서장이 관리책임자가 되고 부책임자는 해당 부서장이 소속부서 연구원들 중에서 지정하여야 한다.

실행지침

· 통제구역에는 다음과 같이 관리책임자와 관리담당자를 알리는 명패를 연구실 또는 실험실 출입문에 부착하여 보안상 위급한 상황이 발생하면 언제든지 연락을 취할 수 있도록 조치하여야 한다.

구분	○○구역 관리책임자	
	직위 또는 직명	성 명
정		
부		

2. 보안과제 관련 연구시설의 출입 관리 규정 마련

· 연구기관의 장은 보안과제를 수행하는 연구시설의 출입을 효율적이고 일관되게 통제하고 관리하기 위하여 통제구역에 대한 출입통제 규정 및 지침을 마련하여야 한다.

· 연구책임자는 보안과제를 수행하는 연구시설에 출입관리대장[별표 4.5.1 참조]을 비치하여 출입자 성명 및 출입 일시 등을 항상 기록하여 관리하여야 한다.

· 통제구역을 보호하기 위한 규정 및 지침을 마련하고 보안장치(CCTV, 적외선 감지기, 카드키, 생체인식시스템 등)를 설치하여 24시간 출입자를 엄격하게 통제하여야 한다.

· 보안과제를 수행하는 연구시설에 출입이 필요한 임직원은 연구책임자와 연구보안책임자로부터 사전 승인을 받아야 하며 출입증관리자는 이를 확인한 후 출입증을 발급해야 한다.

· 연구책임자는 협력업체 직원이나 시설 또는 장비 보수 등을 목적으로 출입하는 정기 방문자는 사전에 신원확인에 필요한 서류를 확보하여 비치하고 보안서약서를 받아야 한다.

· 출입 시 출입 권한이 없는 자가 출입이 허용된 임직원을 뒤따라 와서 출입문을 통과하지 못하도록 별도의 출입통제 장비를 설치하여야 한다.

· 보안과제를 수행하는 연구시설에 출입이 가능한 자라도 참여하고 있는 연구와 관련이 없는 연구시설에는 접근하지 못하도록 출입 권한을 세부적으로 차등 부여하여야 한다.

4.6 외부방문자 출입통제

해당과제	
모든과제	보안과제
	○

이행대상		
연구기관	연구책임자	참여연구원
◎	◎	○

4.6.1 외부방문자 출입통제 및 관리

보안과제와 관련하여 외부방문자가 연구기관을 출입하는 경우에는 일반과제보다 더 엄격하게 출입을 통제하고 관리해야 한다. 또한, 외부방문자는 정기적으로 연구기관을 출입하는 정기 방문자와 필요에 의해 일시적으로 출입하는 임시 방문자로 구분할 수 있다. 따라서 외부 방문 목적 및 방문 형태에 따라 적합한 출입통제 방안을 마련하여 외부방문자를 효율적으로 통제하고 관리하여야 한다.

내용

외부방문자의 방문 형태에 따라 정기 방문자와 임시 방문자로 구분할 수 있는데 정기 방문자로는 연구개발 용역업체 직원과 연구시설 및 장비유지보수 업체 직원, 경비 및 청소용역 직원 등으로 연구기관의 출입이 잦고 연구개발 환경과 연구시설 구조에 익숙하기 때문에 이들에게 연구개발 정보가 노출될 수 있는 기회는 항상 존재한다. 따라서 연구보안대책 수립 시 정기 방문자에 대해 각별히 더 신경을 써야 한다. 그리고 보안과제와 관련된 임시방문자에 대해서는 사전 예약을 통한 사전 승인 및 중요한 시설의 접근 차단, 반·출입 물품 통제 등 물리적·관리적 보안대책을 수립하여 외부인 출입통제를 엄격하게 관리하여야 한다.

실행지침

1. 보안과제 관련 외부방문객의 출입통제 절차 마련

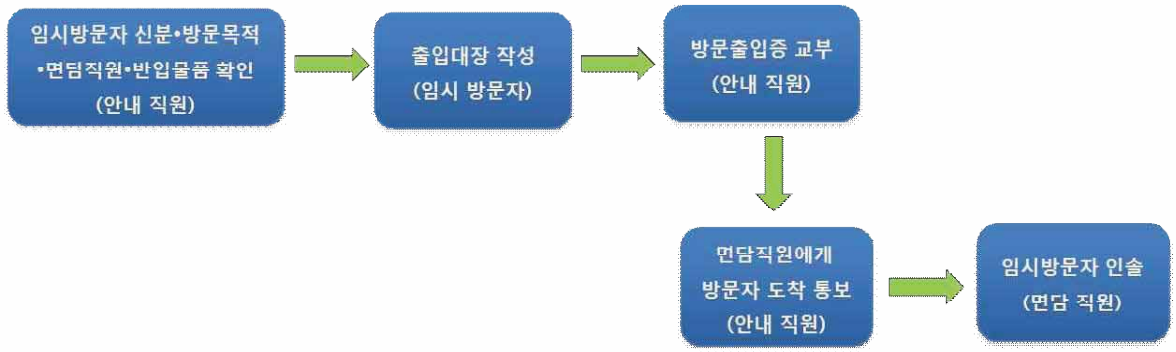
- 보안과제와 관련된 외부방문객은 정기 방문자와 임시 방문자로 구분하여 출입통제 절차를 마련하고 이를 준수하여야 한다.

[임시 방문자]

- 사전에 예약된 방문자에 한하여 연구기관에 출입하도록 통제하여야 한다.
- 안내직원은 방문자의 본인 신분 확인 및 내방 목적과 면담자를 확인한 후 면담자에게 통화하여 임시 방문자와 동행할 수 있도록 조치하여야 한다.
- 안내직원은 임시방문자가 출입관리대장에 소속, 성명, 출입일시, 방문목적, 면담직원 성명 등을 기록하도록 하여야 한다.
- 외부방문자의 반·출입 물품을 검사하여 노트북, 카메라, USB 등 보안상 금지 물품은 반·출입을 허용해서는 아니된다.
- 안내직원은 방문자의 신분증을 보관하고 방문출입증을 발급하되, 임시 방문자가 방문목적을 달성할 수 있는 최소한의 구역만 출입할 수 있는 출입증을 발급하여야 한다.
- 안내직원은 방문자에게 출입증이 잘 보이는 곳에 패용하도록 유도하여야 한다.
- 담당 직원은 임시 방문자를 연구기관에서 마련한 외부접견실에서 만나 면담을 하여야 한다.
- 담당 직원은 외부방문객이 부득이한 사정으로 연구실 또는 실험실의 출입이 필요한 경우 사전에 연구책임자와 보안총괄책임자의 허가를 받아야 하며 임시 방문자의 방문이 끝날 때까지 동행하여 제한구역 또는 출입통제 구역에 출입하지 못하도록 통제 하여야 한다.
- 임시 방문자가 연구실 또는 실험실을 방문하는 경우 중요한 문서나 자료는 이중으로 잠금장치가 되어 있는 캐비넷에 보관하고 주변을 깨끗하게 정리 정돈하여 중요한 정보나 자료가 유출되지 않도록 하여야 한다.
- 보안과제와 관련하여 외국 정부·기관 또는 단체가 연구기관을 방문하는 경우에는 사전에 연구책임자는 [별표 4.6.1] 서식에 연구과제명, 연구책임자명, 방문일시 및 장소, 주요 방문내용 등의 사항을 작성하여 소관 중앙행정기관의 장 및 국가정보원장에게 해당 방문일 5일 전까지 보고하여야 한다. 다만, 방문이 사전에 알린 내용과 다르게 이루어진 경우에는 방문 후에 해당 사항을 추가로 알려야 하며, 방문이 긴급한 경우 등 사전에 보고하지 못하고 방문을 받은 경우에는 방문이 끝난 후에 반드시 보고하여야 한다.

실행지침

- 방문자의 방문이 끝나면 안내 직원은 출입증을 반납 받고, 보관하고 있는 방문자의 신분증 또는 개인물품을 되돌려주어야 한다.



[임시 방문자 출입 절차]

[정기적 방문자]

- 연구책임자는 보안과제를 수행하는데 직접적으로 관련이 있는 정기적 방문자인 경우 보안총괄책임자에게 방문목적 및 신상정보를 제공하여 사전 승인을 받아야 한다.
- 연구책임자는 정기적 방문자로부터 비밀유지와 보안사고에 따른 민형사상 책임을 진다는 보안서약서에 서명을 받아야 한다.
- 연구책임자는 정기적 방문자가 사전에 예약된 날짜와 시간에만 정기적으로 출입할 수 있도록 통제하여야 한다.
- 안내 직원은 방문자의 신분증을 받아 보관하고 방문 목적을 달성할 수 있는 최소한의 지역만 출입할 수 있는 출입증을 발급하고 잘 보이는 곳에 패용하도록 유도하여야 한다.
- 반·출입 물품을 검사하여 노트북, 카메라, USB 등 보안상 금지 물품은 반·출입을 허용하면 아니된다. 다만, 방문 목적에 필요한 물품은 연구책임자와 연구보안관리자의 승인을 득한 경우에만 반·출입이 가능하며 반드시 물품 반출입대장 [별표 4.6.1 참조]에 기입하여야 한다.
- 정기적 방문자는 출입 시 출입대장에 소속, 성명, 출입 장소 및 일시, 퇴실일시, 방문목적 등을 기록하여야 한다.
- 담당 직원은 방문이 끝날 때까지 동행하여 허용되지 않은 제한구역 또는 통제구역에 출입하지 못하도록 통제하여야 한다.
- 안내 직원은 방문자의 방문이 끝나면 출입대장에 퇴실 시간을 기입하게 하고 보관하고 있던 개인소지품은 되돌려주어야 한다.

06

제 5 장
정보통신망 관리

1절. 시스템 관리
- 5.1 업무용 컴퓨터 관리
- 5.2 저장매체 관리
- 5.3 정보시스템 사용 관리
- 5.4 전산장비의 폐기

2절. 데이터 관리
- 5.5 데이터 전송
- 5.6 데이터 유출 제한
- 5.7 데이터 백업

3절. 네트워크 보호
- 5.8 전산망 보호 설비
- 5.9 접근 제한
- 5.10 네트워크 자료 관리

미래창조과학부
Ministry of Science, ICT and Future Planning

5.1 업무용 PC관리

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	연구원
O		

5.1.1 보안관리

스마트폰, 태블릿과 같은 손에 들고 다니는 기기를 통해 기술을 잘 이용할 수 있도록 새로운 방식을 제공하고 있지만 컴퓨터는 여전히 업무상 사용할 수 있는 첫 번째 도구이다. 결과적으로 연구와 관련된 중요한 실험 정보와 자료들이 저장되어 있는 컴퓨터가 사이버 범죄자의 첫 번째 공격 대상이기 때문에 모든 업무용 컴퓨터를 보호하기 위한 보안 대책들을 세워 관리해야 한다.

내용

- 로그온 패스워드란 사용자가 컴퓨터 사용이 허용되어 있는지를 확인하는 수단으로 등록된 사용자만 컴퓨터를 사용할 수 있도록 해주는 기능을 말한다.
- Guest 계정이란 윈도우 설치 시 자동으로 생성되는 계정으로 누구나 접속할 수 있는 권한을 지닌 계정을 말한다.
- BIOS 패스워드는 하드웨어 즉 컴퓨터 메인보드에서 사용자를 확인하는 수단으로 사용하는 비밀번호를 말한다.
- 공유폴더는 윈도우 운영체제에서 사용의 편의를 위해 파일이나 프린터를 다른 사용자가 공유하여 사용하는 기능을 말하다.
- 패치란 윈도우 운영체제나 응용프로그램의 오류나 취약한 부분을 보완해주는 여러 가지 수정 프로그램을 말한다.
- P2P(Peer-To-Peer) 프로그램은 컴퓨터 사용자들끼리 자신이 보관하고 있는 자료를 다른 사용자들과 공유하기 위해 사용하는 프로그램을 말한다.
  ※P2P 프로그램: 프루나, 당나귀, 몽키, 파일구리 동기호테, 이뮬 등

· 백신프로그램은 PC에 감염될 수 있는 웜·바이러스를 사전에 탐지하거나 이미 감염되어 있는 웜·바이러스를 제거해 주는 프로그램을 말한다.
· 웜·바이러스란 컴퓨터에서 동작하는 일종의 프로그램으로 자료를 손상시키거나 다른 프로그램을 파괴하여 정상적인 업무를 방해하는 프로그램을 말한다.

실행지침

1. 업무용 컴퓨터 보안조치

· 업무용 컴퓨터의 보안수준을 강화하기 위하여 다음 사항을 준수하여야 한다.

① 사용자 계정 보안
- 누구나 컴퓨터를 불법적으로 사용할 수 없도록 BIOS와 로그온 패스워드를 설정하여 한다.
- 복잡한 패스워드를 사용하고 있어도 하나의 패스워드를 너무 오랜 기간 사용하게 되면 노출될 가능성이 높으므로 패스워드 사용기간을 제한하여 정기적으로 변경해야 한다.
- 복잡하지 않은 패스워드를 사용하면 공격자가 패스워드를 쉽게 추측하여 악용할 수 있기 때문에 숫자/문자/특수문자를 조합하여 최소 8자리 이상 사용하여야 한다.
- 패스워드 변경 시 패스워드 재사용을 금지하여야 한다.
- 모든 사용자가 Guest 계정을 이용해 시스템에 접근할 수 있기 때문에 Guest 계정은 비활성화하여야 한다.
- BIOS 패스워드를 설정하여 컴퓨터 사용자 인증을 강화하여야 한다.

② 네트워크 보안
- 정보유출이나 해킹 등의 문제를 발생시킬 수 있는 공유폴더의 사용을 제한하여야 한다.
- 업무용 컴퓨터의 보안을 더욱 강화하기 위하여 Windows 방화벽을 사용하여야 한다.
- 잠재적인 위험을 내포하고 있는 위험한 서비스는 비활성화하여야 한다.

③ 시스템 유지/관리 보안
- 컴퓨터 부팅 시 사용자 이름과 패스워드 입력없이 자동으로 로그온되는 기능을 비활성화하여야 한다.
- 모니터 화면의 주요 내용의 노출과 불법사용자에 의한 컴퓨터 사용을 방지하기

위하여 화면보호기 기능을 설정하여야 한다.
- 새롭게 발견된 취약점과 문제점을 해결한 패치프로그램을 수시로 업데이트하여야 한다.
- 웜이나 바이러스의 설치를 차단하거나 보안되지 않은 기능을 막을 수 있도록 웹 브라우저의 보안설정을 강화하여야 한다.
- 인터넷을 통한 프로그램은 신뢰할 수 없으므로 다운로드하지 않도록 조치하여야 한다.
- 악성코드 감염 및 중요한 정보가 노출되지 않도록 P2P 프로그램 사용을 제한하여야 한다.
- 컴퓨터의 성능을 떨어뜨리거나 보안환경을 위협하는 요소로 작용하는 불필요한 프로그램은 정기적으로 제거하여야 한다.

④ 바이러스/웜 보안
- 웜·바이러스를 탐지하고 제거하는 백신프로그램을 설치하여야 한다.
- 업무용 컴퓨터를 안전하게 운영·유지하기 위하여 주기적으로 웜·바이러스 검사를 실시하여야 한다.
- 새로운 웜·바이러스를 탐지하기 위하여 백신프로그램의 업데이트를 수시로 실시하여야 한다.
- 컴퓨터 사용중에 웜·바이러스를 탐지하고 감염파일을 치료하기 위하여 백신프로그램의 실시간 감시 기능을 활성화하여야 한다.

2. 업무용 컴퓨터 보안실태 점검 및 사후조치

·업무용 컴퓨터의 보안조치 사항의 준수여부를 정기적 또는 수시로 점검하여야 한다.
·점검 실태조사에서 발견된 문제점은 그에 따른 해결방안을 마련하여 이행하여야 한다.

5.1 업무용 PC관리

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	연구원
◎	◎	O

5.1.2 소프트웨어 설치

연구를 수행하고 있는 업무용 컴퓨터는 연구와 관련된 정보와 중요한 자료들이 포함되어 있으므로 업무용 컴퓨터에 추가적으로 소프트웨어를 설치하고자 하는 경우에는 보안을 위한 대비책들을 세워 관리하도록 한다.

내용

인가되지 않은 불법 소프트웨어 또는 보안상 인증되지 않은 소프트웨어의 설치로 악성코드에 감염되어 연구정보가 파괴되거나 해킹으로 인해 연구정보가 외부로 유출되는 보안사고를 방지하기 위하여 사전에 세부 보안 절차를 마련하고 시행하여야 한다.

실행지침

•소프트웨어 설치

- 업무상 불필요한 소프트웨어 설치는 제한하여야 한다.
- 출처, 유통경로 및 제작자가 명확하지 않은 소프트웨어의 설치는 제한하며 인터넷 등 상용망으로 입수한 자료는 필히 백신 등 보안프로그램으로 진단하여 악성코드 존재 여부를 확인 후 사용하도록 한다.
- 보안과제의 경우 장비를 설치하는 경우와 마찬가지로 설치하는 소프트웨어 프로그램 이름과 목적 및 출처, 진단 여부를 문서로 작성하여 연구책임자에게 사전 승인을 받는다.

5.2 저장매체 관리

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	연구원
◎	◎	O

5.2.1 하드웨어 관리

연구와 관련된 중요한 실험 정보 및 자료는 궁극적으로 하드웨어에 저장되고 보관된다. 따라서 중요한 연구정보를 보호하기 위하여 하드웨어에 대한 보호대책이 요구되며 설치, 교체, 폐기의 모든 과정에 보안 절차를 마련하고 이행하여야 한다.

내용

- 자료가 저장되는 하드웨어의 종류는 아주 다양하게 존재하며 PC의 주변장치를 모두 포함한다.
  - PC 하드디스크 드라이버
  - 탭 / 패드
  - 웹 카메라
  - 네트워크 디스크 드라이버
  - 실험장비의 하드디스크 드라이버

실행지침

- 연구원이 업무 목적으로 필요한 장비를 구매하고자 할 때에는 구매하기 이전에 기관에 구매요청을 하고 승인을 받아야 한다.
- 일반과제의 경우 장비 구매요청 시 장비의 사용목적, 장비 종류 등을 문서로 작성하여 연구기관에 제출하여 승인을 받는다.
- 보안과제의 경우에는 장비 사용목적, 장비 종류, 사용기간, 해당 연구원의 서명 및 정보유출의 수단으로 장비를 사용하지 않겠다는 서약을 한 후 연구책임자로부터 사전 승인을 받도록 한다. 연구책임자가 제출한 요청서가 타당하다고 판단되면 연구기관에 제출하여 최종승인을 받도록 한다.
- 요청이 승인되어 구매하고자하는 장비에 대하여 구매담당부서는 보안성을 철저히 검토하여 결격사유가 없다고 판단될 때 장비 구매를 수행하도록 한다.
- 연구기관은 구매가 완료되어 설치된 장비에 관리번호를 부여하여 자산관리담당자가 관리하도록 한다.

5.2 저장매체 관리

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	연구원
◎	◎	O

5.2.2 이동형 매체 관리

이동형 저장매체의 특성 상 크기가 작고 고용량의 성능을 보유하고 있어 중요한 정보를 저장하여 외부로 반출하기가 아주 용이하다. 따라서 이동형 저장매체의 신규 구입부터 폐기에 이르는 전 과정을 보안상 효율적으로 관리하기 위하여 보안관리 절차를 수립하고 이를 준수하여야 한다.

내용

- 최근에 이동형 저장매체의 기능과 성능은 크게 향상되었으며 크기와 종류도 아주 다양하다.
  - USB
  - ZIP 드라이브
  - CD(Compact Disk)
  - DVD
  - 외장형 하드디스크(HDD)
- 이동형 저장매체의 반·출입 시 사전승인을 위한 절차를 수립하고 이를 효율적으로 관리하기 위한 관리대장과 폐기 절차도 세부적으로 마련하여야 한다.

실행지침

① 이동형 저장매체를 도입하기 이전에 사전 보안성 검토 절차를 마련하여야 한다.

- 연구기관은 USB 메모리를 도입할 경우 그 제품의 안전성을 검증하기 위하여 다음과 같은 필수 보안기능의 지원 유무를 검토하여야 한다.
  - 사용자 식별·인증기능
  - 지정 데이터 암호화 및 복호화 기능
  - 저장된 자료의 임의 복제 방지 기능
  - 분실 시 저장데이터의 보호를 위한 삭제 기능 등
- USB외 기타 이동형 저장매체 또한 다음과 같은 사항을 확인하여야 한다.
  - 안티바이러스 S/W 통한 악성코드 감염여부 점검
  - 장착된 카메라 렌즈 봉인

② 도입이 허가된 이동형 저장매체의 사용을 통제하고 관리하기 위한 규정 및 지침을 마련하여 정보보안관리자의 감독 하에 이행되도록 한다.

- 저장매체를 효율적으로 관리하기 위하여 도입이 허가된 매체에 한해 '이동형 저장매체 관리번호'를 부여하고 등록해야 한다. 등록방법은 이동형 저장매체 관리대장에 등재하는 것을 말한다.

관리번호	매체형태	등록일자	취급자	폐기일자	폐기방법 (재사용용도)	비고

- 임직원은 등록된 매체만 사용할 수 있으며 업무 목적 외의 사적인 용도로 사용할 수 없다.
- 정보보안관리자는 임직원이 이동형 저장 매체를 무단 반출하거나 미등록 매체를 사용하지 않도록 감독하여야 한다. 불가피하게 이동형 저장 매체를 반출하는 경우 4.1.1 의 내용을 따르도록 한다.
- 정보보안관리자는 관리대장에 최종 변경된 이동형 저장매체의 등록 현황을 등재하여야 한다.
- 정보보안관리자는는 월 1회 이상 이동형 저장매체의 수량 및 보관 상태를 점검하여야 하고 확인·서명하여야 한다.

점검일시	현 보유수량		이상 유무	점검관		비고 (서명)
	일반과제	보안과제		성명	서명	

· 연구기관의 장은 관리책임자로 하여금 보조기억매체를 일괄 구입하여 필요한 부서에 보급할 수 있다.

③ 보안과제용으로 이동형 저장매체가 사용되는 경우에는 일반과제와 분리하여 관리하여야 한다.

· 시건장치가 설치된 금고 또는 이중 캐비닛에 보관하여야 한다.
· 보안용 매체를 사용하여 보안과제를 수행하는 경우 그 작업을 완료하거나 일시 중단할 때에는 PC에서 즉시 분리하여야 한다.
· 보안과제와 관련된 문서파일을 생산하거나 보관할 필요가 있는 경우 등급별로 각각 이동형 저장매체를 마련해야 하며 하나의 매체에 등급이 다른 비밀을 혼합 보관해서는 안된다.

5.3 정보시스템 사용 기록

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	연구원
◎		

5.3.1 정보시스템 사용 기록 관리

정보시스템 기록은 추후에 보안사고가 발생했을 때 그 원인을 규명하거나 발생 경로를 추적하기에 아주 중요한 정보이다. 따라서 정보시스템의 사용기록을 별도로 일정 기간 보관하도록 하는 것은 보안사고 발생을 대비하고 발생 시 사후관리와 대책 수립을 위해 연구기관이 반드시 수행해야 하는 절차이다.

내용

- 정보시스템 사용 기록은 다음과 같은 것들을 포함한다.
  - 기관 내부망의 접속(로그인) 기록
  - 기관에 등록된 네트워크 장비의 사용 정보
  - 응용프로그램 및 소프트웨어 사용 기록
  - 정보의 수집, 저장, 복사, 삭제, 변경, 송수신 기록

실행지침

- 정보시스템의 사용 기록은 원칙적으로 1년 동안 보관하되, 각 연구기관의 상황에 따라 최소 6개월 이상 보관하여야 한다.
- 정보시스템에 대한 사용 기록을 보관하는 경우에는 모든 기록이 동일한 기간 동안 보관될 필요는 없으며 연구기관의 판단 하에 중요도가 높은 기록은 상대적으로 더 오랜 기간 동안 보관해야 하고 그렇지 않은 기록은 짧은 기간 동안만 보관하고 삭제하여 업무수행의 효율성을 높인다.
- 연구기관은 정보시스템 사용기록 관리자를 별도로 지정하여야 하며 담당자는 기록의 분류, 저장, 삭제를 포함하는 관리를 수행하도록 한다.
- 연구기관은 정보시스템 사용기록 관리 현황을 검토할 필요가 있으며 이를 위해 관리자는 정기적으로 관리 현황을 작성하여 서면으로 보안관리자에 제출하도록 한다. (연 2회 권장)
- 정보시스템 사용기록의 열람 권한은 담당자로 한정되어야 하나 보안사고 발생 시 필요한 경우 연구기관의 장과 보안책임자의 승인하에 예외적으로 열람이 허용된다.

5.4 전산장비의 폐기

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	연구원
◎	◎	

5.4.1 전산장비의 처분 및 재사용

업무에 이용된 전산장비가 완전하게 폐기되지 않으면 외부인의 습득에 의해 혹은 외부 이관 시 외부인에 의해 복구되어 민감한 정보가 유출될 수 있다. 이에 처분 과정에서의 실수에 의한 정보 유출을 최소화하여야 하며 이를 위해서는 저장매체의 안전한 처분을 위한 절차를 마련하고 준수하는 것이 필요하다

내용

- 폐기 대상인 전산장비는 다음과 같다.
  - 업무용 PC, 노트북, 서버
  - 업무용 휴대전화
  - 업무용 카메라
  - 업무용 캠코더 등
- 전산장비를 폐기하는 방법은 다음과 같이 여러 가지 방법이 있다.
  - 소자란 저장매체에 역자기장을 이용해 매체의 자화값을 “0” 으로 만들어 저장자료의 복원이 불가능하게 만드는 것을 말한다.
  - 완전포맷이란 저장매체 전체의 자료저장 위치에 새로운 자료(0 또는 1)를 중복하여 저장하는 것을 말한다.
  - 완전파괴(소각·파쇄·용해)란 파쇄조각 크기가 0.25mm 이하가 되도록 물리적으로 파괴하는 것을 말한다.
- 전산장비에 저장된 자료가 다음 사항에 해당되는 경우에는 이를 삭제하여야 한다.
  - 기증 등으로 전산장비가 외부에 영구히 이관되는 경우
  - 사용연한이 경과하여 폐기 또는 양여할 경우
  - 무상 보증기간 중 저장매체 또는 저장매체를 포함한 정보시스템을 교체할 경우
  - 전산장비의 임대기간이 만료되어 반납할 경우

- 고장 수리를 위한 외부 반출 등 보안 통제할 수 없는 환경으로 이동할 경우
- 그 밖에 사용자 변경 등으로 저장자료 삭제가 필요하다고 판단되는 경우

실행지침

① 전산장비 처분을 담당하는 관리자를 지정하고 자료의 안전한 폐기를 위한 규정 및 지침을 마련해야 한다.

• 관리자는 아래 표의 저장 매체 자료별 삭제방법에 의거 삭제하여야 한다.

저장자료 / 저장매체	공개자료	민감 자료 (개인정보 등)	비밀자료 (대외비 포함)
플로피디스크	㉮	㉮	㉮
광 디스크 (CD · DVD 등)	㉮	㉮	㉮
자기 테이프	㉮ · ㉯중 택일	㉮ · ㉯중 택일	㉮
반도체메모리 (EEPROM 등)	㉮ · ㉰중 택일	㉮ · ㉰중 택일	㉮ · ㉰중 택일
	완전포맷이 되지 않는 저장매체는 ㉮ 방법 사용		
하드디스크	㉱	㉮ · ㉯ · ㉰중 택일	㉮ · ㉯중 택일

㉮ : 완전파괴(소각 · 파쇄 · 용해), ㉯ : 전용 消磁장비 이용 저장자료 삭제

㉰ : 완전포맷 3회 수행, ㉱ : 완전포맷 1회 수행

• 전산장비 사용자가 변경된 경우, 비밀처리에 사용한 정보시스템은 완전포맷 3회 이상, 그 외의 정보시스템은 완전포맷 1회 이상으로 저장자료를 삭제하여야 한다

• 전산장비를 외부 이관 또는 용도를 전화하여 사용하고자 할 경우에는 저장된 자료를 완전히 삭제한 후 포맷을 하여야 한다.

• 전산장비 내부 자료의 삭제를 외부업체에 의뢰할 때에는 관리책임자가 입회하여 삭제 절차 · 방법 준수여부 등을 확인·감독하여야 한다.

• 전산장비의 폐기가 완료된 경우 또는 재사용하는 경우에는 부록 서식 *호에 따라 연구보안담당 부서의 확인을 받아야 하며 확인서를 보관하여야 한다.

• 관리책임자는 전산장비 처분 관리대장을 마련하여 폐기일자와 폐기방법을 관리대장에 기록해야 한다.

5.5 데이터 전송

해당과제	
모든과제	보안과제
O	O

이행대상		
연구기관	연구책임자	연구원
◎	◎	O

5.5.1 개인용 저장매체에 전송

업무용 컴퓨터 자료를 복사, 전송, 저장 등의 행위를 통해 기관의 허가 없이 개인용 정보매체에 소지하여 외부로 반출하거나 업무 목적이 아닌 개인적 목적으로 사용할 경우 주요 연구정보가 유출될 가능성이 높다. 따라서 필요에 의해 개인용 저장매체에 저장하고자 하는 경우에는 자체 보안 규정에 따라 절차를 통하여 수행하도록 한다.

내용

- 개인용 저장매체 전송은 업무용 컴퓨터에서 개인용 저장매체로의 자료 이동을 유발하는 일체의 모든 행위를 의미한다.
- 서약서 작성 및 계획
  - 전송 · 복사 · 저장하려는 내용
  - 해당 연구원에 대한 정보
  - 자료 소지의 목적
  - 개인용 저장매체로 자료를 이동하는 날짜
  - 개인용 저장매체에 연구정보를 소지하는 기간
  - 개인용 저장매체로 인해 연구정보가 외부에 유출되어 손실을 입을 경우, 그에 대한 처벌을 받겠다는 서약 및 서명
- 연구책임자 및 연구보안관리자로부터 사전 승인을 득한 후 개인용 저장매체로 자료를 전송할 수 있다.
- 자료 소지 허가 기간 만료 후에는 자료를 완벽하게 제거하는 사후관리 방안을 마련하여야 한다.

실행지침

- 원칙적으로 업무 목적 외에 단순히 개인 목적으로 개인용 저장매체에 연구정보를 소지하는 것은 금지하도록 한다.
- 업무 목적으로 개인용 전송매체에 연구정보를 저장해야하는 경우 해당 연구원은 연구책임자에게 신청서를 작성하여 제출하도록 한다. 신청서에 포함되어야 할 내용은 아래와 같다.
  - 소속 및 이름
  - 저장하려는 연구정보
  - 연구정보 소지 기간
  - 사유
  - 본인의 소지로 인해 연구정보 유출 시에 대한 책임과 서명
- 일반과제의 경우 연구책임자가 신청서 검토 후 승인하는 것으로 절차를 끝내되 보안과제의 경우 연구책임자가 신청서를 검토 후 연구기관에 제출하여 사전 허가를 받도록 한다.
- 연구원으로부터 받은 신청서는 연구기관이 일정기간 보관해야 한다. 신청서를 보관함으로써 누가 어떠한 연구정보를 언제 전송, 복사, 저장하였는지 파악할 수 있으며 추후에 보안사고가 발생했을 시에 이를 토대로 원인과 유출자에 대한 추적에 도움이 될 수 있다.
- 연구기관의 승인 후에 연구원은 보고했던 바와 같이 개인용 저장매체에 복사, 전송 등을 수행하게 되는데, 보안과제의 경우는 연구책임자가 제출한 신청서에 기록된 내용과 연구원이 수행한 바가 일치하는지의 여부를 검토하여야 한다.
- 신청서에 기록된 소지 기간 만료 후에도 연구원이 연구정보를 삭제하지 않은 채 지니고 있다면 삭제할 것을 요구하여야 한다.

5.5 데이터 전송

해당과제	
모든과제	보안과제
	O

이행대상		
연구기관	연구책임자	연구원
◎	◎	O

5.5.2 외부로의 전송

연구를 수행하는 과정에서 필요에 의해 자료를 외부로 전송하는 경우가 빈번하다. 인터넷 망을 통해 정보가 전송되는 과정에서 외부 침입에 의해 혹은 외부기관 수신자에 의해 유출될 가능성을 항상 염두에 두어야 한다. 따라서 자료를 전송하는 과정에서 정보가 악의적으로 유출되는 사고를 방지하기 위한 예방책을 마련하여야 한다.

내용

· 자료를 외부로 전송하는 형태는 다음과 같다.
  - 전자메일
  - 팩스
  - 인스턴트 메시징(instant messaging)
  - 공유디스크

· 외부로 전송할 중요한 자료는 다음과 같이 분류할 수 있다.
  - 보안과제 관련 정보
  - 비밀자료로 분류된 정보
  - Ⅰ, Ⅱ, Ⅲ급으로 분류된 정보
  - 대외비로 분류된 정보

실행지침

1. 자료의 전송형태에 따른 보안대책과 절차의 수립

㉠ 전자메일

- 연구정보 자료의 전송 시, 내부메일이 아닌 외부메일의 사용을 통제해야 한다.
- 전송되는 메일을 필터링하기 위해 내부메일 시스템에 다음과 같은 항목에 규칙을 지정하여 위반 사항이 있을 시 전송을 차단해야 한다.
  - 전송 · ID · 메시지크기 · 키워드(제목, 본문, 첨부 파일)
  - 첨부파일 이름 · 첨부파일 개수 및 용량 · 수신자 주소
- 지정된 규칙을 불가피하게 위반하는 경우, 연구책임자에 보고하여 승인을 받은 후에 전송이 가능하도록 해야 한다.

㉡ 팩스

- 별도로 보안이 강화된 팩스장비를 이용하여 자료를 전송해야 한다. 단, 암호화 장비 도입 시 국정원에 사전 승인을 받아야 한다.

㉢ 인스턴트 메시징

- 메신저와 같은 인스턴트 메시징을 통한 자료 전송은 가급적이면 통제하고 불가피한 사태가 발생한 경우에는 자료를 암호화하여 전송해야 한다.

㉣ 공유 디스크

- 웹하드와 같은 디스크 사용을 자제하고 불가피한 경우에는 자료를 암호화하여 업로드해야 한다.

② 전송하고자 하는 자료의 내용에 따라 보안대책을 마련해야 한다.

ⓐ 보안과제 연구정보 및 비밀자료

- 보안과제의 연구정보 및 비밀자료를 메일로 첨부하여 보내고자 하는 경우에는 첨부파일을 암호화하여 전송해야 한다.
- 전송된 자료의 수신자 확인을 위한 사용자 인증 절차를 수행하도록 해야 한다.

ⓑ 대외비 자료

- 전송하는 자료를 암호화하여 전송해야 한다.

ⓒ 일반자료

- 암호화는 사용자가 필요하다고 판단되는 경우에만 적용하고 그 외에는 암호화를 적용하지 않아도 무방하다.

자료 내용 / 보안 조치	보안과제	비밀자료	대외비	일반자료
자료 암호화	○	○	○	△
(수신자) 사용자 인증	○	○	△	△

(○ : 필수 사항, △: 선택 사항)

5.6 데이터유출 제한

해당과제	
모든과제	보안과제
	O

이행대상		
연구기관	연구책임자	연구원
◎		

5.6.1 데이터 유출가능 경로 관리

최근 들어 발생되고 있는 정보유출 사고는 점차 다양화, 전문화되는 특징을 지니고 있다. 대부분 중요한 연구 정보 또는 자료는 종이매체가 아닌 정보시스템에 저장, 유통되어지고 있기에 이를 통한 정보유출도 많이 발생한다. 따라서 중요한 연구정보가 무단으로 외부에 노출되는 보안사고를 예방하기 위하여 미리 데이터 유출가능 경로를 파악한 후 이에 대한 보호대책 방안을 마련하여야 한다.

내용

· 대표적인 정보유출 경로 및 위협은 아래 표와 같다

정보유출 경로	정보유출 위협
이동식 매체	·불법 복사에 의한 연구정보 유출 ·이동식 매체 분실에 의한 연구정보 유출
홈페이지	·홈페이지 취약점을 이용한 DB 유출 ·피싱·파밍을 통한 연구정보 유출
물리적 요인	·정보자산 분실에 의한 연구정보 유출 ·외부자의 출입에 의한 연구정보 유출
악성코드	·악성 Active X에 의한 연구정보 유출 ·스마트폰용 악성코드에 의한 연구정보 유출
무선인터넷	·악의적인 무선 AP설치를 통한 연구정보 유출 ·무선 AP 해킹에 의한 연구정보유출 ·Wibro, 4G 등 불법 접속에 의한 연구정보유출

내용

· 이동식 저장매체를 통한 연구정보 유출
- 이동식 저장매체는 누구나 손쉽게 구할 수 있고 가격도 저렴하며 크기가 작고 가벼워 휴대성이 뛰어난 특성으로 인해 많은 사람들이 사용하고 있다. 하지만 이동식 저장매체는 저장용량도 크고 저장속도도 빠르고 휴대하기가 간편하여 불법적으로 연구정보를 유출하기가 아주 용이할 뿐 만 아니라 분실하기도 쉽다.
- 이동식 저장매체의 반·출입 기록과 사용을 제한하는 내부 통제정책이 없다면 중요한 연구 정보가 외부로 유출되는 보안사고가 반복적으로 발생할 수 있다.
- 연구정보 유출은 이동식 저장매체에 대한 적절한 통제가 이루어지지 않은 점도 있지만 사용자의 보안의식 결여가 가장 큰 문제이며, 이러한 문제는 단순히 연구기관의 차원을 넘어 국가 경제와 경쟁력과 직결되어 있으며 국가 안보에도 큰 영향을 미치게 된다.

· 웹서비스를 통한 연구정보 유출
- 최근 웹 애플리케이션 취약점을 이용한 해킹으로 인해 연구정보가 불법적으로 유출될 가능성이 높아지고 있어 이를 차단하고 방어하기 위한 웹 보안에 대한 관심이 높아지고 있다.
- 대부분의 해킹사고는 웹 애플케이션 취약점을 이용한 해킹이라는 조사 결과가 있듯이 웹 취약점을 이용한 연구정보 유출을 위한 보안 위협은 날로 증가하고 있어 웹 방화벽의 필요성에 대한 인식이 확대되고 있다.
- 홈페이지 변조 사고는 매년 꾸준히 발생하고 있으며 그 방법에 따라 악성코드 유포 및 데이터베이스 유출까지 다양한 침해 사고가 존재한다. 이에, OWASP[1]에서 10가지의 중요한 웹 애플리케이션 보안 위협들에 대해 제시하고 있다. 이러한 10가지 중요한 웹 애플리케이션 보안 위협(OWASP Top 10)의 주 목적은 10가지 보안 위험의 중요성에 대해 개발자, 설계자, 아키텍쳐, 경영자, 그리고 조직을 교육하는데 있으며 그 항목은 아래와 같다.

1) OWASP(Open Web Application Security Project) 비영리 기관으로 공개 웹 애플리케이션 보안 프로젝트를 주도하는 그룹이다.

내용		
번호	구분	설명
A1	인젝션	SQL, OS, LDAP 인젝션과 같은 인젝션 결함은 신뢰할 수 없는 데이터가 명령어나 질의어의 일부분으로써 인터프리터에 보내질 때 발생한다. 공격자의 악의적인 데이터는 예기치 않은 명령 실행이나 적절한 권한없이 데이터에 접근하도록 인터프리터를 속일 수 있다.
A2	훼손된 인증과 세션관리	인증과 세션 관리와 연관된 애플리케이션 기능은 종종 공격자가 다른 사용자 ID를 가장할 수 있도록 암호, 키 또는 세션 토큰을 손상하거나 다른 구현 결함들을 악용할 수 있는 취약점을 발생시킨다.
A3	크로스사이트 스크립팅(XSS)	XSS 취약점은 애플리케이션이 신뢰할 수 없는 데이터를 가져와 적절한 검증이나 제한없이 웹 브라우저로 보낼 때 발생한다. XSS는 공격자가 피해자의 브라우저에 스크립트를 실행하여 사용자 세션 탈취, 웹사이트 변조, 악의적인 사이트로 이동할 수 있다.
A4	불안정한 직접 객체 참조	직접 객체 참조는 개발자가 파일, 디렉토리, 데이터베이스 키와 같이 내부적으로 구현된 객체를 참조하는 것이 노출할 때 발생한다. 접근 통제를 통한 확인이나 다른 보호수단이 없다면 공격자는 노출된 참조를 조작하여 허가받지 않은 데이터에 접근할 수 있다.
A5	보안상 잘못된 구성	훌륭한 보안은 애플리케이션, 프레임워크, 애플리케이션 서버, 웹 서버, 데이터베이스 서버 및 플랫폼에 대해 보안구성이 정의되고 적용되기를 요구한다. 기본으로 제공되는 값은 종종 불안하기 때문에 보안 설정은 정의 구현되고 유지해야 한다. 또한 소프트웨어는 최신의 상태로 유지해야 한다.
A6	민감한 데이터 노출	많은 웹 애플리케이션들이 중요한 연구정보와 데이터를 제대로 보호하지 않는다. 따라서 공격자는 약하게 보호된 데이터를 훔치거나 수정할 수 있다. 중요 자료가 저장 또는 전송중이거나 브라우저와 교환하는 경우 특별히 주의해야 하며 암호화와 같은 보호조치를 하여야 한다.

내용

번호	구분	설명
A7	함수수준의 접근통제 누락	대부분의 웹 애플리케이션은 UI에 해당 기능을 표시하기 전에 기능 수준의 접근 권한을 확인한다. 그러나 애플리케이션은 각 기능에 접근하는 서버에 동일한 접근제어 검사를 수행한다. 요청에 대해 적절히 확인하지 않을 경우 공격자는 적절한 권한없이 기능에 접근하기 위한 요청을 위조할 수 있다.
A8	크로스사이트 요청 변조	CSRF 공격은 로그온(Log-on)된 피해자의 취약한 웹 애플리케이션에 피해자의 세션 쿠기와 기타 다른 인증정보를 자동으로 포함하여 위조된 HTTP요청을 강제로 보내도록 하는 것이다. 이것은 공격자가 취약한 애플리케이션이 피해자로부터의 정당한 요청이라고 착각하게 만드는 요청들을 생성하기 위해 피해자의 브라우저를 강제할 수 있다.
A9	알려진 취약점이 있는 컴포넌트 사용	컴포넌트, 라이브러리, 프레임워크 및 다른 소프트웨어 모듈은 대부분 항상 전체 권한으로 실행된다. 이러한 취약한 컴포넌트를 악용하여 공격하는 경우 심각한 데이터 손실 또는 서버 탈취를 용이하게 한다. 알려진 취약점과 컴포넌트를 사용하는 애플리케이션은 애플리케이션 바어 체계를 손상하거나 공격 가능한 범위를 활성화하는 등의 영향을 미친다.
A10	검증되지 않은 리다이렉트 및 포워드	웹 애플리케이션은 종종 사용자들을 다른 페이지로 리다이렉트하거나 포워드하고 대상 페이지를 결정하기 위해 신뢰할 수 없는 데이터를 사용한다. 적절한 검증 절차가 없으면 공격자는 피해자를 피싱 또는 악성코드 사이트로 리다이렉트하거나 승인되지 않은 페이지에 접근하도록 전달할 수 있다.

· 물리적 정보 유출

- 물리적으로 접근 권한이 없는 외부방문객 또는 내부직원이 중요한 연구시설에 출입하거나 중요한 연구정보가 담긴 내부문서 또는 PC, 노트북, 하드디스크와 같은 저장매체의 부적절한 폐기로 인해 핵심기술 정보가 유출될 수 있다.
- 따라서 철저한 출입통제 정책을 수립하고 주요 연구시설물은 출입 제한구역 또는 통제구역으로 지정하여야 한다. 또한, 중요한 문서 및 저장 매체의 완전한 폐기를 위한 절차도 수립하여야 한다.

내용

항목	내 용
시설보안팀 운영	주요 연구시설의 안전을 위한 전체적인 보안계획 수립, 운용 및 통제 필요
보안상황실	보안 경보장치, 보안센서, CCTV 등 각종 보안 관련 장비의 기능 수행에 의해 통합적인 감시활동을 수행하고 보안장비의 작동상황 파악 필요
인력 경비	24시간 교대 근무로 주요 시설, 정문 및 외곽감시를 수행하며 경보상황에 신속하게 대처
외곽 감시	외부의 불법 침입자를 감지 센서와 CCTV를 통하여 일차적인 침입상황을 감시
정문 보안	출입 인원 및 차량을 통제·검색하며 장애물을 설치하여 만약의 사태에 대비
주 출입구	건물 내부 출입자 및 물품에 대한 통제 및 검색
출입통제	주요시설에 대한 적절한 출입통제를 통해 비인가자의 출입을 제한하여 주요 시설을 보호하고 이를 위해 출입허용 대상을 지정하여 개폐장치가 식별
CCTV	주요 장소 및 위치에 CCTV를 설치하여 그 장소의 상황을 직접 모니터 화면을 통해 감시
침입감지	침입 가능 예상 지역에 감지장치를 설치하여 무단침입 가능성을 미리 방지
유리창문	창문을 통한 침입을 감지하고 외부에서 내부 시설물을 볼 수 없도록 보안장치 설치
위치추적	방문자, 작업자 미치 주요 장비의 위치를 확인하여 무단출입 및 무단방출을 감시
방문자관리	방문자의 출입 목적, 출입 시간, 출입 장소를 확인

[주요 시설 보호조치 세부 기준(예시)]

내용

· 악성코드를 통한 정보 유출

- 악성코드 기술은 나날이 발전하여 새로운 기능이 추가되고 유입경로도 다양해지고 있다. 초창기에 수동으로 전파되던 바이러스와 달리 최근에는 주로 이메일이나 해킹된 웹 페이지, 그리고 메신저, USB 등 다양한 방법으로 유입되고 있다. 이러한 악성코드에 감염된 PC나 정보시스템에 저장된 중요한 연구정보는 고스란히 외부로 순식간에 유출될 수도 있다.

종 류	설명
컴퓨터 바이러스	프로그램을 통해 감염시키는 악성코드
웜	네트워크를 통해 스스로 감염시키는 악성코드
웜바이러스	컴퓨터 바이러스와 웜의 감염방법을 동시에 갖춘 악성코드
트로이 목마	악성 루틴이 숨어있는 프로그램
스파이웨어	사용자 동의없이 설치되어 각종 정보를 수집하는 악성코드
애드웨어	컴퓨터 사용 시 자동적으로 광고가 표시되게 하는 악성코드
하이재커	의도하지 않은 사이트로 이동을 시키는 악성코드

[악성 코드의 종류]

· 무선 인터넷을 통한 정보 유출

- 무선 인터넷은 이동전화, 개인 휴대 정보 단말기(PDA) 등의 무선단말기와 무선랜, 블루투스와 같은 무선데이터 통신망을 이용해 인터넷으로 접속하여 데이터 통신이나 인터넷 서비스를 이용하는 것으로 정의하고 있다.
- 이러한 무선 통신은 노트북이나 PDA에 내장된 무선 LAN, 무선 모뎀, 블루투스 기능 등을 이용하거나 이동 전화기를 무선 모뎀 대신 연결하여 사용하는 등 다양한 방식의 무선 통신이 존재한다.
- 이동성과 전송용량 및 속도 우위에 따라 무선 고정 인터넷과 무선 이동 인터넷으로 나눌 수 있으며 무선 고정 인터넷은 이동성이 제한되나 전송용량 및 속도에서 우위에 있기 때문에 무선 멀티미디어 서비스 제공이 가능하고 반면에, 무선 이동

내용·

인터넷은 이동성에는 제한이 없고 전송용량 및 속도에 제한이 따른다. 최근에는 스마트폰 보급이 급증함에 따라 무선랜을 비롯한 3G/4G 등 일반 음성통신망을 이용한 데이터 통신도 점차 무선 인터넷의 한 부분으로 자리 잡고 있다.

- 무선 인터넷은 이동하면서 언제 어디서나 유선과 동등한 인터넷 서비스를 이용할 수 있다는 편리성으로 인해 많은 연구기관에서 도입을 고려하거나 한정된 장소에서 부분적으로 사용하고 있는 추세이다.
- 하지만, 아직까지 무선망은 유선망보다 정보유출 관점에서 다양한 취약점이 존재한다.

항 목	내 용
무선인터넷 관리지침 부재	무선 인터넷 보안관리 규정 및 지침 부재
무선 AP정보 수집	SSID, MAC, 암호화방식 등 당양한 정보를 WarDriving을 통해 수집
취약한 계정관리	기본 또는 유추 가능한 ID/Password를 통한 접근 시도
전파관리	고도한 전파세기로 인한 외부에서 무선 AP 탐지
물리적 접근제어	무선 AP Reset 및 도난 위협
취약한 암호화 및 인증	·취약한 암호알고리즘의 사용으로 도청 및 비인가 접속 위협 ·인가 MAC 정보수집을 통한 내부 MAC 인증 우회 가능
서비스 거부	무선 AP 장비에 대한 비정상 패킷 전송하여 서비스 장애
비인가 무선인터넷 장비	·내부 비인가 AP설치에 따른 외부 침입 ·가짜 무선 AP설치 및 내부 사용자 접근 유도 ·취약한 외부 무선 AP에 의한 정보 유출 ·허가받지 못한 무선 통신장비를 이용한 연구정보 유출

[무선 인터넷 위협]

실행지침

· 중요한 연구정보 및 자료 유출 경로를 차단하기 위한 보안대책을 다음과 같이 수립하여야 한다.

① 이동식 저장매체 보안대책

- 이동식 저장매체를 통제하기 위한 보안정책을 수립하고 반·출입 승인 절차를 마련하여야 한다.(5.5.2 이동형 매체 관리 참조)
- 이동식 저장매체의 분실 및 제3자의 불법적인 접근을 방지하기 위하여 장치 및 데이터에 적절한 암호화가 이루어져야 한다. 이러한 암호화는 이동매체에 저장되는 모든 정보에 강제적으로 적용되도록 하고 인증된 사용자에게만 접근이 허용되도록 하며 분실 시 저장 데이터의 보호를 위한 삭제 기능 등을 탑재한 이동식 저장매체를 사용하여야 한다.

② 홈페이지 보안대책

- DB 보안을 통한 연구정보를 보호하여야 한다.
  현재 DB 보안 관련 솔루션은 크게 암호화와 접근통제로 구분된다. 아주 중요한 정보는 암호화를 통해 보호하고 권한이 있는 자만 DB에 접근 가능하도록 보호하여야 한다.
- 웹서비스 보안 설정 정책을 마련하여야 한다.
  웹 프로그래밍 작업 시 OWASP Top 10 등 보안 취약점을 고려하여 설계하여야 한다. 따라서 프로그래밍 개발 완료 후 별도의 취약점 점검을 실시하여 취약점을 보완하여야 하며 시큐어코딩 솔루션을 도입하여 개발하면서 취약점을 점검할 수도 있다.
- 웹방화벽을 도입하여 운영하여야 한다.
  웹 애플리케이션 상에서 기본적으로 보안을 고려하여 설계를 하면 다소 안전하지만, 웹 개발자도 예상하지 못한 취약점은 항상 존재하기 때문에 웹방화벽을 도입하여 간편하게 설치함으로써 외부로부터의 공격을 차단하여야 한다.

③ 물리적 보안대책

- 연구기관 출입 통제 대책을 마련하고 주요 시설에 대한 보호 대책을 마련하여야 한다.
  연구기관을 출입하는 방문객의 출입을 통제하고 주요 시설의 불법적인 접근을 차단하기 위하여 보안구역(통제 또는 제한구역)으로 지정하여 비인가자의 출입을 통제하며 이를 감시하기 위한 CCTV와 접근통제를 위한 생체인식장비 등을 설치하고 운영하여야 한다. 또한, 출입관리대장을 구비하여 출입자를 항시 관리하여야 한다.

실행지침

- 문서 및 디스크 폐기 정책을 수립하여야 한다.

  PC상에 주요 연구정보를 삭제해도 쉽게 복구가 가능하여 제 3자에게 정보가 유출될 수 있다. 따라서 주요 문서는 문서파쇄기로 처리하여 복구가 불가능하도록 조치하여야 하며 저장 매체는 의미없는 데이터를 수 차례 덮어쓰기(Over-write)하거나 강한 자기장을 이용하는 방법, 물리적으로 파쇄하는 방법 등 적절한 방법을 사용하여 저장된 데이터가 복구되지 않도록 조치하여야 한다.

④ 악성코드 보안대책

- 정보시스템의 정식 프로그램 설치 및 주기적인 업데이트 정책을 수립하고 시행하여야 한다.

  PC 또는 서버, 이동식 저장매체 등에 불법 프로그램 설치를 자제하고 전용 백신 프로그램을 의무적으로 설치하도록 해야 한다. 또한, 백신 프로그램 및 운영체제를 포함하여 모든 프로그램의 취약점을 제거하기 위하여 주기적으로 최신 버전으로 업데이트하여야 한다.

- PC 또는 서버에 악성코드가 유입되지 않도록 보안 정책을 적용하여야 한다.

  모든 정보시스템은 도입 시 설정된 최초 환경 설정값을 악성코드 감염으로 인한 중요한 연구정보가 유출되지 않도록 내부 보안정책에 맞게 변경하여야 한다.

⑤ 무선 인터넷 보안대책

- 무선 인터넷 관리 정책 및 지침을 수립하여야 한다.

  무선 인터넷 서비스 범위 및 용도를 정의하고 접근 통제 및 관리 방안 등을 구체적으로 마련하여야 한다.

- 무선 인터넷 장비 관련 보안설정 및 주기적인 보안점검 등을 실시하여야 한다.

  무선 장비 관리자 계정 관리를 강화하고 무선 AP 브로드캐스터 기능의 비활성화를 통해 보안 수준을 향상시킬 수 있으며 무선통신 구간의 강력한 암호화 및 인증으로 연구정보를 보호할 수 있다. 또한 비인가 무선 AP 탐지 및 비인가 단말기 탐지 등 주기적인 보안점검을 통해 불법적인 접속을 차단하여야 한다.

5.6 데이터유출 제한

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	연구원
◎		O

5.6.2 전산자료에 대한 접근 통제

연구과제 관련 정보 및 연구기관 운영 정보까지 주요 자료들의 불법 유출과 오·남용을 방지하기 위하여 이에 대한 접근을 엄격하게 통제하는 보안 대책이 필요하다. 따라서 담당 관리자를 지정하여 직책 및 업무에 따라 각종 전산 자료에 대한 접근권한을 차등적으로 제한하고 접근기록을 관리할 필요가 있다.

내용

- “접근권한” 이라 함은 정보시스템에 접속하여 정보자원을 활용할 수 있는 권한과 정보를 생성·변경·열람·삭제 등 이용할 수 있는 권한을 말한다.
- “전산자료”라 함은 전산장비에 의하여 전자기적 형태로 입력·보관되어 있는 각종 정보를 말한다.
- 주요 정보에 대한 접근 권한을 효율적으로 운영하기 위해서는 정보의 중요도에 따른 등급과 접근권한 부여 기준을 사전에 마련하고 접근권한 심사위원회와 접근권한 담당자를 임명하여 체계적으로 운영하여야 한다.
- 접근 권한의 오·남용 및 정보 유출 여부를 검증하기 위하여 정보의 생성·변경·열람·삭제 등의 이용 내역을 기록하고 보관하여야 한다.
- 주기별 점검 사항은 사전에 마련하여 시행하여야 하며 내용은 다음과 같다.
  - 월간: 사용자 등록 및 변경현황 유지
  - 분기: 인사이동에 따른 사용자 계정 삭제 또는 사용중지 조치여부, 시스템별 접근권한 오·남용 여부 확인
  - 반기: 시스템 운영부서 또는 소속기관의 접근권한 관리실태 점검

실행지침

1. 접근권한 관리책임자 지정・운영

・연구기관의 장은 이용자에 대한 본인확인 및 접근권한 부여에 대한 책임부서 및 책임자를 지정하고 운영하여야 한다.

・권한관리책임자는 이용자의 본인확인 및 접근권한 확인을 위한 업무를 수행하여야 한다.

2. 접근권한 정책 수립

・연구기관의 장은 정책 수립 시 전산자료의 보호등급 분류 기준 및 업무담당자의 접근 권한 부여 기준을 마련하여야 한다.

・접근권한은 해당 업무와 관련된 정보시스템, 응용 프로그램 및 정보만 접근할 수 있도록 직위 및 임무에 따라 차등적으로 부여하여야 한다.

・권한관리책임자는 시스템 관리자가 적절한 승인 절차없이 주요 정보를 생성・열람・가공할 수 없도록 하여야 하며 주요 정보 및 개인정보 등에 직접 접근할 수 없도록 보안조치를 하여야 한다.

・정보자료 보안 등급별 분류는 「국가정보보안기본지침」 제27조 2항을 따르거나 자체 규정에서 정할 수도 있다.

3. 접근권한 심사위원회 구성・운영

・심사위원회 구성은 위원장 1명과 위원 3~4명으로 한다.

・운영 방법은 자료 제공 및 이용 여부 등 주요 사항을 심사・의결한다.

4. 본인확인 방법 및 절차 마련

・권한관리책임자는 업무담당자, 서비스 이용자, 시스템관리자, 외주직원 등의 본인확인 방법 및 절차를 마련하여 시행하여야 한다.

5. 이용내역의 기록 및 보관, 시스템 구축

・접근 기록은 로그인 성공여부와 무관하게 기록・유지하여야 하며 그 내용은 다음과 같다.

- 이용자 접근기록 및 이용 시간
- 이용자 식별 정보
- 이용자 및 시스템관리자가 생성・변경・열람・삭제한 정보의 내용 및 사유
- 그 밖에 접근권한 오・남용 및 정보유출 여부를 검증하기 위해 필요하다고 판단되는 정보

- 정보 이용내역과 관련된 자료는 최소 3년이상 보관·관리하여야 한다.
- 이용내역에 대한 기록이 변경·삭제될 수 없도록 시스테을 구현해야 하며 권한관리책임자의 사전 승인이 없는 한 시스템관리자 외에는 접근할 수 없도록 하여야 한다.
- 정보시스템 접속 시도 오류발생 시 시스템관리자에게 자동 통보하는 기능을 구현하여야 한다.
- 접근기록의 양이 많을 경우 자동화된 분석 도구를 사용하여 점검하여야 한다.

6. 접근권한 점검 및 관리

- 조직개편·인사발령·업무분장의 변경 등으로 업무담당자의 접근권한을 변경해야 할 경우 권한관리책임자는 지체없이 접근권한을 변경하여야 한다.
- 권한관리책임자는 소관 정보시스템 및 주요 정보에 대해서 접근권한 관리의 적절성 및 접근권한 오·남용 여부를 주기적으로 점검하여야 한다.

5.7 데이터 백업

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	연구원
◎	O	

5.7.1 사내 백업시스템

내부 연구원에 의한 실수, 외부 공격에 의한 파일손상, 도난, 기타 의도하지 않은 시스템 손상 및 오류 등에 의해 연구정보를 담고 있는 시스템 파일이 손상될 수 있다. 이에 대비하여 원내에 자체적으로 원본파일을 보호할 수 있도록 백업정책을 수립하고 백업시스템을 구축하여야 한다.

내용

- “백업”은 임시 보관을 일컫는 말로 데이터를 미리 임시로 복제하여 문제가 발생하여도 데이터를 쉽게 복구할 수 있도록 복사 및 저장하여 보관하는 것을 의미한다.
- 연구기관은 백업시스템을 도입하기 이전에 백업 시스템의 체계적인 운영을 위하여 아래와 같은 사항을 검토하여야 한다.

㉠ 백업담당자 및 관리자 지정

㉡ 백업 대상(필요한 백업 정보의 수준 식별)

- 업무와 관련된 데이터의 적절한 백업을 위해서는 백업의 대상이 되는 데이터의 종류, 용량, 중요도를 잘 파악해야 한다.
- 백업 대상의 예는 다음과 같다

· 운영체제(OS)	· 소스
· 데이터베이스	· 사용자 데이터
· 시스템소프트웨어	· 메일 / 이미지
· 엔진 및 구성(파라미터)파일	· 일반 파일
· 응용프로그램	· 기타 업무와 관련된 모든 데이터

㉢ 복구 시 소요되는 시간

㉣ 백업 주기 및 보관기간
- 백업 주기는 전체 백업(백업 시점에서 대상 데이터 전체를 백업)을 기준으로 데이터의 중요도에 따라 일 단위, 주 단위, 월 단위 등으로 나누어 수행한다. 보관기간은 데이터의 중요도에 따라 다르게 적용되는데 연구기관별로 보유한 자료 보존 연한 등 시스템의 외부적 요인에 의해 결정될 수 있다. (보관기간 예: 2주, 4주, 6개월, 영구)

㉤ 백업 방법
- 백업방식은 일회 백업 시 전체를 백업대상으로 하거나 변경분만을 대상으로 하는 가에 따라 전체 백업과 증분 백업으로 구분되며 백업 시의 업무서비스 제공여부에 따라 온라인 백업(실시간 백업)과 오프라인 백업으로 분류할 수 있다.

㉥ 백업 수행 시간대
- 업무의 흐름을 파악하여 백업을 수행하기 위한 최적의 시간대를 결정해야 한다. 데이터 백업 시 데이터의 손실을 최소화하고 백업시간 동안 서버 부하 등으로 업무에 미치는 영향을 최소화하기 위함이다.

㉦ 보관 장소
- 항온항습장치가 구비되고 장애 및 재해로부터 안전하게 보호할 수 있는 장비가 구비된 장소에 백업매체를 보관하여야 한다.

㉧ 백업 파일 보관 기간 및 삭제

㉨ 백업 관리 대장의 기록

실행지침

1. 백업담당자 및 관리자의 지정

· 연구기관에서는 백업시스템의 체계적인 운영을 위하여 백업시스템의 전반적인 관리를 책임지고 운영할 담당자와 관리자를 임명하여야 한다. 백업시스템 관리자가 수행하여야 할 백업 관련 주요업무는 다음과 같다
- 백업 대상 구성 및 추가
- 백업 및 복구 수행
- 백업 수행 결과 모니터링
- 백업 장비 및 백업 매체 관리
- 백업 장애 발생 시 장애처리

- 개선 사항 확인 및 적용
- 백업 관리 대장 기록 및 보관

2. 백업 대상

· 백업 대상에 따라 백업의 종류는 크게 두 가지로 분류되며 시스템 백업과 데이터 백업으로 나뉜다. 시스템 백업은 컴퓨터의 시스템 파일(OS, 시스템 설정 파일, 시스템 로그 등)에 대한 백업을 의미하며 데이터 백업은 연구과제와 관련된 모든 파일(응용 프로그램 파일, 연구관련 정보 등)에 대한 백업을 의미한다.

· 업무 및 백업의 효율성 측면에서 생산되는 모든 데이터를 백업하는 것은 좋은 방법이 아니다. 따라서 초기 백업 시스템 구축 시 백업 대상으로 보안등급이 일정 수준 이상이거나 연구기관에서 중요하다고 판단되는 시스템 파일 및 데이터로 한정하여 백업하도록 백업정책을 마련하여야 한다.

3. 백업 주기 및 보관 기간

㉠ 주간 백업

- 매주 지정된 요일에 실시하며 주간 백업을 이용한 데이터 복구 시 장애시점으로부터 최대 일주일 전의 데이터로 복구되어 최대 일주일간의 데이터가 손실될 수 있다. 그러나 사용자 작업 혹은 주중의 증분 백업을 이용하여 데이터 손실을 최소화 할 수 있다.

  주간 백업은 주로 일일 백업대상에서 제외되는 경우 또는 백업시간 확보가 일주일에 한번만 가능한 경우에 수행되며, 일일 백업 시 변경분만 백업하는 증분 백업의 경우에는 반드시 주간 전체 백업을 받아야 한다.

㉡ 월간 백업

- 매월 지정된 날에 실시하며 보관 기간 역시 사용자 요청에 의해 보관한다. 시스템 예방점검과 연계하여 월 1회 이상 시스템 점검 및 월간 전체 백업을 실시하는 경우도 많다.

㉢ 연간 백업

- 매년 말이나 그 다음해 초에 실시하며 보관 기간은 사용자 요청에 의해서 하기보다는 데이터의 특징에 따라 1년/5년/10년과 같이 장기로 보관할 필요가 있을 때 실시하며, 시스템 전체(OS, 응용프로그램, 관련 사용자 데이터 등)를 백업하는 것이 좋다.

㉣ 임시 또는 수시 백업

- 주요 변경작업 전 또는 설치작업 완료 후에 실시하는 백업이다. 또는 보안과제 관련 업무 중 중요한 중간 결과물의 발생 시 연구책임자의 요청에 의한 비정기 백업도 임시 백업에 포함된다. 보관 주기는 각 백업 요청 시점에 보관 주기에

대한 요청을 받아 그에 따라 보관한다. 하루에서 영구 백업에 이르기까지 다양한 보관 주기로 이루어진다.

· 백업주기 및 보관기간 설정 등에 대한 최종 결정은 해당 업무담당자가 백업주기 및 보관기간 등이 명시된 백업 요청 문서(부록 백업신청서 참조)를 백업관리자에게 보내어 상호 조정함으로써 이루어지게 된다. 이러한 결정과정의 상호 조정 및 문서화하는 것은 향후 문제 발생 시 책임 소재의 명확화 등을 위해 중요하며 결정된 사항들은 가급적 백업정책에 반영하여야 한다.

4. 백업 방법

㉠ 오프라인 백업과 온라인 백업

- 오프라인 백업: 오프라인 백업은 업무가 종료된 후 데이터베이스를 다운시키고 별도로 백업하는 시간을 확보 후 백업을 수행하는 방식이다, 업무상 다운시간을 확보할 수 있는 경우에 사용되며 가장 확실한 데이터베이스 백업 방식이다. 오프라인 백업의 경우 백업파일의 보관 매체는 플로피 디스크, 자기테이프, 광 디스크, 플래시 메모리, 광학 자기 디스크. 하드 디스크 혹은 종이문서를 활용하는 방법이 있다.
- 온라인 백업 : 실시간 백업이라고도 불리며, 오프라인 백업과 달리 컴퓨터나 데이터베이스가 운영 중인 상태에서 백업하는 것을 의미한다. 오프라인 백업의 경우 업무 종료 후 진행되도록 계획을 세우는 반면 온라인 백업은 과제 수행과 관련된 파일의 생성이나 편집, 응용 프로그램의 설치, 운영 체제에 패치 적용 등 활발하게 업무가 진행 중인 상황에서 백업하는 방식으로 기존의 백업과는 백업이 진행되는 시점에 있어서 차이가 있다. 온라인 백업의 목적은 데이터 손실의 최소화이다. 연구 과제를 수행하는 동안에는 많은 파일이 수정되거나 생성되고 삭제될 수 있다. 업무 후에 진행하는 백업은 업무의 최종 결과가 저장된 파일만을 백업할 뿐 과정은 백업할 수가 없다. 온라인 백업은 하나의 파일에 대해서도 수정된 횟수 만큼 파일의 버전을 저장하고 기존의 버전으로 복원할 수 있다.

㉡ 전체 백업과 중분 백업

- 전체 백업 : 백업하고자 하는 데이터 전체를 백업하는 형식이며 월간백업 혹은 연간백업과 같은 백업 시기의 간격이 긴 경우에 실시한다.
- 중분 백업 : 전체 백업이후로 다음 전체 백업이 실시되기 직전까지 전체 백업 이후의 변화된 데이터를 백업하는 방식이다. 다음 백업까지의 공백기간 동안 생성된 파일의 손실에 대한 위험을 방지할 수 있다.

5. 보관 장소

· 오프라인 백업의 경우 별도의 하드웨어 형태의 보관 매체가 존재하는데 이를 보관하는 장소 또한 신중히 고려되어야 한다. 백업파일이 저장되어 있는 매체는 적정 온도와 습도 하에서 내화 금고에서 보관되는 것이 가장 이상적이다. 이는 외부의 충격이나 화재 또는 수재 등의 재해에도 견딜 수 있기 때문이다. 내화 금고와 같은 특수한 설비가 구비되지 않았다면 보관용 캐비넷 등을 이용하여 별도의 독립된 장소에서 분리하여 보관할 수 있어야 한다. 다음은 일반적인 백업매체 관리요령이다.

  - 습기나 직사광선은 피하도록 한다.
  - 고압선, 발전장치 등 자기장이 발생할 수 있는 물체를 멀리한다.
  - 손상된 백업매체는 드라이브에 강제로 장착하지 않는다.
  - 전산운영에 적합한 수준의 공조 및 소방시설과 내화금고가 갖추어진 장소에 보관한다.

· 또한 백업 매체에 식별 가능한 문자, 숫자 또는 기호 등을 부착하여 관리해야 한다. 다음은 백업매체 라벨링 사례이다.

가.

1	2	3	4	5	6	7	8	9

나. 1~2) 기관 구분
다. 3~4) 업무명 또는 데이터명
라. 5~6) 백업년도 또는 데이터 용도
마. 7~9) 백업 주기별 일련번호 또는 월일

6. 백업관리대장의 기록

· 백업관리자는 백업을 수행할 때마다 그 내용에 대해서 관리대장에 기록하여 백업 시스템이 체계적으로 운영되고 있는지 검토하여야 한다.

5.7 데이터 백업

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	연구원
◎		

5.7.2 원격지 백업

자체 내부 백업시스템에 의해 중요한 자료들을 백업한다 하더라도 화재, 수해, 지진 등 자연재해로 인해 자체적으로 보관하고 있던 백업자료가 모두 소실될 수 있다. 따라서 이러한 경우를 대비하여 원거리 지역 보안시설에 백업 자료의 사본을 별도로 보관하도록 한다.

내용

- 백업 실시 후 재난 및 재해에 대비하여 백업 테이프를 외부에 보관하는 경우가 많은데 이를 원격지 백업 또는 볼팅(Vaulting)이라 한다.
- 원격지 백업 시 고려할 사항은 다음과 같다.
  - 원거리 백업 장소의 결정
  - 백업 방법
  - 백업 주기
  - 원격지 백업시스템의 정기적 점검

실행지침

1. 원거리 백업 장소

- 원격지 백업의 장소로 동일 건물 내 또는 너무 멀리 있는 원격지는 적절하지 못하다. 동일 건물 내 보관하는 경우, 건물 재난 발생 시에 백업시스템과 동시에 데이터 소실이 일어날 수가 있으며 너무 멀리 있는 원격지에 보관하게 되면 오프라인 백업 시 보관 매체의 운송시간이 과다하게 길어져 백업, 복구하는 경우에 비효율적이다. 따라서 연구기관에서 발생한 재난의 피해를 피하기에 충분하고 너무 멀지 않은 장소를 고려하여 결정해야 한다.

실행지침

- 원격지용으로 백업된 테이프는 테이프 공급자들이 권장하는 온도와 습도 하에서 내화 금고에 보관되는 것이 가장 이상적이다. 이는 외부의 충격이나 화재 또는 수재 등의 재해에도 견딜 수 있기 때문이다. 내화 금고와 같은 특수한 설비가 구비되지 않았다면 테이프 보관용 캐비넷 등을 이용하여 별도의 독립된 장소에서 분리하여 보관할 수 있어야 한다.

2. 백업 방법

- 원격지 백업은 정기적인 스케줄로 운영하며 원격지에 테이프를 보관하는 것으로 백업 소프트웨어에서 원격지 백업만을 위해 별도 백업을 수행하기도 하지만 정기 백업 시 두벌씩 데이터를 백업하거나, 백업 완료 후 매체 복사를 통해 한 벌을 소산할 수 있다.
- 외부로 소산되는 테이프들은 매체 관리대장을 만들어 기입하고 식별이 용이하도록 저장매체에 라벨링 작업을 해야 한다. 매체 관리대장 양식의 예제는 부록을 참고한다.
- 원내 백업과 마찬가지로 원거리 백업도 온라인 백업과 오프라인 백업으로 나뉠 수 있다.

㉠ 온라인 백업

- 서버를 이용하여 원격지에 자동으로 데이터가 백업되도록 하는 방식이다. 보안제와 같은 중요한 연구를 수행할 때 연구 과정에서 산출되는 모든 자료의 소실을 방지하기 위하여 온라인 원격지 온라인백업이 권장된다.

㉡ 오프라인 백업

- 오프라인 백업의 경우 온라인 백업과 달리 보관 매체를 통하여 보관하는 것이므로 원격지 보관용 매체를 별도로 두어야 한다. 또한 원거리 백업만을 위해 별도로 백업을 수행하기도 하지만 정기 백업 시 두벌씩 데이터를 백업하거나 백업완료 후 매체 복사를 통해 원격지 보관용 한 벌을 백업할 수 있다. 원거리에 보관되는 매체들은 별도로 라벨링 작업을 하여 쉽게 식별이 가능하도록 하며 백업관리 대장에 기록하여 백업현황을 관리하여야 한다.

3. 정기적 점검

- 원격지 백업시스템은 필요 시 비상용으로 사용됨을 보장하기 위하여 정기적으로 시스템 점검 작업을 실시하고 모의 복구시험도 실시하여야 한다.

5.8 전산망 보호 설비

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	연구원
◎		

5.8.1 정보통신망 보호 설비 마련

중요한 연구 정보 및 성과물을 저장·보관하고 있는 PC나 서버 등으로부터 정보를 유출하기 위해서는 정보통신망의 취약점을 이용하여 내부망에 침입하여야 한다. 내부 PC와 서버가 아무리 보안이 잘 유지되고 있다 하더라도 정보통신망의 불법적인 침해로 인해 중요한 정보가 유출되거나 소실될 가능성은 항상 존재한다. 따라서 정보통신망은 외부의 불법적인 침해로부터 보호해야 할 중요한 대상임으로 이를 위한 보호대책을 마련하고 보안시스템을 구축하여야 한다.

내용

· 외부망과 연계되는 구간에 정보통신망의 안전성을 제고할 수 있는 정보보호시스템을 설치하고 운영하여야 하며 정보보호시스템은 다음과 같다.
  - 침입차단시스템(Firewall)은 IP 주소와 접속 포트 등을 기준으로 접속을 선택적으로 차단/허가할 수 있도록 구현된 시스템을 말한다.
  - 침입탐지시스템(IDS: Intrusion Detection System)는 네트워크 상 또는 시스템 내부에 알려진 해킹시도나 비정상 행위가 발견될 경우 이에 대해 경보를 해주는 시스템을 말한다.
  - 침입방지시스템(IPS: Intursion Prevention System)은 인터넷 웜 등의 악성코드 및 해킹 등에 기인한 유해트래픽을 차단하는 시스템을 말한다. 침입탐지시스템의 공격탐지를 뛰어넘어 탐지된 공격에 대해 웹 연결을 끊는 등 적극적으로 공격을 차단하는 시스템이라고 할 수 있다.
  - 가상사설망(VPN: Virtural Private Network)은 공중망을 이용하여 개별망들을 하나의 사설망처럼 구성하여 안전한 통신을 할 수 있도록 보장하는 것으로 인증, 암호화, 터널링 등의 기술로 보안을 가능하게 하는 것을 말한다.

- 바이러스월(Virus-wall)은 외부망으로부터의 악성 바이러스 및 불법적인 공격을 사전에 차단함으로써 내부망의 자원을 보호해줄 수 있는 시스템을 말한다.
- 통합보안장비(UTM: Unified Threat Management)은 하나의 장비에서 여러 보안 기능을 통합적으로 제공하는 시스템을 말한다.

실행지침

1. 정보통신망 보안장비 설치

- 정보통신망에 영향을 주는 웜, 바이러스, 해킹 등의 침입을 방어하고 외부망과 연계되는 주요 회선의 안전성을 강화하기 위해 보안장비를 설치하여야 한다.
- 보안장비 설치에 따른 통신속도 저하 등의 문제가 발생하지 않도록 구성하여야 한다.
- 안전한 네트워크 서비스에 대한 지속적인 제공과 업무 연속을 위해 정보보호시스템에 대한 부하분산을 할 수 있도록(로드밸런싱 및 이중구조 등) 구성하여야 한다.

2. 정보통신망 보안장비 운영

- 정보통신망을 효과적으로 보호하기 위해 보안장비들을 통합 관리할 수 있는 세부지침을 마련하여야 한다.
- 보안장비에 적절한 필터링 규칙 등을 설정하고 적시에 기능을 할 수 있도록 주기적으로 확인하여야 한다.
- 보안장비의 보안 기능이 설정한대로 작동되고 있는지를 주기적으로 점검하여야 한다.
- 보안장비를 운영하는데 있어 가장 중요한 부분인 네트워크에 영향을 주는 웜, 바이러스, 해킹 등의 최신 공격 패턴에 대한 업데이터 및 시스템 자체에 대한 보안패치가 수시로 설치될 수 있도록 조치하여야 한다.
- 보안장비의 가용성을 적절히 확보하여 운영되고 있는지를 주기적으로 점검하여야 한다.

5.9 접근 제한

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	연구원
◎	◎	

5.9.1 내부망 연결 제한

외부로부터의 불법적인 침입을 차단하기 위하여 신원이 불분명한 사용자 또는 내부망의 보안관리정책을 준수하지 않은 시스템의 내부망 접근을 차단하기 위하여 내부망 접속 시 적절한 보안대책을 마련하고 이행하여야 한다.

내용

- 내부망에 연결된 정보통신장비를 비롯하여 전산장비와 중요한 연구관련 자료를 보호하기 위하여 불법적인 내부망 접속을 제한하는 대표적인 방법으로 라우터/스위치 네트워크 장비에 보안정책을 설정하는 방법과 네트워크 접근제어(NAC: Network Access Control) 전용 장비를 설치하는 방법이 있다.

① 라우터/스위치에 의한 내부망 연결 제한

- 외부망과 내부망을 연결하는 라우터/스위치 등의 네트워크 장비에 접근제어 설정 기능이 없다면 침해사고 발생 시 즉각적으로 대응할 수 없다. 이런 경우 특정 프로토콜 및 서비스를 허용하게 되는 상황이 발생하여 전체 네트워크 보안을 전반적으로 약화시킬 수 있으며 내부 네트워크 구성요소들을 외부의 공격으로부터 보호할 수가 없다.
- 라우터/스위치 등의 네트워크 장비는 단순히 데이터 전송을 위한 라우팅/스위칭 장비로서의 역할을 담당할 뿐 만 아니라 보안 기능을 탑재한 장비로서 다음과 같은 보안 설정 기능을 지니고 있다.
  - 불필요한 트래픽 및 프로토콜 필터링
  - 서비스 제거
  - 비인가자의 접속제한 조치 등

② 침입차단시스템에 의한 연결 제한

· 외부망과 내부망 사이에 침입차단시스템을 설치하여 허용되지 않은 사용자와 서비스가 내부망에 접근하지 못하도록 접근통제를 실시할 수 있다.

출발지 주소	출발지 포트	목적지 주소	목적지 포트	정책
외부	Any	내부메일호스트	SMTP	허용
외부	Any	내부뉴스호스트	NNTP	허용
외부	Any	내부NTP호스트	NTP	허용
외부	Any(UDP)	내부DNS호스트	DNS(UDP)	허용
Any	Any	Any	Any	거부

[접근통제 규칙 설정 예]

· 이처럼 IP주소와 서비스 포트(Port)에 대해 접근을 허용할 것인지 거부할 것인지 설정하여 연구기관의 접근통제 정책에 따라 인가되지 않은 접근은 차단할 수 있다.

· 장비의 부하를 분산하고 내부망의 연결 제한을 효율적으로 운영·관리하기 위하여 라우터/스위치와 침입차단시스템의 보안 기능을 적절하게 혼용하여 사용하는 것이 좋다.

③ NAC을 통한 내부망 연결 제한

· 네트워크 접근제어(NAC)는 내부망에 접근하는 접속 단말의 보안성을 강제화할 수 있는 시스템으로 허가되지 않은 사용자나 웜 또는 바이러스, 악성 봇넷에 감염된 장비가 네트워크에 접속하는 것을 원천적으로 차단하여 전체 네트워크를 보호하기 위한 시스템을 말한다.

· 네트워크 접근제어 장비가 지원하는 주요 보안 기능은 다음과 같다.

- 접속제한

  신원이 불분명한 사용자와 네트워크 보안관리 정책을 준수하지 않은 장비에 대하여 내부망 접속을 제한하는 기능이다.

- 접속장비 무결성 검사

  내부망에 접속하고자 하는 단말기가 내부망에에 접근할 수 있도록 허용하기 전에 단말기의 보안상태(최신 보안패치 적용, 악성코드 감염여부, 주요 보안제품 설치여부 등)를 점검하고 필요한 경우 조치를 취하도록 한다.

- 차단/격리

  무결성 검사 결과에 따라 단말기의 내부망 접근을 차단/격리하고 문제를 해결하도록 하는 기능이다. 내부망 전체에 악영향을 미칠 수 있는 단말기가 내부망에 접속

하는 것을 원천적으로 차단하여 내부망의 시스템과 중요한 자료를 보호할 수 있다.

- 사용자 인증
  내부망 접속 사용자의 신원과 역할을 확인한다.

실행지침

1. 내부망의 연결 제한 지침 마련

- 외부의 악의적인 침입 및 불법적인 접근으로부터 내부망을 보호하기 위하여 내부망의 접속을 제한하기 위한 보안정책을 마련하여야 한다.
- 내부망의 연결을 제한하기 위한 보안장비들 간의 효율적인 운영 및 관리 지침을 명시하여야 한다.

2. 내부망의 연결제한 보안장비 운영 관리

- 불법적인 내부망 접근을 차단하기 위하여 라우터/스위치, 침입차단시스템, 네트워크 접근제어시스템의 보안 기능 설정에 대한 적합성과 타당성을 정기적으로 점검하고 관리하여야 한다.
- 보안장비의 네트워크 실시간 트래픽 및 로그정보를 정기적으로 분석하여 침해사실 여부를 모니터링하여야 한다.
- 보안장비를 보호하고 고유 기능을 완벽하게 수행하기 위하여 시스템 관리자 접속 인증을 강화하고 OS패치, 보안패치, 보안규칙(Rule) 패치 등 최신 버전(Version)로 항상 유지하고 관리하여야 한다.

5.9 접근 제한

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	연구원
◎		

5.9.2 무선통신망 관리

무선통신망은 유선통신망에 비해 이동성과 편의성이 뛰어나지만 외부로부터 불법적인 도청 또는 침입이 보다 수월하기 때문에 보안 측면에서 상대적으로 취약한 구조를 지니고 있다. 따라서 무선 구간에 대한 보안을 강화하여 연구정보의 기밀성, 가용성, 무결성을 높이기 위한 조치 방안을 마련하고 시행하여야 한다.

내용

- 무선(AIR)구간은 무선전송 방식으로 통신이 이루어지는 구간을 말한다.
- 사용자 인증은 무선랜에서 사용하는 802.1x의 프로토콜에 따라 인증방식이 다르지만 기본적으로 사용자 아이디와 비밀번호를 부여하는 인증방식과 인증서를 이용하여 인증하는 방식이 존재한다.
- 무선랜 스니핑은 무선랜에서 사용하는 802.1x 프로토콜중에서 일부 프로토콜은 기본적으로 통신에서 사용하는 데이터의 암호화를 제공하고 있지 않아 악의적인 목적을 가진 내부 사용자나 외부 사용자가 무선랜 상에 전송되는 데이터를 도청하는 것을 말한다.
- WPA2(Wi-Fi Protected Access)는 무선랜 데이터의 보안성을 제공하기 위해 Wi-Fi Alliance에 의해 정의된 보안 프로토콜이며 IEEE 802.11i 표준을 기반으로 AES 암호 알고리즘을 적용하고 있다. WPA2는 단말을 인증하고 데이터 프라이버시를 제공하는데 사용된다.
- WAP(Wireless Application Protocol)은 사용자가 무선 단말기를 사용해서 인터넷상의 정보를 신속하게 검색, 표시할 수 있는 통신 규약으로 WAP 게이트웨이는 무선망과 인터넷 사이에 설치하여 정보를 전송한다.
- 무선랜 서비스는 최근 이동성과 편의성으로 인하여 급속하게 사용되고 있지만 무선랜 프로토콜 상의 다양한 취약점으로 인하여 특별한 인증절차없이 엑세스포인터(AP)에 접속하여 비인가된 사용자가 주요 네트워크에 접근할 수 상황이 발생할 수 있으므로 다양한 보안기술을 적용하여 보안을 강화하여야 한다.

- 사용자는 항상 인증을 통해서 엑세스 포인터에 접속할 수 있도록 하고 전송되는 데이터의 암호화만 이루어져도 무선랜 구간에서 발생하는 대부분의 해킹을 차단할 수 있으므로 암호화 전송이 가능하도록 구성하여야 한다.
- 등록되지 않은 엑세스포인트의 사용에 대한 점검 등 무선랜 장비에 대한 관리적·기술적·물리적 보안대책 및 정기점검 방안을 마련하여야 한다.

실행지침

1. 무선통신망 보안관리 지침 마련

- 무선통신망의 효율적인 보안 관리 및 운영을 위하여 무선통신망 관리자를 지정·운영하여야 한다.
- 보안상 취약한 무선통신망의 신설 또는 증설은 최대한 자제하고 무선랜은 유선 네트워크 설치가 어려운 장소에 한하여 한시적으로 사용하도록 한다.
- 무선랜 서비스가 보안상 취약한 구간이 될 수 있음을 인지하고 이에 대한 보안방법과 이행절차, 사용자 인증, 무선구간 데이터 암호, 무선랜 장비 관리 등을 명시하여야 한다.

2. 무선통신망 접근제어 및 암호화

- 접근을 제어하는 방법으로는 접근하고자 하는 정보기기 인증방법과 접속하고자 하는 사용자에 대한 사용자 인증방법이 있다.
- 무선 단말기가 엑세스포인트로 접속할 때는 만드시 사용자 인증을 거치도록 하여야 한다.
- 아이디와 비밀번호를 통한 기본 인증외에 접속권한을 가진 사용자의 MAC 주소를 등록하여 지정된 MAC 주소의 랜카드를 장착한 PC에서만 접속할 수 있도록 제한하여야 한다.
- 무선통신망의 특성 상 외부의 침입에 의한 정보유출의 가능성이 높은데 이를 방지하기 위하여 암호화하여 통신해야 한다. 암호화 방식에는 WEP, WPA, WPA2 등이 있는데 최신 버전인 WPA2 방법을 적용하여야 하며 128bit 이상 가능한 최대 크기의 암호키를 사용하도록 하여야 한다.

3. 무선통신망 관리

- 부서 이동, 휴직, 퇴직 등 인사에 변동사항이 발생할 경우에는 관리자는 해당 계정을 회수하거나 차단하여 접속할 수 없도록 조치하고 주기적으로 계정 사용자 목록을 점검하여 부적절하게 사용되는 계정은 없는지 확인해야 한다.
- 일정기간 (예; 3개월) 사용되지 않는 휴면 계정은 접속권한을 해지하여야 한다.
- 무선통신망의 설치 시에는 반드시 정보보안 관리자의 사전승인을 받고 인가된 것만 설치하도록 하며 정보보안 관리자는 인가되지 않은 무선통신 장치 사용 여부를 주기적으로 점검하여야

5.10 네트워크 자료 관리

해당과제	
모든과제	보안과제
O	

이행대상		
연구기관	연구책임자	연구원
◎		

5.10.1 네트워크 자료 관리

내부 네트워크 관련 자료가 외부로 유출될 경우 불법적으로 내부망에 접속하고자 하는 비인가자는 이를 이용하여 내부망에 쉽게 침입할 수 있다. 따라서 연구기관 내부에 설치된 네트워크 구성 및 장비 등과 관련된 자료가 외부로 유출 또는 공개되지 않도록 특별한 보안대책이 요구된다.

내용

- 외부에 유출되지 않도록 보안조치가 필요한 네트워크 관련 자료는 아래와 같다.
  - 내부 네트워크 장비의 구성도
  - 내부 정보시스템의 네트워크 구성도
  - 내부 네트워크장비와 정보시스템의 IP 주소 현황
  - 내부 네트워크장비와 정보시스템 운영·관리 현황
  - 내부 네트워크장비와 정보시스템의 보안정책 자료 등
- 네트워크 관련 문서의 생성-활용-보관-폐기 등의 보안절차를 수립하고 문서관리자를 별도로 지정하여 외부에 유출되지 않도록 각별히 주의하여야 한다.
- 네트워크 관련 자료가 저장된 정보시스템은 물리적·관리적 보안대책을 마련하여 보호해야 하며 네트워크 관련 자료는 암호화 등을 통해 외부 유출 시에도 안전하게 보호할 수 있는 방안도 마련하여야 한다.

실행지침

1. 네트워크 자료의 보호대책 마련 및 이행

- 네트워크 자료를 관리하는 책임자와 담당자를 지정·운영하여야 한다.
- 네트워크 자료를 대외비로 지정하여 접권권한이 있는 자에 한하여 자료를 수정하거나 삭제, 열람할 수 있도록 조치하여야 한다.
- 네트워크 자료의 보존 형태에 따른 보안대책을 마련하여야 한다.
  - 전자파일 형태로 보존하는 경우에는 인터넷이 연결되지 않은 정보시스템에 자료를 암호화하여 저장하고 보관하여야 한다. 또한 이 정보시스템은 최소한의 인원만 접근 가능하도록 접근권한을 철저하게 통제하여 권한이 있는 자만이 사용할 수 있도록 물리적, 관리적 보호대책을 마련하여야 한다.
  - 문서 형태로 보존하는 경우에는 제한구역 또는 통제구역에 보관하되, 이중 잠금장치가 있는 캐비넷에 보관하여야 한다.

2. 문서열람대장 비치 및 관리

- 네트워크 관련 자료를 열람하는 자는 반드시 문서열람대장에 소속, 성명, 일시 등을 기입하여야 한다.
- 문서열람대장은 네트워크 문서관리자가 관리하여야 한다.

3. 네트워크 자료 폐기

- 네트워크 자료를 폐기하는 경우에는 복구가 불가능하도록 문서파쇄기로 파기하여야 한다.
- 네트워크 자료를 보관하고 있는 정보시스템을 폐기하고자 하는 경우에는 하드디스크를 복구할 수 없도록 물리적 또는 논리적으로 영구 삭제하여야 한다.

07

부 록

연구보안관리규정 예시

국가연구개발사업
보안관리 조치사항(제 10조 관련)

각종 양식

연구보안관리 우수·미흡사례

미래창조과학부
Ministry of Science, ICT and Future Planning

[별첨 1.1.1]

예 시

연구보안관리 규정(지침)

제1장 총 칙

1 목적

연구보안관리 규정을 제정하는 목적으로 국가연구개발사업의 보안에 관한 업무를 효율적으로 수행하는데 필요한 방법과 절차를 규정하기 위함임을 구체적으로 명시

[참고] 국가연구개발사업의 관리 등에 관한 규정 제1조

제1조(목적) 본 지침의 목적은 「국가연구개발사업의 관리 등에 관한 규정」에 따른 OOO연구기관(이하 '연구원'이라 한다)이 수행하는 국가연구개발사업의 보안대책을 수립·시행함에 있어 필요한 방법 및 절차를 정함으로써 국가연구개발사업의 보안에 관한 업무를 효율적으로 수행하는데 있다.

2 용어 정의

규정의 용어 정의는 「국가연구개발사업의 관리 등에 관한 규정」과 동일하게 적용하되, 이외 사용하는 용어는 추가적으로 명시

[참고] 국가연구개발사업의 관리 등에 관한 규정 제2조

제2조(용어의 정의) 본 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」, 「디자인 보호법」, 「상표법」, 「저작권법」 등 법률에 의하여 지식재산으로 보호되는 모든 성과물을 말한다.

3 적용 범위

규정이 적용되는 범위는 국가연구개발사업으로 한정하고, 소속 연구기관이 주관연구기관인 과제에 참여하는 기관들도 소속 연구기관의 규정이 적용됨을 명시 [참고] 국가연구개발사업의 관리 등에 관한 규정 제3조, 제24조제1항

제3조(적용범위) ①본 지침은 기관이 수행하는 국가연구개발사업에 대하여 적용한다.
②제2조에 따라 기관이 주관연구기관 또는 협동연구기관으로 수행하는 국가연구개발과제에 참여하는 참여기관은 본 지침에 따른다.

4 보안대책 수립・시행

실질적으로 보안업무를 수행하는 보안관리 담당자 지정 및 업무 수행에 필요한 보안관리 지침 마련 등 보안대책 수립과 이행의 필요성 명시 [참고] 국가연구개발사업의 관리 등에 관한 규정 제24조제1항

제4조(보안대책 수립・시행) 연구기관의 장은 국가연구개발사업 관련 보안관리 담당자를 지정하고 보안관리 지침을 마련하는 등 보안대책을 수립・시행하여야 한다.

5 연구보안심의회 구성

보안업무를 자문하고 심의하기 위한 위원회 구성과 운영에 관한 세부적인 내용을 규정 [참고] 국가연구개발사업의 관리 등에 관한 규정 제24조의3

제5조(연구보안심의회) ①보안업무의 효과적인 수행과 운영관리에 관한 사항을 심의하기 위하여 연구보안심의회(이하 '위원회'라 한다)를 둔다.
②위원회는 위원장 1인을 포함하여 5인 이상 10인 이내의 위원으로 구성한다.
③위원회의 위원장은 OOO로 하며, 위원은 직원 중에서 기관장이 임명하고 위원의 임기는 2년으로 하되 연임할 수 있다.
④위원장은 위원회를 통할하며 위원장이 유고 시는 위원장이 지명하는 위원이 그 직무를 대행한다.
⑤위원회의 서무를 처리하기 위하여 간사 1인을 두며 간사는 보안담당부서의 장이 된다.
⑥심의안건 중 경미한 사항은 서면결의로 처리할 수 있다.
⑦위원회는 다음 각 호의 사항을 심의·의결한다.
1. 국가연구개발사업과 관련된 기관 보안관리 규정의 제·개정
2. 연구개발과제의 보안등급 변경에 관한 사항
3. 국가연구개발사업과 관련된 보안사고의 처리 및 보안 관련 규정 위반자의 처리에 관한 사항
4. 연도별 보안업무 세부시행계획 수립에 관한 사항
5. 보안업무 감사·지도·점검에 관한 사항
6. 그 밖에 연구보안심의회의 위원장이 필요하다고 인정하는 사항

제2장 보안등급 분류

6 보안등급 분류 기준

상위법과 일치하도록 보안등급 분류기준을 명시하고 보안등급 표기 의무화와 보안업무규정 및 군사기밀보호법 시행령에 의한 예외적 사항도 규정 [참고] 국가연구개발사업의 관리 등에 관한 규정 제24조의4

제6조(분류기준) ①연구개발과제의 보안등급은 다음 각 호와 같이 분류한다.
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」 제2조제2호의 국가핵심기술과 관련된 연구개발과제

라. 「대외무역법」 제19조제1항 및 같은 법 시행령 제32조의2에 따른 수출허가 등의 제한이 필요한 기술과 관련된 연구개발과제

마. 그 밖에 중앙행정기관의 장이 보안과제로 분류되어야 할 사유가 있다고 인정하는 과제

2. 일반과제: 보안과제로 지정되지 아니한 과제

②연구개발과제 수행 과정 중 산출되는 모든 문서에는 제1항에 따라 분류된 보안등급을 표기하여야 한다.

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

7 보안등급 분류절차

중앙행정기관의 장이 공고한 보안등급 준수와 보안등급 선정 결과 통보 주체 및 대상범위 명시
[참고] 국가연구개발사업의 관리 등에 관한 규정 제24조의5

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

②연구계약 담당부서는 보안과제 보호를 위해 필요시 연구제목을 가제목으로 부여할 수 있다.

③연구계약 담당부서는 중앙행정기관 또는 전문기관에서 결정된 보안과제 선정 결과를 연구책임자 및 보안 관련 부서에 통보하여야 한다.

8 보안등급 변경

보안등급 변경에 필요한 사항과 변경 절차에 대해 명시하고 보안등급 결과의 통보 대상범위 규정
[참고] 국가연구개발사업의 관리 등에 관한 규정 제24조의6

제8조(보안등급 변경) ①연구책임자가 연구개발과제의 보안등급을 변경하고자 하는 때에는 변경내역, 변경사유 등을 명시하여 연구계약담당부서에 제출한다.

②연구계약 담당부서는 연구책임자가 제출한 연구개발과제의 보안등급 변경사항을 연구보안심의회의 심의를 거쳐 연구기관의 장의 승인을 받아 소관 중앙 행정 기관의 장에게 변경

내용, 변경 사유 등을 제출하여야 한다.

③연구계약 담당부서는 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.

④연구계약 담당부서는 소관 중앙행정기관에 제출한 보안등급의 변경을 철회 할 것을 소관 중앙행정기관으로부터 통보받을 경우 특별한 사유가 없는 한 이와 관련된 기관, 연구책임자 및 보안 관련 부서에 통보하여야 한다.

9 연구개발결과에 대한 보안등급

연구개발과제 결과물은 최종평가 시 결정된 보안등급으로 변경하고 준수해야 함을 명시
[참고] 국가연구개발사업의 관리 등에 관한 규정 제24조의8

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

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

제3장 보안 조치

10 보안등급에 따른 조치

연구기관의 장 및 연구책임자는 보안대책을 수립하고 보안등급에 따른 조치사항들을 이행해야 함을 명시
[참고] 국가연구개발사업의 관리 등에 관한 규정 제24조의7

제10조(보안등급에 따른 조치) ①연구기관의 장은 필요시 연구개발과제의 관리와 관련하여 보안대책을 수립·시행하여야 한다.

②연구기관의 장 및 연구책임자는 제9조의 보안등급에 따른 보안관리 조치를 이행하여야 하며 그 내용은 별표 2와 같다.

③주관연구기관의 장은 중앙행정기관의 장과 보안과제에 대하여 협약을 체결하는 경우 별표 2의 조치사항을 이행하여야 함을 협약에 명시하여야 한다.

11 참여연구원에 대한 보안조치

참여연구원에 의한 기술유출 사고가 많이 발생함에 따라 유출혐의자의 참여 배제 및 보안과제에 참여한 연구원의 비밀취급인가 취득, 외국인 접촉시 보고서 작성, 퇴직 시 조치사항 등 명시 [참고] 국가연구개발사업의 관리 등에 관한 규정 별표2의3

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

1. 연구성과 유출 혐의(전력)자는 연구개발과제에 참여를 원칙적으로 제한한다. 단, 불가피한 사유가 있다고 판단되는 경우에는 연구기관장의 사전 승인을 받아야 한다.
2. 보안과제를 수행하는 참여연구원은 비밀취급인가를 받아야 한다.
3. 보안과제를 수행하는 참여연구원이 당해 연구와 관련하여 외국인을 접촉하였을 경우에는 '참여연구원 외국인 접촉보고서'(별표5)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 '퇴직자보안서약서'(별표6)를 작성하게 하고, 반출(예상)자료에 대한 보안성 검토 및 연구개발결과물 회수, 전산망 접속차단 등에 대한 조치를 하여야 한다.

12 외국기업 및 외국인 등에 대한 보안조치

핵심기술의 국외 유출을 방지하기 위하여 외국기업 및 외국인의 보안과제 참여는 원칙적으로 배제하고 불가피한 사유가 발생한 경우에는 사전 승인절차가 필요함을 명시하고 외국인 연구원에 대한 별도의 보안조치를 마련해야 함을 규정 [참고] 국가연구개발사업의 관리 등에 관한 규정 별표2의3

제12조(외국기업 및 외국인 등에 대한 보안조치) 보안과제의 첨단기술의 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 연구참여승인신청서(별표3)를 작성하여 연구기관의 장에게 사전

승인을 받아야 한다.

3. 연구기관의 장 및 연구책임자는 영문보안서약서 작성, 출입지역 제한, 특이 동향 관리 등 외국인 연구원에 대한 별도의 보안조치를 강구하여야 한다.

13 연구개발결과 공개 시 보안조치

연구개발 결과 공개 시 보안성검토 절차의 필요성을 명시하고 비공개에 해당되는 사항 및 그에 따른 비공개 시한 명시 [참고] 국가연구개발사업의 관리 등에 관한 규정 제18조, 별표2의3

제13조(연구개발결과 공개 시 보안조치) ①연구개발 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, 비공개기간 연장이 필요한 특별한 사유가 있는 경우에는 기간 만료일부터 3개월 이전에 중앙행정기관의 장의 승인을 받아 최대 3년의 범위에서 연장할 수 있다.

1. 중앙행정기관의 장이 제10조제2항에 따른 보안등급을 검토한 결과 보안과제로 분류된 경우: 최대 3년 이내의 범위에서 해당 보안과제에서 정한 기간
2. 주관연구기관의 장이 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

14 통신기기 등의 활용에 대한 보안조치

IT기술의 발달로 휴대용 정보통신기기 및 이메일에 의해 정보가 유출하는 사례가 빈번하게 발생함으로 이에 대한 보안대책 수립과 시행이 필요함을 명시 [참고] 국가연구개발사업의 관리 등에 관한 규정 별표2의3

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

15 연구정보의 국외 유출방지 보안대책

연구개발 정보 및 결과물의 국외 유출을 방지하기 위하여 보안대책을 수립·시행하여야 함을 명시하고 특히, 보안과제인 경우 외국정부나 기관 방문 시 또는 방문할 경우의 조치 사항과 통보대상 범위 규정 [참고] 국가연구개발사업의 관리 등에 관한 규정 제24조제5항, 제6항

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

②보안담당부서의 장은 참여연구원이 보안과제와 관련하여 외국 정부·기관 또는 단체를 방문하거나 방문을 받을 경우에는 연구과제명, 연구책임자, 방문일사장소 및 주요 방문내용 등의 사항을 문서로 소관 중앙행정기관의 장 및 국가정보원장에게 해당 방문일 5일전까지 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 통보 하여야 한다.

16 국제공동연구 시 보안조치

보안과제로 국제공동연구를 진행할 경우 사전 승인 절차 및 협약서에 포함되어야 할 보안조치 사항들을 명시하고 제공되는 정보나 연구개발 결과물에 대한 보안대책의 필요성 규정 [참고] 국가연구개발사업의 관리 등에 관한 규정 별표2의3

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

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

1. 국제 공동연구를 위해서 제공한 자사의 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

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

17 해외 기술이전 시 보안조치

연구개발결과의 해외 기술이전 시 준수해야 할 보안조치 사항이 규정된 관계법령 명시 [참고] 국가연구개발사업의 관리 등에 관한 규정 별표2의3

제17조(해외 기술이전 시 보안조치) 연구개발결과 해외 기술이전(양도) 추진 시는 「산업기술의 유출방지 및 보호에 관한 법률」 제11조(국가핵심기술의 수출 등) 및 제11조의2(국가핵심기술을 보유하는 대상기관의 해외인수·합병 등), 「기술개발촉진법」 제13조(전략기술 수출의 승인 등)를 준수하여야 한다.

18 연구개발 성과물관리

연구개발 성과물을 보호하기 보호대책 수립 및 조치사항들을 명시하고 기술실시 계약 및 연구개발결과 활용 시 고려사항 규정 [참고] 국가연구개발사업의 관리 등에 관한 규정 제20조제6항, 별표2의3

제18조(연구개발 성과물관리) ①연구개발 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.

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

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

19 연구개발과제 보안관리 현황보고

연구개발과제 보안관리 현황 보고대상 범위와 현황 보고내용을 구체적으로 명시 [참고] 국가연구개발사업의 관리 등에 관한 규정 제24조의9

제19조(연구개발과제 보안관리 현황보고) ①보안담당부서의 장은 연구과제의 보안관리 현황을 매년 전문기관의 장에게 보고하여야 한다. 전문기간의 장이 없는 경우 중앙행정기관의 보안관리심의회에 직접 보고하여야 한다.

② 제1항에 따른 구체적인 현황보고 내용은 별표 7과 같다.

20 보안관리 실태점검 조치

국가연구개발사업에 대한 보안관리실태 점검결과에 따른 개선조치 시한과 보고대상 범위 규정 [참고] 국가연구개발사업의 관리 등에 관한 규정 제24조제3항

제20조(보안관리 실태점검 조치) 중앙행정기관의 장 등 관계기관이 국가연구개발 사업에 대한 보안관리 실태를 점검한 후 개선명령을 받은 경우에는 연구기관의 장이 개선명령을 받은 시점부터 6개월 이내 개선조치에 대한 후속조치 결과를 중앙 행정기관의 장 및 국가정보원장에게 보고하여야 한다.

제4장 보안사고 처리

21 보안사고 발생 시 처리

연구개발과제와 관련된 정보의 유출, 누설, 분실 또는 도난 등의 보안사고 유형 및 정의를 구체화하고 보안사고 발생 시 처리방안과 절차 규정 [참고] 국가연구개발사업의 관리 등에 관한 규정 제24조제7항

제21조(보안사고 발생 시 처리)

①연구개발과제와 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, 손괴 또는 파괴
3. 그 밖에 중앙행정기관의 장이 정하는 보안관련 사고

②보안담당부서의 장은 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.
③해당 연구책임자 및 참여연구원, 보안관련 부서담당자는 조사가 종결될 때까지 관련 내용을 제2항에서 명시한 기관 외에 공개하지 아니한다.
④보안담당부서의 장은 보안사고 관련 내용을 연구보안심의회에 보고하여야 하며, 연구보안심의회에서는 보안사고에 대한 내용을 심의하여 처리방법 및 재발방지 대책을 마련하고 필요한 경우 국가정보원의 장에게 보안사고를 예방하기 위한 보안교육 등 관련 대책 지원을 요청할 수 있다.
⑤연구기관의 장 및 연구책임자, 보안관련 부서의 장은 중앙행정기관과 국가정보원 등 관계기관과 합동으로 보안사고 관련 경위를 조사할 경우 조사에 성실히 협조하여야 한다.

22 보안관리 위반 시 처리

보안관리 준수 의무사항을 규정하고 보안관리 위반사항에 따른 처리내용 명시 [참고] 국가연구개발사업의 관리 등에 관한 규정 제24조의10

제22조(보안관리 위반 시 조치) ①연구책임자, 참여연구원, 보안담당부서장 등은 본 규정에서 정하는 사항 및 관련 국가연구개발사업 보안관리규정을 지켜야 한다.
②연구기관의 장은 제10조제2항에 따른 보안관리 조치 및 제24조제1항에 따른 보고 등을 정당한 사유 없이 이행하지 않은 자에 대하여 관계법규 또는 자체 내규 등에 따라 인사상 불리한 조치를 취할 수 있다.
③참여연구원 및 연구 관련 부서 담당자 등은 연구기간 중은 물론 연구종료 후에도 보안유지에 최선을 다하여야 하며, 위반 시 관계법규에 따라 책임을 진다.

제5장 기 타

23 기타

연구보안규정에 모든 사항을 포괄할 수 없기 때문에 연구보안규정 내용 이외의 사항들은 관계법령에 따르도록 명시

제23조(기타) 본 규정에 규정한 내용 이외의 사항에 대해서는 「국가연구개발사업의 관리 등에 관한 규정」 등 관계법령 등에 따른다.

[첨부 1]

보 안 서 약 서

성 명
주민등록번호

상기 본인은 ○○○○연구과제 개발 일원으로 참여하면서 다음 사항을 준수할 것을 서약합니다.

1. 연구보안관리 규정에 따라 과제 이행시 책임과 의무를 다하여 보안을 준수한다.

2. 본 연구과제를 수행하는 과정에서 알 수 있었던 연구기밀에 대해 연구과제 수행중은 물론이고 종료후에도 ○○○연구기관장 허락없이 자신 또는 제3자를 위하여 사용하지 않는다.

3. 본 연구과제 추진성과가 적법하게 공개된 경우라고 하여도 미공개 부문에 대해서는 앞에서와 같이 비밀유지 의무를 부담한다.

4. 본 연구과제가 완료되거나 연구과제를 수행할 수 없게 된 경우, 그 시점에서 본인이 보유하고 있는 연구기밀을 포함한 관련 자료를 즉시 연구개발책임자에게 반납하여 앞에서와 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)

○○○ 연구기관장 귀하

[첨부 2]

국가연구개발사업 보안관리 조치사항(제10조 관련)

1. 보안관리 체계

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

2. 참여연구원 관리

해당 과제	세부 조치사항	이행 대상	
		연구기관	연구 책임자
모든 과제	1. 참여연구원(외국인 포함)의 채용·갱신·퇴직 시 고용 계약서 및 보안서약서를 받고, 이 경우 연구과제 보안 관리 의무 및 그 위반 시의 제재 등을 명시	○	○
모든 과제	2. 연구과제 수행 연구원의 보안의식을 높이기 위한 보안 관련 교육 이수		○
모든 과제	3. 퇴직(예정)자의 반출(예상)자료에 대한 보안성 검토, 연구성과물 회수, 전산망 접속 차단 등을 제때 조치	○	
모든 과제	4. 외부기관 파견자 등 임시직 및 방문자에 대한 별도 보안조치	○	○
모든 과제	5. 연구성과 유출 혐의(전력)자가 과제에 참여할 경우 특별 관리조치	○	
모든 과제	6. 참여연구원의 해외 출장 시 사전 보안교육 및 귀국보고 실시	○	○
보안 과제	7. 외국인 연구원의 별도 보안조치(영문 보안서약서 작성, 출입지역 제한, 반출·반입 물품 제한, 특이 동향 관리 등)	○	
보안 과제	8. 보안과제 참여연구원이 과제와 관련하여 접촉하는 외국인 현황 관리	○	○
보안 과제	9. 외국인 연구원의 보안과제 참여 시 소속 기관장의 승인절차 이행		○

3. 연구개발내용 및 결과의 관리

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

4. 연구시설 관리

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

5. 정보통신망 관리

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

[첨부 3]

외국인 연구 참여 승인신청서

□ 연구책임자
○ 소속 :
○ 직명(직위) :
○ 성명 :
○ 연구과제명 : 국문)
영문)

□ 외국인 연구 참여자

소속 :		직명(직위·급,학년) :
성명 :	국적 :	연락처 :
연구과제 수행 역할 :		

□ 위 외국인이 보안연구과제에 반드시 참여해야하는 사유 :

위와 같이 불가피한 사유로 외국인이 보안연구과제에 참여하게 되었으므로 위 외국인 연구 참여자에게 국가기술개발과제 수행과정상의 보안관리 지침을 숙지시키고 이를 준수시킬 것을 다짐하며, 위 해당자의 출입지역 및 열람가능 자료를 제한토록 하고 특이동향 인지시 그 내용을 보고할 것을 서약하오니 위 외국인이 연구과제에 참여하도록 승인하여 주시기 바랍니다.

년 월 일

연구과제책임자: (인)

○○○ 연구기관장 귀하

[첨부 4]

서 약 서

(Written Oath)

본인은 년 월 일부터 ○○○연구원 연구실에서 근무함에 있어 다음 사항을 준수할 것을 서약한다.

I Hereby pledge myself to observe the fellowing regulations while working in laboratory, the Korea institute of ○○○○ starting on

1. 본인은 귀 연구원의 모든 보안관계 법규를 준수한다.
   to observe all the rules of security.
2. 본인은 근무 중 지득한 기밀사항에 대해 연구 활동 계약기간 중은 물론 계약 종료 후에도 누설하지 않는다.
   not to leak out confidential information which is obtained while at my research work not only during but also after my stay at the ○○○.
3. 본인은 업무수행과 관련하여 사전 허용된 지역에만 출입하고 그 외 허용되지 않은 지역은 출입하지 않는다.
   while carrying out my research work, only to enter premise which has been authorized by the ○○○ advance.
4. 본인은 귀연구원의 내·외부시설에 대한 사진촬영을 하지 않겠으며, 관리책임자의 승인 없이 어떠한 물건도 반출하지 않는다.
   not to take pictures of any ○○○facilities
   not to take any ○○○ assets out of its premise without permission.
5. 본인은 위 사항을 위반하였을 경우 관계 법률에 의해 처벌받게 된다는 사실을 충분히 인식하고 이에 서명한다.
   I duly sigh here with full understanding that I will be punished for any violation of above mentioned regulations.

년 월 일
(Date : .)

국 적 :
(Nationality)
소속 및 직책:
(Position)
여 권 번 호:
(Passport No.)
성 명:
(Name)

Signature : _____

[첨부 5]

참여연구원 외국인 접촉 보고서

결재				

연구과제명			
연구책임자		소속	
연구비 총액		연구기간	
지원기관			

참여연구원		접촉 외국인			접촉일시	접촉사유	비고
직급	성명	소속	직급	성명			

상기와 같이 참여연구원의 외국인 접촉내용을 보고합니다.

년 월 일

연구책임자 : (인)

㈜ 보안과제와 관련하여 외국인을 접촉한 경우에만 작성함.

[첨부 6]

퇴직자 서약서

본인은 ○○○연구기관(이하 "○○연구원"이라 한다)에서 퇴직함에 있어 다음 사항을 숙지하고 이를 이행하지 않을 경우 관계법령에 의거 처벌받을 것은 물론 "○○○연구원"에 손해를 입힐 경우에는 그 손해액을 지체없이 변상할 것을 엄숙히 서약합니다.

1. "○○○연구원"에 근무 중 지득한 국가보안 등에 관한 제반 비밀과 직무상 지득한 과학기술정보 관련 제반 비밀사항 및 중요 기술비밀을 관련법령, 인사규정 제00조, 취업규칙 제 00조의 규정에 따라 일체 누설하거나 도용하지 않는다.
2. "○○○연구원"에 근무 중의 모든 발명, 고안, 장착 및 발견 등에 대하여 "○○○연구원" 또는 그 지정인에게 이를 공개, 양도할 것에 동의하고 그 절차에 적극 협력한다.
3. "○○○연구원"에 근무 중의 모든 연구자료 및 연구결과보고서, 설계서, 청사진 등과 보조기억장치 등에 대하여는 누락 없이 "○○○연구원" 또는 그 지정인에게 인계하고 이를 소지하거나 유출하지 않는다.
4. 퇴직 후 2년간은 "○○○연구원"의 사전승인 없이 "○○○연구원"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 관련법규(국가보안법, 형법, 부정경쟁방지 및 영업 비밀보호에 관한 법률)에 따른 어떠한 처벌도 감수한다.

년 월 일

서약인 주소 :
주민등록번호 :
성 명 : (인)

○○○ 연구기관장 귀하

[첨부 7]

퇴직자의 새 고용기관에 대한 통지서

○ 소속 :

○ 직위 :

○ 성명 :

*** 기관명

**** 귀하

귀 사(기관)의 무궁한 발전을 기원합니다.

귀 사(기관)에 취업한 *** 은 저희 연구기관 재직 중 (~간) *** 업무에 종사하면서 중심적 역할을 하였고 이에 관련하여 저희 연구기관의 중요 연구정보를 보유하고 있습니다.

그러므로 저희 연구기관에서는 이에 대한 저희 연구기관의 연구정보를 유지 관리하기 위하여 위의 사람에게 비밀유지서약서를 제출받은 바 있습니다. 따라서 귀사에서 위의 사람이 저희 연구기관에서 하던 업무와 유사한 업무에 종사하게 되면 저희 연구기관의 중요 연구정보의 비밀을 침해할 우려가 있음을 알려드리오니 부디 저희 연구기관의 연구정보의 비밀을 침해하는 일이 없도록 주의하여 주시도록 통지하여 드립니다.

20 ** 년 월 일

위 서약인 (인)

[첨부 8] (1쪽)

연구개발과제 보안관리 현황

(담당부서: 담당자: 전화번호:)

□ 기관명: □ 기간: 20 . 1. 1 ~ 20 . 12. 31 (1년)

1 연구보안심의회 운영 현황

개최 일자	심의 건수	주요 사항	비고

2 사업 및 과제 현황

대사업명	중사업명	세부사업명	세부(단위)과제			비고
			보안과제수	일반과제수	계	

주1) 대사업명은 프로그램 단위 사업명 기재(예: 미래원천사업, 기초사업, 원자력사업 등)
주2) 중사업명은 중간단계 사업명 기재(예: 미래원천사업 중 나노사업, 바이오사업, 우주사업 등)
주3) 세부사업명은 최하위단계 사업명 기재(예: 나노사업 중 나노원천사업, 나노기반협력사업 등)
주4) 세부(단위)과제는 보고기간에 수행한 세부(단위)과제 수를 기준으로 작성
- 계속과제는 1개 과제로 하되, 보안등급이 변경된 경우에는 변경 후 보안등급으로 기재

3 보안과제 관리 현황

세부사업명	세부(단위)과제명	연구책임자	연구기간		보안과제 지정일자	보안과제 관리 사유
			'10년도	'11년도		
			'10. . .~'11. . .	'11. . .~'13. . .		

주1) 보안과제로 지정되어 있는 과제만 기재(일반과제에서 보안과제로 변경된 과제도 포함)

(2쪽)

4 보안등급에 따른 조치 현황

조치 사항	보안과제 건수	일반과제 건수	비고
① 외국기업 및 국외연구기관 위탁 시 중앙행정기관 승인			
② 외국인 참여 시 기관장 승인			
③ 연구 성과물 대외공개 시 보안대책 수립			
④ 보안점검 및 보안교육 실시 횟수	( )회 실시		
⑤ 국가연구개발사업과 관련된 자체 보안관리 규정 마련 여부	(Y / N)		관련 규정, 조항
⑥ 보안사고 대응체계 마련 여부	(Y / N)		관련 대책 별첨

5 보안과제 해제 현황

세부사업명	세부(단위)과제명	연구책임자	연구기간		보안과제 해제일자	보안과제 해제 사유
			'10년도	'11년도		
			'09. . .~'10. . .	'10. . .~'11. . .		

6 연구개발과제 보안사고 관리 현황

세부사업명	세부(단위)과제명	연구책임자	보안사고 발생일자	보안사고 주요내용	보안사고 처리결과

주1) 필요시 세부명세 첨부

7 그 밖의 건의사항

위와 같이 본 기관의 연구개발과제 보안관리 현황을 제출합니다.

20 . . .

보안관리 부서장: (인)

연 구 기 관 장: (직인)

OOO 연구기관장 귀하

[별첨 1.5.1]

추천대상자 명부

순	소 속	직 위	성 명	공적기간	공적 개요(50자 내외)	기서훈	①징계	②물의 야기
	<예시>							
	경영정보팀	연구원	홍길동	10.05			'95 견책(사면)	무

※ 작성 참고

- 소속 : 해당 부서 기입
- 징계 : 징계처분·불문경고 처분을 받은 연도와 종류 및 사면·말소 여부를 표기
- 물의야기 : 감사원·검·경 등 조사・수사개시, 기소, 민・형사재판 계류, 언론보도 등 업무를 통하여 물의를 일으켜 포상이 합당치 않다고 판단되는 내용 및 일자 표기

공 적 조 서(개인용)

<table>
<tr><td>①성 명</td><td colspan="3">(한 자)</td></tr>
<tr><td rowspan="2">②주민등록번호</td><td rowspan="2"></td><td>③군 번
(군인의 경우)</td><td></td></tr>
<tr><td>④국 적
(외국인의 경우)</td><td></td></tr>
<tr><td>⑤주 소</td><td colspan="3"></td></tr>
<tr><td>⑥소 속</td><td></td><td>⑦재직기간</td><td></td></tr>
<tr><td>⑧직 위</td><td></td><td>⑨직 급</td><td></td></tr>
<tr><td colspan="4">⑩공적요지(50자 이내)</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="4">조 사 자</td></tr>
<tr><td>⑪소 속</td><td colspan="3"></td></tr>
<tr><td>⑫직위(직급·계급)</td><td></td><td>⑬성 명</td><td>(인)</td></tr>
<tr><td colspan="4">위의 기록이 틀림없음을 확인합니다.</td></tr>
<tr><td colspan="4">년 월 일</td></tr>
<tr><td>추 천 관</td><td>직 위</td><td>성 명</td><td>직인</td></tr>
</table>

(뒷 면)

⑭주요경력	
연 월 일	이력사항
. . . ~ . . .	
. . . ~ . . .	
⑮과거 포상기록(훈장·포장·표창별로 기록)	
수여일자(연 월 일)	포상종류
. . .	
. . .	
공 적 내 용	

추천서류 작성요령

Ⅰ. 공적조서

1. 공적조서는 반드시 별첨 서식에 의거 A4용지 종이로 작성
2. 유의사항
   (1) 성명 : 성명은 한글 및 한자로 기재
   (2) 주민등록번호 : 주민등록증에 표시된 주민등록번호를 정확하게 기재
   (3) 군번 : 미기재(공란으로 둠)
   (4) 본적 : 미기재(공란으로 둠)
   (5) 주소 : 읍·면·동·번지까지 자세히 기재
   (6) 소속 : 해당 부서명의 정식 명칭을 기재
   (8) 직위 : 직위가 있는 경우 직위명을 기재
   (9) 직급 : 해당 직급명을 기재
   (10) 공적요지 : 100자 내외로 핵심공적 사항 기재
   (11) ~ (13) 조사자 : 해당 연구보안관리자가 기재하고 반드시 날인
   (14) 주요 경력 : 경력이 많을 경우 묶어서 기재
   (15) 과거 포상기록 : 내부 및 외부 포상 이력을 기재

[별첨 1.5.2]

보안위규 사항 및 처리기준(예시)

구분 / 항목	위반내용		처리기준			
			파면	중징계	경징계	경고
비밀누설	적 또는 가상적국에 누설		○			
	동맹국이 아닌 제3국에 누설		○			
	비인가자에 비밀공개 및 제공			○		
비밀분실	비밀물건 분실			○	○	
	비밀분실 후 미신고			○	○	
	비밀습득 후 미신고			○	○	
비밀미분류	과소 분류				○	○
	일반문으로 분류			○	○	○
비밀관리소홀	비밀물건 방치			○	○	
	비밀보관함 개방				○	○
	비밀 불법 지출 및 대출	인가자			○	○
		비인가자		○	○	
	비밀 임의 파기			○	○	○
	대외비 문건 분실			○	○	
	비인가자에 비밀취급			○	○	
기타	승인절차에 의하지 않고 공개 또는 제공	비밀자료		○	○	
		일반자료			○	○
	신원조사 미필고용원 채용				○	○
	비인가자 통제구역 출입				○	○
	업무목적 이외 비밀수집			○		
	신원정보 누설	임의노출		○	○	
		관리부실			○	○
	승인을 받지 않는 촬영제한 대상 및 지역 촬영	통제구역		○	○	○
		보호구역			○	○
	승인을 받지 않은 자료 열람 및 복사	비밀자료		○	○	
		일반자료			○	○
	기타 규칙상의 제반규정불이행				○	○

[별첨 2.5.1]

국외 출장 귀국보고서

1. 출장 목적

○

○

2. 출장 동기 및 배경

○

○

3. 방문국, 출장기간, 출장자

○방 문 국:

○출장기간: . . . ~ . . .

○출 장 자:

4. 세부 출장 일정

일 자	출발지	도착지	방문기관	업무수행내용

5. 출장 결과

○

○

6. 접촉 인물

기관명	부서명	직책	성명

7. 수집 자료

○

○

[별첨 2.9.1]

외국인접촉 신청서

<table>
<tr><td>접촉 일시</td><td colspan="4"></td></tr>
<tr><td>접촉 장소</td><td colspan="4"></td></tr>
<tr><td rowspan="5">신 청 자</td><td>소속</td><td>직급</td><td>성명</td><td>비고</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td rowspan="5">피접촉
외국인</td><td>소속(소재지)</td><td>직책</td><td>성명</td><td>국적</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td>목 적</td><td colspan="4"></td></tr>
<tr><td colspan="5">상기와 같이 외국인을 접촉하고자 하오니 승인하여 주시기 바랍니다.
20 . .
신청자 직급 : 성명 : (인)</td></tr>
<tr><td>승인권자</td><td colspan="4">소속 : 직급 : 성명 : (인)</td></tr>
</table>

[별표 2.9.1]

외국인접촉 결과서

접촉일시				
접촉장소				
접 촉 자	소 속	직 급	성 명	비 고
피접촉 외국인	소속(소재지)	직 책	성 명	국 적
목 적				
접촉내용 (6하원칙 구체화)				
특이사항				
보 고 자	상기와 같이 외국인 접촉결과를 보고합니다. 20 . . . 직급 : 성명 : (인)			
승인권자	소속 : 직급 : 성명 : (인)			

[별표 2.10.1]

(Written Oath)

본인은 년 월 일 부터 ○○○○연구원 ○○○○○○연구실에 근무함에 있어 다음 사항을 준수할 것을 서약한다.
I hereby pledge myself to observe the following regulations while working in laboratory, ○○○○○(기관명) on _____

1. 본인은 귀연구원의 모든 보안관계 법규를 준수한다.
   to observe all the rules of security.
2. 본인은 근무 중 지득한 기밀사항에 대해 연구 활동 계약기간 중은 물론 계약 종료 후에도 누설하지 않는다.
   not to leak out confidential information which is obtained while at my research work not only during but also after my stay at the ○○○○○(기관명).
3. 본인은 업무 수행과 관련하여 사전 허용된 지역만 출입하고 그외 허용되지 않은 지역은 출입하지 않는다.
   while carring out my research work, only to enter the premise which has been authorized by the ○○○○○(기관명) in advance.
4. 본인이 귀 연구원의 내·외부시설에 대한 사진 촬영을 하지 않겠으며, 관리책임자의 승인 없이 어떠한 물건도 반출하지 않는다.
   not to take pictures of any ○○○○○(기관명) facilities,
   not to take any ○○○○○(기관명) assets out of its premise without permission.
5. 본인이 위 사항을 위반하였을 경우 관계법률에 의해 처벌을 받게 된다는 사실을 충분히 인식하고 이에 서명한다.
   I duly sign here with full understanding that I will be punished for any violation of above mentioned regulation.

년 월 일
(Date : , 20)

국 적(Nationality):
여권번호(Passport No):
이 름(Name):
소속 및 직책(Position):

서명(Signature):

[별표 4.6.1]

외국 정부・기관・단체 방문계획

구분		내용	비고
연구과제명			
연구책임자			
방문일시			
방문장소			
방문 정부·기관·단체	정부·기관·단체명		
	방문인원/대표자명		
	방문목적		
주요방문내용 (6하원칙)			
보안조치사항			

[별첨 2.10.1]

보안서약서 (용업업체 계약체결용)

○ 업 체 명 :

○ 출입인력 수 :

*** 연구기관장 귀하

본 업체는 *** 연구기관의 ( ) 업무수행을 위해 (용역) 계약한 업체로서,

1. 계약에 의거 업무수행에 최선을 다하며
2. 당 업체 직원에 대한 신원확인을 철저히 수행했으며
3. 직원이 책임감을 가지고 규정을 준수하며 성실히 근무할 수 있도록 적극적으로 지도, 관리하고
4. 직원이 업무상 취득한 연구정보에 대하여 비밀유지를 (***~간) 의무적으로 유지하도록 할 것을 다짐합니다.

아울러, 상기사항 소홀 및 불이행으로 발생되는 제반사고 및 손실에 대해서는 관련법에 의한 손해배상은 물론 모든 법적처벌을 감수할 것을 서약합니다.

20 ** 년 월 일

업 체 명:

사업자 등록번호:

대표자: (인)

[별첨 2.10.1]

보안서약서 (용업업체 인력 개인별)

○ 기관명 :

○ 직위:

○ 출입시간:

○ 출입목적:

본 업체는 *** 연구기관의 ( ) 업무수행을 위해 (용역) 계약한 업체 직원으로서 연구 과제를 수행함에 있어 아래 사항을 충분히 숙지하고 성실히 이행 하겠습니다.

1. 본인은 연구 과제를 수행하면서 알게 된 연구기관의 연구정보를 고용 중은 물론 고용 종료 후에도 연구기관의 허락 없이 유출 또는 공개하지 않으며 부정한 목적으로 사용하지 않을 것을 서약합니다.

2. 본인이 연구 과제를 수행하면서 발견 또는 창출한 정보 자산에 대한 권리는 연구기관에 귀속됨을 인정합니다.

3. 고용종료 시에는 기관 내부에서 보유하였던 연구정보와 관련된 모든 자료를 반납 할 것을 서약합니다.

20 ** 년 월 일

성명: (인)

[별첨 2.10.1]

보안서약서 (기타상시출입자)

○ 출입시간:

○ 출입목적:

본인은 ***연구기관의 업무관계 및 방문 중 지득 또는 인지하게 된 연구정보 및 기타 관련 비밀에 대하여 그 어떤 내용도 외부에 누설시키지 않을 것을 서약하며, 아울러 차후 상기의 내용을 누설한 경우 그에 대한 형사상·민사상 책임질 것을 서약합니다.

20 ** 년 월 일

서약자: (인)

[별첨 5.4.1]

전산장비 불용처리 확인서

아래와 같이 보조기억매체(　종　점) 불용처리 및 보조기억매체(　종　점) 재사용에 대해 확인을 요청함

연번	관리번호 (S/N)	매체형태	사유	불용처리	재사용
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

확인일자 :　　년　　월　　일

요 청 자 : (소속、직책　　) 성명 :　　(인)

확 인 자 : 연구보안책임자　　성명 :　　(인)

[별첨 5.7.1]

백업 신청서

1. 일반 사항

신청일자					
신청자 성명		전 화		부서명	

2. 백업 정보

구 분	내 용			
서 버 명(IP주소 명기)				
백업 대상 (해당항목 'Y')	OS ( ) 데이터베이스 ( ) 사용자 일반파일 ( ) 기타 ( )			
백업 주기 (해당항목 'Y')	일간 ( ) 주간 ( ) 월간 ( ) 연간 ( ) 수시 ( )			
백업본 보관기간				
백업 대상 위치				
백업 전체 용량				
백업 희망시간	시작 시간		완료 시간	
특기사항				

※ 신청서 접수정보

접수일시		접수자 성명	
백업 적용일자			
백업 장치		백업 소프트웨어	
특기사항	※ 백업적용 후 신청자에게 회신할 것		

[별첨 5.7.1]

백업결과 보고서

일시	작업자

백업 마스터 서버	백업 대상 서버명	백업 대상	백업 형태 (F/S・DB)	백업 주기	백업결과			백업 도구	비고
					성공	부정확	실패		

【연구보안관리 우수·미흡 사례】

1. 학계

1.1 보안관리체계

▣ 우수 사례

항 목	우수 사례
보안관리 규정	-연구보안 담당부서인 산학협력단에서 '연구자를 위한 지식재산 및 기술이전 매뉴얼'을 제작 배포하고 내용도 아주 우수
공동 및 위탁 연구 시 사전 승인 절차이행	-별도 법인으로 운영 중인 사업단(사무국)에서 부처·관리기관·참여기관 간 과제 협약과 과제 진행 상황을 효율적으로 관리
	-상위 기관과 체결한 연구협약서에 연구보안관리 내용 명시
국외기술 이전 시 관리	-참여기관이 他 기관과 체결한 기술이전계약 현황, 계약서 등을 사업단(사무국)에서 효율적으로 과제 관리

▣ 미흡 사례

항 목	미흡 사례
보안관리 규정	-대학 자체의 '연구보안관리세칙' 및 '국가연구개발보안관리지침'을 최근에 개정된 국가R&D 관리규정 내용 반영 권고
보안관리자 지정	-기관 전체의 보안업무는 본부에서 전담하고 산학협력단은 국가연구개발과제의 연구보안 업무를 총괄 책임 운영 필요
연구보안심의회 운영 및 보안관리 규정	-기관 '보안업무규정'을 '07년 제정·운영중이지만 기관의 보안정책 등을 심의·의결하기 위한 '보안심사위' 실질적 개최 실적 全無하고 규정에 근거한 月 1회 보안진단도 未실시중 *기관의 보안규정을 자체 보안역량을 고려하여 개정, 제도의 현실화 권고
	-'연구개발사업 보안업무규정'을 별도로 마련·운영중이지만 '심의위'도 단 1회만 개최하였고 '08년 제정 이후 現 보안환경을 반영한 규정 개정 全無

	*연구개발과제에 대한 보안성 검토 등을 심의하기 위한 '연구보안심의위' 활성화 권고 *보안과제가 없더라도 연구개발사업의 보안이 필요하다고 판단되는 부분(규정개정, 지침수립, 자체점검반 구성, 보안성 검토 등)에 대해서 보안심의회의 적극적 활동 권고 *同 지침에 따라 마련된 연구보안심의회의 실질적 개최 권고
보안교육 실시	-전 임직원 대상으로 연 1~2회의 연구보안교육 실시 및 국가연구개발사업 수행중인 연구책임자(교수) 및 참여연구원(석박사 등)들의 국가R&D 보안 관련 규정에 대한 인식제고 노력 미흡
보안점검 실시	-기관 자체 '보안점검' 계획 수립, 점검 및 후속조치 등 미흡

1.2 참여연구원 관리

▣ 우수 사례

항 목	우수 사례
외국인 연구원 관리	-내·외국인 채용 시 보안서약서(영문 등) 징구

▣ 미흡 사례

항 목	미흡 사례
외국인 연구원 관리	-전체 참여 연구원 중 외국인 참여인력에 대한 현황 관리 부재
국외 출장 시 고려사항	-해외 출장 시 발표하는 자료에 대한 출장자의 자료 지출내용, 방법, 지재권확보 여부 등에 대한 자가 체크 항목 마련 부재

1.3 연구개발 결과 및 내용의 관리

▣ 우수 사례

항 목	우수 사례
연구결과물 관리	-메뉴얼에 '연구실에서의 연구성과물 보호' 항목을 별도로 마련하여 국가연구개발사업 결과물 보호 노력
연구개발성과물의 권리확보	-특허권/지식재산권 확보를 위해 별도의 전문 관리 부서를 두고 있으며, 연구 성과물 보안을 위해 보안서약서 및 비밀유지서약서 징수, 계약서를 통한 상호 동의 후 이행 등 성과물 보호 노력 강구 -연구개발사업보안업무 규정, 지식재산관리규정, 지식재산권 및 기술이전 관리 매뉴얼(기술사업부 제작), 보안서약서 징구 등 연구보안 및 지재권 관리를 위한 관련 규정 및 제도 마련
연구개발 성과의 대외공개 시 관리	-연구 성과의 대외 공개·제공 시 연구책임자의 검토 후 이행, 기술이전 시 관계 법령 및 절차 준수 등 연구결과물 관리 철저
국외기술 이전 시 관리	-기술이전 관련 부서의 전문성을 기반으로 기술이전계약 체결 시 비밀유지약정(NDA) 체결, 과정별 상세 절차 마련 등 관리

▣ 미흡 사례

항 목	미흡 사례
연구성과물 관리	-과제산출물에 대한 보안등급 표기 未적용, 성과 공개 시 사전 보안성 검토 절차 未수립, 연구보안 담당부서 및 연구보안 심의회의 활동 미흡 등 전반적 연구결과물 관리체계 미흡
보안관리 규정	-자체규정을 이행할 수 있는 구체적인 절차 또는 지침(성과물의 무단 유출 방지를 위한 유의사항, 연구 성과 공개 시 보안성 검토 절차, 세부과제 공동연구 및 위탁계약 시 연구 성과 귀속 및 지재권 정의, 연구보안 자체점검 리스트 및 점검반 구성 등)을 수립하여 규정 이행 및 연구보안에 대한 인식제고를 위한 관심과 노력 필요

연구개발 성과 대외 공개 시 관리	-성과물의 대외 공개 시 보안성 검토 등 연구결과물에 대한 보안 관리가 기관차원의 체계적인 관리절차(지침) 없이 연구책임자 책임 하에 자체 관리로 이루어지고 있으므로 기관차원의 대책 필요

1.4 연구시설 관리

▣ 우수 사례

항 목	우수 사례
출입 통제 시스템	-대학內 각 건물마다 출입통제시설이 모두 갖추어져 있어 출입증 없이 외부인 출입은 불가하고 중요 연구실 등은 보안키로 관리
출입 감시장치	-민간 보안업체의 카드인식 출입통제시스템, CCTV 및 침입감지 센서 등 보안장비 설치 · 운용 *CCTV 290대, 자체 시건장비 370대, 세콤 시건장비 541대 등 운영 중
외부 정보통신매체 반출입 통제	-노트북 외장형 하드디스크 드라이버 등 정보통신매체 반출입 통제 및 매체제어 실시

▣ 미흡 사례

항 목	미흡 사례
연구시설 출입자 통제 및 관리	-집중형 연구실은 번호키 등으로 폐쇄되어 있으나 나머지 각 층 연구실 문은 상시 개방되어 있어 보안취약 요인으로 작용 -연구실 출입통제시스템의 개인별 차등 출입통제 체계 未운용
외부 정보통신매체 반출입 통제	-이동식저장매체 반출입 절차 등에 대한 통제정책 마련 필요 -교수 및 소속 학생 등 개인 노트북·이동식 저장매체 반출입에 대한 통제 다소 미흡
보호구역 별도 관리	-연구실이 제한· 통제구역 등 보호구역으로 지정되어 있지 않고 별도의 보안관리 조치도 부재

외부방문자 출입 통제 및 관리	-외부인의 연구실 방문시, 연구원이 방문자와 퇴실시까지 동행한다고 하나 사실상 내부 실내가 협소한 관계로 안내·통제가 무의미함으로 차선책 마련 필요

1.5 정보통신망 관리

▣ 우수 사례

항 목	우수 사례
내부망 연결 제한 /무선통신망 관리	-사용자 인증기반을 통해 무선랜 접속을 허용하고 외부인의 WiFi 및 유선랜을 통한 접근 통제
내부망 연결 제한	-연구실별 물리적·논리적 망분리 예정 -유선랜 연결 통제를 통해 내부망 접속 제한
보안관리	-PMS 솔루션을 이용, 보안S/W·패치 未설치 PC에 대해 강제 설치 등 보안관리 강화

▣ 미흡 사례

항 목	미흡 사례
보안관리 /소프트웨어 설치	-Scan폴더 공유가 패스워드 설정없이 공유되고 있으며 스캔 결과물이 삭제되지 않고 남아있어 정보유출 위험 존재 -주기적인 보안점검, 취약 서비스 및 공유폴더 허용, 비인가 S/W 설치여부 점검 未실시 등 전반적 보안관리 미흡
무선통신망 관리	-WiFi의 별도 인증절차 부재로 외부인의 학교 내부망 접속 용이 -유·무선 공유기 사용 현황 관리 부재 -유선 폐쇄망에 랜 스위치허브를 연결하여 연구원의 개인 PC 공유
이동형 매체 관리	-연구실의 비인가 개인용 정보통신매체 반출입 통제가 미흡하여 USB 등 외장형 저장매체를 통한 자료유출에 취약 -USB 등 저장매체에 대한 반출입 통제, 내부망 연결 제한 등 보안대책이 마련되어 있지 않아 내부 자료 유출 가능성 존재

외부 반출자료 관리	-연구원에 의한 자료반출 및 e-mail 첨부파일 등 통제 부재
외부 전송자료 관리	-메신저, 웹하드, 외부 이메일 등 자료 유출 저장경로 접속 차단 부재
이동형 매체 관리 /전산장비의 처분 및 재사용	-USB 자동실행 기능 허용으로 악성코드에 감염된 USB 접속시 해킹 피해가 예상되고 파일 공유 S/W를 통한 자료 유출 가능성 존재 -저장매체 폐기 시 사전 승인 및 이관 절차 등 규정 未준수

2. 산업계

2.1 보안관리체계

▣ 우수 사례

항 목	우수 사례
보안관리규정	-'정보보안규정 및 규칙'에 따라 사업장 보안환경을 반영한 ' 정보보안기준' 제정 시행 -他 기업과 달리 '국가연구개발사업에 대한 보안관리기준'을 별도로 마련하여 국책과제의 국가핵심기술, 보안과제 등 면밀 검토·관리 -기관 보안업무 규정인 '산업보안규정' 제정 이래 내·외부 보안환경 변화에 따라 적기 규정 개정
연구보안심의회 운영	-기관 '보안업무규정' 제정 후 보안환경 변화에 따라 기관 특성에 맞는 개정 작업을 수차례 진행하고 기관 차원의 보안관련 사항을 심의·의결하기 위한 '보안업무협의회' 운영
보안관리자 지정	-정보보안규정 및 규칙에 따라 최고 보안책임자를 두고 최근 보안기준을 개정하여 실제 보안책임자(CTO)를 규정하여 보안책임자간 명확한 관계 설정
홍보	-산업보안 표어·포스트 공모전을 실시하는 등 기관 차원의 보안 관심도 제고 노력 우수

보안우수자 /보안위반자	-보안 우수자·위규자에 대한 구체적 포상·징계 기준이 우수하며 위규자에 대한 통계 현황 관리 적절(2년간 유지 관리) *다만, 월별 시행하는 '보안신호등'(월별 팀별로 100점을 부여하고 보안위규·우수 사례별 가감) 제도에 따른 우수 팀·개인 대상 포상·인센티브 시행 권고 -보안점검 위규자에 대해서는 임원이더라도 보안경고 스티커를 부착하는 등 실질적 점검 시행 -휴대폰 보안스티커 未부착 등 보안위규자들을 보안점검에 동참케 함으로써 보안위규자의 보안중요성 인식 배가
비상시 대응계획 수립	-사업장 환경·보안 등 위기 상황별 구체적 대응매뉴얼 구축 -화재·지진·테러 등 비상상황별 대응 프로세스 체계도 우수

▣ 미흡 사례

항 목	우수 사례
보안관리규정	-'연구개발사업 보안업무규정'을 별도로 마련·운영 중이지만 '심의위'도 단 1회만 개최하였고 규정 제정 이후 現 보안환경을 반영한 규정 개정 全無
연구보안심의회 운영	-보안업무협의회를 최근 3년간 개최한 실적이 없으며 보안업무규정 개정시에도 개최하지 않는 등 실질적 심의 기능 다소 미흡
보안점검 및 보안교육 실시	-기관 자체 '보안점검' 계획 수립, 점검 및 후속조치 등 미흡
보안우수자	-사업장 자체의 보안우수팀·인력에 대한 포상 실시 필요
보안 홍보	-기관 차원의 '보안 표어·슬로건' 대회를 개최하여 보안에 대한 부담감을 최소화하고 자연스러운 보안관심도 제고 및 분위기 확산 노력 필요

2.2 참여연구원 관리

▣ 우수 사례

항 목	우수 사례
신입채용 시 고려사항	-사시 징구하는 '영업비밀보호 등 서약서' 이외에 연 1회 '전자서명'을 징구하여 연구원 대상 지속적 보안경각심 제고
채용 시 인원관리 /퇴직자 관리	-입·퇴사시 보안서약서 내용·징구 적절
재직 중 인원관리	-국책과제 수행자에 대한 보안서약서 별도 징구 -사내 변호사를 통해 마련한 보안서약서(3페이지 분량)를 징구받고 임원 등 상위 직급자 대상 '기밀취급자 서약서'도 추가로 징구
국외출장자 관리	-국책과제 해외 출장자의 외국인 접촉 현황 관리 -해외출장자 등에 의한 강연·발표 자료에 대한 보안성 검토과정 우수
보안 점검 실시	-팀별로 교차 확인 방식의 자체 보안점검을 통해 상호간 긴장감을 유도하고 자체 보안강화 개선점 발굴 유도
보안교육	-국책과제에 대한 온라인보안교육 실시 -온라인 보안교육 이수율이 94%가 될 정도로 참여 독려 노력 우수하므로 법정교육화 권고 -직원 대상 '보안교육'을 청렴·성희롱 예방교육 등과 같이 '법정교육'하여 운영(지속적 실시 권고)
외국인 연구원 관리	-내외국인용 보안서약서를 구비하고 있으며 입·퇴사시는 물론 연 1회 보안서약서 징구를 통해 연구인력의 보안경각심 주기적 제고
일시 출입자의 구분 /일시출입자 관리	-외부인 방문시 온라인 회원가입을 통한 방문예약 및 보안 서약서 제출 의무화(출입자별 출입 권한 차등 부여를 통해 출입자 관리)

▣ 미흡 사례

항 목	우수 사례
재직 중 인원관리	-보안서약서 개정시 全직원 대상 개정된 신규서약서 징구는 적절하나 연 1회 정기 징구를 통한 지속적 보안경각심 제고 필요 -정규직뿐만 아니라 비정규직에게도 보안서약서 징구 필요
퇴직자 관리	-입사시 보안서약서 내용에 퇴사 후의 비밀유지의무가 포함되어 있어 퇴사시 별도 보안서약서를 징구하지 않는 관행 개선 필요
국외 출장 시 고려사항	-해외 출장자에 대한 보안관리 강화 권고 *지참자료에 대한 연구책임자에 의한 보안성검토 과정과 별도의 '해외 출장시 보안유의사항'(팝업 형태 또는 출장신청서상에 확인란 추가) 마련 권고
보안 점검 실시	-연구실 보안점검 결과를 형식적으로 작성하고 연구원들에게 전파하고 있지도 않으므로 보안경각심 제고를 위해 구체적 위규 사례를 적시한 결과 작성·배포 필요
외국인 연구원 관리	-보다 엄격히 관리되어야 하는 외국인 연구인력에 대한 보안서약서를 징구하지 않고 있으므로 영문 서약서를 마련하여 징구 필요

2.3 연구개발 결과 및 내용의 관리

▣ 우수 사례

항 목	우수 사례
연구개발 성과물의 권리 확보	-연구개발 사업 보안업무 규정, 지식재산관리규정, 지식재산권 및 기술이전 관리 매뉴얼(기술사업부 제작), 보안서약서 징구 등 연구보안 및 지재권 관리를 위한 관련 규정 및 제도 양호 -논문발표에 따란 지재권 획득 여부, 연구결과물 보호방안에 대해 과제책임자 등에 의한 보안성 검토 과정 우수

연구성과물의 보안등급 부여	-연구성과물의 보안등급 부여 자체 보안규정에 따라 생성되는 문서, 성과물에 보안등급을 나누어 관리하고 DRM 처리
외부기관과 공동 협약 시 연구 결과물의 관리	-해당 과제 관련으로 내부규정에 적정하게 공동·위탁 연구 진행 중 -40개국 122개 기관과 공동연구를 진행 중으로 공동연구 협약서 내용상에 연구보안 내용 우수
문서 생성	-문서 생성 산출되는 모든 문서는 보안용지를 사용하며, 보안 등급 및 내부 품의 프로세스 처리 후 DRM 처리
문서활용/문서보관	-모든 생산 문서를 암호화하여 관리하고 문서반출입 승인시스템 운영 -문서 등급을 'Internal, Confidential, Secret' 등 내용에 따라 3단계로 구분 운영
연구개발 성과의 대외 공개 시 관리	-연구개발 성과의 대외 공개 시 연구성과물의 공개 및 외부 제출시 내부 결재과정을 통해 DRM 해제 처리 후 제공 -연구내용을 외부 공개 시 내부 결재과정을 거쳐 보안성 검토
국외기술 이전 시 관리	-자체 기술이전 프로세스에 따라 기술이전 실시계약 체결 -기술이전 관련 부서의 전문성을 기반으로 기술이전계약 체결시 비밀유지약정(NDA) 체결, 과정별 상세 절차 마련 등 관리 우수 -기술이전계약 전 협상단계에서의 '비밀유지의무'(NDA) 체결 과정 우수

▣ 미흡 사례

항 목	미흡 사례
문서 생성	-연구노트 양식이 노트별로 상이하고 작성요령을 준수하지 않고 있으므로(연구주제, 기간, 작성날짜, 책임자에 의한 확인란 등 기재 미비) 올바른 연구노트 작성을 유도하고 작성 교육 필요
문서 활용	-개인용 문서 반출 시 출입문 보안요원의 '직접 확인'에 의한 반출 시스템은 보안상 취약요인이 많으므로 개선 방안 마련 필요

문서보관	-연구노트 작성이 의무화되어 있진 않지만 특허 등 지식재산권의 안정적 등록·분쟁 대비 올바른 작성요령에 따라 기재 및 교육 권고

2.4 연구시설 관리

▣ 우수 사례

항 목	우수 사례
주요시설물 관리	-본사 보안정책에 따른 외곽 울타리, CCTV 설치 등 시설보안 양호 -연구시설 보안을 위해 적외선감지기 및 광센서, 스피드게이트 등 첨단장비를 설치·운용하고 있어 물리적 시설 보안부분 우수 -민간 보안업체의 카드인식 출입통제시스템, CCTV 및 침입감지센서 등 보안장비 설치 · 운용
방문자 출입통제	-주출입문에 지문인식 출입통제시스템 운영 및 CCTV설치, 협력업체 직원 등 외부인 방문시 방문목적에 따라 3단계로 세분화된 방문자 출입증을 휴대토록 하는 등 시설보안 양호
외부 정보통신매체 반출입 관리	-외부 정보통신매체 반출입 관리▸ 외장형하드·USB 등 정보통신기기 반출입 및 내부 자료 반출을 위한 보안관리 절차가 3개 부서 승인을 거치도록 세부적으로 마련
보호구역 별도 관리	-연구개발과제와 관련된 핵심기술 및 정보를 보관하는 전산실 및 중요시설물에 대해서 보호구역 지정 및 관리

▣ 미흡 사례

항 목	미흡 사례
주요시설물 관리	-기관 정문 인원·차량 통제 이외에 전반적 시설보안 미흡 -외곽 울타리에 대한 CCTV 이외 적외선 센서 또는 침입탐지 센서 도입 검토 필요(자체 진단 내용)
보호구역의 지정 /보호구역 관리	-국책과제 내용, 예산, 개발방향, 참여인원 및 연구실 등 연구 관련 사항과 일반 행정업무 영역 구분 명확화 필요

	-연구실이 제한· 통제구역 등 보호구역으로 지정되어 있지 않고 별도의 보안관리 조치도 부재
외부 입주기관 통제 및 관리	-기관 내부 창업보육센터에 입주한 20개 기업과 체결한 입주계약서에 비밀유지조항을 추가하고 기업 대표자의 보안서약서 징구 필요
연구시설 출입자 통제 및 관리	-연구구역을 보호구역으로 지정·운영하여 외부인 접근 차단 효과는 있으나 내부 직원에 대한 개인별 차등 출입통제 부재로 완벽한 출입통제 미비
외부방문자 출입통제 및 관리	-외부인의 연구실 방문시 연구원이 방문자와 퇴실시까지 동행한다고 하나 사실상 내부 실내가 협소한 관계로 안내·통제가 무의미함으로 별도의 보안대책 필요

2.5 정보통신망 관리

▣ 우수 사례

항 목	우수 사례
보안관리	-내부정보 유출 대비 全 직원 PC에 보안솔루션을 설치하고 非인가 저장매체 사용제한 및 未인가 S/W 설치·파일업로드 차단 -PC 취약공유 폴더 자동 검색 솔루션 이용 -주기적으로 취약점 점검 실시
내부망 연결 제한 /전산망 보호 설비 마련	-내부 네트워크 보호를 위해 관리등급·권한을 차등 부여하고 웜·바이러스 유입 및 해킹 공격에 대비하여 각종 보안장비를 통합 모니터링하고 정기적인 로그분석 실시
외부로의 전송관리	-상용 웹메일을 통한 파일전송을 차단하고 그룹메일을 통해 팀장 승인 하에 자료 전송 가능토록 조치 -주요 파일유출 경로 차단 (P2P, Web Storage, DropBox, ucloud 메신저 등) *카카오톡·MSN 메신저 등 텍스트만 허용(파일 첨부 차단)
무선통신망 관리	-무선통신망 보안강화 정책으로 직원들의 스마트폰 제어를 위해 'Mobile on' 프로그램 설치, 카메라·블루투스·테더링 등 자동 차단

	-사설AP·공유기 사용 여부를 주기적으로 스캔 실시 -무선랜(WiFi) 사용 관련, IP·MAC인증을 실시하여 내방객 및 임직원이 임의로 내부망을 통해 인터넷 사용 불가
내부망 연결제한	-NAC을 통한 내부 IP관리 및 네트워크 접근제어를 실시하고 외부에서 내부 네트워크 접속 시 VPN 솔루션 이용(특정기간만 사용허가) -IP·MAC인증을 통해 내방객·임직원의 임의 내부망·인터넷망 연결 차단

▣ 미흡 사례

항 목	미흡 사례
보안관리	-외부에서의 접속은 방화벽으로 차단하고 있으나 일부 사용자에게는 원격접속, 파일서버 접근을 허용하고 있어 해킹 경로 가능성 존재 -암호설정 없이 공유폴더를 사용(일부)함으로써 접근권한이 없는 사용자에 의한 자료유출 가능성 존재 -실험용 일부 PC에서 비밀번호 없이 실험데이터를 공유하고 있으며 설치가 금지된 문서작성 프로그램 사용 -외부 세미나·출장 등 개인 노트북 사용 후 내부 네트워크로 반입 시 중앙 VMS 점검 이외 해킹·악성코드 보안점검 未실시 *출장용 노트북을 도입 운영하고 사용 후에는 image 백업 및 보안점검 실시토록 권고
장비 관리	-일부 스마트폰을 이용한 PC연결로 매체제어시스템 우회 저장 가능
이동형 매체 관리	-부팅패스워드 未관리로 USB 부팅을 통해 매체제어를 우회하여 자료유출 가능(단, USB 등에 대한 물리적통제 실시) *부팅패스워드 관리 및 시스템 드라이버 설치 제한 권고 -매체제어솔루션이 없어 USB 등 이동형저장매체를 자유롭게 사용 가능
정보시스템 사용기록 관리	-퇴직 전 로그기록 확인과정을 거치나 보안시스템 未구축으로 실질적 로그 분석 불가능

개인용 저장매체 전송 /외부로의 전송 관리	-물리적·네트워크 통제가 되지 않아 개인 USB, e-mail 등을 통한 자료유출에 무방비 -USB 차단시스템 운영이 미흡(단순히 로그는 남기고 있으나 분석은 안됨)하여 개인용 외부저장매체를 통한 내부자료 유출 가능성 존재 *파일명 변경이나 압축을 통한 유출의 경우 사후 추적·분석 不可 -웹메일·웹하드 등으로의 전송자료 로그는 남기고 있으나 未차단
전산망 보호 설비 마련	-네트워크 장비의 기본설정값(private, public) 사용으로 네트워크 정보 노출 등 서비스거부공격(DOS)에 취약
내부망 연결 제한	-IP·MAC 도용시 내부망 접속이 가능하며 공유폴더 접근 등 내부망의 취약성을 이용하여 자료유출 가능
무선통신망 관리	-무선IPS를 일부 사용하여 내부에서 WiFi 테더링을 통한 인터넷 접속을 차단하고 있으나 적용 건물이 제한되어 있어 전반적인 무선보안은 미흡(Wifi, USB 테더링 차단 기능 없음)

국가연구개발사업 보안관리
표준 매뉴얼

발행처 : 미래창조과학부
발행인 : 미래창조과학부 연구제도과
발행일 : 2014년 3월