과학기술정보통신부 소관 과학기술 분야 연구개발사업 보안관리지침

[시행 2019. 10. 15.] [과학기술정보통신부훈령 제90호, 2019. 10. 15., 일부개정]

과학기술정보통신부(연구개발정책과), 044 - 202 - 4523

제1조(목적) 이 지침은 「과학기술정보통신부 소관 과학기술분야 연구개발사업 처리규정」(이하 처리규정이라 한다) 제40조 제4항에 따라 과학기술정보통신부 소관 연구개발사업(이하 "연구개발사업"이라 한다)의 보안관리에 필요한 사항을 정함으로써 첨단과학기술 및 연구결과의 유출을 방지하는 것을 목적으로 한다.

제2조(적용대상 및 적용범위) ① 이 규정은 과학기술정보통신부 소관 연구개발사업을 수행하는 기관 및 연구자, 처리규정 제10조의 전문기관 및 제11조의 연구개발사업단에 적용한다.

② 사업의 보안관리에 관하여 다른 법률에 특별한 규정이 있는 경우에는 그 법률을 따른다.

제3조(보안관리심의회) ① 과학기술정보통신부 소관 연구개발사업의 보안 관리에 관한 사항을 심의하기 위해 심의회(이하 "보안관리심의회"라 한다)를 둔다.

② 보안관리심의회는 다음 각 호의 사항을 심의한다.

1. 연구개발사업 관련 보안관리 규정의 제 · 개정
2. 연구개발과제 보안등급 변경에 관한 사항
3. 연구개발과제 보안관리현황 보고 사항
4. 연구개발사업과 관련된 보안사고의 처리
5. 그 밖에 연구보안심의회의 위원장이 필요하다고 인정하는 사항

③ 보안관리심의회의 위원장은 연구개발사업의 보안관리 업무 담당국장(급) 공무원으로 하고, 위원은 위원장이 지명하는 연구개발사업 관련 과장 10인 이내로 한다.

④ 보안관리심의회에 간사 1인을 두되, 간사는 연구개발사업의 보안관리업무 담당과장이 된다.

⑤ 보안관리심의회 회의는 재적위원 과반수 출석으로 개의하고 출석위원 과반수 찬성으로 의결한다.

⑥ 보안관리심의회의 운영에 관한 사항은 위원장이 정한다.

⑦ 위원장은 필요한 경우 관계자를 출석시켜 의견을 진술하게 할 수 있다.

제4조(연구기관 보안관리심의회) ① 전문기관의 장 및 연구기관의 장은 다음 각 호의 사항을 심의하기 위하여 연구보안관리심의회(이하 "연구보안심의회"라 한다)를 구성 · 운영하여야 한다. 다만, 「중소기업기본법」에 따른 중소기업, 「벤처기업육성에 관한 특별조치법」에 따른 벤처기업 등 조직체계상 연구보안심의회를 운영하기 어려운 연구기관은 그러하지 아니하다.

1. 제5조에 따른 연구개발사업과 관련된 자체 보안관리 규정의 제정 · 개정
2. 연구개발과제 보안등급 변경에 관한 사항
3. 연구개발사업과 관련된 보안사고의 처리

4. 그 밖에 연구보안심의회의 위원장이 필요하다고 인정하는 사항

② 연구보안심의회의 구성과 운영에 관한 사항은 연구보안심의회가 소속된 기관의 장이 정한다.

제5조(연구기관 자체 보안관리 규정) ① 전문기관의 장 및 연구개발사업을 수행하는 연구기관의 장은 연구개발사업을 수행과 관련된 주요 보안 자료 등의 무단유출을 방지하기 위하여 다음 각 호의 사항을 반영하여 자체 보안관리 규정을 마련·운영하여야 한다.

1. 연구보안심의회 구성 및 운영에 관한 사항
2. 연구개발사업 과제 수행과 관련된 보안 등급 분류 및 보안 조치
3. 연구개발사업 과제 수행과 관련된 정보자료, 연구시설, 참여연구원에 대한 보안 조치
4. 연구내용 및 성과물의 대외발표 시 보안조치

제6조(참여연구원에 대한 보안조치) ① 연구기관의 장은 연구책임자 및 참여연구원이 보안과제를 수행 할 경우 과제 협약 시 [서식 1]의 보안서약서를 징구하여야 한다.

② 연구기관의 장은 보안과제로 분류된 과제를 수행하는 연구책임자 및 참여연구원의 변경 시에는 신규연구원의 보안서약서를 징구하여야 한다.

제7조(보안등급의 분류) 연구개발과제는 다음 각 호의 기준에 따라 보안등급을 분류한다.

1. 보안과제 : 결과물 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 미래핵심기술로서 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 과학기술정보통신부 장관(이하 "장관"이라 한다)이 보안과제로 분류되어야 할 사유가 있다고 인정하는 과제
2. 일반과제 : 보안과제로 지정되지 아니한 과제

제8조(보안등급 분류 절차) ① 연구책임자가 처리규정 제16조제4항에 따라 연구개발계획서를 작성할 때에는 같은 조 제2항에 따라 중앙행정기관의 장이 공고한 연구개발사업의 보안등급을 따라야 한다.

② 장관 또는 전문기관의 장은 연구개발과제를 선정할 때에 처리규정 제17조제1항에 따른 연구개발과제평가단으로 하여금 보안등급 분류의 적정성을 검토하게 하고 그 결과를 반영하여 보안등급을 결정하고 해당 연구기관의 장에게 통보한다.

제9조(보안등급 변경) ① 전문기관의 장 및 연구기관의 장이 연구개발과제의 보안등급을 변경할 경우에는 국가연구개발사업과 관련된 자체 보안관리 규정에서 정한 절차에 따라 연구보안심의회의 심의를 거쳐 변경할 수 있으며, 소관 중앙행정기관의 장에게 변경내용, 변경 사유 등을 제출하여야 한다.

② 장관은 제1항에 따라 제출받은 보안등급의 변경내용 등이 적절하지 않다고 판단될 때에는 그 보안등급의 변경을 철회할 것을 명할 수 있다.

③ 전문기관의 장 및 연구기관의 장은 보안등급을 변경한 경우 이와 관련된 연구기관에 통보하여야 한다. 다만, 일반과제에서 보안과제로 변경한 경우에는 관련 내용을 국가정보원장에게 통보하여야 한다.

제10조(연구개발과제 보안관리 현황 보고) ① 전문기관의 장은 연구기관의 국가연구개발사업 보안관리 현황을 [서식 2]에 따라 조사할 수 있다.

② 전문기관의 장은 제1항에 따른 결과를 종합하여 장관에게 조사가 완료된 날로부터 15일 이내에 보고하여야 한다.

제11조(보안관리 실태점검) ① 장관은 전문기관의 장 및 해당 사업 담당과장(담당관을 포함한다.)이 효율적인 보안업무 수행을 위해 필요한 경우 연구수행기관 및 연구책임자를 대상으로 보안교육을 실시하여 보안의식을 고취시키며 보안업무수행에 대한 실태점검을 실시하게 할 수 있다.

② 실태점검결과 위법 또는 부당하다고 인정되는 사항이 있을 때에는 대상기관 또는 관련자에게 필요한 조치를 취할 수 있다.

제12조(보안책임) 연구기관 및 참여연구원은 연구활동 계약기간 중은 물론 계약종료 후에도 보안유지에 최선을 다하여야 하며, 위반 시 관계법규에 따라 책임을 진다.

제13조(기타) 본 지침 및 연구기관 자체보안관리규정에서 규정한 내용 이외의 사항에 대해서는 「보안업무규정」, 「보안업무규정 시행규칙」을 따른다.

제14조(재검토기한) 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 2017년 7월 1일을 기준으로 매 3년이 되는 시점(매 3년째의 6월 30일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

부칙 <제90호,2019.10.15.>

이 지침은 공포한 날부터 시행한다.