정보통신·방송 연구개발 보안관리 규정

[시행 2021. 3. 23.] [과학기술정보통신부훈령 제152호, 2021. 3. 23., 일부개정]

과학기술정보통신부(정보통신방송기술정책과), 044-202-6237

제1장 총 칙

제1조(목적) 이 규정은 「국가연구개발혁신법」제21조, 「국가연구개발혁신법 시행령」제44조에서 제48조 및「정보통신・방송 연구개발 관리규정」제52조제1호에 따라 정보통신・방송 연구개발 사업을 추진・관리하거나 수행하는 기관의 보안대책 수립・시행에 필요한 방법 및 절차를 정함을 목적으로 한다.

제2조(적용대상) 이 규정의 적용대상은 다음과 같다.

1. 전문기관 및 임・직원
2. 사업에 참여하는 연구개발기관 및 참여연구자
3. 사업의 기획, 선정, 단계, 최종 등을 위한 종합심의위원회・심의위원회 및 평가위원회 참여자
4. 기타 사업과 관련한 업무를 수행하는 자

제3조(적용범위) 사업의 보안 관리와 관련하여 다른 법령에 특별한 규정이 있는 경우를 제외하고는 이 규정에 따른다.

제2장 보안대책 수립 및 관리 체계 등

제4조(보안대책 수립) ① 과학기술정보통신부장관(이하 "장관"이라 한다) 및 연구개발기관의 장은 영 제44조에 따라 보안대책을 수립・시행하여야 한다.

② 삭제

③ 전문기관의 장은 연구개발기관의 실태점검 등을 통하여 연구개발기관에서 수립・시행하는 보안대책 등에 이의가 있을 경우 수정을 요구할 수 있으며, 해당 연구개발기관의 장은 특별한 사유가 없는 한 이에 응하여야 한다.

④ 연구개발기관의 장은 사업의 일부를 위탁하는 경우 보안조치와 관련되는 사항을 협약서에 명시하여 보안조치를 이행할 수 있도록 하여야 한다.

⑤ 삭제

제5조(국외유출 방지 등) ① 장관은 사업 관련 정보의 국외 유출을 방지하기 위하여 국가정보원장과 협조하여 별도의 보안대책을 수립・시행할 수 있다.

② 연구개발기관의 장은 과제와 관련된 중요 연구정보의 국외 유출을 방지하기 위하여 제12조제2항에 따른 보안관리 조치사항과 그 밖에 연구개발기관의 장이 필요하다고 인정하는 사항을 포함하여 자체 보안대책을 수립・시행하여야 한다.

③ 연구개발기관의 장은 보안과제와 관련하여 외국 정부・기관 또는 단체를 방문하거나 방문을 받을 경우에는 과제명, 연구책임자, 방문 일시・장소 및 주요 방문내용 등의 사항을 장관 및 국가정보원장에게 해당 방문일 5일 전까지 알려야 한다. 다만, 방문이 사전에 알린 내용과 다르게 이루어진 경우에는 방문 후에 해당 사항을 추가로 알려야 하며, 방문이 긴급한 경우 등 사전에 알리지 못하고 방문하거나 방문을 받은 경우에는 방문이 끝난 후에 알릴 수 있다.

제6조(보안관리심의회 구성・운영 등) ① 장관은 사업의 보안관리에 관한 사항을 심의하기 위해 심의회(이하 "보안관리심의회"라고 한다)를 구성・운영하여야 한다.

② 보안관리심의회는 과학기술정보통신부 담당관을 보안관리심의회 위원장으로 하고, 과학기술정보통신부 사업 담당 부서의 과장 및 관련 분야 민간전문가를 위원으로 7명 내외로 구성한다.

③ 보안관리심의회는 다음 각 호의 사항을 심의한다.

1. 사업 관련 보안관리 규정의 제・개정
2. 전문기관의 보안관리현황 보고사항
3. 사업 관련 보안사고 발생시 사후 조치사항
4. 그 밖에 보안관리심의회 위원장이 필요하다고 인정하는 사항

④ 보안관리심의회는 재적위원 과반수 이상 출석과 출석위원의 과반수 이상의 찬성으로 의결하되, 가부동수인 경우 부결된 것으로 본다.

⑤ 보안관리심의회 위원장은 제3항의 심의에 필요하다고 판단되는 경우 관계자를 출석시켜 의견을 진술하게 할 수 있다. 이 경우 출석하는 자에게는 예산의 범위 안에서 수당과 여비를 지급할 수 있다.

제7조(연구보안심의회 구성 및 운영 등) ① 전문기관의 장 및 연구개발기관의 장은 사업과 관련한 보안업무의 효율적인 수행과 운영관리에 관한 중요사항을 심의하기 위해 심의회(이하 "연구보안심의회"라고 한다)를 구성하여야 한다.

② 연구보안심의회의 구성과 운영에 관한 사항은 해당기관의 장이 별도로 정할 수 있으며,「중소기업기본법」에 따른 중소기업,「벤처기업육성에 관한 특별조치법」에 따른 벤처기업 등 조직체계상 심의회의 운영이 어려운 연구개발기관에서는 연구개발기관의 장의 검토로 심의회 기능을 대신할 수 있다.

③ 연구보안심의회는 다음 각 호의 사항을 심의・의결한다.

1. 사업 관련 보안관리 규정의 제・개정
2. 과제 보안등급 분류에 대한 적정성 및 등급 변경에 관한 사항
3. 사업 관련 보안관리 현황보고 사항
4. 사업 관련 보안사고 처리 및 사후조치 사항
5. 그밖에 전문기관 또는 연구개발기관의 장이 필요하다고 인정하는 사항

④ 전문기관의 장은 제3항제2호에 대한 심의・의결은 종합심의위원회・심의위원회 또는 평가위원회에 위임할 수 있다.

제8조(보안관리 담당자 지정 및 임무 등) ① 전문기관 및 연구개발기관의 장은 보안관리 책임자를 지정하되, 연구개발기관은 해당기관의 실정에 따라 기관별 책임자가 이에 대한 업무를 대신할 수 있다.

② 보안관리 책임자는 다음 각 호의 사항을 총괄한다.

1. 사업 관련 보안관리에 대한 계획 수립 및 감독
2. 사업 관련 보안관리 지도 감사 및 교육
3. 사업 관련 연구시설 출입 등에 대한 보안조치
4. 기타 사업 관련 보안관리 전반에 관한 지도 및 조정

제3장 보안 등급 분류

제9조(보안등급 분류기준) 연구개발과제의 보안과제 분류는「국가연구개발혁신법 시행령」제45조에 따른다.

제10조(보안등급 분류절차) ① 과제 신청기관의 장이 과제신청서를 제출할 때에는 연구책임자가 [별지 제1호 서식]으로 보안등급을 분류하고, 해당기관의 연구보안심의회의 심의를 거쳐 확정한 후 과제신청서에 표기하여 전문기관의 장에게 제출하여야 한다.

② 전문기관의 장은 과제 선정 평가위원회에 제1항에 따른 과제의 보안등급을 제출하고, 평가위원회는 보안등급 분류의 적정성을 심의한다.

③ 전문기관의 장은 제2항에 따른 평가위원회 심의결과를 장관에게 보고하여야 하며, 장관은 전문기관의 장이 보고한 보안등급에 대한 심의결과를 참조하여 보안등급을 확정한다.

④ 연구책임자가 연구개발계획서를 작성할 때에는 장관이 공고한 연구개발사업의 보안등급을 따라야 한다.

⑤ 삭제

제11조(보안등급 변경) ① 전문기관의 장 및 주관연구개발기관의 장은 과제의 보안등급을 변경하고자 하는 때에는 사업과 관련된 자체 보안관리 규정에서 정한 절차에 따라 연구보안심의회의 심의를 거쳐 변경할 수 있으며, 장관에게 변경내용, 변경사유 등을 제출하여야 한다.

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

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

제4장 보안등급에 따른 보안조치

제12조(보안등급에 따른 조치) ① 전문기관의 장은 과제의 선정・평가・관리와 관련하여 보안과제와 일반과제를 구분하고 이에 따른 보안대책을 수립・시행 하여야 한다.

② 연구개발기관의 장 및 연구책임자는 제9조의 보안등급에 따른 보안관리 조치를 하여야 하며 그 내용은 [별표 1]과 같다.

③ 전문기관의 장은 연구개발기관의 장과 협약을 체결하는 경우 [별표 1]의 조치사항을 이행하여야 함을 협약에 명시하여야 한다.

제13조(연구개발결과의 보안등급) ① 연구개발결과의 보안등급은 제10조에 따라 결정되거나 제11조에 따라 변경된 연구개발과제 보안등급으로 한다.

② 장관 또는 전문기관의 장은 연구개발과제에 대해서 최종평가를 할 때에는「정보통신・방송 연구개발 관리규정」(이하 "관리규정"이라 한다) 제8조의 평가위원회로 하여금 제1항에 따른 연구개발결과 보안등급의 적정성을 검토하게 하고 그 결과를 반영하여 보안등급을 변경할 수 있다.

제5장 보안관리 현황보고 및 보안사고에 대한 조치 등

제14조(보안실태 점검 등) ① 장관은 사업 보안실태 점검 등을 통해 제4조제1항의 보안관리 규정에 대하여 개선조치를 명할 수 있다. 이 경우 관계 중앙행정기관이 여럿일 경우에는 협의를 통하여 개선조치 사항을 정하며, 연구개발기관의 장은 개선명령을 받은 후 6개월 이내에 개선조치에 대한 후속조치 결과를 장관 및 국가정보원장에게 보고하여야 한다.

② 전문기관의 장은 연구개발기관의 국가연구개발사업 보안관리 현황을 과학기술정보통신부령으로 정하는 서식에 따라 조사할 수 있다.

③ 전문기관의 장은 제2항에 따른 결과를 종합하여 장관이 정하는 기한 내에 보고하여야 한다.

제15조(보안관리 지도감사) ① 전문기관 및 연구개발기관의 장은 수시 보안점검을 통해 취약부분에 대해 보안관리 책임자로 하여금 조치하도록 하고, 매년 보안업무 수행에 대한 보안지도감사를 실시할 수 있다.

② 주관연구개발기관의 장은 필요한 경우 공동연구개발기관 및 위탁연구개발기관에 대한 보안관리 지도감사 등의 조치를 취할 수 있다.

제16조(보안사고) 보안사고라 함은 다음 각 호의 사항을 위반하였을 때를 말한다.

1. 비밀의 누설, 유출, 분실, 도난 등의 경우
2. 기타 본 요령과 정부의 보안업무 관련 규정을 위반한 경우

제17조(보안사고에 대한 조치) 전문기관 및 연구개발기관의 장은 다음 각 호에 해당하는 보안사고가 발생하였을 경우 즉시 피해를 최소화하는 조치를 취하여야 한다.

1. 정보시스템실 또는 정보통신망의 무단 침입
2. 정보시스템의 유출, 파괴 또는 변조
3. 정보시스템실의 화재, 재난 또는 도난
4. 바이러스 피해 또는 비밀번호의 유출
5. 정보보안시스템의 손괴
6. 연구개발 관련 중요 정보자료의 무단 유출
7. 기타 기관 보안에 위협 요소가 발생한 경우

제18조(보안사고의 보고체계) ① 전문기관의 장 또는 연구개발기관의 장은 연구개발 관련 정보자료의 무단유출, 연구개발 정보시스템 해킹 등 보안사고가 발생하였을 경우 그 사고를 인지한 즉시 필요한 조치를 함과 동시에 장관

에게 보고하여야 하며, 사고일시・장소, 사고자 인적사항, 사고내용 등 세부적인 사고 경위를 보고일로부터 5일 이내에 추가로 제출하여야 한다. 다만, 과제가 보안과제이거나 보안사고가 외국과 관련된 경우에는 인지한 즉시 국가정보원장에게 보고하여야 한다.

② 장관은 보안사고 발생 시 그 경위를 조사하여야 하며, 필요한 경우 국가정보원과 합동으로 조사할 수 있다. 이 경우 연구개발기관, 관련자 등은 사고조사에 성실히 협조하여야 하고 장관, 전문기관의 장, 연구개발기관의 장은 이에 대한 조사가 종결될 때까지 관련내용을 공개하지 아니하여야 하며, 사고를 수습한 후 재발방지 대책을 마련하여야 하고, 필요한 경우 국가정보원장에게 보안사고를 예방하기 위한 보안교육 등 관련 대책 지원을 요청할 수 있다. 다만, 과제가 보안과제이거나 보안사고가 외국과 관련된 경우에는 국가정보원과 합동으로 사고경위를 조사하여야 한다.

제19조(보안관리 위반시 조치) ① 전문기관, 연구개발기관, 연구책임자 및 참여연구자 등은 이 훈령에서 정하는 사항 및 관련 국가연구개발사업 보안관리규정을 지켜야 한다.

② 장관은 제11조 및 제17조를 정당한 사유없이 이행하지 않은 자에 대하여 사업의 선정 또는 평가에서 참여제한 등의 불리한 조치를 취할 수 있음을 관리규정 제23조제1항제12호에 따라 협약의 내용에 포함하여야 한다.

제20조(보안관리의 위탁) 장관은 이 규정에 따른 보안관리 수행에 필요한 사항을 전문기관에 위탁할 수 있다.

제21조(재검토 기한) 장관은「훈령・예규 등의 발령 및 관리에 관한 규정」에 따라 이 훈령에 대하여 2017년 1월 1일을 기준으로 매3년이 되는 시점(매 3년째의 12월 31일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

부칙 <제152호,2021.3.23.>

제1조(시행일) 이 영은 공포한 날부터 시행한다.

제2조(경과조치) 이 규정 시행 이전에 종전의 규정에 따라 처리된 사항은 이 규정에 따라 처리된 것으로 간주된다.