

2017년도 특정감사

특정감사 결과보고

- 정보보안 실태점검 -

2018. 1.

Keit 한국산업기술평가관리원
Korea Evaluation Institute of Industrial Technology

감 사 실

목 차

I. 감사실시 개요	1
1. 감사배경 및 목적	1
2. 감사대상 및 범위	1
3. 감사기간 및 인원	2
4. 감사 중점사항	2
II. 감사결과	3
1. 총평	3
2. 지적사항 총괄	3
3. 지적사항 요약	3
III. 지적사항에 대한 처분요구	5
1. 처분요구사항 일람표	5
2. 현지조치사항 일람표	5
3. 모범사례 일람표	5
첨부. 감사결과 처분요구서	6

1. 감사실시 개요

1. 감사배경 및 목적

한국산업기술평가관리원(이하 '평가관리원'이라 한다)은 산업통상자원부가 지원하는 연구개발사업의 평가관리를 주요업무로 정하고 있으며, 선정된 연구기관에게 연구비를 지급하고 관리하고 있다. 금번의 특정감사는 R&D 관리 및 행정업무에서 발생하는 정보의 보안에 관한 실태 전반에 대한 점검을 실시하였다.

이번 감사를 통하여 정보보안의 체계를 마련하고 효율적인 정보보안이 이루어 질 수 있도록 규정 및 업무체계의 개선 계기를 마련하고자 하였다.

2. 감사대상 및 범위

감사대상은 보안 및 문서관리 업무를 총괄하는 □□□□□팀, R&D사업의 보안 업무를 총괄하는 ●●●●팀, 과제관리 등 정보시스템의 총괄관리를 담당하는 ▲▲▲▲팀, 보안과제를 관리하고 있는 평가부서를 대상으로 감사를 실시하였고, 감사범위는 해당부서의 정보보안 관련 업무 전반으로 하였다.

3. 감사기간 및 인원

본 감사는 2017.12.13.부터 같은 해 12.15.까지 서면자료 수집·분석 및 예비조사를 실시하고 예비조사 결과 나타난 문제점을 토대로 감사반장 1명, 감사인 3명을 투입하여 12.18.부터 12.20.까지 3일(근무일수 기준)간 실지감사를 실시하였다.

4. 감사 중점사항

평가관리원의 R&D 사업관리 및 행정업무에서 발생하는 보안관련 감사를 실시하되, 보안사고 예방과 정보보안 체계 마련에 중점을 두어 감사를 실시하였다. 주요 점검내용은 다음과 같다.

- 산업기술혁신사업 공통 운영요령의 준수여부 점검
 - 우리원 지원과제의 사업정보 보안 관리 정책 및 현황
 - 공통운영 요령 제41조 및 제43조의 준수
- 산업기술혁신사업 보안관리요령의 준수여부 점검
 - 보안등급 분류 등 보안과제 관리 정책 점검
 - 보안과제로 지정된 R&D 과제의 관리 실태 점검
- 우리원 보안규칙 등 자체규정의 준수여부 점검
 - 정보보안 내규의 이행 및 준수 여부 점검
 - 우리원 퇴직자에 관한 보안관리 정책 및 현황

II. 감사결과

1. 총평

평가관리원 정보보안 업무 전반을 점검하고 정보보안 체계 마련을 위한 관련자 교육 실시, 관련규정의 정비, 정보시스템의 개선 등을 통한 정보보안 사고 예방에 기여

2. 지적사항 총괄

(단위: 건, 천원)

총 건수	합계		변상 (금액)	징계 (인원)	시정(금액)				주의 경고 (인원)	주의 (팀)	개선	권고	통보	고발 (인원)	모범 사례 (인원)
	신분상 조치인원	재정상 조치금액			소계	추징	감액	기타							
6	-	-	-	-	-	-	-	3	-	-	-	-	3	-	-

3. 지적사항 요약

1) 보안 교육 및 안내 미흡

평가관리원 보안규칙 제12조에 의하면 일반보안담당부서장은 전 직원에게 연 1회 이상 보안교육을 실시하고 신규채용자, 비밀취급인가 예정자 등에 대하여 사유발생시 보안교육을 실시하도록 명시하고 있으며 기술혁신사업보안담당부서장은 R&D 과제수행자를 대상으로 연 1회 이상 R&D 과제수행시 지켜야할 보안사항을 설명하도록 명시하고 있다.

보안규칙 제12조에 의한 비밀취급인가 예정자 교육이 필요하고 R&D 과제수행자에게는 보안사항 안내가 필요하다.(통보 2건)

2) 정보보안 업무처리 부적정

평가관리원은 산업기술혁신사업 보안관리요령 및 기술혁신사업보안세칙에 의거하여 보안과제의 평가관리 업무를 수행하고 있다.

평가관리원의 『비밀세부분류기준』에서 정하는 비밀문서의 처리 및 관리기준을 보안과제에 적용함에 있어 해석의 혼동 여지가 있어 기술혁신사업보안세칙 등의 개정이 필요하고(통보 1건) 산업기술혁신사업 보안관리요령 제12조에 의하면 보안과제의 협약체결시 보안관리 조치사항을 명시하도록 규정하고 있으나 이를 반영하고 있지 않아 이와 관련한 업무의 시정이 필요하며(시정요구 2건) 기술혁신사업보안세칙 제8조에 의거하여 보안과제와 일반과제의 정보시스템 접근권한 구분이 필요하다.(시정요구 1건)

III. 지적사항에 대한 처분요구

1. 처분요구사항 일람표

지 적 사 항	순번	조 치 요 구 사 항	조치 구분	처분 요구일	조치 기한일	처리부서
보안 교육 및 안내 미흡	1	○비밀취급인가 예정자에 대한 보안교육 실시	통보	2018.1	2018.4 (3개월)	□□□□□팀
	2	○R&D 과제수행자에 대한 보안사항 안내 실시	통보	2018.1	2018.4 (3개월)	●●●팀
정보보안 업무처리 부적정	3	○보안과제 관리기준 및 방법 등에 대한 근거 마련(원규 개정)	통보	2018.1	2018.4 (3개월)	●●●팀
	4	○보안과제의 협약서식 마련 및 협약업무 시정	시정	2018.1	2018.3 (2개월)	●●●팀
	5	○보안과제의 정보시스템 협약서식 변경	시정	2018.1	2018.3 (2개월)	▲▲▲▲팀
	6	○보안과제와 일반과제의 정보시스템 접근권한 구분 관리	시정	2018.1	2018.3 (2개월)	▲▲▲▲팀

2. 현지조치사항 일람표

(해당사항 없음)

3. 모범사례 일람표

(해당사항 없음)

첨부 : 감사결과 처분요구서

[첨부] 감사결과 처분요구서

일련번호	1	감사자	○○○ ○○○	공개(○), 비공개()	
신분상 조치인원	-	재정상 조치방법	-	재정상 조치금액	-
수감부서 (처리할 부서)	경영기획본부, 산업혁신기술본부 (□□□□□팀, ●●●팀)	처분요구일	2018.1.	회신 기한일	2018.4.

통보

제 목 보안 교육 및 안내 미흡

관 계 부 서 경영기획본부(□□□□□팀), 평가지원단(●●●팀)

조 치 부 서 경영기획본부(□□□□□팀), 평가지원단(●●●팀)

내 용

1. 업무개요

한국산업기술평가관리원(이하 ‘평가관리원’이라 한다.)은 보안업무를 수행하는데 필요한 제반사항을 규정하고 관련 법령을 준수하기 위하여 『보안규칙』을 운용하고 있다. 보안업무는 업무수행 내용에 따라 일반 보안업무, 정보보안업무, 산업기술사업보안업무로 구분하고 있다. 일반 보안업무는 인력, 시설물, 문서, 통신 등과 관련된 기관의 업무활동 전반에 걸친 업무이며 일반보안담당부서장(경영기획본부장)을 책임자로 정하고 있다. 정보보안업무는 전산실, 전산자료, 정보망, 정보보안시스템 등과

관련된 업무이며 정보보안담당부서장(사업기획단장)을 책임자로 정하고 있다. 산업기술사업보안업무는 R&D 사업 수행 및 기획·평가·관리와 관련된 보안업무이며 기술혁신사업보안담당부서장(평가지원단장)을 책임자로 정하고 있다.

보안규칙 제12조에 의하면 경영기획본부장은 전직원에게 연 1회 이상 보안교육을 실시하고 신규채용자, 비밀취급인가 예정자, 기타 보안교육이 필요하다고 인정되는 자에 대하여는 사유발생시 보안교육을 실시하도록 명시하고 있으며, 기술혁신사업보안담당부서장은 기술개발사업 수행자들을 대상으로 연 1회 이상 R&D 과제 수행시 지켜야할 보안사항을 설명하도록 명시하고 있다.

2. 감사결과 확인된 문제점

금번 감사에서 보안 관련 교육실시 현황을 점검하였으나, 비밀취급인가 예정자 및 R&D 과제수행자에 대한 보안교육 실적이 미흡하였다. 이에 보안규칙 제12조 제1항 및 제3항에 의하여 비밀취급인가 예정자에 대한 보안교육을 실시하고 과제수행자에게는 정보보안에 관한 사항을 안내하여야 한다.

관계부서 의견

□□□□□팀 및 ●●●팀에서는 감사결과를 전반적으로 수용하면서

보안 교육 및 안내의 필요성을 인정하였다.

조치할 사항

- ① 경영기획본부장(□□□□□팀장)은 비밀취급인가 예정자에 대한 보안 교육을 실시하여 주시고 (통보)
- ② 평가지원단장(●●●팀장)은 R&D 과제수행자에게 보안관련 사항을 안내하여 주시기 바랍니다.(통보)

일련번호	2	감사자	○○○ ○○○	공개(○), 비공개()	
신분상 조치인원	-	재정상 조치방법	-	재정상 조치금액	-
수감부서 (처리할 부서)	평가지원단, 사업기획단 (●●●팀, ▲▲▲▲팀)	처분요구일	2018.1.	회신 기한일	2018.4.

통보·시정요구

제 목 정보보안 업무처리 부적정

관 계 부 서 평가지원단(●●●팀), 사업기획단(▲▲▲▲팀)

조 치 부 서 평가지원단(●●●팀), 사업기획단(▲▲▲▲팀)

내 용

1. 업무개요

한국산업기술평가관리원(이하 ‘평가관리원’이라 한다.)은 산업기술 혁신촉진법 제39조에 의하여 설립된 기관으로 같은 법 제11조의 산업 기술개발사업을 평가·관리하고 있으며 R&D 지원과제의 세부적인 관리 사항은 산업기술혁신사업 공통 운영요령(이하 ‘공통 운영요령’이라 한다.) 및 산업기술혁신사업 보안관리요령(이하 ‘보안관리요령’이라 한다.) 등 산업통상자원부 고시를 준수하여야 한다. 또한 평가관리원은 R&D과제의 보안관리를 위하여 『기술혁신사업 보안세칙(이하 ‘세칙’이라 한다.)』 등의 내부규정을 운영하고 있다.

보안관리요령은 공통 운영요령에 의하여 지원되는 R&D 사업의

추진·관리 또는 과제수행자의 보안대책 수립·시행에 필요한 방법 및 절차를 정하고 있으며, 평가관리원은 이에 따라 R&D사업의 관리를 위한 보안대책 수립, 보안관리 담당자 지정, 보안등급 분류 및 관리 등의 보안관련 업무를 이행하고 있다.

2. 감사결과 확인된 문제점

금번 감사에서는 평가관리원이 지원하는 과제 중 보안과제 현황을 파악하고 관련 규정의 준수 여부를 점검하였다. 평가관리원이 보안과제의 수행자와 협약을 체결할 경우에는 보안관리요령 제12조의 보안관리 조치사항(별표 1)을 명시하여야 하고 세칙에 따라 평가·관리하여야 하며 제8조에 따라 정보시스템 관리 권한을 구분하여 보안을 유지하여야 한다.

그러나 보안과제의 협약체결 서류를 점검한 결과 보안관리요령 제12조에 의한 보안관리 조치사항 제시가 누락된 채 협약체결이 이루어지고 있었다. 평가관리원은 공통요령의 표준서식을 활용하여 전자협약을 체결하고 있는데, 정보시스템에서 제공되는 협약서 양식이 보안관리요령에 부합하지 않아 보안관리 조치사항이 누락된 것으로 확인되어 업무처리의 개선이 필요하다. 또한 보안과제에서 생산되는 문서, 과제의 평가관리 정보 등의 관리기준과 관리방법이 명확하지 않아 원규에서 정하는 비밀 문서의 관리방법과 혼돈의 여지가 있다. 이러한 점은 보안과제 관리의 혼란을 유발할 수가 있어서 보안과제의 관리기준, 관리방법 등의 의견

수렴을 거쳐 세칙에 근거조항을 추가하고 관리방법을 명확하게 명시할 필요가 있다.

아울러 평가관리원이 운용중인 정보시스템에서는 보안과제와 일반과제를 구분하여 사용자의 접근권한을 부여하고 있지 않아 세칙 제8조를 이행하지 못하고 있어 정보보안 사고 발생이 우려된다. 이에 정보시스템의 권한관리 체계를 개선(일반과제와 보안과제를 구분하여 사용자 접근 권한 부여)하여 사고예방 노력이 필요하다.

이에 따라 산업기술혁신사업 보안과제의 협약체결 및 관리기준을 명확히 하고 정보시스템의 접근권한 등의 시정이 필요하다.

관계부서 의견

●●●팀 및 ▲▲▲▲팀에서는 감사결과를 전반적으로 수용하면서 개선 및 시정의 필요성을 인정하였다.

조치할 사항

① 평가지원단장(●●●팀장)은

산업기술혁신사업 보안과제 관리기준 및 방법 등에 관한 근거를 마련토록 원규(세칙)를 개정하여 주시고(통보)

② 보안과제의 협약서식 마련 및 반영 등 업무를 시정하여 주시고(시정요구)

③ 사업기획단장(▲▲▲▲팀장)은

정보시스템에서 보안과제의 협약체결 서식을 변경하여 주시고(시정요구)

- ④ 보안과제와 일반과제를 구분하여 정보시스템의 사용자 접근권한을 부여할 수 있도록 시정하여 주시기 바랍니다(시정요구)