2022년도 특정감사

특정감사 결과보고서
- IT시스템 적정성 점검 -

2022. 11.

한국산업기술평가관리원
Korea Evaluation Institute of Industrial Technology
감 사 실

목 차

Ⅰ. 감사실시 개요 ····· 1
1. 감사배경 및 목적 ····· 1
2. IT감사 체계 수립 ····· 2
3. 감사대상 및 범위 ····· 8
4. 감사기간 및 인원 ····· 16
5. 감사실시 과정 ····· 16
6. 감사 중점사항 ····· 18

Ⅱ. 감사결과 ····· 19
1. 총평 ····· 19
2. 지적사항 총괄 ····· 19
3. 지적사항 요약 ····· 19

Ⅲ. 지적사항에 대한 처분요구 ····· 25
1. 처분요구사항 일람표 ····· 25
2. 현지조치 일람표 ····· 27
3. 모범사례 일람표 ····· 28

첨부. 감사결과 처분요구서 ····· 29

Ⅰ. 감사실시 개요

1. 감사배경 및 목적

新 정부는 산업별 디지털 혁신 가속화와 사이버 보안 대응을 강조하며 120대 국정과제 중 '민·관 협력을 통한 디지털 경제 패권국가 실현', '세계 최고의 네트워크 구축 및 디지털 혁신 가속화', '국가 사이버안보 대응역량 강화'를 제시하며 산업·기술 디지털 융합·혁신 가속화로 국가 디지털 경쟁력 제고, 인재 육성 등을 통해 사이버안보 기반 공고화를 유도하고 있다.

한국산업기술평가관리원(이하 "평가관리원"이라 한다)은 기관 고유업무인 산업기술 R&D 기획·평가·관리 업무를 수행하기 위하여 연구비 집행관리 관련 연구비통합관리시스템인 RCMS 및 전자평가시스템인 스텔라(STELLA) 등 IT 정보시스템을 운영하고 있다. 이러한 시스템의 업무 처리절차 및 운영방식은 업무 편의성, 효율성, 적법성 등에 미치는 영향이 매우 크다.

이에 따라 본 감사에서는 IT감사 정의('IT감사 가이드라인', 감사연구원, 2017)에 근거하여 IT시스템과 관련된 통제장치에 대한 합법성, 효율성, 경제성, 그리고 효과성을 검증하기 위해 주요 시스템을 대상으로 IT일반통제(프로그램 변경, 접근보안, 시스템 운영), IT응용통제(자동처리 통제), 개인정보 통제(개인정보 거버넌스, 수집·보관·폐기, 기술적 보안)의 설계와 운영의 적절성을 점검하여 문제점을 도출하고 관련 개선방안을 제시하여 평가관리원의 IT기반 내부통제 체계를 공고히 할 수 있도록 감사를 실시하였다.

2. IT감사 체계 수립

가. IT감사의 정의

일반적으로 IT감사를 IT기반 감사와 혼동해 사용하는 경우가 많으나, IT감사는 IT 통제 감사를 지칭(예 : 회계감사 - 회계 통제의 적절성에 대한 감사)하고 있으며 최근 기관 업무 프로세스에서 시스템 의존도가 크고, 많은 통제들이 시스템 내 구현되어 있기 때문에 감사의 내부통제 점검 차원에서 IT감사를 통한 IT통제 점검은 필수적이다.

감사연구원 'IT감사 가이드라인'(2017년)에 따르면 "IT감사란 IT 시스템과 관련된 통제장치에 대한 합법성, 효율성, 경제성, 그리고 효과성 관련 원칙들이 준수되는지 보증(assurance)을 얻거나 이를 위반하는지 확인하기 위하여 IT시스템과 관련 통제장치를 검토 및 검사하는 것이다"라고 정의하고 있다. 아울러 IT감사시 고려할 위험에는 크게 내재적 위험, 통제 위험, 그리고 적발위험 범주로 나눌 수가 있으며 각각의 정의는 [표 1]과 같다.

또한 IT감사는 감사 대상 IT통제 종류에 따라 점검방법이 달라지며, IT통제는 [그림 1]과 같이 IT일반통제, IT응용통제, IT의존 수기통제, 개인정보 통제로 구분 할 수 있다.

[표 1] "IT감사시 위험" 유형

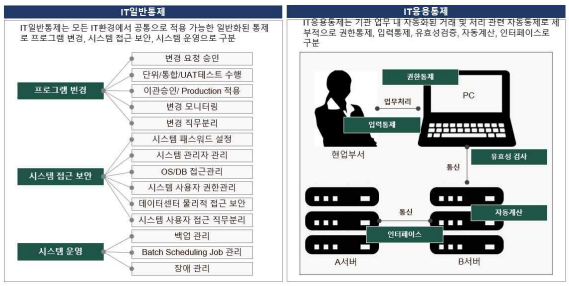
유 형	정 의
내재적 위험	조직이 수행해야 하는 기능 실행에 영향을 미칠 수 있는 위험요소로서 조직 시스템에 내재해 있는 것임. 조직 내에는 내재적 위험요인에 대한 통제조치가 확립되어야 함. 어떤 경우, 위험요인이 중대하지 않고 그 위험 수준이 감당할 정도라면, 이에 대한 대응조치 없이 그대로 이를 받아들일 수 도 있음.
통제 위험	통제 조치가 실패할 가능성이 있을 경우의 위험 요소임. 이런 경우에는 중대한 오류가 있을 수 있으며, 이는 즉시 확인되어야 함. IT시스템은 응용통제와 일반통제를 통하여 이러한 문제를 처리함. 조직과 IT시스템이 기능을 잘 수행하기 위해서는 이러한 통제장치들이 잘 되어 있어야 함.
적발 위험	IT 및 관련 통제의 부존재 혹은 실패, 그리고 IT시스템의 기능과 관련된 문제를 적발하지 못할 위험을 가리킴

[그림 1] IT통제의 종류



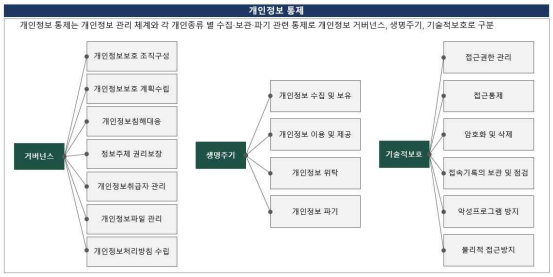
세부적으로 [그림 2]와 같이 IT일반통제는 프로그램 변경, 시스템 접근 보안, 시스템 운영으로 구분하여 점검을 수행하며, IT응용통제는 기관 내 자동화된 거래 중 중요도 기준으로 세부 통제를 식별하여 점검을 수행한다.

[그림 2] IT일반, IT응용 통제



개인정보 통제는 [그림 3]과 같이 개인정보 관리 체계와 각 개인종류 별 수집·보관·파기 관련 통제로 개인정보 거버넌스, 생명주기, 기술적보호로 구분 된다.

[그림 3] 개인정보 통제



따라서 IT감사의 태생이 내부감사 활동 중에 시스템에서 자동 처리되는 부분(IT응용통제)에 대한 보증의 필요성, IT응용통제를 지원하는 IT시스템의 관리·운영 프로세스(IT일반통제) 신뢰성·안전성에 대한 보증의 요구로 인한 것이므로 IT감사는 IT응용통제, IT일반통제 효과의 적절성을 검증하는 절차로 진행된다.

나. IT감사 체계 수립

평가관리원 감사실은 전략적이고 체계적인 IT감사 실시를 위하여 [그림 4]와 같이 "중장기 감사전략"과 연계한 "IT감사 전략"을 수립(2022.8.12.)하고 이에 따른 체계, 이행로드맵 등을 도출하였다.

아울러, [그림 5]와 같이 IT감사의 수행범위, 방법 등을 구체화 시킨 매뉴얼을 개발하여 일회성 감사를 지양하고 지속적으로 IT감사 체계 강화 및 감사인 능력을 배양할 수 있는 기반을 마련하여 IT감사에 착수하였다.

[그림 4] "중장기 감사전략"과 연계한 "IT감사 전략"

□ "중장기 감사전략"과 연계한 "IT감사 전략" 체계



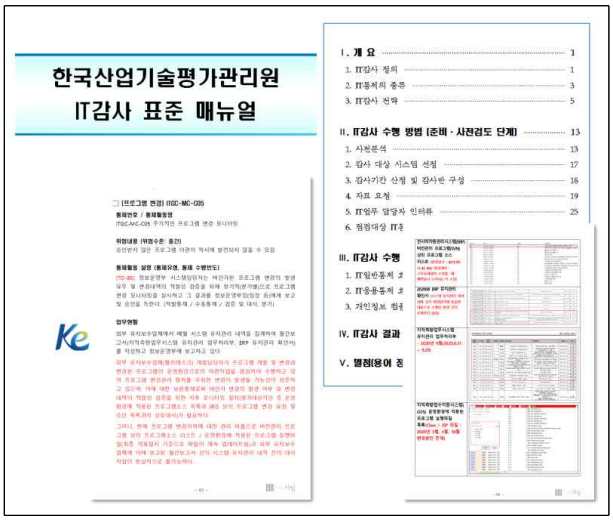
□ "IT감사 전략" 체계

감사미션	공정하고 신뢰할 수 있는 R&D 생태계 조성		
IT감사 전략 목표	지속적인 IT 내부통제 점검을 통해 R&D 정보시스템 신뢰성 강화에 기여		
영역	보증	인력	인프라
전략방향	IT 내부통제 점검 강화	IT감사인 양성	IT감사 체계 구축
전략과제	IT감사 다양화 및 범위 확대	IT전문 감사인 양성 및 역량강화	IT감사 이행 감사규정 반영
	IT 내부통제 강화 경영권고 시행	IT감사 이해 제고 및 외부전문가 활용	IT감사 방법론 수립 및 표준 감사매뉴얼 개발

□ 이행 로드맵

	전략방향	전략과제	단기(2022)	중기(2023)	장기(2024)
보증	IT내부통제 점검 강화	[전략과제 #1] IT감사 다양화 및 범위 확대	기관 주요 거래시스템 감사	위험 기반 감사대상 확대	고위험군 감사대상 조정
		[전략과제 #2] IT 내부통제 강화 경영권고 강화	IT내부통제 일부 현안 개선 권고	이전 권고 이행관리 및 추가 권고	
인력	IT감사인 양성	[전략과제 #3] IT전문 감사인 양성 및 역량강화	IT전문감사인 지정	DBMS 분석 역량 강화	프로그램 분석 역량 강화
		[전략과제 #4] IT감사 이해 제고 및 외부전문가 활용	상임감사, 감사인 IT이해 교육 강화 / 외부전문가 협업 IT감사	IT감사전문위원 지정 자체IT감사 (외부전문가 진원)	외부전문가 협업 IT감사
인프라	IT내부통제 점검 강화	[전략과제 #5] IT감사 이행 감사규정 반영	IT감사 실행 조항 신설	IT 감사 범위 개정	
		[전략과제 #6] IT감사 방법론 수립 및 표준 감사매뉴얼 개발	IT감사 체계 및 매뉴얼 구축	IT역량 강화 및 자체감사 시행	IT 체계 및 매뉴얼 고도화

[그림 5] IT감사 표준 매뉴얼



3. 감사대상 및 범위

감사대상은 IT시스템 업무를 담당하는 ◎◎◎◎◎단 및 R&D사업을 총괄하는 ☆☆☆☆팀을 대상으로 IT시스템 관련 IT거버넌스, IT일반통제, IT응용통제 및 개인정보보호 관련 업무 전반에 대한 조사를 실시하였다.

평가관리원에서 운영 중인 IT시스템은 [그림 6]과 같으며 관련 조직·업무분장은 [그림 7]과 같이 ◎◎◎◎◎단 내 4개 팀(○○○◎◎팀, ○○○◇◇팀, ◇◇◇□□팀, ○○○○○팀)에서 운영하고 있다.

[그림 6] 평가관리원에서 운영중인 IT시스템



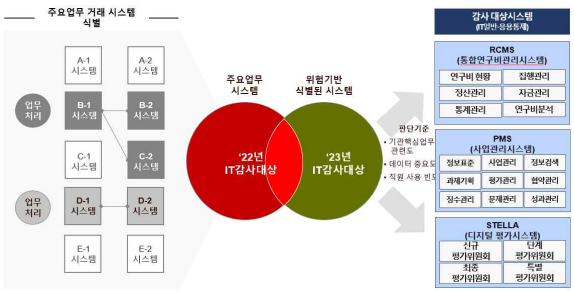
[그림 7] IT 관련 조직 현황



세부적으로 2022년 7월 기준으로 운영 중인 정보시스템은 기관홈페이지, R&D정보포털(ITECH), 연구비통합관리시스템(RCMS), 사업관리시스템(PMS), (인터넷, 업무망)전자우편, 데이터기반 디지털평가시스템(STELLA), 그룹웨어(전자결재 포함) 등 17개 시스템으로 나눠지며, 개인정보보유 현황은 평가관리원 통합회원정보, 산업기술R&D참여연구원정보, 산업기술혁신평가단 공동활용정보 등 5개 개인정보를 보유하고 있다.

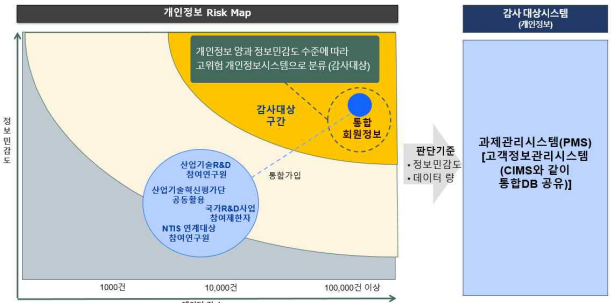
감사대상 선정 관련해서는 [그림 8]과 같이 기관 고유 업무인 R&D 평가·관리 업무의 중요도를 고려하여 IT일반 통제 및 응용통제 감사대상 시스템을 연구비통합관리시스템(RCMS), 사업관리시스템(PMS) 및 디지털 평가시스템(STELLA)로 선정하였으며, 개인정보 점검대상 시스템은 [그림 9]와 같이 정보민감도와 데이터 건 수를 고려하여 개인정보 감사대상 시스템을 PMS(사업관리시스템)로 정하였다.

[그림 8] IT일반통제, IT응용통제 대상 시스템

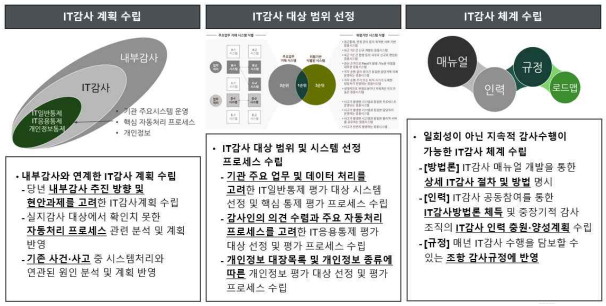


종합적으로 [그림 10]과 같이 평가관리원 내부감사의 방향·현안과제 및 정보시스템의 중요도를 고려하여 IT감사 대상을 선정하고 IT감사 매뉴얼, 인력, 규정, 로드맵을 포함한 종합적인 IT감사 체계를 수립하였고 IT감사 지속성 및 품질을 제고하기 위하여 [그림 11]과 같이 IT감사 기간 및 감사반 구성 계획도 수립하였다.

[그림 9] 개인정보 점검 대상 시스템



[그림 10] 감사 대상 선정 및 IT감사 체계 수립



[그림 11] IT감사 기간 산정 및 감사반 구성(안)



최종적으로 점검대상 IT감사 대상 시스템에 대한 점검대상(통제)은 [그림 12]와 같이 IT일반통제 26개, IT응용통제 2개 및 개인정보 점검 17개가 되며, 세부 점검대상 내역은 [표 2], [표 3], [표 4]와 같다.

[그림 12] IT감사 통제 대상(요약)



[표 2] IT일반통제 점검 대상

순번	분류	통제명	점검사항
1	프로그램 변경	프로그램 변경 요청 및 승인	프로그램 변경 요청 시 변경절차에 따라 공식적인 요청문서가 작성되고 발생 가능한 오류는 사전에 충분히 검토 및 수정되며, 적절한 승인권자의 승인을 득한 후 프로그램 변경이 수행되는지 점검
2		사용자 인수테스트	변경된 프로그램이 사용자 요구사항을 적절하게 반영되고 있는지 개발/테스트환경에서 사용자 인수테스트가 수행되고 테스트 결과가 적절하게 문서화되고 있는지 점검
3		프로그램 이관 요청 및 승인	변경된 프로그램을 개발/테스트환경에서 운영환경으로 이관 시 공식적인 요청문서가 작성되고 적절한 승인권자의 승인을 득한 후 운영환경에 적용되는지 점검
4		개발자와 이관담당자의 직무분리	- 회사의 주요 전산시스템이 개발/테스트환경과 운영환경으로 물리적/논리적으로 분리되어 있는지 점검 - 변경절차를 우회한 프로그램 변경을 사전에 방지하기 위해 개발자와 이관담당자의 직무 및 권한이 적절하게 분리되어 있는지 점검
5		주기적인 프로그램 변경 모니터링	비인가된 프로그램 변경의 발생 유무 및 변경절차 준수의 적절성 검증을 위해 정기적으로 프로그램 변경 모니터링이 실시되고 예외사항 발생 시 적시에 조치되고 있는지 점검
6		IT Infra 변경관리	회사 주요 전산시스템의 IT Infra 변경 시 공식적인 문서가 작성되고 발생 가능한 오류는 사전에 충분히 검토 및 수정되며, 적절한 승인권자의 승인을 득한 후 IT Infra 변경이 수행되는지 점검
7	시스템 접근 보안	사용자계정 신규생성 및 권한부여	신규입사나 부서이동 등으로 인해 사용자계정 신규생성 및 권한부여 시 공식적인 요청문서가 작성되고 적절한 승인권자의 승인을 득한 후 계정생성 및 권한이 부여되는지 점검
8		권한 변경 요청 및 승인	부서이동이나 업무변경 등으로 인해 권한변경 필요 시 공식적인 요청문서가 작성되고 적절한 승인권자의 승인을 득한 후 권한이 변경되는지 점검
9		퇴직자 계정관리	퇴직자 발생 시 퇴직발령 통보문서를 근거로 혹은 공식적인 요청문서가 작성되고 적절한 승인권자의 승인을 득한 후 계정 및 권한이 즉시 삭제/잠금처리되는지 점검
10		주기적인 사용자계정 검토	회사의 주요 전산시스템에 대한 사용자계정 및 업무권한에 따른 접근권한의 적절성 여부에 대한 주기적인 검토가 실시되고 예외사항 발생 시 적시에 조치되고 있는지 점검
11		관리자계정 관리 (애플리케이션)	회사 주요 전산시스템의 애플리케이션에 대한 시스템관리자 계정은 해당 직원의 Job / Function Description 에 기반하여 업무 상 필요한 소수의 직원에게만 부여되어 있는지 점검
12		관리자계정 관리 (OS, DBMS)	회사 주요 전산시스템의 애플리케이션 관련 서버의 OS, DBMS 에 대한 시스템관리자 계정은 해당 직원의 Job / Function Description 에 기반하여 업무 상 필요한 소수의 직원에게만 부여되어 있는지 점검
13		사용자 접근로그 모니터링	사용자 접근로그 모니터링 대상(예: 관리자계정 활동 및 업무시간 이외의 접근/ 다수의 로그인 실패 등 비정상적으로 간주되는 활동 등)이 설정되어 정기적으로 접근로그 모니터링이 예외사항 발생 시 적시에 조치되고 있는지 점검
14		계정 및 패스워드 관리 (애플리케이션)	회사의 정보보안절차에 따라 주요 전산시스템의 애플리케이션에 대한 패스워드 보안정책이 시스템에 구현되어 있는지 점검
15		계정 및 패스워드 관리 (OS, DBMS)	회사의 정보보안절차에 따라 주요 전산시스템의 애플리케이션 관련 서버의 OS, DBMS 에 대한 패스워드 보안정책이 시스템에 구현되어 있는지 점검
16		데이터 변경	데이터 변경 요청 시 변경절차에 따라 공식적인 요청문서가 작성되고 발생 가능한 오류는 사전에 충분히 검토 및 수정되며,

		요청 및 승인	적절한 승인권자의 승인을 득한 후 데이터 변경이 수행되는지 점검
17	시스템 운영	네트워크 보안	네트워크 취약점으로 인해 비인가된 내부 네트워크 접근을 사전 방지하기 위해 외부로부터 회사 내부의 전산시스템으로의 접근이 필요 시 공식적인 요청문서가 작성되고 적절한 승인권자의 승인을 득한 후 계정생성 및 권한이 부여되는지 점검
18		전산실 출입통제 및 출입기록 관리	- 회사의 주요 전산시스템은 현업부서와는 별도의 독립된 공간(예 : 데이터센터)에 위치되어 있으며, 정보보안절차에 따라 물리적 접근통제시스템이 구현되어 있는지 점검 - 전산실(서버룸)에 대한 출입은 업무 상 필요한 소수의 직원으로 엄격히 제한되어 있고, 외부 방문객 출입 시 사전에 적절한 승인권자의 승인을 득하고 관련 출입기록이 적절히 관리되고 있는지 점검
19		전산실 환경통제	- 정전이나 화재 등 발생가능한 재해로부터 전산시스템을 보호하기 위해 전산실(서버룸) 내 환경통제 설비(항온항습기, 화재감지기, 소화장비, UPS 등)가 구축되어 있는지 점검 - 매일 정기적으로 정상 작동 유무에 대한 점검을 수행하고 그 결과는 문서화되어 적절한 승인권자에게 보고 및 승인을 득하는지 점검
20		백업관리	- 시스템 운영절차 상에 백업대상별 백업주기 및 백업방법, 보관기간 등의 백업정책이 규정되어 있는지 점검 - 사전에 등록된 백업스케줄에 따라 백업솔루션을 통해 백업이 자동으로 이루어지고 있는지 점검 - 매일 정기적으로 백업 정상 종료 여부에 대한 점검이 수행되고 그 결과는 문서화되어 적절한 승인권자에게 보고 및 승인을 득하는지 점검
21		백업 복구테스트	백업 데이터의 물리적 손상에 대비하여 정기적으로 백업 복구테스트가 수행되고 그 결과는 문서화되어 적절한 승인권자에게 보고 및 승인을 득하는지 점검
22		백업 소산	예상치 못한 재해로 인한 시스템 및 백업 데이터의 유실에 대비하여 백업 데이터에 대한 원격지 소산이 이루어지고 그 결과는 문서화되어 적절한 승인권자에게 보고 및 승인을 득하는지 점검
23		배치작업 관리	- 배치작업 등록 / 변경 / 삭제 요청 시 공식적인 요청문서가 작성되고 발생 가능한 오류는 사전에 충분히 검토 및 수정되며, 적절한 승인권자의 승인을 득한 후 배치작업이 등록 / 변경 / 삭제가 수행되는지 점검 - 매일 정기적으로 배치작업 정상 종료 여부에 대한 점검이 수행되고 그 결과는 문서화되어 적절한 승인권자에게 보고 및 승인을 득하는지 점검
24		장애처리	회사의 주요 전산시스템에 장애 발생 시 업무에 미치는 영향 최소화를 위해 적시에 원인 파악 및 조치가 이루어지고, 그 결과는 문서화되어 적절한 승인권자에게 보고 및 승인을 득하는지 점검
25		외주업체 계약관리	회사의 주요 전산시스템에 대한 보안성/가용성/처리무결성과 관련 회사의 통제절차에 대한 외주업체의 준수의무가 계약서 내용에 적절하게 명시되어 있는지 점검
26		외주업체에 대한 독립적인 평가	회사의 주요 전산시스템에 대한 보안성/가용성/처리무결성과 관련 외주업체가 회사의 통제절차를 적절하게 준수하고 있는지에 대한 정기적인 평가가 수행되고, 그 결과에 따라 외주계약의 갱신 및 계약금액이 조정되고 있는지 점검

[표 3] IT응용통제 점검 대상

번호	분류	통제명	점검사항
1	인터페이스	평가위원 자동 선정의 적정성 검토	산업기술혁신사업 공통운영요령 제7조에 따라 연구개발과제 평가단은 평가 대상 연구개발과제의 기술 중분류와 50% 이상 일치 및 산업체 관련 전문가 1/3 이상 참여하도록 구성되며, 제척조건에 해당되는 경우 평가위원 선정 시 자동으로 제외되는지 점검
2		일일계좌 시재점검의 적정성 검토	RCMS 일일계좌 시재점검 시 배치작업을 통해 잔액조회 전문에 의한 은행 실시간 잔액 조회 및 검증이 이루어지며, 이를 근거로 RCMS 상의 계좌잔액 등록 및 은행별/사업별 시재마감이 등록되는지 점검

[표 4] 개인정보 점검 대상

번호	분류	통제명	점검사항
1	거버넌스	개인정보보호 조직구성	개인정보보호책임자를 지정하고 역할 및 책임이 부여되어 있는지 점검
2		개인정보보호 계획수립	내부관리계획을 수립하고, 이행실태를 점검하고 있는지 점검
3		개인정보침해 대응	개인정보침해사고 대응절차가 수립되어 있고 모의훈련을 실시하는지 점검
4		정보주체 권리보장	정보주체의 권리보장절차가 수립되어 있고 이의제기 할 수 있는 절차가 수립되어 있는지 점검
5		개인정보 취급자 관리	개인정보취급자를 최소 인원으로 지정하고 관리감독하는지 점검
6		개인정보파일 관리	개인정보파일대장을 관리하고 행정안전부장관에게 등록하는지 점검
7		개인정보처리 방침 수립	개인정보처리방침을 수립하고 공개하고 있는지 점검
8	생명주기	개인정보 수집 및 보유	수집하는 개인정보가 최소한의 범위이고, 적절하게 동의받는지 점검
9		개인정보 이용 및 제공	제3자게 제공하는 개인정보가 최소한의 항목이고, 적절하게 동의받는지 점검
10		개인정보 위탁	개인정보 위탁사실을 공개하고, 수탁자에 대한 교육과 관리감독하는지 점검
11		개인정보 파기	개인정보 보유기간 경과 시 파기하고, 파기관리대장을 관리하는지 점검
12	기술적 보호	접근권한 관리	개인정보취급자의 계정에 대한 안전한 인증방식과 적절한 권한부여인지 점검
13		접근통제	접근통제시스템을 구축하고 보호조치여부를 점검
14		암호화 및 삭제	중요 개인정보를 저장 또는 전송 시 암호화여부 점검
15		접속기록의 보관 및 점검	접속기록을 보관하고 정기적으로 점검하는지 점검
16		악성프로그램 방지	단말기에 백신설치 및 보안업데이트 수행여부 점검
17		물리적 접근방지	물리적인 보호구역을 지정하고, 출입통제 및 물품의 반출입통제 여부 점검

4. 감사기간 및 인원

본 감사는 2022. 5. 27.부터 같은 해 7. 26.까지 IT 및 감사 컨설턴트 전문가 그룹과 함께 사전점검을 실시하고, 2022. 8. 31.부터 같은 해 9. 15.까지 2주간의 예비조사 기간을 거쳐 나타난 문제점 및 개선 필요사항을 토대로 감사반장 1명, 감사인 8명(준감사인 1명, 교차감사인 3명 포함)을 투입하여 2022. 9. 23.부터 같은 해 9. 29.까지 5일간 실지감사를 실시하였다. 감사결과는 내·외부 감사인 검토과정을 거쳐, 2022. 11. 22. 상임감사가 최종 확정하였다.

5. 감사실시 과정

이번 감사에서는 평가관리원의 IT시스템 적정성에 대한 점검을 위하여 다음의 절차를 취하였다.

가. 사전조사

효과적이고 효율적인 감사 수행을 위하여 IT 및 감사 컨설턴트 전문가 그룹과 함께 IT감사 체계 수립 및 사전 IT시스템 효용성 점검(IT일반통제, IT응용통제, 개인정보보호 준수 등)를 2022. 5. 27.부터 같은 해 7. 26.까지 실시하였다. 아울러, 감사인 대상 착안사항 발굴회의를 개최하였고 감사대상 부서인 ◎◎◎◎◎단 단장 및 팀장을 대상으로 간담회 개최하여 감사 추진 방향 및 주요 감사착안사항(안)에 대하여 설명하고, 감사대상 부서의 의견을 청취하였다.

나. 예비조사

2022. 8. 31.부터 같은 해 9. 15.까지의 예비조사를 통하여 감사인 별

중점 추진방향을 설정하고, 실지감사를 위한 관련 증빙 수집, 감사대상 및 대상자와 감사범위에 대해 논의하였으며, 감사인 별로 제척·회피 자가진단을 실시하였다.

다. 실지감사

착안사항 발굴 회의와 예비조사를 거쳐 2022. 9. 23.부터 같은 해 9. 29.까지 5일간 감사인원 9명(준감사인 1명, 교차감사인 3명 포함)을 투입하여 감사 중점사항을 토대로 실지감사를 실시하였다.

라. 마감회의 및 내부변호인 제도 안내

감사 종료 후에는 조치요구사항과 관련되는 부서를 대상으로 실지감사 마감회의(강평)를 통해 특정감사 결과에 대한 개략적인 평가와 주요 문제점, 개별적인 지적사항 등을 설명하고, 업무상의 애로 및 건의사항을 청취하여 감사 수용도 제고를 위해 노력하였다.

마. 윤리자가진단 및 제3자 검증 시행

감사 종료 후, 감사인은 윤리 자가진단을 실시하였으며, 감사에 참여하지 않은 감사인(제3자)이 피감부서장 및 피감인에게 접촉하여 감사활동 중 감사인의 비위행위 등 윤리준수 적절성을 검토 후 제3자 검증 의견서를 작성하는 등 개별감사에 대한 감사인의 객관성 및 윤리기준을 강화코자 노력하였다.

바. 감사실무위원회

감사결과를 보다 합리적이고 공정하게 처리하기 위하여 감사팀장을

위원장으로 하여 감사반 및 감사부서 직원이 참석하여 감사처분요구서 초안에 대한 검토를 진행하였다.

사. 감사심의위원회

감사심의위원회를 개최하여 처분요구(안)에 대해 내·외부감사인 검토를 진행하고, 제3자 검증의 적절성을 검토하였다.

6. 감사 중점사항

이번 특정감사는 IT시스템 관리업무 전반에 대한 적정성 및 적법성을 검증하고 문제점에 대한 단순 지적보다는 컨설팅이나 개선방안을 제시하는데 중점을 두었으며, 내부통제 위험요소에 기반하여 [표 5]와 같이 사전조사 및 예비조사 기간 동안 검토한 주요 점검사항에 대해 선택과 집중을 통한 효율적, 전략적 감사 실현을 위해 노력하였다. 또한, 감사규정 및 감사원의 자체감사 통합매뉴얼 준수 등을 통해 원칙과 객관성을 확보하여 공정한 감사가 될 수 있도록 역량을 집중하였다.

[표 5] 감사 중점 추진사항

연번	중점 추진방향	
1	IT 거버넌스	· IT 거버넌스 적정성 · IT 부서 업무분장의 적정성
2	IT일반 통제	· 프로그램변경, 시스템 접근 보안 및 시스템 운영의 적정성
3	IT응용 통제	· IT응용통제 적정성 - 평가위원 자동선정 - RCMS 일일계좌 시재
4	개인정보	· 개인정보 관리 체계 적정성 · 개인정보 생명주기(수집, 보관, 파기) 관리 체계 적정성 등
5	IT시스템 운영 모범사례 발굴	

Ⅱ. 감사결과

1. 총평

IT시스템 운영 업무 전반에 대한 점검을 통하여 업무 적정성을 확인하고 개선점을 발굴하여 이를 개선토록 요구함으로써 평가관리원의 IT 기반 내부통제 체계를 공고히 함

2. 지적사항 총괄

(단위: 건, 백만원)

합계			변상 (금액)	징계 (인원)	시정(금액)				주의 경고 (인원)	주의 (인원)	개선	권고	통보	고발 (인원)	현지 조치	모범 사례 (인원)
총 건수	신분상 조치인원	재정상 조치금액			소계	추징	감액	기타								
23	-	-	-	-	- (-)	-	-	- (-)	-	-	10	1	6	-	4	2

3. 지적사항 요약

【처분요구사항】

1) 정보화 업무 관련 규정 제정

정보화 업무를 합리적이고 효율적으로 추진하고 정보자원을 효율적으로 관리하기 위하여 정보화 업무 관련 규정 제정이 필요하다. (개선)

2) 지능정보화책임관 지정 및 정보화추진위원회 운영

정보화 시책의 효율적인 수립·시행과 정보화 사업 조정 등의 업무를 총괄하기 위하여 지능정보화책임관을 지정하고 정보화 관련 정책 판단의 합리성과 업무 추진의 효율성 제고를 위하여 중요 사항을 심의·의결하는 정보화추진위원회 구성·운영이 필요하다. (개선, 권고)

3) 사업관리시스템(PMS) 변경 프로그램 이관·승인 업무 강화

사업관리시스템(PMS) 변경 프로그램 이관·승인 관련하여 테스트 관련 증빙, 변경 전 · 후 프로그램 내역 첨부 등 검증 절차를 마련하여 프로그램 변경이 발생되거나 응용 시스템 내에 오류가 포함되어 데이터의 신뢰성 훼손이 없도록 해야 한다. (개선)

4) 개인정보처리시스템 사용자 접근 모니터링 강화

개인정보처리시스템의 접속기록 점검시 다양한 비정상 행위를 점검할 수 있도록 점검 대장 양식을 보완해야 한다. (개선)

5) 디지털평가시스템(STELLA) 평가위원 선정 기능 개선

디지털평가시스템(STELLA)상 연구개발평가단 구성 시 관련 평가위원선정 규정을 위배하지 않도록 평가위원 확정 과정에서 산업체 전문가 비율을 점검할 수 있는 시스템 개선이 필요하다. (개선, 통보)

6) "개인정보보호 내부 관리계획" 개선 및 개인정보보호 관리조직 체계 보완

개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 안전을 확보할 수 있는 개인정보보호 "내부 관리계획" 수립시 이행항목-점검항목 매칭, 이행·점검 일정 추가 등 명시적이고 충실한 관리계획 수립이 필요하며 개인정보 보호책임자 및 분야별 개인정보 보호책임자(보호담당자)에 대해「개인정보보호지침」에 제시된 역할과 동등하게 보완 및 후속 관리가 필요하다. (통보, 개선)

7) 개인정보 처리 및 관리 강화

평가관리원 직원이 사업관리시스템(PMS)의 통합인력정보 조회 기능을 통해 개인정보를 다운로드 받고자 하는 경우, 부서장 승인 절차를 마련하는 등 개인정보 관리가 철저히 이루어지도록 관련 시스템을 개선하고 통합인력정보 조회 기능 내 개인정보 처리 주의 안내 및 경고 문구 설치가 필요하다. (개선, 통보)

8) 콜센터 개인정보 처리 위탁업무 관리 강화

"개인정보 처리 위탁업무" 대상에 포함되어 있지 않은 R&D 상담센터 및 RCMS 고객센터를 대상에 포함시키고 관련 내용을 평가관리원 홈페이지에 공개하고 RCMS 고객센터 위탁 관련하여 수탁자와 "개인정보처리위탁" 계약 및 관련 수탁자 대상 개인정보교육 실시가 필요(단,

R&D상담센터는 현지조치로 시정)하다. (개선, 통보)

9) R&D정보서비스 가입시 개인정보 수집·이용 동의 절차 강화

평가관리원 통합정보서비스 가입 절차에 대해 「개인정보보호법」 및 「개인정보 처리 방법에 관한 고시」를 준용하여 동의절차 및 안내 문구에 대한 개선이 필요하다. (개선, 통보)

10) 개인정보보호법에 따른 "개인정보 및 과세정보 제공활용 동의서" 서식 개정

"개인정보 및 과세정보 제공활용 동의서"에 대해 「개인정보보호법」 및「개인정보 처리 방법에 관한 고시」를 준용하여 주민등록번호 수집 및 안내 문구에 대한 개선이 필요하다. (개선, 통보)

【현지조치사항】

1) 콜센터 개인정보 처리 위탁업무 관리강화

R&D상담센터 관련하여 "개인정보처리위탁 계약 및 개인정보보호 교육 등 「개인정보 보호법」에서 정하는 업무를 실시하도록 조치하여 개인정보보호 강화에 노력하였다.

2) 개인정보처리 및 관리 강화 - 사업관리시스템(PMS)

사업관리시스템(PMS)의 통합인력정보 조회 기능에서 회원 및 인력에 대한 계좌 및 주소 정보 조회 기능을 삭제하였으며, 평가관리원 임직원의 정보는 PMS에서 조회되지 않도록 조치하여 PMS의 개인정보 유출 리스크를 최소화하였다.

3) 개인정보처리 및 관리 강화 - 경영정보시스템(MIS)

경영정보시스템(MIS)의 심의수당 지급 관련 기능에서 평가위원의 계좌정보를 삭제하고, 교통비 지급을 위한 최소한의 주소정보만을 조회할 수 있도록 조치하여 MIS의 개인정보 유출 리스크를 최소화하였다.

4) 개인정보보호를 위한 암호키 관리 강화

"암호키 관리 절차서"내 "개인정보의 안전성 확보조치 기준(개인정보보호위원회 고시)"에 의거 누락되어 있는 암호화 적용기준 및 암호화 키 갱신 내역 추가하도록 조치하여 개인정보보호 강화에 노력하였다.

【모범사례】

1) RCMS 연구개발비 불인정 안내서비스 개발을 통한 오·유용 사전 예방에 기여

관련자는 적극적인 업무자세로 기존 평가관리원 과제 담당자 전용 RCMS 집행 분석 모니터링 서비스를 업그레이드하여 연구개발기관이 직접 불인정 연구개발비 사용 내역을 확인할 수 있는 서비스 개발 및 시범 운영을 하는 등 연구수행자에게 불인정 연구개발비 사용에 대한 실시간 사전 안내로 연구비 오·유용 사전예방 및 연구행정 효율화에 기여하였다.

2) 자동화기술을 통한 업무처리방식 개선

관련자는 적극적인 업무자세로 자동화 기술을 통한 업무처리 방식을 "입금 회계처리 업무"에 우선적용하여 유효성을 검증 후 아이디어 공모전을 통해 확대 추진하는 등 효율적으로 일하는 방식을 개선하여 업무경감 및 자금처리 오류 방지에 기여하였다.

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
정보화 업무 관련 규정 제정	1	○정보화 업무를 합리적이고 효율적으로 추진하고 정보자원을 효율적으로 관리하기 위하여 정보화 관련 규정 제정	개선	2022. 11.	2023. 1. (2개월)	○○○◎◎팀
지능정보화 책임관 지정 및 정보화 추진위원회 운영	2	○정보화 시책의 효율적인 수립·시행과 정보화 사업 조정 등의 업무를 총괄하기 위하여 지능정보화책임관을 지정	개선	2022. 11.	2023. 1. (2개월)	○○○◎◎팀
	3	○정보화 관련 정책 판단의 합리성과 업무 추진의 효율성 제고를 위하여 중요 사항을 심의·의결하는 정보화 추진위원회 구성·운영	권고	2022. 11.	2023. 1. (2개월)	○○○◎◎팀
사업관리시스템(PMS) 변경 프로그램 이관·승인 업무 강화	4	○사업관리시스템(PMS) 변경 프로그램 이관·승인 관련하여 테스트 관련 증빙, 변경 전·후 프로그램 내역 첨부 등 검증 절차를 마련하여 시행	개선	2022. 11.	2023. 1. (2개월)	○○○◇◇팀
개인정보처리 시스템 사용자 접근 모니터링 강화	5	○개인정보처리시스템의 접속기록 점검시 다양한 비정상 행위를 점검할 수 있도록 점검 결과보고서 양식 등을 보완하여 ○○○◇◇팀, ◇◇◇□□팀에 통보	개선	2022. 11.	2023. 1. (2개월)	○○○○○팀
디지털평가 시스템(STELLA) 평가위원 선정 기능 개선	6	○디지털평가시스템(STELLA)상 연구개발평가단 구성 시 산업체 관련 전문가 1/3 이상 참여에 대한 기준을 마련하여 ○○○◇◇팀에 통보	개선	2022. 11.	2023. 1. (2개월)	☆☆☆☆팀
	7	○☆☆☆☆팀에서 작성한 기준을 참고하여 평가위원을 확정하기 전에 산업체 관련 전문가 비율을 확인할 수 있도록 디지털평가시스템을 개선	통보	2022. 11.	2023. 1. (2개월)	○○○◇◇팀

지 적 사 항	순번	조 치 요 구 사 항	조치 구분	처분 요구일	조치 기한일	처리부서
"개인정보보호 내부 관리계획" 개선 및 개인정보보호 관리조직 체계 보완	8	○개인정보보호 "내부 관리계획" 수립시 이행항목에 대한 점검 방법 매칭, 이행·점검 일정 등을 포함한 명시적이고 충실한 관리계획을 수립	통보	2022. 11.	2023. 1. (2개월)	○○○○○팀
	9	○개인정보보호 내부관리계획"에서 ①개인정보 보호책임자의 역할을 명확히 하기 위해 개인정보 보호책임자의 역할을 「개인정보보호지침」에 제시된 역할과 동등하게 보완 및 ② "개인정보처리시스템 접근 권한 및 접속기록 관리"에서 분야별 개인정보보호책임자(보호담당자)를 포함한 관리 체계 구성	개선	2022. 11.	2023. 1. (2개월)	○○○○○팀
개인정보처리 및 관리 강화	10	○평가관리원 직원이 사업관리시스템(PMS)의 통합인력정보 조회 기능을 통해 개인정보를 다운로드 받고자 하는 경우, 부서장 승인 절차를 마련하는 등 개인정보 관리가 철저히 이루어지도록 관련 시스템을 개선	개선	2022. 11.	2023. 1. (2개월)	○○○◇◇팀
	11	○평가관리원 사업관리시스템(PMS)의 통합인력정보 조회 기능 내 개인정보 처리 주의 안내 및 경고 문구를 설치	통보	2022. 11.	2023. 1. (2개월)	○○○◇◇팀
콜센터 개인정보 처리 위탁업무 관리 강화	12	○ R&D 상담센터 및 RCMS 고객센터를 "개인정보 처리위탁업무" 대상에 포함하고 관련 위탁하는 업무의 내용과 수탁자를 평가관리원 홈페이지에 공개	개선	2022. 11.	2023. 1. (2개월)	○○○○○팀
	13	○RCMS 고객센터 위탁 관련하여 수탁자와 "개인정보처리위탁" 계약 및 관련 수탁자 대상 개인정보교육 등을 실시	통보	2022. 11.	2023. 1. (2개월)	◇◇◇□□팀
R&D정보서비스 가입시 개인정보 수집·이용 동의 절차 강화	14	○평가관리원 통합정보서비스 가입 절차에 대해 「개인정보보호법」 및 「개인정보 처리 방법에 관한 고시」를 준용하는 기준을 마련하여 ○○○◇◇팀에 통보	개선	2022. 11.	2023. 1. (2개월)	○○○○○팀
	15	○○○○○○팀에서 송부하는 기준을 준용하여 평가관리원 통합정보서비스 가입 절차를 개선	통보	2022. 11.	2023. 1. (2개월)	○○○◇◇팀

지 적 사 항	순번	조 치 요 구 사 항	조치 구분	처분 요구일	조치 기한일	처리부서
개인정보 보호법에 따른 “개인정보 및 과세정보 제공활용 동의서” 서식 개정	16	○“개인정보 및 과세정보 제공활용 동의서”에 대해 「개인정보보호법」 및 「개인정보처리 방법에 관한 고시」를 준용하는 기준을 마련하여 ☆☆☆☆팀에 통보	개선	2022. 11.	2023. 1. (2개월)	○○○○○팀
	17	○○○○○○팀에서 송부하는 기준을 준용하여 “개인정보 및 과세정보 제공활용 동의서”를 보완하여 평가평가관리원 통합정보서비스 가입 절차를 개선	통보	2022. 11.	2023. 1. (2개월)	☆☆☆☆팀

2. 현지조치사항 일람표

지 적 사 항	순번	조 치 요 구 사 항	조치 구분	처리부서
콜센터 개인정보 처리 위탁업무 관리강화	1	○R&D상담센터 관련하여 “개인정보처리위탁 계약 및 개인정보보호 교육”등 「개인정보보호법」에서 정하는 업무를 실시하도록 조치	현지 시정	☆☆☆☆팀
개인정보처리 및 관리 강화	2	○사업관리시스템(PMS)의 통합인력정보 조회 기능에서 회원 및 인력에 대한 계좌 및 주소정보 조회 기능을 삭제하였으며, 평가관리원 임직원의 정보는 PMS에서 조회되지 않도록 조치	현지 시정	○○○◇◇팀
	3	○경영정보시스템(MIS)의 심의수당 지급 관련 기능에서 평가위원의 계좌정보를 삭제하고, 교통비 지급을 위한 최소한의 주소정보만을 조회할 수 있도록 조치	현지 시정	○○○◇◇팀
개인정보보호를 위한 암호키 관리 강화	4	○“암호키 관리 절차서”내 “개인정보의 안전성 확보조치 기준(개인정보보호위원회 고시)”에 의거 누락되어 있는 암호화 적용기준 및 암호화 키 갱신 내역 추가하도록 조치	현지 시정	○○○○○팀

3. 모범사례 일람표

제목	순번	관계부서	성명	공적요약	기대효과
RCMS 연구개발비 불인정 안내 서비스 개발을 통한 오·유용 사전예방에 기여	1	◇◇◇ □□팀	○☆● △■	○RCMS 집행 분석 모니터링 서비스를 업그레이드하여 연구개발기관이 직접 불인정 연구개발비 사용내역을 확인할 수 있는 서비스 개발 및 시범 운영	○불인정 연구개발비 사용에 대한 실시간 안내로 연구비 오·유용 사전예방 및 연구행정 효율화에 기여
자동화 기술을 통한 업무처리 방식 개선	2	○○○ ◇◇팀	◎★◇ □■	○자동화 기술을 통한 업무처리 방식을 “입금 회계처리 업무”에 우선적용하여 유효성을 검증 후 아이디어 공모전을 통해 확대 추진하는 등 효율적으로 일하는 방식을 개선하여 고부가가치 업무에 집중 할 수 있는 환경 조성에 기여	○자동화 기술을 통한 업무처리 방식 개선으로 업무경감 및 자금처리 오류 방지에 기여

[첨부] 감사결과 처분요구(안)

일련번호	1	감사자	★■○, ◎◆▼ (교차감사)	공개(○), 비공개( )	
신분상 조치인원	-	재정상 조치방법	-	재정상 조치금액	-
수감부서 (처리할 부서)	◎◎◎◎◎단(○○○◎◎팀)	처분요구일	2022.11.	회신 기한일	2023. 1. (통보일로부터 2개월)

개 선

제 목 정보화 업무 관련 규정 제정

소 관 부 서 ◎◎◎◎◎단(○○○◎◎팀)

조 치 부 서 ◎◎◎◎◎단(○○○◎◎팀)

내 용

1. 업무 개요

평가관리원은 ◎◎◎◎◎단 편제하에 ○○○◎◎팀, ○○○◇◇팀, ◇◇◇□□팀, ○○○○○팀을 통해 정보화 관련 업무를 수행하고 있으며 원내 중장기 정보화 전략 수립 및 데이터 기반 행정 업무 총괄은 디지털기획팀에서 수행하고 있다.

2. 정보화 업무 관련 규정 제정

가. 관련 법령 및 판단기준

「전자정부법」 및 「행정기관 및 공공기관 정보시스템 구축·운영 지침」등에 따라 일부 R&D전문기관[1]에서는 정보화 관련 합리적인 업무수행 및 정보자원을 효율적으로 관리하기 위하여 정보화를 총괄하는 규정을 제정하여 운영하고 있다

나. 감사결과 확인된 문제점

평가관리원은 정보보안 관련하여「정보보안규칙」 및 「개인정보보호지침」등 개별 사안별로 규정을 제정하여 운영하고 있으나, 정보화 업무 수행에 대해 총괄하는 규정이 없이「전자정부법」등 관련법에 규정된 사항을 사안별로 참고하여 업무를 진행하고 있어 업무처리기준 위배 및 업무 추진의 혼선 등 체계적인 정보화 업무 수행의 어려움이 예상된다.

관계부서 의견

○○○◎◎팀에서는 감사결과를 전반적으로 수용하면서 정보화 업무 관련 규정을 제정하겠다는 의견을 제시하였다.

1) 한국연구재단 「정보화업무규칙」, 한국산업기술진흥원 「정보화업무규칙」, 국토교통과학기술진흥원 「정보화 추진 및 운영관리에 관한 규칙」 등을 제정하여 운영중

조치할 사항

◎◎◎◎◎단(○○○◎◎팀장)은 정보화 업무를 합리적이고 효율적으로 추진하고 정보자원을 효율적으로 관리하기 위하여 정보화 업무를 총괄하는 규정을 제정해 주시기 바랍니다. **【개선】**

일련번호	2	감사자	★■○, ◎◆▼ (교차감사)	공개(○), 비공개( )	
신분상 조치인원	-	재정상 조치방법	-	재정상 조치금액	-
수감부서 (처리할 부서)	◎◎◎◎◎단(○○○◎◎팀)	처분요구일	2022.11.	회신 기한일	2023. 1. (통보일로부터 2개월)

개선 · 권고

제　　목　지능정보화책임관 지정 및 정보화추진위원회 운영

소 관 부 서　◎◎◎◎◎단(○○○◎◎팀)

조 치 부 서　◎◎◎◎◎단(○○○◎◎팀)

내　　용

1. 업무 개요

평가관리원은 ◎◎◎◎◎단 편제하에 ○○○◎◎팀, ○○○◇◇팀, ◇◇◇□□팀, ○○○○○팀을 통해 정보화 관련 업무를 수행하고 있으며 원내 중장기 정보화 전략 수립 및 데이터 기반 행정 업무 총괄은 디지털기획팀에서 수행하고 있다.

2. 지능정보화책임관 지정 및 정보화추진위원회 운영

가. 관련 법령 및 판단기준

「지능정보화 기본법 시행령」 제6조(지능정보화책임관의 업무)에 따르면 지능정보화책임관은 지능정보화사업과 정보자원을 한 행정기관의 전체적인 목표 및 발전전략, 행정혁신과 연계하여 종합적으로 기획·조정·관리하는 책임자를 말한다.

이에 따라 산업통상자원부는 「정보화 업무규정」 제4조(지능정보화책임관 지정)에 의거, 정보화 시책의 효율적인 수립·시행과 정보화 사업 조정 등의 업무를 총괄하기 위하여 지능정보화책임관을 지정하여 운영하고 있으며 동 규정 제2조(적용범위)에 의거 산업통상자원부장관의 지도·감독을 받는 공기업·준정부기관·기타 공공기관 등 산하 공공기관도 적용 대상이 된다.

나. 감사결과 확인된 문제점

본 특정감사의 사전조사 및 예비조사 결과, 평가관리원은 지능정보화책임관 제도를 운영하고 있지 않은 채, 전산시스템을 운영하는 부서별로 정보화 업무를 별도로 추진하고 있어 정보화 시책의 효율적인 수립 및 시행이 어려운 상태로 확인되었다.

이에 따라 산업통상자원부장관의 지도·감독을 받는 평가관리원은 산업통상자원부는「정보화 업무규정」제4조(지능정보화책임관 지정)에

따라 정보화 시책의 효율적인 수립·시행과 정보화 사업 조정 등의 업무를 총괄하기 위한 지능정보화책임관을 지정하여 운영할 필요가 있다.

한편, 지능정보화책임관을 운영하고 있는 대부분의 공공기관은 정보화 정책 판단의 합리성과 업무 추진의 효율성을 제고하기 위하여 정보화 중장기 계획의 확정 및 변경 등 정보화 추진과 관련한 중요사항 등을 심의·의결하는 정보화추진위원회[2]를 구성하여 운영하고 있다.

그러나 평가관리원의 중장기 정보화 전략 수립 및 데이터 기반 행정업무 총괄을 ○○○◎◎에서 수행하고 있으나, 정보화 중장기 계획의 확정 및 변경, 정보자원 관리정책(정보시스템 개발, 폐기, 관리 체계 등) 결정 등을 ○○○◇◇팀 등 관련 정보화 부서 등과 유기적으로 연계·조정하는 기능이 필요함에도 이를 심의·의결하는 위원회가 없어 정책 판단의 합리성과 업무 추진의 효율성이 저하될 우려가 있다.

관계부서 의견

○○○◎◎팀에서는 감사결과를 전반적으로 수용하면서 지능정보화책임관 지정 및 정보화추진위원회를 구성·운영하겠다는 의견을 제시하였다.

2) 서울교통공사, 서울주택도시공사, 인천관광공사, 한국관광공사, 한국연구재단, 한국지역난방공사 등

조치할 사항

① **◎◎◎◎◎단(○○○◎◎팀장)은** 정보화 시책의 효율적인 수립·시행과 정보화 사업 조정 등의 업무를 총괄하기 위하여 지능정보화 책임관을 지정하여 주시기 바랍니다. **【개선】**

② **◎◎◎◎◎단(○○○◎◎팀장)은** 정보화 관련 정책 판단의 합리성과 업무 추진의 효율성 제고를 위하여 중요 사항을 심의·의결하는 정보화추진위원회를 구성·운영해 주시기 바랍니다. **【권고】**

일련번호	3	감사자	★■○	공개(○), 비공개( )	
신분상 조치인원	-	재정상 조치방법	-	재정상 조치금액	-
수감부서 (처리할 부서)	◎◎◎◎◎단(○○○◇◇팀)	처분요구일	-	회신 기한일	-

개 선

제 목 사업관리시스템(PMS) 변경 및 승인 절차 강화

소 관 부 서 ◎◎◎◎◎단(○○○◇◇팀)

조 치 부 서 ◎◎◎◎◎단(○○○◇◇팀)

내 용

1. 업무 개요

평가관리원은 R&D사업의 세부과제 협약변경, 사후관리 등 효율적인 R&D사업 관리를 위하여 사업관리시스템(PMS)를 활용하고 있으며 ○○○◇◇팀에서 시스템 운영 및 유지·보수 업무를 담당하고 있다.

2. 사업관리시스템(PMS) 변경 및 승인 절차 강화

가. 판단기준

금융회사 또는 전자금융업자는 「전자금융감독규정」 제29조(프로그램 통제)에 따라 프로그램 변경 전·후 내용을 기록 및 관리하여야 하며, 프로그램 등록·변경·폐기내용의 정당성에 대해 검증하고, 변경 필요시 해당 프로그램을 개발 또는 테스트 시스템으로 복사 후 수정하여야 하며, 운영시스템 적용은 처리하는 정보의 기밀성·무결성·가용성을 고려하여 충분한 테스트 및 관련 책임자 승인 후 실시토록 하고 있다.

또한, 한국상장회사협의회에 따르면 상장회사는 「전자금융감독규정」 제29조(프로그램 통제)에 준하여 '상장회사 IT 감사체크리스트'를 마련하여 정보시스템 유지보수에 대한 감사항목을 설정하고 있다.

나. 감사결과 확인된 문제점

본 감사의 사전조사 기간인 2022. 6. 21.부터 같은해 6. 24. 동안 평가관리원 사업관리시스템(PMS) 프로그램의 기능추가 및 수정에 대한 업무처리 절차를 점검하였다.

평가관리원 사업관리시스템(PMS)을 관리하는 외주 위탁운영팀(케이씨씨정보통신(주))은 현업부서의 PMS 기능 추가 또는 수정을 요청받은 경우 별도의 시스템에서 프로그램 변경 및 테스트 완료 후, '프로그램 적용 계획서'를 작성하여 ○○○◇◇팀 PMS 관리 담당자의 확인(결재) 절차를 거쳐 해당 프로그램을 PMS로 이관하여 적용하고 있다.

그러나 ○○○◇◇팀은 프로그램 변경 및 승인에 대한 적정성 점검을

위하여 월 단위로 프로그램 변경 내역을 확인하는 수준에 머물고 있어, 프로그램 변경에 따른 실질적인 문제점을 사전 또는 사후에 확인하여 대응하기 힘든 상황이다.

이에 프로그램 변경 후 테스트 관련 증빙, 변경 전·후 프로그램 내역 등을 관리하고, 이를 검토 및 승인 후 PMS로 이관함으로써 프로그램 변경 및 승인 절차를 강화할 필요가 있다.

관계부서 의견

○○○◇◇팀에서는 사업관리시스템(PMS) 변경 프로그램에 대한 이관·승인 업무 관련 감사결과를 전반적으로 수용하면서 프로그램 변경 건에 대해 처리 결과 검토를 강화하겠다는 의견을 제시하였다.

조치할 사항

◎◎◎◎◎단(○○○◇◇팀장)은 사업관리시스템(PMS) 변경 프로그램 이관·승인 관련하여 테스트 관련 증빙, 변경 전·후 프로그램 내역 첨부 등 검증 절차를 마련하여 시행해 주시기 바랍니다. **【개선】**

일련번호	4	감사자	★■○	공개(○), 비공개(　)	
신분상 조치인원	-	재정상 조치방법	-	재정상 조치금액	-
수감부서 (처리할 부서)	◎◎◎◎◎단(○○○○○○팀, ○○○◇◇팀, ◇◇◇□□팀)	처분요구일	2022.11.	회신 기한일	2023. 1. (통보일로부터 2개월)

개 선

제　　목　개인정보처리시스템 사용자 접근 모니터링 강화

소 관 부 서　◎◎◎◎◎단(○○○○○○팀, ○○○◇◇팀, ◇◇◇□□팀)

조 치 부 서　◎◎◎◎◎단(○○○○○○팀)

내　　용

1. 업무 개요

평가관리원은「개인정보 보호법」에 따라 R&D과제 수행자 등 개인정보에 대해 개인정보취급자[3]의 개인정보처리스템[4] 접속기록을 점검하고 있으며, 이러한 업무는 개인정보를 취급하는 ○○○◇◇팀, ◇◇◇□□팀 및 ○○○○○팀에서 수행하고 있다.

3) 개인정보를 처리하는 업무를 담당하는 임직원, 용역기관(자) 등을 의미
4) 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템

2. 개인정보처리시스템 사용자 접근 모니터링 강화

가. 관련 법령 및 판단기준

「개인정보 보호법」제29조(안전조치의무)와 같은 법 시행령 제30조(개인정보의 안전성 확보 조치) 및 평가관리원「개인정보 보호지침」제63조(접속기록의 보관 및 점검)에 의거 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 여부 등에 대응하기 위해 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하도록 되어 있다.

나. 감사결과 확인된 문제점

평가관리원은 평가관리원 통합 DB(데이타베이스), e-R&D(사업관리시스템) 연계 DB 및 RCMS(통합연구비관리시스템)운영 DB 등 개인정보처리시스템에 대해 접속기록 보관·관리 여부, 부정접속 시도, 암호화대상 관련 현황 등 점검을 2019.7월부터 2022.7월까지는 개인정보를 총괄하고 있는 ○○○○○팀에서 매월 정기점검을 하였으나 2022.8월 부터는 효율성 및 책임성 제고를 위하여 평가관리원 통합 DB, e-R&D 연계 DB는 ○○○◇◇팀, RCMS운영 DB는 ◇◇◇□□팀 등 해당 DB 사용·관리하는 실무 부서에서 점검하고 있다.

개인정보보호위원회의 "2022년 개인정보 관리수준 진단 평가지표"에 따르면 개인정보처리시스템의 접속기록 점검시 [표 7]과 같이 다양한 '비정상 행위'에 대하여 점검하여야 하나 점검 결과보고서에는 미인가자 접속

시도 및 휴일 등 근무시간 외 접속시도/기준을 초과하여 개인정보조회·다운로드 등 일부분만 점검한 것으로 확인되었다. 이는 [그림 13]과 같이 결과보고서 양식에 접속기록 비정상 행위 사례 중 일부만 표기 되어 있고 이를 점검하는 실무부서에서 준용하여 점검한 것이다. 따라서 비정상 행위에 대한 다양한 사례를 점검할 수 있도록 양식 보완 등이 필요하다.

[표 7] 접속기록 비정상 행위 주요 예시

- (계정) 접근권한이 부여되지 않는 계정으로 접속한 행위 등
- (접속일시) 출근시간 전, 퇴근시간 후, 새벽시간, 휴무일 등 업무시간 외 접속한 행위
- (접속지 정보) 인가되지 않은 단말기 또는 지역(IP)에서 접속한 행위 등
- (처리한 정보주체 정보) 특정 정보주체에 대해 과도하게 조회, 다운로드 등의 행위
- (수행업무) 대량의 개인정보에 대한 조회, 정정, 다운로드, 삭제 등의 행위 등
- (기타) 짧은 시간에 하나의 계정으로 여러지역(IP)에서 접속한 해위 등

관계부서 의견

○○○○○팀에서는 감사결과를 전반적으로 수용하면서 개인정보처리시스템의 접속기록 점검시 다양한 비정상 행위에 대해 점검할 수 있도록 관리점검 결과 양식 등을 보완하겠다는 의견을 제시하였다.

조치할 사항

◎◎◎◎◎단(○○○○○팀장)은 개인정보처리시스템의 접속기록 점검시 다양한 비정상 행위를 점검할 수 있도록 점검 대장 양식을 보완해 주시기 바랍니다.**【개선】**

[그림 13] 개인정보처리시스템 관리실태 점검결과 보고 양식

개인정보 접근기록 및 암호화 현황 점검대장

❑ 점검 대상

점검대상 시스템명	
점검기간	yyyy.mm.dd ~ yyyy.mm.dd

❑ 개인정보 보유 현황 (단위: 건)

개인정보 보유량	주민등록번호 보유량	주민등록번호 암호화 현황
	실명인증 CI보유량	실명인증 DI 보유량

❑ 점검결과 (요약)

1	접근권한(3년이상) 보관현황 점검결과	
2	접속기록(2년이상) 보관현황 점검결과	
3	미인가자 접속 점검결과	
4	휴일 등 근무시간외 접속 점검결과	
5	기준을 초과하여 개인정보 조회/다운로드 여부 점검결과	
6	암호화대상 관리현황 점검결과	
7	기타 점검결과	

20 년 월 일

개인정보처리시스템 담당자 : (인)
개인정보처리시스템 관리자(분야별 부서장) : (인)

한국산업기술평가관리원

일련번호	5	감사자	▽■○	공개(○), 비공개(　)	
신분상 조치인원	-	재정상 조치방법	-	재정상 조치금액	-
수감부서 (처리할 부서)	◎◎◎◎◎단(○○○◇◇팀) ●○●○●○단(☆☆☆☆팀)	처분요구일	2022.11.	회신 기한일	2023. 1. (통보일로부터 2개월)

개 선 · 통 보

제　　목　디지털평가시스템(STELLA) 평가위원 선정 기능 개선

소 관 부 서　① ◎◎◎◎◎단(○○○◇◇팀)

조 치 부 서　① ●○●○●○단(☆☆☆☆팀)

② ◎◎◎◎◎단(○○○◇◇팀)

내　　용

1. 업무 개요

평가관리원은「산업기술혁신촉진법」 제39조(한국산업기술평가관리원의 설립 등)에 따라 산업기술혁신사업의 과제기획·관리 및 평가 등의 업무를 수행하고 있으며, 사업의 평가 및 관리는 「산업기술혁신사업 공통운영요령(이하 “공통운영요령”이라 한다)」 및 「산업기술혁신사업 기술개발 평가관리지침(이하 “평가관리지침”이라 한다)」 등 관련 규정에 따른다.

평가관리원은 디지털평가시스템(STELLA)을 활용하여 평가 대상

연구개발과제의 분과 구성, 사전검토, 평가위원 구성, 전자평가 등의 업무를 처리하고 있으며, 해당 시스템의 운영과 고도화는 ○○○◇◇팀, 사업의 평가 및 관리 총괄업무는 ☆☆☆☆팀에서 담당하고 있다.

2. 디지털평가시스템(STELLA) 평가위원 선정 기능 개선

가. 관련 법령 및 판단기준

공통운영요령 제7조제1항에 따르면 장관은 전문기관의 장으로 하여금 연구개발과제평가단(이하 "평가단"이라 한다) 등을 구성하여 선정평가, 단계평가, 특별평가, 최종평가 등을 심의하게 할 수 있다.

평가관리지침 제6조제1항에 따르면 연구개발과제평가단은 사업의 추진과 관련하여 공통운영요령 제7조제1항 각 호의 사항을 심의하며, 같은 지침 제6조제2항에 따라 평가관리원은 연구개발평가단 위촉 시 평가 대상 연구개발과제의 기술 중분류와 50% 이상 일치[5], 산업체 관련 전문가가 1/3 이상 참여[6] 등의 조건을 만족하도록 되어 있다.

5) 평가관리지침 제6조제2항제1호 공통운영요령 제7조에 따라 평가 대상 연구개발과제의 기술 중분류와 50% 이상 일치하도록 7명 내외로 구성함을 원칙으로 하되 연구개발과제별 또는 사업별 특성에 따라 평가위원을 추가로 구성 가능하고, 필요시 다음의 위원을 포함할 수 있음
가. 경제·시장전문가 2명 이상
나. 단계·최종평가의 경우 해당연구개발과제의 과거 평가위원(신규, 단계) 중 2명 이상
다. 책임평가위원
라. 제21조 신규평가의 경우 개념평가 위원중 2명 이상
마. 표준연계 연구개발과제의 경우 신규 및 최종평가에 표준전문가 1명 이상

6) 평가관리지침 제6조제2항제4호 연구개발과제평가단은 산업체 관련 전문가(기업, 업종별단체 및 민간협회 등 포함)가 1/3 이상 참여하는 것을 원칙으로 함

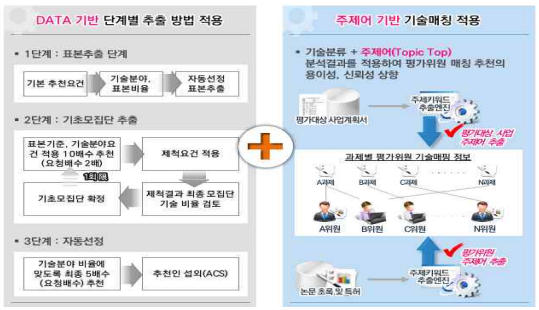
나. 감사결과 확인된 문제점

이번 감사에서는 평가관리원에서 운영하고 있는 디지털평가시스템의 연구개발과제평가단 구성이 관련 규정에 부합하게 업무를 처리할 수 있도록 IT시스템 통제 기능이 구현되어 있는지를 중점 점검하였다.

평가관리원은 연구개발과제평가단 구성의 공정성과 전문성 확보를 위하여 자동추천(디지털평가시스템에서 선정)과 특별추천(평가관리원 담당자가 선정) 방식을 혼용하여 운영하고 있다.

[그림 15]와 같이 자동추천 방식은 기술분류[7]와 주제어[8] 기반 매칭을 통해 평가대상 연구개발과제와 정합도가 높은 평가위원 50명을 디지털평가시스템에서 자동으로 추출하는 기능으로, 평가관리원 담당자는 이중에서 7명 내외의 평가위원을 위촉하여 확정하고 있다.

[그림 15] STELLA 자동추천위원 방식(기술분류+주제어)>



7) 과제 신청자가 선택한 산업기술분류의 소분류와 평가위원이 평가위원 등록 시 선택한 산업기술분류 일치 정도를 매칭

8) 평가위원 주요 정보(연구이력 등 항목)와 과제평가·과제수행 이력을 포함하여, 신청과제에 정합도가 높은 전문가 선정

첫째, 디지털평가시스템에서 평가위원 자동추천 시 평가관리지침 제6조제2항에 따라 평가대상 연구개발과제와 연구개발평가단의 기술중분류가 50% 이상 일치하는지 여부를 점검하였다.

그 결과 [그림 16]과 같이 디지털평가시스템에서 평가위원을 자동으로 추출할 때 평가대상 연구개발과제와 평가위원의 기술분류가 일치하도록 ‘평가위원 기술분야’ 1순위 70%, 2순위 20%, 3순위 10%로 추천조건이 설정되도록 시스템이 적절하게 구현되어 있었다.

둘째, 디지털평가시스템에서 평가위원 자동추천 시 평가관리지침 제6조제2항에 따라 연구개발평가단 중 산업체 관련 전문가가 1/3 이상 참여하는지 여부를 점검하였다.

그 결과 [그림 17]과 같이 디지털평가시스템에서 평가위원을 자동으로 추출할 때 산업체 관련 전문가가 30% 추출되도록 표본비율이 설정되어 있었다.

그러나 평가관리원 담당자가 자동 추출된 평가위원 50명 중에서 7명을 확정하는 과정에서 산업체 관련 전문가 비율을 확인하지 못하여 관련 규정(산업체 관련 전문가 1/3 이상 참여하는 것을 원칙)을 준수하지 못할 위험성이 존재하는 것으로 확인되었다.

따라서 평가관리원 담당자가 디지털평가시스템에서 평가위원을 확정하기 전 위촉된 평가위원 중 산업체 관련 전문가 비율이 만족하지 않는 경우, 팝업 메시지를 생성 등으로 이를 체크할 수 있도록 IT응용통제 관점에서 기능을 추가할 필요가 있다.

[그림 16] 자동추천(추천조건 설정)



[그림 17] 자동추천(표본비율 설정)



관계부서 의견

☆☆☆☆팀과 ○○○◇◇팀은 감사결과를 전반적으로 수용하면서 디지털평가시스템의 평가위원 확정 과정에서 산업체 전문가 비율을 점검할 수 있는 기능을 구현하겠다는 의견을 제시하였다.

조치할 사항

① **●○●○●○단(☆☆☆☆팀장)은** 연구개발평가단 구성 시 산업체 관련 전문가 1/3 이상 참여에 대한 기준을 마련하여 ○○○◇◇팀에 안내하여 주시기 바랍니다.**【개선】**

② **◎◎◎◎◎단(○○○◇◇팀장)은** ☆☆☆☆팀에서 작성한 기준을

참고하여 평가위원을 확정하기 전에 산업체 관련 전문가 비율을 확인할 수 있도록 디지털평가시스템에 반영해 주시기 바랍니다.**【통보】**

일련번호	6	감사자	★■○, ○●☆ (교차감사) ○◇● (교차감사)	공개(○), 비공개( )	
신분상 조치인원	-	재정상 조치방법	-	재정상 조치금액	-
수감부서 (처리할 부서)	◎◎◎◎◎단(○○○○○팀)	처분요구일	2022.11.	회신 기한일	2023. 1. (통보일로부터 2개월)

통보 · 개선

제 목 “개인정보보호 내부 관리계획” 개선 및 개인정보보호 관리조직 체계 보완

소 관 부 서 ◎◎◎◎◎단(○○○○○팀)

조 치 부 서 ◎◎◎◎◎단(○○○○○팀)

내 용

1. 업무 개요

평가관리원은 개인정보 보호를 위하여「개인정보보호지침」및「정보보안규칙」을 제정하여 운영하고 있으며 이를 토대로 매년 ”개인정보보호 내부 관리계획“(이하 “내부 관리계획”이라 한다)을 수립하여 이행·점검하고 있다. 개인정보보호 관련 업무는 디지털 보안팀에서 수행하고 있다.

2. “개인정보보호 내부 관리계획” 수립 개선 및 개인정보보호 관리조직 체계 보완

가. 관련 법령 및 판단기준

평가관리원의 “내부 관리계획”은 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 및 물리적 안전조치에 관한 사항을 정하고 이행 및 그 결과를 점검하도록 하고 있다.

나. 감사결과 확인된 문제점

2022.06.09.에 수립된 “내부 관리계획”에는 개인정보보호 관련 이행 항목[표 8]과 점검(이행) 방법[표 9]이 제시되어 있으나, 점검 주기(일정) 및 이행 항목에 따른 점검 방법이 구체적이지 않아 업무에 혼선이 우려된다. 일례로 점검 방법 중 “인공지능(AI) 개인정보보호 자율점검표”([표 9]-3)와 관련하여 2022년 상반기에 “인공지능(AI) 개인정보보호 자율점검”(2022. 1. 28.) 제정 후 ○○○◎◎팀 등 관련부서에 대해 (자체)점검을 하였으나 “개인정보보호 내부관리계획에 따른 개인정보보활동 이행실적 점검결과 보고”(2022. 8. 29.)에서는 누락되었다.

[표 8] “개인정보보호 내부 관리계획”내 이행 항목

이행 항목
1. 개인정보 보호책임자의 지정에 관한 사항
2. 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항
3. 개인정보취급자에 대한 교육에 관한 사항
4. 접근 권한의 관리에 관한 사항
5. 접근 통제에 관한 사항

6. 개인정보의 암호화 조치에 관한 사항
7. 접속기록 보관 및 점검에 관한 사항
8. 악성프로그램 등 방지에 관한 사항
9. 물리적 안전조치에 관한 사항
10. 개인정보 보호조직에 관한 구성 및 운영에 관한 사항
11. 개인정보 유출사고 대응 계획 수립·시행에 관한 사항
12. 위험도 분석 및 대응방안 마련에 관한 사항
13. 재해 및 재난 대비 개인정보처리시스템의 물리적 안전조치에 관한 사항
14. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항
15. 그 밖에 개인정보 보호를 위하여 필요한 사항

[표 9] "개인정보보호 내부 관리계획"내 점검(이행) 방법(목차만 표시)

점검 방법(목차만 표시)
1. 개인정보취급자에 대한 관리·감독 점검표
2. 개인정보보호 실태점검표
3. 인공지능(AI) 개인정보보호 자율점검표
4. 개인정보처리시스템 접근권한 및 접속기록 관리 정책서(안)
5. 개인정보 목적 외 이용·제3자 제공 절차서(안)
6. 개인정보 침해•유출사고 대응 절차서(안)
7. 개인정보처리시스템 재해·재난대비 위기대응 매뉴얼
8. 정보주체 권리보장 절차서
9. 가명정보 처리 절차서(안)
10. 2022년 개인정보보호 교육계획(안)
11. 수탁사 대상 개인정보보호 교육·관리감독 계획
12. 「OOO」용역 수탁자 대상 개인정보보호 교육 및 관리·감독 결과
13. 개인정보처리위탁 계약서
14. 외주 용역사업 보안특약 조항

또한 같은 날 수립된 "내부 관리계획"에는 [표 10]과 같이 개인정보 보호책임자의 역할을 명시하고 있으나, 평가관리원「개인정보 보호지침」제24조에서 정한 개인정보 보호책임자의 역할이 누락되어 업무 수행의 혼선이 우려된다. 예를 들어 "개인정보 보호 관련 지침 제·개정", "분야별 개인정보 관리자의 지휘·감독", "인터넷 접속정보파일 등 개인정보를 자동

으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항" 및 "가명정보 처리에 관한 사항" 등이 누락되었다.

한편「개인정보보호지침」제25조, 제26조에서는 분야별 개인정보 보호책임자 및 개인정보 보호담당자의 지정 및 역할에 대해 명시하고 있으나, "내부관리계획"에는 "개인정보처리시스템 접근 권한 및 접속기록 관리"와 관련하여 ○○○○○팀의 개인정보 보호담당자의 역할 등에 대해서만 언급되어 있을 뿐 분야별 개인정보 보호책임자(보호담당자)와 관련해서는 언급되어 있지 않다

[표 10] 개인정보 보호책임자의 역할

항목	개인정보보호 내부관리계획	개인정보보호지침(제24조)
개인정보보호책임자 역할	1. 개인정보 보호 계획의 수립 및 시행 2. 개인정보 처리 현황 점검 및 개선 3. 개인정보 처리와 관련한 불만의 처리 및 피해 구제 4. 개인정보 유출 및 오용.남용 방지를 위한 내부통제 체계구축 5. 개인정보 보호 교육 계획의 수립 및 시행 6. 개인정보파일의 보호 및 관리 감독 7.「개인정보 보호법」 제30조에 따른 개인정보 처리방침의 수립.변경 및 시행 8. 개인정보 보호 관련 자료의 관리 9. 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기 관리.감독 10. 개인정보보호 관련 자료의 관리 11. 개인정보파일 현황은 개인정보보호원회 개인정보보호포털에 등록 12. 개인정보파일 등록 또는 변경 신청을 받은 경우 등록·변경 사항을 검토하고 그 적정성을 판단한 후 개인정보보호포털에 등록 13. 개인정보 파기시행 후 파기 결과를 확인하고 개인정보 파일 파기 관리대장 작성 14. 개인정보파일 등록의 삭제를 요청받은 경우 그 사실을 확인하고, 지체 없이 등록사실 삭제 및 개인정보보호포털에 통보 15. 연1회 이상으로 내부관리계획의 이행실태를 점검·관리	1. 개인정보 보호 관련 지침 제·개정 2. 개인정보 보호 계획 수립 및 시행 3. 개인정보 처리 실태 점검 및 개선 권고 4. 개인정보 처리와 관련한 불만 처리 및 피해 구제 5. 개인정보 유출 및 오용·남용 방지를 위한 내부 관리계획의 수립·시행 및 내부통제시스템의 구축 6. 개인정보 보호 교육 계획의 수립 및 시행 7. 개인정보파일의 보호 및 관리·감독 8. 개인정보 보호 관련 자료의 관리 9. 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기 10. 분야별 개인정보 관리자의 지휘·감독 11. 개인정보 처리방침의 수립 및 시행 12. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항 13. 가명정보 처리에 관한 사항

관계부서 의견

○○○○○팀에서는 감사결과를 전반적으로 수용하면서 "내부 관리계획" 수립시 이행항목에 대한 점검 방법의 구체화 및 개인정보 보호책임자 역할을 명시하겠다는 의견을 제시하였다.

조치할 사항

① **◎◎◎◎◎단(○○○○○팀장)은** "개인정보보호 내부 관리계획" 수립시 이행항목에 대한 점검 방법 구체화, 점검 주기(일정) 적시 등 개인정보보호 관리 계획을 내실화하여 주시기 바랍니다. **【통보】**

② **◎◎◎◎◎단(○○○○○팀장)은** "개인정보보호 내부관리계획" 수립시 분야별 개인정보 보호책임자(보호담당자)를 명시하고, 개인정보 보호책임자의 역할 구체화 등 분야별 개인정보 보호책임자(보호담당자)를 포함한 관리 체계를 구성하여 주시기 바랍니다. **【개선】**

일련번호	7	감사자	▽☆◎	공개(○), 비공개(　)	
신분상 조치인원	-	재정상 조치방법	-	재정상 조치금액	-
수감부서 (처리할 부서)	◎◎◎◎◎단(○○○◇◇팀)	처분요구일	2022.11.	회신 기한일	2023. 1. (통보일로부터 2개월)

현지시정 · 개선 · 통보

제　　목　개인정보 처리 및 관리 강화

소 관 부 서　◎◎◎◎◎단(○○○◇◇팀)

조 치 부 서　◎◎◎◎◎단(○○○◇◇팀)

내　　용

1. 업무 개요

평가관리원은 「국가연구개발혁신법」 제19조에 근거하여 국가연구개발사업에 참여하는 연구자의 참여제한 여부 확인, 자격요건 확인 등을 위하여, 「개인정보 보호법」제15조에 의거 수집하려는 개인정보 항목, 목적, 보유·이용기간, 거부 권리 및 거부에 따른 불이익 등을 구체적으로 알린 후 연구자 동의에 따라 개인정보를 수집·이용하고 있는 등 개인정보보호를 위한 노력을 기울이고 있다.

2. 개인정보처리 및 관리 강화

가. 판단기준 및 분석방법

「개인정보보호법」 제2조(정의)에 따르면 개인정보란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보, 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보 등을 말한다.

평가관리원은 같은 법 제3조(개인정보 보호 원칙)에 따라 목적에 필요한 범위에서 적합하게 개인정보를 처리[9]하여야 하며, 그 목적 외의 용도로 활용해서는 안되며, 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 하고, 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.

평가관리원은 개인정보 처리를 함에 있어서도 같은 법 제28조(개인정보취급자에 대한 감독)에 의거 개인정보가 안전하게 관리될 수 있도록 개인정보를 처리하는 자에 대하여 적절한 관리·감독을 행하여야 한다.

또한, 평가관리원은 같은 법 제19조(개인정보를 제공받은 자의 이용·제공 제한)에 따라 개인정보를 제공받은 목적 외의 용도로 이용하거나 이를 제3자에게 제공하여서는 안되며, 같은 법 제24조(고유식별정보의 처리 제한)에 의거 고유식별정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 하여야 한다.

9) 「개인정보보호법」 제2조(정의)에 따르면 "처리"란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위

나. 감사결과 확인된 문제점

본 특정감사를 통하여 확인한 결과, 평가관리원이 국가연구개발사업 기획평가관리 등을 위하여 대상자로부터 개인정보 수집·이용 동의를 받아 산업기술 R&D 정보포털(이하 "ITECH"라 한다)에서 관리중인 "회원"과, ITECH 정보 이용, 연구개발과제 단순참여 등을 이유로 등록된 "인력" 수는 휴면회원을 제외하고 총 717,045명[10]에 달하며, 여기에는 평가관리원 임직원의 정보도 포함되어 있다.

평가관리원 임직원은 ITECH에 등록된 회원 및 인력 정보에 대하여 사업관리시스템(이하 "PMS"라 한다)의 통합인력정보 조회 기능을 통하여 조회가 가능할 뿐만 아니라, "개인정보 다건 조회"기능을 통하여 다수의 회원 및 인력의 개인정보를 다운로드 가능한 것으로 조사되었다.

PMS 통합인력정보 조회 기능에서 조회 및 다운로드가 가능한 세부정보를 살펴본 결과, 대상자의 성명, 소속기관, 주민등록번호, 주소, 휴대전화 번호, 이메일 주소, 계좌번호 등 민감한 개인정보가 포함되어 있음을 확인하였다.

이에 최근 5년 간 평가관리원 임직원이 PMS에서 다운로드 받은 개인정보 내역을 조사한 결과, 최근 5년 간 4,308회에 걸쳐 221,887명의 개인정보를 다운받은 것으로 나타났다.

해당 개인정보 처리의 적정성을 확인한 결과, 연구개발과제 담당자가 다수의 연구개발과제 협약 과정에서 책임자 등의 채무불이행, 참여제한

10) 이 중 주민등록번호가 입력되어 있는 인원은 637,932명, 계좌번호가 입력되어 있는 인원은 135,224명, 우편번호 상의 기본주소 외 상세주소까지 입력되어 있는 인원은 50,122명임.

여부, 의무사항 불이행 여부 등의 자격 부합 여부를 확인하기 위하여 개인정보를 다운로드 받았으며, 제공받은 목적 외의 용도로 개인정보를 이용한 건은 없는 것으로 검토되었다.

그럼에도 불구하고 평가관리원 직원이 PMS를 통해 개인정보를 다운로드 받는 과정에서 관리자 또는 부서장의 승인 없이 요청사유만을 기입하고 다수의 개인정보를 다운받을 수 있어, 직원이 개인정보를 제공받은 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있는 리스크가 존재하므로, 「개인정보 보호법」 제28조(개인정보취급자에 대한 감독)에 의거 적절한 관리·감독이 되도록 시스템 개선이 필요하다.

또한, 「국가연구개발혁신법」 제19조에 따른 개인정보 수집·이용에 동의하지 않은 평가관리원 임직원의 개인정보는 PMS에서 조회되지 않도록 조치할 필요가 있다.

최근 회사의 통신망을 이용한 스토킹 살인 범죄 사례, 개인정보 판매를 통한 공무원 및 공공기관 직원의 금품·뇌물 수수 사례 등 개인정보보호법 위반 관련 사회 이슈가 증가하고 있는 만큼, 개인정보 동의서의 수집 목적에 사용되는 최소한의 정보 외 개인정보 노출 최소화를 강화할 필요가 있다. 이에 PMS에서 개인정보 처리 목적 외 불필요한 정보인 계좌번호와 주소 정보 조회 기능을 삭제할 필요가 있다.

또한, 개인정보 처리 과정에서도 정보보호 강화 및 법률 위반 시 벌칙 조항을 안내하는 등[11] 평가관리원 임직원의 개인정보처리 및 관리 강화를 위한 경각심을 고취시킬 필요가 있다.

또한, 평가관리원은 연구개발과제 평가위원회에 참석한 평가위원의 심의수당, 교통비 등의 지급을 위하여, 직원이 경영정보시스템(이하 "MIS"라 한다)을 활용하여 평가위원의 계좌번호와 상세주소 정보를 조회할 수 있도록 되어 있다.

하지만, ☆★☆★팀 소속 외 직원은 MIS에서 평가위원의 계좌정보를 이용할 사유가 없으며, 교통비 지급을 위한 평가위원의 주소 정보도 상세주소가 아닌 우편번호 단위의 기본주소만으로도 그 목적 달성이 가능하므로, MIS에서 평가위원의 계좌 및 상세주소 정보가 조회되지 않도록 조치할 필요가 있다.

관계부서 의견

○○○◇◇팀 PMS 및 MIS의 각 담당자는 감사 중 확인된 개인정보처리 및 관리 문제를 공감하고, PMS에서 평가관리원 임직원 정보, 회원 및 인력의 주민등록번호, 계좌정보 등이 조회되지 않도록 하고, MIS에서 평가위원의 계좌와 상세주소 정보가 조회되지 않도록 하는 등 개인정보관리를 강화하겠다는 의견을 밝혔다.

11) 한국산업기술평가관리원 감사실에서는 2021년 경영전략본부 종합감사를 통하여 정보공개청구 업무의 민원인 개인정보 강화를 처분한 바 있으며, 이에 따라 정보공개청구 업무 처리 화면에 안내 및 경고 문구, "개인정보 보호 철저 요청 : 개인정보 노출 위험 최소화를 위하여 청구인 개인정보는 표시되지 않습니다. 청구내용 등에 개인정보가 포함되어 있을 수 있으니, 개인정보 보호에 각별히 유의하여 주시기 바람. 또한 청구인 인적사항 등 개인정보와 청구내용은 정보공개대응 목적으로만 사용해야 하며, 정보 주체의 동의 없이 무단으로 제3자에게 제공한 경우에는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처할 수 있습니다.(개인정보보호법 제17조 및 제71조, 민원처리에 관한 법률 제7조)"를 설치함.

현지조치 사항

① ◎◎◎◎◎단(○○○◇◇팀장)은 평가관리원 사업관리시스템(PMS)의 통합인력정보 조회 기능에서 회원 및 인력에 대한 계좌 및 주소 정보 조회 기능을 삭제하였으며, 평가관리원 임직원의 정보는 PMS에서 조회되지 않도록 조치하였다. **【현지시정】**

② ◎◎◎◎◎단(○○○◇◇팀장)은 평가관리원 경영정보시스템(MIS)의 심의수당 지급 관련 기능에서 평가위원의 계좌정보를 삭제하고, 교통비 지급을 위한 최소한의 주소정보만을 조회할 수 있도록 조치하였다. **【현지시정】**

조치할 사항

① ◎◎◎◎◎단(○○○◇◇팀장)은 평가관리원 직원이 사업관리시스템(PMS)의 통합인력정보 조회 기능을 통해 개인정보를 다운로드 받고자 하는 경우, 부서장 승인 절차를 마련하는 등 개인정보 관리가 철저히 이루어지도록 관련 시스템을 개선하여 주시기 바랍니다. **【개선】**

② ◎◎◎◎◎단(○○○◇◇팀장)은 평가관리원 사업관리시스템(PMS)의 통합인력정보 조회 기능 내 개인정보 처리 주의 안내 및 경고 문구를 설치하여 주시기 바랍니다. **【통보】**

일련번호	8	감사자	★■○	공개(○), 비공개(　)	
신분상 조치인원	-	재정상 조치방법	-	재정상 조치금액	-
수감부서 (처리할 부서)	◎◎◎◎◎단(○○○○○팀), ◎◎◎◎◎단(◇◇◇□□팀) ●○●○●○단(☆☆☆☆팀)	처분요구일	2022.11.	회신 기한일	2023. 1. (통보일로부터 2개월)

현지시정 · 개선 · 통보

제　　목　콜센터 개인정보 처리 위탁업무 관리 강화

소 관 부 서　① ◎◎◎◎◎단(○○○○○팀)

② ◎◎◎◎◎단(◇◇◇□□팀)

③ ●○●○●○단(☆☆☆☆팀)

조 치 부 서　① ◎◎◎◎◎단(○○○○○팀)

② ◎◎◎◎◎단(◇◇◇□□팀)

내　　용

1. 업무 개요

평가관리원은 R&D 과제기획에서부터 사후관리에 이르기까지 고객 문의를 지원하는 R&D 상담센터와 연구비 집행 및 정산 관련 고객문의를 지원하는 RCMS(통합연구비관리시스템) 고객센터 등 2개의 콜센터를 운영하고 있다. R&D 상담센터는 ☆☆☆☆팀, RCMS 고객센터는 ◇◇◇□□팀에서 담당하고 있으며 개인정보보호 관련 총괄 업무는 ○○○○○팀에서 수행하고 있다.

2. 콜센터 개인정보 처리 업무 위탁 관리 강화

가. 관련 법령 및 판단기준

콜센터 업무 등 개인정보 수집·이용 등의 처리를 제3자(수탁자)에게 위탁하거나 개인정보의 이용·제공 등 처리가 수반되는 업무를 수탁자에게 위탁하는 경우에는「개인정보 보호법」제26조 제1항에 의거 위탁업무 수행 목적외 개인정보의 처리 금지에 관한 사항, 개인정보의 기술적· 관리적 보호조치에 관한 사항 및 개인정보의 안전한 관리를 위한 사항 등을 위탁 계약 문서에 포함해야 한다[12]. 또한, 같은 법 제26조 제2항 및 제3항에 따라 위탁하는 업무의 내용과 수탁자를 인터넷 홈페이지 등을 통하여 공개해야 하며, 같은 법 제26조 제4항에 따라 수탁자에 대한 교육 등을 하여야 한다.

나. 감사결과 확인된 문제점

예비조사(8.31～9.15)에 앞서 실시한 사전점검(6.21～6.24)시 평가관리원은 정보시스템 운영 및 유지관리 업무를 위탁하는 케이씨씨정보통신(주) 및 주식회사 커뮤에 대해서만 "개인정보 처리 위탁업무" 대상으로 하여 "개인정보처리위탁 계약", 위탁하는 업무의 내용과 수탁자를 평가관리원 홈페이지를 통한 공개 및 수탁자에 대한 교육 등을 실시하고 있다. 하지만 R&D 상담센터 및 RCMS 고객센터 등 2개의 콜센터는

12) 개인정보보호위원회에서는 「개인정보 보호법」 제26조제1항에 따라 위탁 계약에 있어 개인정보 처리에 관하여 문서로 정하여야 하는 기본 사항인 "표준 개인정보처리위탁 계약서(안)" 제공중

"개인정보 처리 위탁업무" 대상으로 포함하고 있지 않음을 확인하였다.

이중, R&D 상담센터 관련해서는 "개인정보처리위탁 계약" 및 개인정보보호 교육 등 「개인정보 보호법」에서 정하는 업무를 수행하도록 현지시정하였다.

관계부서 의견

○○○○○팀 및 ◇◇◇□□팀에서는 감사결과를 전반적으로 수용하면서 콜센터에 대해서 "개인정보 처리 위탁업무" 관련 「개인정보 보호법」에서 제시하는 사항을 준수하겠다는 의견을 제시하겠다.

현지조치 사항

① ●○●○●○단(☆☆☆☆팀장)은 R&D상담센터 관련하여 개인정보처리위탁 계약 및 개인정보보호 교육 등 「개인정보 보호법」에서 정하는 업무를 실시하도록 조치하였다. **【현지시정】**

조치할 사항

① **◎◎◎◎◎단(○○○○○팀장)은** R&D 상담센터 및 RCMS 고객센터를 "개인정보 처리 위탁업무" 대상에 포함하여 주시고 관련 위탁하는 업무의 내용과 수탁자를 평가관리원 홈페이지에 공개하여 주시기 바랍니다. **【개선】**

② **◎◎◎◎◎단(◇◇◇□□팀)은** RCMS 고객센터 위탁 관련하여 수탁자와 “개인정보처리위탁” 계약 및 수탁자 대상 개인정보교육 등을 실시하여 주시기 바랍니다. **【통보】**

일련번호	9	감사자	★■○	공개(○), 비공개( )	
신분상 조치인원	-	재정상 조치방법	-	재정상 조치금액	-
수감부서 (처리할 부서)	◎◎◎◎◎단(○○○○○팀), ◎◎◎◎◎단(○○○◇◇팀)	처분요구일	2022.11.	회신 기한일	2023. 1. (통보일로부터 2개월)

개선 · 통보

제　　목　R&D정보서비스 가입시 개인정보 수집·이용 동의 절차 강화

소 관 부 서　◎◎◎◎◎단(○○○○○팀, ○○○◇◇팀)

조 치 부 서　◎◎◎◎◎단(○○○○○팀, ○○○◇◇팀)

내　　용

1. 업무 개요

평가관리원은 기관 안내, R&D사업 지원 및 정보 제공 등을 위하여 기관 홈페이지, 실시간통합연구비관리시스템인 RCMS, 산업기술 R&D 정보포털인 ITECH 등의 정보서비스를 제공하고 있으며 이러한 정보서비스는 「개인정보보호법」 및 평가관리원「개인정보보호침」에 근거하여 개인정보 보호를 하고 있다. 한편, 정보서비스 시스템 운영 총괄은 ○○○◇◇팀, 개인정보보호는 ○○○○○팀에서 담당하고 있다.

2. R&D정보서비스 가입시 개인정보 수집·이용 동의 절차 강화

가. 관련 법령 및 판단기준

평가관리원은 [표 11]과 같이 기관 홈페이지, 실시간통합연구비관리시스템인 RCMS, 산업기술 R&D정보포털인 ITECH 등의 정보서비스를 제공하고 있으며 이용자 편의를 위하여 일회의 가입 절차를 통하여 최대 7개 정보서비스를 이용할 수 있는 통합로그인 서비스를 제공하고 있다.

[표 11] 평가관리원 통합 정보서비스 대상 시스템

시스템명	홈페이지 주소
한국산업기술평가관리원 홈페이지(KEIT)	www.keit.re.kr
산업기술R&D정보포털(ITECH)	itech.keit.re.kr
실시간통합연구비관리시스템(RCMS)	www.rcms.go.kr
국가균형발전종합정보시스템(NABIS)	www.nabis.go.kr
소재부품장비정보포털(소부장넷)	www.sobujang.net
디지털기획시스템(ROME)	rome.keit..re.kr
디지털평가시스템(STELLA)	stella.keit.re.kr

정보서비스 회원 가입시 「개인정보보호법」 제22조(동의를 받는 방법)에 따라 정보주체의 동의를 받을 때에는 각각의 동의 사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고 각각 동의를 받아야 하며, 「개인정보 처리 방법에 관한 고시(개인정보보위원회)」에 따르면 동의 확인 문구에 대해서는 다른 내용보다 20퍼센트 이상 크게하여 알아보기 쉽게 하고 글씨의 색깔, 굵기 또는 밑줄 등을 통하여 그 내용이 명확히 표시되도록 하고 있다.

나. 감사결과 확인된 문제점

[그림 18]와 같이 평가관리원 정보서비스 통합로그인 화면에서는 다수의 정보서비스를 가입하고자 할 경우「개인정보보호법」 제22조에 의해 각각의 서비스에 대한 개인정보 수집·활용 동의를 받아야 하나 일괄 동의를 받고 있으며, 또한,「개인정보 처리 방법에 관한 고시」에 따라 일반 안내 문구와 차별성이 있도록 하여야 하나 일반 안내 문구와 동일한 수준에서 동의 화면을 구성하고 있어 개선이 필요하다.

관계부서 의견

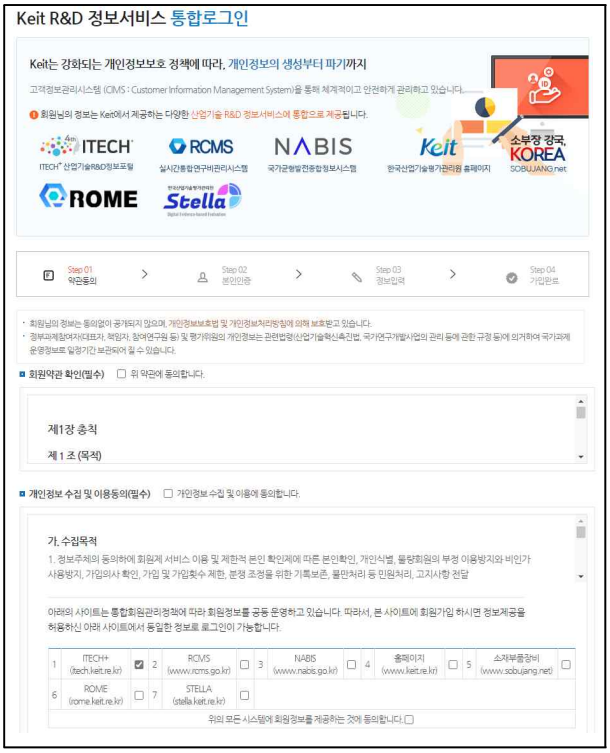
○○○○○팀 및 ○○○◇◇팀에서는 감사결과를 전반적으로 수용하면서 평가관리원 정보서비스 통합로그인 가입 절차를 개선하겠다는 의견을 제시하였다.

조치할 사항

① **◎◎◎◎◎단(○○○○○팀장)은** 평가관리원 통합정보서비스 가입 절차에 대해 「개인정보보호법」및「개인정보 처리 방법에 관한 고시」를 준용하는 기준을 마련하여 ○○○◇◇팀에 안내해 주시기 바랍니다. **【개선】**

② **◎◎◎◎◎단(○○○◇◇팀장)은** ○○○○○팀에서 송부한 기준을 준용하여 평가관리원 “통합로그인 서비스”에 반영하여 주시기 바랍니다. **【통보】**

[그림 18] 평가관리원 정보서비스 통합로그인 화면



일련번호	10	감사자	★■○, ○◎ (준감사인)	공개(○), 비공개( )	
신분상 조치인원	-	재정상 조치방법	-	재정상 조치금액	-
수감부서 (처리할 부서)	◎◎◎◎◎단(○○○○○팀), ●○●○●○단(☆☆☆☆팀)	처분요구일	2022.11.	회신 기한일	2023. 1. (통보일로부터 2개월)

개선 · 통보

제　　목 개인정보보호법에 따른 “개인정보 및 과세정보 제공활용 동의서” 서식 개정

소 관 부 서 ① ◎◎◎◎◎단(○○○○○팀)
② ●○●○●○단(☆☆☆☆팀)

조 치 부 서 ① ◎◎◎◎◎단(○○○○○팀)
② ●○●○●○단(☆☆☆☆팀)

내　　용

1. 업무 개요

평가관리원은 산업기술혁신촉진법 제11조(산업기술개발사업)에 의거하여 R&D사업을 지원하고 있으며 사업공고, 평가 및 사업관리 등은 ‘산업기술혁신사업 공통 운영요령’에 따라 수행하고 있다. R&D사업을 지원하는 과정에서 개인정보는 「개인정보보호법」 및 평가관리원 「개인정

보보호침」에 근거하여 개인정보를 보호하고 있다. 한편, R&D사업 총괄 업무는 ☆☆☆☆팀, 개인정보보호는 ○○○○○팀에서 담당하고 있다.

2. 개인정보보호법에 따른 “개인정보 및 과세정보 제공활용 동의서” 서식 개정

가. 관련 법령 및 판단기준

산업기술혁신사업 신규과제 공고 및 과제 접수시 [그림 19]와 같이 국가연구개발사업 참여제한 여부 확인 및 채무불이행 정보 관련 신용조회 등을 위한 산업기술혁신사업 표준서식인 “개인정보 및 과세정보 제공활용 동의서”(이하 “개인정보 동의서”라 한다)를 징구하고 있다. “개인정보 동의서” 징구시 「개인정보보호법」 제16조(개인정보의 수집 제한)에 따라 정보처리자는 목적에 필요한 최소한의 개인정보를 수집해야 하며, 같은 법 제24조의2(주민등록번호 처리의 제한)에 따라 주민등록번호 수집에 대해 엄격히 제한하고 있다. 또한 「개인정보 처리 방법에 관한 고시(개인정보보위원회)」에 따라 수집 동의 확인 문구에 대해서는 다른 내용보다 20퍼센트 이상 크게 하여 알아보기 쉽게 하고 글씨의 색깔, 굵기 또는 밑줄 등을 통하여 그 내용이 명확히 표시되도록 하고 있다.

나. 감사결과 확인된 문제점

산업기술혁신사업 신규과제 공고 및 과제 접수시 받고 있는 “개인정보 동의서”에 참여연구자 및 연구근접지원인력[13]에 대해 “소속기관“,

”성명“, ”주민등록번호“, ”국가연구자번호“ 등의 개인정보를 받고 있다.

그러나 개인정보보호법 제16조 및 제24조의2에 의거 주민등록번호 수집에 엄격히 제한이 있고 참여연구자등의 정보는 국가연구자번호[14]를 통해 확인할 수 있음에도 주민등록번호를 수집하고 있으며 「개인정보 처리 방법에 관한 고시」에 따라 동의 절차 확인 관련하여 일반 안내 문구와 차별성이 있는 화면 구성을 해야 하나 일반 안내 문구와 동일한 수준에서 동의 화면을 구성하고 있어 개선이 필요하다.

[그림 19] 개인정보 및 과세정보 제공 활용 동의서(일부)

개인정보 및 과세정보 제공활용동의서

세부사업명 내역사업명(해당 시 작성)		연구개발과제번호	
연구개발과제명			
주관연구개발기관명		연구책임자	
전체 연구개발기간			

국가연구개발사업에 참여하는 연구자의 개인정보 및 과세정보를 중요시하며, 「국가연구개발혁신법」 제19조, 제20조, 「개인정보보호법」 제15조, 제17조, 제22조 및 제24조, 「국세기본법」 제81조의13제1제7호에 따라 아래와 같이 동의를 얻고자 합니다.

아래 사항을 충분히 읽어 보신 후, 동의하시는 경우 서명하여 주시기 바랍니다.

※ 유의사항 : 귀하는 상기 동의를 거부할 수 있습니다. 그러나 해당 수집 항목은 국가연구개발사업 수행에 반드시 필요한 사항으로, 정보 제공 동의를 하지 않을 경우에는 국가연구개발사업 참여 등에 제한을 받으실 수 있습니다.

.....

13) 비영리기관 연구부서에 소속되어 해당 연구개발과제 수행을 지원하는 인력
14) 과학기술정보통신부에서 국가연구개발에 참여하는 연구자의 개인정보보호를 위하여 주민등록번호를 대신할 수 있는 번호로 범부처통합연구지원시스템 (http://www.itris.go.kr)에서 가입 가능

□ 참여연구자 정보

소속기관	성명	직위	주민등록번호[2]	국가연구자번호	국가연구개발사업 전체 인건비 계상률 (3백/5공)[3]	개인정보 및 과세정보 제공활용동의 (자필서명)
○○○[1]					90% (2/5)	

□ 연구근접지원인력

소속기관	성명	직위	주민등록번호[2]	국가연구자번호	국가연구개발사업 전체 인건비 계상률[3]	개인정보 및 과세정보 제공활용동의 (자필서명)
○○○[17]					100%	

개인정보의 제3자 제공에 대한 동의

□ 개인정보의 제3자 제공 목적

◦ 국가연구개발사업 참여제한 여부 확인 및 채무불이행 정보 등 신용조회
◦ 감사원 감사, 국정감사 시 과제수행현황(참여연구자)을 포함한 요구자료 제공
◦ 연구개발 사업 관련 타 전문기관의 동일업무 수행

□ 개인정보를 제공받는 자 : 과학기술정보통신부, 산업통상자원부 등 중앙행정기관, 국회, 감사원 등 정부기관, 한국연구재단, 한국산업기술평가관리원 등 「국가연구개발혁신법」 제2조제4호에 따른 전문기관, 연구개발비 관리 및 취급은행, 국가 R&D 기획, 평가관리 및 성과조사, 기술료 징수 등의 전문기관으로부터 업무의 일부를 위탁받아 수행하는 기관

□ 개인정보를 제공받는 자의 이용 목적

◦ 국가연구개발사업 참여의 적법적정성 판단
◦ 과제수행에 대한 적법·적정성 판단
◦ 과제 선정, 평가, 관리 업무의 수행

□ 제공하는 개인정보 항목

◦ 개인 성명(영문), 성별, 생년월일, 국가연구자번호, 소속기관, (자택, 직장) 주소, (사무실, 휴대폰) 전화번호, 전자우편 주소, 학력(학교, 전공, 학위, 연구개발분야 등), 경력, 특허/논문 실적, 국가연구개발사업 수행실적, 현재 수행 중인 국가연구개발사업 전체 인건비 계상률, 지급기준 정보(연봉, 월 수령기능금액 등), 연구개발비 지출을 위한 신용카드 및 금융거래내역, 채무불이행 정보 등 재무건전성 여부를 확인하기 위한 신용정보 등 인적사항, 전자세금계산서의 거래내역, 과세정보(연구개발비 지급 심사에 필요한 과세정보에 한함)

□ 개인정보를 제공받는자의 개인정보 보유·이용 기간 : 동의서가 작성된 시점부터 상기 개인정보 제3자 제공목적 달성 시까지

■ 개인정보의 제3자 제공에 대한 동의 여부 : **동의함 □ 동의하지 않음 □**

관계부서 의견

○○○○○팀 및 ☆☆☆☆팀에서는 감사결과를 전반적으로 수용하면서 "개인정보 동의서"를 개선하겠다는 의견을 제시하였다.

조치할 사항

① **◎◎◎◎◎단(○○○○○팀장)은** "개인정보 및 과세정보 제공활용 동의서"에 대해 「개인정보보호법」 및 「개인정보 처리 방법에 관한 고시」를 준용하는 기준을 마련하여 ☆☆☆☆팀에 안내해 주시기 바랍니다. **【개선】**

② **●○●○●○단(☆☆☆☆팀장)은** ○○○○○팀에서 송부하는 기준에 따라 "개인정보 및 과세정보 제공활용 동의서"를 보완해 주시기 바랍니다. **【통보】**

일련번호	11	감사자	★■○	공개(○), 비공개(　)	
신분상 조치인원	-	재정상 조치방법	-	재정상 조치금액	-
수감부서 (처리할 부서)	◎◎◎◎◎단(○○○○○팀)	처분요구일	-	회신 기한일	-

현지시정

제　　목　개인정보보호를 위한 암호키 관리 강화

소 관 부 서　◎◎◎◎◎단(○○○○○팀)

내　　용

1. 업무 개요

평가관리원은「개인정보 보호법」제23조(민간정보의 처리 제한), 제24조(고유식별정보의 처리제한)에 따라 R&D과제 수행자 등 고객정보에 대해여 고유식별정보[15], 비밀번호, 바이오 정보 등을 암호화하여 보관 및 이용 중에 있으며 이러한 개인정보보호 업무는 ○○○○○팀에서 수행하고 있다.

2. 개인정보보호를 위한 암호키 관리 강화

가. 관련 법령 및 판단기준

평가관리원은 암호화 개인정보 관리의 안전성 확보를 위해 안전한

15) 주민등록번호, 외국인등록번호, 운전면허등록번호, 여권번호 등

알고리즘 적용뿐만 아니라 체계적인 암호키[16] 관리를 하고 있으며, 암호키 생성, 이용, 보관, 배포 및 파기 등에 관한 관리 절차서[17]를 운용하고 있다. 이러한 "암호키 관리 절차서" 내용에는 개인정보보호위원회 「개인정보 안전성 확보 관련 지침」 및 고시 등을 반영해야 한다.

나. 감사결과 확인된 문제점

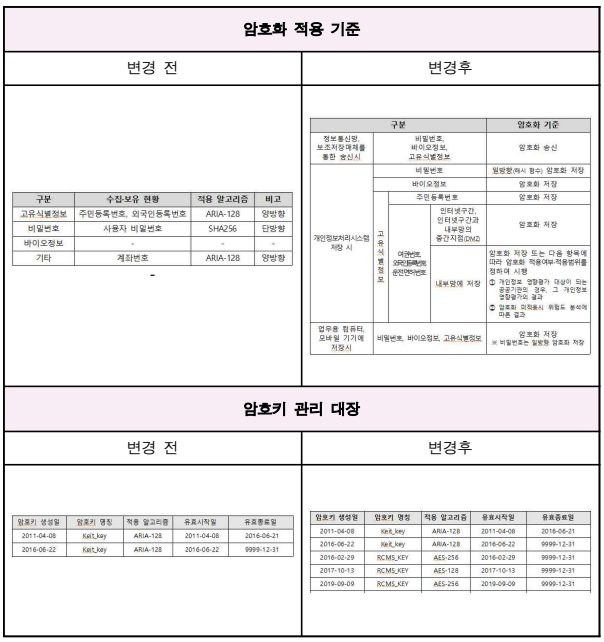
예비조사(8.31~9.15)에 앞서 실시한 사전점검(6.21~6.24)시 "암호키 관리 절차서"에는 개인정보보호위원회 "개인정보의 안전성 확보조치 기준"(고시 제2020-2호)에서 제시하는 개인정보처리자의 암호화 적용 기준이 누락되어 있었고 암호화 키 관리대장에는 2016.06.22. 이후 갱신내역(2건)이 없는 것으로 확인되어 현지시정을 통해 [그림 14]과 같이 암호화 적용기준[18] 제시 및 암호화 키 갱신 내역을 현행화 하도록 조치하였다.

현지조치 사항

◎◎◎◎◎단(○○○○○팀장)은 "암호키 관리 절차서"내 "개인정보의 안전성 확보조치 기준(개인정보보호위원회 고시)"에 의거 누락되어 있는 암호화 적용기준 및 암호화 키 갱신 내역 추가하도록 조치하였다. **【현지시정】**

16) 암호학적 변환(암호화, 복호화, 암호학적 검사 함수 계산, 서명 계산, 서명 검증 등)의 작동을 조절하는 기호의 열을 의미하며 간단히 문장 또는 수를 암호화, 복호화 하는 데 사용되는 값
17) 2016.12월 "암호키 관리 절차서" 제정하였으며 2018.06월 신규시스템 구축 등 변경사항 반영하여 개정
18) "정보통신망, 보조저장매체를 통한 송신시", "개인정보처리시스템 저장 시", "업무용 컴퓨터, 모바일 기기에 저장시"에 따른 암호화 기준 제시

[그림 14] “암호키 관리 절차서” 현행화 내역



암호화 적용 기준

변경 전

구분	수집·보유 현황	적용 알고리즘	비고
고유식별정보	주민등록번호, 외국인등록번호	ARIA-128	양방향
비밀번호	사용자 비밀번호	SHA256	단방향
바이오정보	-	-	-
기타	계좌번호	ARIA-128	양방향

-

변경후

구분			암호화 기준
정보통신망, 보조저장매체를 통한 송신시	비밀번호, 바이오정보, 고유식별정보		암호화 송신
개인정보처리시스템 저장 시	비밀번호		일방향(복호 필요) 암호화 저장
	바이오정보		암호화 저장
	고유식별정보	주민등록번호	암호화 저장
		여권번호, 운전면허번호, 외국인등록번호	인터넷구간, 인터넷구간과 내부망의 중간지점(DMZ) 암호화 저장
			내부망에 저장	암호화 저장 또는 다음 항목에 따라 암호화 적용여부·적용범위를 정하여 시행 ① 개인정보 영향평가 대상이 되는 공공기관의 경우, 그 개인정보 영향평가의 결과 ② 암호화 미적용시 위험도 분석에 따른 결과
업무용 컴퓨터, 모바일 기기에 저장시	비밀번호, 바이오정보, 고유식별정보		암호화 저장 ※ 비밀번호는 일방향 암호화 저장

암호키 관리 대장

변경 전

암호키 생성일	암호키 명칭	적용 알고리즘	유효시작일	유효종료일
2011-04-08	Kek_key	ARIA-128	2011-04-08	2016-06-21
2016-06-22	Kek_key	ARIA-128	2016-06-22	9999-12-31

변경후

암호키 생성일	암호키 명칭	적용 알고리즘	유효시작일	유효종료일
2011-04-08	Kek_key	ARIA-128	2011-04-08	2016-06-21
2016-06-22	Kek_key	ARIA-128	2016-06-22	9999-12-31
2016-02-29	RCMS_KEY	AES-256	2016-02-29	9999-12-31
2017-10-13	RCMS_KEY	AES-128	2017-10-13	9999-12-31
2019-09-09	RCMS_KEY	AES-256	2019-09-09	9999-12-31

일련번호	12	감사자	○▽○	공개(○), 비공개( )	
신분상 조치인원	-	재정상 조치방법	-	재정상 조치금액	-
수감부서 (처리할 부서)	◎◎◎◎◎단(◇◇◇□□팀)	처분요구일	2022. 11.	회신 기한일	-

모범사례 1

제 목 RCMS 연구개발비 불인정 안내 서비스 개발을 통한 오·유용 사전예방에 기여

관 계 부 서 ◎◎◎◎◎단(◇◇◇□□팀)

내 용

평가관리원은 실시간통합연구비관리시스템(이하 “RCMS”이라 한다)는 국가연구개발비의 투명한 사용·관리를 위해 2010년부터 구축하고 운영 중인 서비스이며, 정부출연금을 일괄로 지급하지 않고 RCMS를 통해서 건별 사용하는 구조로 연구비의 사용내역을 상시 모니터링 할 수 있는 정부 최초의 연구비 집행관리 서비스이다.

최근 국가연구개발혁신법을 통해 중소벤처기업부, 환경부, 해양수산부, 농진청, 방사청 등 범부처의 연구개발사업이 공동 이용하는 서비스로 지정되어 ‘22년 10월 현재 19개 R&D 전문기관의 연간 약 9조원의 연구개발비를 사용·관리하는 서비스로 성장하였다.

RCMS에서의 이체 규모는 연간 약 200만건이며, R&D 전문기관 과제 담당자에게 ‘16년부터 집행분석 모니터링 서비스[19]를 제공하고 있으나, 연구비 정산 결과를 보면 최근 2년간 정산이 완료된 약 35,193개 연구개발기관의 15.7%(5,542개 기관)가 사용내역에 대한 사후 연구개발비 사용 불인정을 경험하였으며 그 내용도 중복·과다집행(인건비, 연구수당 등), 부가세 미복원, 증빙자료 미비 순으로 나타났다. 이는 관리중심의 서비스에 한계가 있음을 보여주는 것이라 할 수 있으며, 집행분석 모니터링 결과를 연구개발기관에게 사전에 안내한다면 정산 불인정에 따른 추가적인 소명절차와 반납절차 등 불필요한 행정절차를 미연에 방지할 수 있다. 더구나 국가연구개발혁신법 시행으로 연차별 정산이 폐지됨에 따라 다년도 협약과제의 사후 불인정이 연구개발기관의 통상적인 회계 결산에도 부담될 소지가 있는 상황임을 고려할 때 수시 모니터링 및 사전 안내는 중요하다.

◇◇◇□□팀 ○☆● △■은 모니터링 서비스의 정확도와 적정성을 검증하기 위하여 위탁 회계법인의 자문과 사례 검토, 자체정산 매뉴얼, 국가연구개발혁신법의 매뉴얼을 참고하며 RCMS상의 불인정 유형을 세분화하였다.

아울러, 건강보험공단과 국세청의 행정정보를 연계하여 소속기관의 인건비 사용 적정성과 전자세금계산서의 유효성 검증을 강화하는 등

19) 개인사업자 거래빈도, 개발기간 대비 과다·과소집행, 연구개발기관과 연구비가 집행된 거래처의 주주명부, 소재지 비교, 연구개발기관의 휴·폐업 등 10여가지의 룰 패턴을 기초로 주단위로 이상 징후를 발생된 건에 대하여 R&D 전문기관 과제 담당자에게 안내하고 확인, 조치내역을 등록하는 서비스

연구개발기관에게 모니터링 서비스가 적정성 있는 데이터로 제공될 수 있도록 노력하였다.

2022년 5월부터 시범운영[20]한 결과 ‘과제 수행 초기에 미리 발견하여 최종정산 전 도움이 되었다’, ‘중복 지출된 연구개발비 항목을 발견하여 복원처리 가능하였다 ’ 등 긍정적인 의견이 있었으며 ‘22. 9월말까지 RCMS 복원금액 중 35%(약 98억원)가 모니터링 안내를 통해 처리되어 연구개발비의 부적정 사용을 사전 예방하는 효과를 거두었다

연구개발기관들의 오·유용 방지를 위한 새로운 시각과 방법을 도출하였으며 시범운영 결과를 토대로 범부처가 공동이용하는 RCMS의 서비스 질 제고와 연구비 사용 투명성 및 연구행정 효율성 향상이 기대된다.

조치할 사항

◎◎◎◎◎단(◇◇◇□□팀장)은 부적정한 연구개발비 사용에 대한 실시간 사전 안내로 연구비 오·유용 사전예방 및 연구행정 효율화에 기여한 ○☆● △■에게 타의 모범이 될 수 있도록 격려해주시기 바랍니다. **【모범사례】**

20) 기존 14개의 불인정 유형을 33개의 불인정 유형으로 세분화 하고, S/W적으로 자동 모니터링이 가능한 7개 항목(중복집행, 부가세 미복원, 연구개발기관간 거래, 장비 미등록 집행, 동일법인내 사업장간 거래, 인적물적 구분이 모호한 영리법인 거래 등)에 대해 시범적용.

감사결과 모범사례

소 속	직 급	성 명
◇◇◇□□팀	△■	○☆●
제목 : RCMS 불인정 안내로 연구비 오·유용 사전예방에 기여		
추 천 내 용		

□ RCMS 운영현황 및 예방도우미 서비스 추진배경

○ RCMS는 국가 연구개발 출연금의 투명한 사용·관리를 위해 이용건별 집행 개념을 적용하여 장기간 소요되는 R&D 과제수행 기간에도 집행내역과 관련 증빙자료를 손쉽게 모니터링이 가능

○ 연구개발혁신법('21.1월 시행)에 따라 범부처 공동이용 서비스로 지정, '22.10월 현재 9개 부처·지자체 19개 전문기관이 확대 이용 중*

* 4.3만개 연구개발기관이 RCMS를 통해 연간 약 9.2조원, 월 평균 6천억원 집행

○ 집행 패턴에 따라 집행분석 서비스가 운영되고 있으나, 정상거래와 담당자 미조치 내역이 많은 등 現 집행분석 서비스의 개선 필요성을 반증

□ 예방도우미 서비스 개선내용

○ 정산 매뉴얼 분석, 회계법인 자문회의, 연구수행자 설문조사를 통해 정산 불인정 유형구분을 14→33개 재정의 및 세부항목 별 증빙 구체화

○ 신규 패턴분석 기능을 DS(Detect Score, 감지점수)로 명명하고, 기존의 AS(연관)·BS(행동)·CS(신용) 분석과 알고리즘을 병합, 알람 대상*도 확대

* (기존)전문기관 담당자 → (변경)연구자·회계법인 알람을 제공

○ 연구개발혁신법 제19조를 근거로 행정데이터 연계 추진하여 불인정을 보다 손쉽고 정확하게 분석·판별(국세청 및 건강보험공단)

○ 연구개발기관이 별도 매뉴얼이 없이도 서비스를 이해하고 활용 할 수 있도록 단계별 활용 가이드와 처리절차를 정의·안내

* 불인정 탐지 시 관계규정 조항 및 사례집 링크 제공을 통해 자가진단 및 집행내역 수정

□ 파급효과 및 발전방안

○ 시범운영을 경험한 이용자의 반응은 긍정적이었으며 집행내역을 스스로 복원 또는 담당자 확인절차 진행('22.5.~'22.10., 복원금액/비율, 98억원/35%)

○ RCMS 고객센터 內 전담파트 신설 및 회계법인을 통한 원스톱 절차*마련

* 상황별 해석에 대한 혼선 최소화, 규정관련 문의를 회계법인·담당자 상담 후 일괄회신

최선의 오·유용 근절은 「사전예방」 ➔ 오·유용 사전감지(Detect) 강화
☞ 집행 시점에 불인정 요소를 안내, 연구자 스스로 자정 기회와 경각심 효과를 유도

일련번호	13	감사자	○▽○	공개(○), 비공개( )	
신분상 조치인원	-	재정상 조치방법	-	재정상 조치금액	-
수감부서 (처리할 부서)	◎◎◎◎◎단(○○○◇◇팀)	처분요구일	2022. 11.	회신 기한일	-

모범사례 2

제 목 자동화기술을 통한 업무처리방식 개선

관 계 부 서 ◎◎◎◎◎단(○○○◇◇팀)

내 용

평가관리원은 코로나19 감염병 발생과 확산으로 인한 디지털 전환(DX)이 활성화됨에 따라, 범정부 차원에서 디지털 최신 기술(빅데이터, 인공지능(AI), 클라우드 등)을 활용하여 스마트하게 업무를 수행하고 공공업무 효율성을 제고하기 위해 노력 하고 있다. 新정부에서도 디지털 혁신 정책을 국정과제[21]로 지정하여 공공기관의 일하는 방식 혁신 활동을 중점 추진 중이다.

한편 평가관리원 혁신성장 TF는 내부직원 및 대국민을 대상으로 혁신 아이디어 공모전을 개최('22.5)하였고, 이 때 '로봇과 함께 일하는 업무

21) 국정과제⑪ 모든 데이터가 연결되는 세계 최고의 디지털플랫폼 정부 구현

혁신 플랫폼 구축' 아이디어가 선정('22.7)된 바 있는데, ○○○◇◇팀에서는 선정된 아이디어를 구체화하여 실행하였다. 즉, 행정관리시스템에서 단순 반복적인 일은 SW 로봇이 대신하고, 직원은 보다 창의적이고 혁신적인 업무를 수행하도록 RPA[22]를 이용하여 일하는 방식의 혁신을 추진하였다. PoC[23]를 실시하여 RPA 기술의 적용 가능성을 확인하고, '22. 5. 19부터 ☆★☆★팀에 배치된 K봇[24]를 이용하여 정산금 및 기술료에 대한 입금 회계 처리 업무를 대행하도록 하였다. 이를 통해 연간 약 7백만원의 인건비 절감은 물론 자금처리 오류를 방지할 것으로 기대된다.

즉, 업무 담당자인 ○○○◇◇팀 ◎★◇ □■은 RPA 기술과 제품을 분석하여 평가관리원에 적합한 제품을 도입하고 업무 담당자와 협업을 통해 업무 절차를 상세화하는 등 K봇이 담당자를 대신하여 업무를 수행할 수 있도록 PoC를 성공적으로 추진하였다.

< 해당 업무 처리 프로세스 >



아울러 정산금 및 기술료에 대한 입금 회계 처리 업무외에 평가관리원의 업무에 확대 적용하기 위한 자동화 대상 업무 발굴을 위해 'RPA 아이디어 공모전'('22.8)을 개최하여 14건의 아이디어를 접수하고

22) RPA (Robotic Process Automation) : 정형화 / 반복 업무에 대해 지능형 로봇 프로세스를 활용해 자동화 하는 기술
23) PoC (Proof of Concept) : 새로운 프로젝트가 실제로 실현 가능성이 있는지, 효과와 효용, 기술적인 과점에서 검증을 하는 과정
24) K봇 : KEIT SW Robot

6건의 적용 업무를 도출하였으며, 업무 자동화 구축 사업을 통해 2023년 상반기까지 업무에 적용할 예정이다. 현재 추진계획을 마련하여 사업 수행자 선정을 위한 공고를 진행하고 있으며, 인프라 구축, 자동화 구현, 안정화 및 내재화 등의 추진과제로 구성되어 있다.

아울러 전 직원의 참여를 유도하기 위해 공모전을 추진하고, 심사과정에 KEIT 내부 혁신단을 참여시키는 등 사용자 관점에서 업무를 수행하여 사업 수행이 완료되면 정형화된 단순 반복적인 업무는 로봇이 수행하고, 직원은 보다 창의적이고 혁신적인 활동에 몰입 할 수 있는 업무환경 변화가 기대된다.

또한 데이터 기반 선진 경영 정보 체계 구축을 통한 일하는 방식 혁신을 위해 '자동기안 처리 확대를 통한 중복업무 최소화' 등 10개 핵심 추진과제를 발굴하여 '차세대 경영시스템 구축사업 추진계획'을 수립('22.9)하여 추진 중에 있는 등 '로봇과 함께 일하는 업무 혁신 플랫폼'을 평가관리원에 최초 적용하여 공공기관 업무 혁신의 선도기관으로 발돋움 할 수 있도록 토대를 마련하고 기여하였다.

조치할 사항

◎◎◎◎◎단(○○○◇◇팀장)은 행정 자동화 기술을 이용한 업무 시스템 개선을 통해 행정능률 향상에 기여한 ○○○◇◇팀 ◎★◇ □■에게 타의 모범이 될 수 있도록 격려해주시기 바랍니다. **【모범사례】**

감사결과 모범사례

소 속	직 급	성 명
○○○◇◇팀	□■	◎★◇

제목 : 자동화 기술을 통한 업무처리 방식 개선으로 업무경감 및 자금처리 오류 방지에 기여

추 천 내 용

□ RPA PoC를 통한 로봇과 함께 일하는 업무 환경 마련

○ 단순·반복적인 업무는 로봇을 활용하고, KEITian은 보다 창의적이고 혁신적인 활동에 몰입 가능한 효율적 업무 환경 마련을 위한 RPA 기술 도입

- (PoC 수행) 환수금 입금내역 회계처리 업무에 ☆★☆★팀 'K봇' 으로 자동 처리

* 로봇이 매일 10분간 업무 수행으로 해당 업무를 대체하고, 이를 통해 7백만원/년 절감

- (성과) 적용 가능 업무를 선정하여 RPA 로봇의 자동수행 가능성을 확인하고 연중 지속적인(365日*24H) 업무 수행으로 생산성 향상 기대

⇒ 로봇이 기안문을 생성하고 결재 상신하는 자동화 프로세스 최초 적용

□ 업무 효율화 효과가 높은 업무 발굴을 위한 공모전 개최

○ (추진내용) 심사위원회 개최하여 최종 실행 아이디어로 6개 내외 과제 선정

* RPA적용가능성, 기대효과 우수성, 사용자 및 빈도 및 의견수렴을 기준으로 정성 심사

○ (추진결과) 선정된 과제 구현 및 적용을 위한 IT용역 사업 추진

* 14건의 아이디어가 접수되어 6건의 우선 적용 업무 도출 (경영영역 3개, 사업영역 3개)

⇒ RPA 기술 전사 적용을 위한 전 직원 대상 아이디어 수집

□ 공모전 결과 선정된 아이디어의 실행을 위한 구축 사업 추진중

○ (인프라 구축) RPA 과제 구현을 위해 필요한 솔루션(관리·개발·수행도구) 탑재 및 구동을 위한 하드웨어·소프트웨어 구성

○ (업무 자동화 구현) RPA 공모전 결과 선정된 과제의 아이디어를 실행

* ①자금 입금내역의 수입 회계처리 업무 자동화 ②전결문서 대내 대외 발송 업무 자동화 ③정산 결과정리 업무 자동화 ④출장비 지급신청 절차 간소화 ⑤평가관리 안내통지 서비스

○ (RPA 안정화) RPA 과제의 안정적인 운영을 위한 과제별 실행 스케줄 최적화 및 오류 대응 절차 등 처리 방안 마련

⇒ 효율적으로 일하는 방식 개선으로 고부가가치 업무에 집중 할 수 있는 환경 조성