

대한지적공사

성과감사 결과보고서

감사기간 : 2013. 8. 20. ~ 8. 30. (9일간)

감사인원 : 4명

지적사항 : 별첨 참조

I. 감사개요

1. 감사목적

- 공사의 IT기술 및 자원의 효율적 활용 및 관리체계를 정립함으로써 한정된 자원을 효과적으로 사용하기 위한 방안을 수립하고, 단순지적이 아닌 제도에서부터 프로세스 개선까지 공사 IT 정보자원의 전반적 감사를 통해 잠재된 리스크를 도출하고 경제성, 능률성, 효과성을 검증하여 경영 효율을 개선하는데 그 목적이 있음.

2. 감사개요

- 감 사 기 간
 - 본 감 사 : 2013. 8. 20. ~ 8. 30.(9일간)
- 대 상 기 관 : 대한지적공사 본사
- 감 사 자 : 감사부장 외 3인
- 감 사 범 위 : 이번 감사는 공사 정보자원을 대상으로 하여 감사시점에서 운영되고 있는 제반 IT 정보시스템 관련 부문을 감사범위로 설정

3. 감사방법과 절차

- IT부문 전반을 대상으로 우선순위 평가결과 자산관리, 보안, 개발, 변경, 운용 등의 일반통제 및 대내외 서비스의 운영현황을 분석하여 효과성 향상을 위한 대안을 마련하는데 중점을 두었음.

II. 감사처분현황

감 사 실

개 선

제 목 IT 정보전략계획 및 정책 수립 체계 소홀
관 계 기 관 본사 ○○○○부
내 용

공사는 비전 2025 선포를 통해 전사 비전 및 목표 재정립과 주요 전략을 강도 높게 추진하고 있으며, 이러한 경영환경에 맞추어 ○○○○부에서도 정보보안 마스터 플랜 수립(2013.07) 등을 통하여 전사적인 정보전략계획을 적극적으로 고도화하고 있습니다.

더불어, ○○○○부에서 추진하는 정보전략계획은 공사의 경영전략과 연계하여 공사 정보화의 총체적 방향 제시가 필요하다는 명제 하에 경영활동의 전개에 필요한 종합적인 정보지원(관리) 체계를 정립하고 향후 중장기적인 공사 경영전략에 있어서 정보시스템의 역할을 정의해 나가야 합니다.

그리고, 정보전략계획을 수립하기 위해서는 공사내의 전략적 정보 요구를 식별하고, 비즈니스 활동과 이에 대한 자료 영역을 기술하며, 현행 정보지원의 수준을 평가하고, 정보시스템 개발을 위한 통합된 프레임워크를 제공하며, 이의 구현을 위한 통합 정보시스템 계획을 작성하는 체계적인 접근이 필요합니다.

또한, 정보전략계획은 공사가 목표하는 경영전략 등을 효과적으로 수행할 수 있도록 전사 IT 정보시스템과 연계하여 장기적인 비전과 목표를 제

공함으로써 미래 지향적이고 일관성 있는 정보시스템 구축을 지원하기 위해 정책을 수립하는 것이 타당합니다.

[대한지적공사 내부규정]

「경영전략 및 분석평가에 관한 규정」

제5조 (장기경영전략의 수립절차) ① 기획부서의 장은 장기경영전략을 수립하고자 할 때에는 그 수립지침을 작성하여 이를 각 주무부서의 장에게 통보하여야 한다.
② 각 주무부서의 장은 제1항에 따라 부문전략을 작성하여 이를 기획부서의 장에게 제출하여야 한다.

제10조 (중기경영계획의 수립) ① 기획부서의 장은 중기경영계획 수립지침을 작성하여 7월 31일까지 이를 각 주무부서의 장에게 통보하여야 한다.
② 각 주무부서의 장은 제1항의 지침에 따라 다음 연도를 포함한 5회계연도 이상의 소관 사업 또는 업무에 대한 부문별 경영계획을 설정하여 8월 31일까지 이를 기획부서의 장에게 제출하여야 한다.
③ 기획부서의 장은 제2항에 따라 각 주무부서의 장이 제출한 부문별 경영계획을 확정하여 이를 10월 31일까지 소관 정부 부처에 제출하고, 각 주무부서의 장에게 통보하여야 한다.
④ 각 주무부서의 장은 다음 연도 업무계획 수립 시 소관 경영목표를 달성하기 위한 세부추진계획을 같이 수립·추진하여야 한다.

[타기관 관련규정]

「○○○○부 정보화업무 처리규정」

제6조(중기 정보화계획의 수립) ① 정보화책임관은 ○○○○부 정보화의 효율적, 체계적 추진을 위하여 「국가정보화기본법」 제6조(국가정보화기본계획의 수립)에 의한 국가정보화기본계획을 고려하여 5년마다 안전행정부 중기 정보화계획(이하 "중기계획"이라 한다)을 수립한다.
② 정보화사업부서의 장은 정보화업무에 대한 중기사업계획 수립 시 제1항에 의한 중기계획을 참조하여야 한다.

「○○○○공사 전산업무규정」

제4조(기본계획의 수립) ① 전산주관부서의 장은 공사의 경영정보체제 구축과 사무자동화 등 종합적이고 체계적인 업무전산화 추진을 위하여 5년 단위로 전산업무 중장기기본계획(이하 "기본계획"이라 한다)을 수립하여야 한다.

②제1항의 기본계획에는 다음 각호의 사항이 포함되어야 한다.

제5조(연간계획의 수립) 전산주관부서의 장은 제4조의 전산업무 중장기 기본계획을 효율적으로 추진하기 위하여 전년도 12월말까지 연간업무계획(이하 "연간계획"이라 한다)을 수립하여야 한다.

제6조(세부 개발계획의 수립) ①전산주관부서의 장은 제5조의 규정에 의한 연간계획에 의거 개발대상 업무의 업무단위별 세부계획을 관계부서의 장과 협의하여 수립하여야 한다.

②제1항의 세부개발계획에는 다음 각호의 사항이 포함되어야 한다.

「○○○○○공사 정보화업무규정」

제16조(정보전략계획 수립) ① 정보화주관부서의 장은 종합적이고 체계적인 정보화 추진을 위하여 「경영관리규정」에 따른 중장기 전략경영계획과 연계된 정보전략계획을 5년마다 수립하여야 하며, 대·내외 환경을 고려하여 지속적으로 변화관리를 하여야 한다.

② 정보화주관부서의 장은 정보전략계획 수립 내용을 심의위원회의 회의에 부쳐야 하며, 정보전략계획 변경사항에 대해서는 조정위원회에 회의를 부치고 그 결과를 정보화총괄임원에게 보고하여야 한다.

제17조(연간정보화사업계획 수립) ① 정보화주관부서의 장은 다음 연도의 정보화사업계획 수립을 위한 지침을 작성하여 각 현업부서의 장에게 통보하여야 하며, 각 현업부서의 장은 소관분야의 정보화 사업계획을 작성하여 정보화주관부서의 장에게 제출하여야 한다.

② 정보화주관부서의 장은 각 현업부서의 장이 제출한 정보화 사업계획과 다음 연도 정보서비스 전략, 정보자원 운영방안 등을 연간정보화사업계획에 반영한 후 그 결과를 정보화총괄임원에게 보고하여야 한다.

제18조(실적평가) 정보화주관부서의 장은 필요하다고 판단되는 경우 정보화 추진실적을 평가하여 정보화총괄임원에게 보고하여야 하며, 정보전략계획 및 연간정보화사업계획 수립 시 반영하여야 한다.

그러나, 위 현황과 같이 타 공사의 경우 정보전략계획을 수립하는 규정과 정책을 마련하여 운영하는 반면, 공사의 정보전략계획 추진에 근간이 되는

규정에는 기본계획 수립, 연관계획 수립, 세부 개발 계획 수립 등의 구체적인 절차와 정책이 마련되어 있지 않습니다.

따라서, 공사 경영환경과 전사전략을 연계한 통합적인 정보전략계획 수립과 추진사항을 모니터링(평가)하는 체계 마련과 공사 경영목표 달성 극대화를 지원하는 정보전략계획을 체계적으로 수립할 수 있는 규정 마련이 필요합니다.

조치할 사항

○○○○부장은 공사 경영환경과 전사전략을 연계한 통합적인 정보 전략계획 수립과 추진사항을 모니터링(평가)할 수 있도록 정보전략계획 수립(추진) 규정 및 정책을 마련하시기 바랍니다.

감 사 실 권 고

제 목 IT 정보시스템 보안 관리 체계 개선
관 계 기 관 본사 ○○○○부
내 용

1. IT 정보시스템 보안 관리 인프라 개선

「전산자원 통합 운영관리지침(예규 제42호)」, 「대한지적공사 정보 보안업무지침(예규 제60호)」, 「개인정보 보호지침(예규 제67호)」에 의하여 ○○○○부는 전산자원의 효율적 관리 및 운영과 전산자원에 대한 절도, 파손, 침입에 대비한 예방조치를 강구하여야 하며, 정보유출이나 침입에 대비한 보안조치, 전산자원 운영관리자의 지정 등을 통하여 최선의 노력을 다하도록 규정하고 있습니다.

또한 「개인정보보호법」 제33조(개인정보영향평가) 및 「같은 법 시행령」 제35조(개인정보 영향평가 대상)에 따라 일정규모 이상의 개인정보 파일을 운영하는 경우 개인정보 영향평가를 의무적으로 수행하도록 하고 있습니다.

따라서, 「개인정보보호법」 및 「대한지적공사 정보보안업무지침」, 「개인정보 보호지침」에 의하여 ○○○○부에서는 정보유출에 의한 사회적 파장 및 공사의 이미지에 부정적인 영향을 끼칠 수 있는 위험을 사전에 예방하여야 합니다.

[정보보안 운영 점검 현황]

- 개인정보 침해요인이 있는 위험 요소 현황
 1. 개인정보보호 관리체계 침해요인: #개
 2. 바로처리시스템 개인정보보호 관리체계 침해요인: #개
 3. 개인정보 처리단계별 보고호치 침해요인: #개
- 침해요인을 개선하기 위한 개선방안 현황
 1. 개인정보보호 관리체계 침해요인 개선방안: #개
 2. 바로처리시스템 개인정보보호 관리체계 침해요인 개선방안: #개
 3. 개인정보 처리단계별 보호조치 침해요인 개선방안: #개

그러나, ○○○○부에서는 위 현황과 같이 식별된 침해요인의 개선을 위한 체계적이고 통합적인 로드맵 마련 등의 계획이 미흡한 것으로 나타났으며, 이러한 원인은 정보자산 보호를 위한 내부 인프라 부족과 주요 우선순위에 따른 업무관리가 미흡함으로 인하여 발생된 것으로 보여집니다.

2. 정보보안 지침 및 정책의 점검·평가 체계 구축 소홀

공사는 「국토해양부 정보보안업무규정」에 의거 정보보안업무에 필요한 세부사항을 규정하고자 「대한지적공사 정보보안업무지침」, 「개인정보 보호지침」에 의하여 ○○○○부는 전산자원의 효율적 관리 및 운영과 전산자원에 대한 절도, 파손, 침입에 대비한 예방조치를 강구하여야 하며, 정보유출이나 침입에 대비한 보안조치, 전산자원 운영관리자의 지정 등을 통하여 최선의 노력을 다하도록 규정하고 있습니다.

[정보보안 체계 진단 결과]

- 2013년도 외부 전문가로부터 보안관리 체계를 진단받은 결과를 보면, 아래와 같이 일부 미흡한 부분이 있어 개선이 필요한 것으로 분석되고 있습니다.
 1. 체계적인 정보보안 정책 미흡
 2. 정책을 구현하기 위한 세부 기준 및 절차가 미흡

그러나 위 현황과 같이 공사의 정보보안 정책 및 보안업무를 수행하는 지침이 내·외부 환경을 반영하여 신속하게 현행하는 체계적인 프로세스가 미흡하고, 보안전문가에 의해 상시적으로 급변하는 정보보안 트렌드를 반영하는 체계가 미흡한 것으로 진단되었습니다.

3. 정보보안 감사 운영 소홀

「개인정보보호법」이 개정되면서 공사가 수집한 다양한 개인정보에 대한 보호대책과 더불어 “정보감사”가 중요한 부분을 차지하고 있으며, 정보보안 측면에서의 정보감사란, 정보보호를 위한 다양한 활동 및 정책, 솔루션 등이 원활하게 운영되는지, 제대로 된 역할을 하고 있는지 등을 검증하는 행위라고 볼 수 있습니다. 즉, 「개인정보보호법」의 개정과 더불어 개인정보 유출에 대한 사전 예방적 활동의 중요성이 증가하고 있으므로, 공사 역시 자체적으로 예방체계를 고도화하고 단계별 로드맵에 의하여 점진적으로 정교화하는 과정이 필요합니다.

「대한지적공사 정보보안업무지침」

- 제10호(정보보안감사) ① 제4조에 따라 연1회 이상 자체 정보보안 감사를 실시하여야 한다
- ② 정보보안 감사의 주체는 정보보안담당관이 되며, 수감대상기관은 본사, 지적연수원, 공간정보연구원, 본부 및 지사가 된다.
 - ③ 정보통신에 대한 보안감사 실시계획과 감사결과를 다음 각 호의 기간 내에 장관에게 제출하여야 한다. 다만, 불시점검 결과는 심사분석에 포함하여야 한다.
 - 1. 해당 연도의 정보보안감사 실시계획 : 1.20까지
 - 2. 전년도 3분기부터 해당 연도 2분기까지의 정보보안감사 실시결과 : 7.25까지

그러나 「정보보안업무지침」 제10호(정보보안감사) 제①항에 따라 연1회 이상 자체 정보보안 감사를 실시하여야 하며, 정보통신에 대한 보안감

사 실시계획과 감사결과를 일정 기간 내에 장관에게 제출하여야 하는데도 감사일 현재 정보보안감사 실시계획과 점검 등이 소홀합니다.

4. 정보보안각서 및 서약서 징구 소홀

「정보보안업무지침」 제4조(정보보안담당관 운영) 제1항에 따라 공사의 효율적·체계적인 정보보안 업무를 수행하기 위하여 정보보안 업무지식을 보유한 인력을 확보하고 관련 전담조직을 구성·운영하여야 하며, 또한 제5항에 의해 정보보안담당관은 각급기관의 효율적인 정보보안의 업무를 수행하기 위하여 정보보안 관련 전문기술인력을 확보 및 양성하여야 하며, 신규직원에 대한 정보보안 교육·보안각서(별지 제4호 서식) 징구, 퇴직직원에 대한 정보보안서약서(별지 제5호 서식)를 징구 하여야 합니다.

더불어, 정보보안을 위하여 주관부서의 권한관리자와 운영자가 직원에 대한 권한부여 및 퇴직직원에 대해 권한을 회수하여야 하며, 주관부서의 권한관리자는 직무에 맞는 부서의 권한을 부여하고 직무가 변경된 경우에는 부여된 권한을 회수하여야 합니다. 또한, 정보 통제를 통해 정보유출에 의한 사회적 파장 및 공사의 이미지에 부정적인 영향을 끼칠 수 있는 사례를 사전에 예방하여야 합니다.

그리고, 정보보안을 위해서는 보안정책을 근거로 물리적 및 논리적인 접근통제가 적절하게 이루어져야 하며, 특히 정보가 유출될 경우 파급효과가 큰 정보에 대해서는 보안관리가 적절하게 운영되어야 합니다.

[정보보안각서 및 서약서 징구 현황]

(기간 : 2012. 1 . 1. ~ 현재)

구 분	대상인원	미 정 구	비 고
신규직원	78명	78명	보안각서
퇴직직원	51명	51명	보안서약서
계	129명	129명	

그런데도 위 현황과 같이 2012. 1. 1. ~ 감사일 현재까지 신규직원에 대한 정보보안 보안각서(별지 제4호 서식) 미징구(78명), 퇴직직원에 대한 정보보안서약서(별지 제5호 서식) 미징구(51명) 등으로 인하여 지적측량의 퇴인 정보 및 측량화일 등이 유출될 우려가 있으므로 보안체계를 개선할 필요가 있습니다.

5. 보안심사위원회 구성 및 운영 소홀

국토교통부 및 산하기관에서는 「국토교통부 보안업무 시행세칙」에 의거 보안업무에 관한 주요사항을 심의·조정하기 위하여 보안심사위원회를 구성하여 운영하고 있으며, 더불어 우리공사도 보안심사위원회의 역할을 「대한지적공사 정보보안업무지침」에 명시하고 있습니다.

[국토해양부 보안업무 시행세칙]

「보안업무 시행세칙」

제4조 (보안심사위원회) 보안업무에 관한 주요사항을 심의·조정하기 위하여 본부와 4급 이상의 기관장을 둔 소속기관 및 산하기관에 보안심사위원회(이하 “위원회”라 한다)를 둔다.

[공사 보안심사위원회 역할 및 기능]

「대한지적공사 정보보안업무지침」

제4조(정보보안담당관 운영) 제4항 제3호 보안심사위원회에 정보보안 분야 안건 심의 주관

제14조(정보보안 사고 조사 및 징계) 제2항 규정에 따른 관련자를 공사 보안심사위원회 또는 각급기관의 위원회에 징계 요청할 수 있다.

제30조(홈페이지 게시자료 보안관리) 제3항 홈페이지에 정보를 게시하고자 하는 부서의 장은 정보보안담당관과 협의하여 사전에 자체 보안심사위원회의 심사를 거쳐 비밀 등 비공개 자료가 게시되지 않도록 하여야 한다. 다만, 기존에 게시한 자료 내용중 단순하게 수치를 변경하는 경우나 경미한 사항은 그러하지 않을 수 있다.

제33조(업무망 보안관리) 제4항 업무망을 다른 기관의 망 및 인터넷과 연동하고자 할 경우에는 보안관리 책임한계를 설정하고 망 연동에 따른 보안대책을 마련하여 자체 보안 심사위원회 심의 후 장관을 경유하여 국가정보원장에게 보안성 검토를 의뢰하여야 한다.

제68조(보안성 검토 절차) 제1항 국토해양부 장관을 경유하여 국가정보원장에게 정보통신망 보안성 검토를 의뢰하는 업무 절차는 자체적으로 수립한 보안대책에 대하여 자체 보안심사위원회 심사를 거친 후 장관을 경유하여 국가정보원장에게 보안성 검토를 요청한다.

그러나, 공사 내부 지침에 보안심사위원회의 구성 및 기능(심의사항), 회의 및 의안의 제출 등에 대한 구체적인 사항이 명시되어 있지 않고, 운영 실적을 확인 할 수 없습니다. 따라서 위원회 구성과 운영 사항에 대한 지침 개정을 통해 적정한 보안심사위원회 운영과 보안업무에 대한 통제 절차를 강화할 필요가 있습니다.

조치할 사항

○○○○부장은 ① 보안업무 관리 체계의 침해요인의 위험 순위를 평가하여 즉시 개선하시기 바라며, 근본적인 문제점 해소와 정보보호 관리 체계 고도화를 위해 합리적인 인프라 도입 및 구축·운영을 권고합니다.

② 정보보안 관련 최신정보를 정기적으로 수집할 수 있는 프로세스를 마련하고, 그 결과(법·정책 등의 변경사항 등)를 공사 정보보안 정책에 반영할 수 있는 체계를 구축할 것을 권고합니다.

③ 정보보안의 사각지대를 없애고, 예방문화의 기반이 되는 정보보안감사(본사, 연구원, 연수원, 본부, 지사 대상)를 즉시 계획 수립 및 실시하시기 바라며, 향후 체계적인 운영과 관리가 이루어 질 수 있도록 내부 절차를 개선하시기 바랍니다.

④ 공사 신규직원과 퇴직직원에 대한 보안각서 및 정보보안서약서가 체계적으로 징구 될 수 있도록 징구 프로세스를 개선하시기 바랍니다.

⑤ 공사 내부 지침에 보안심사위원회의 구성 및 기능(심의사항), 회의 및 의안의 제출 등에 대한 구체적인 사항이 내부 지침에 명시되고 운영될 수 있도록 지침을 개정하시기 바랍니다.

감 사 실

개 선

제 목 개인정보 보호 관리 체계 개선
관 계 기 관 본사 ○○○○부
내 용

1. 개인정보 보호 교육 체계 강화

공사 개인정보 보호를 위한 교육 체계는 현재 온라인을 통한 교육과 직접 현장을 방문하여 교육하는 오프라인 교육 채널을 구축하고 운영되고 있습니다.(다만, 이-러닝은 ○○○○○에서 개발중)

먼저 본부 자체교육(12개 기관 3,305명)을 통하여 전사적인 의식 개선과 개인정보의 중요성에 대하여 교육을 실시하였으며, ○○○○○ 집합교육(9회 288명)을 대상으로 본사 ○○○○부 소속 정보보호전문가를 활용하여 전문교육을 실시하고 있습니다.

[개인정보 보호 교육 체계 현황]

- 「개인정보 보호법」 제28조 제2항(개인정보취급자의 정기적인 교육)에 따라 지적연수원 및 각 본부 집합교육 등을 통하여 개인정보 교육을 실시하고 있습니다. <○○○○부-77(2013.1.8.) 참조>
- 개인정보 보호 교육 추진현황
 - 개인정보보호 및 정보보안 이-러닝 교육(감사일 현재 개발중)
 - 본사 직원 참여(주관) 집합교육(1~2시간) : 135명
 - 각 본부별 집합교육(1~2시간) : 3,305명
 - 지적연수원 집합 교육(1~2시간) : 288명

위 현황과 같이 ○○○○부에서는 개인정보를 취급하는 내부직원들에 대한 교육을 상시적으로 온라인/오프라인을 통하여 지속적으로 실시하고는 있으나, 개인별 교육 실시 여부 및 교육 주기 그리고 담당업무(사무 및 역할 등)를 고려한 심화교육 계획 수립과 교육성과를 평가하는 피드백 절차가 마련되어 있지 않습니다.

2. 개인정보취급자 금지행위 지침 반영 소홀

「개인정보보호지침」 제3조(정의) 제7항에 따른 “개인정보취급자”란 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 직접 개인정보에 관한 업무를 담당하는 자와 그 밖에 업무상 필요에 의해 개인정보에 접근하여 처리하는 모든 자를 말한다. 라고 규정되어 있습니다.

「개인정보보호법」

제59조(금지행위) 개인정보를 처리하거나 처리하였던 자는 다음 각 호의 어느 하나에 해당하는 행위를 하여서는 아니된다.

1. 거짓이나 그 밖의 부정한 수단이나 방법으로 개인정보를 취득하거나 처리에 관한 동의를 받는 행위
2. 업무상 알게 된 개인정보를 누설하거나 권한 없이 다른 사람이 이용하도록 제공하는 행위
3. 정당한 권한 없이 또는 허용된 권한을 초과하여 다른 사람의 개인정보를 훼손, 멸실, 변경, 위조 또는 유출하는 행위. 라고 규정되어 있습니다.

[개인정보 보호법 개정 사항의 미반영 현황]

「개인정보보호지침」

- “개인정보 취급자”의 금지행위 : 공사 운영지침에 미 규정

그러나, 공사 「개인정보보호지침」 상의 “개인정보 취급자”의 금지행위에 대한 현행화가 미흡하여 개인정보의 수집·유출·오용·남용으로 인해 국민의 사생활의 비밀 등이 침해될 우려가 있습니다. 따라서, 「개인정보 보호법」 개정에 맞춰 “개인정보 취급자”의 금지행위를 구체적으로 마련하는 등 「개인정보보호지침」에 대한 개정이 필요합니다.

3. 개인정보 보호 인증제도 도입 철저

공사는 최적화된 정보보호 관리체계 구축을 통해 보유하고 있는 다양한 정보(개인정보 포함)를 보호하기 위해서 「대한지적공사 정보보안업무지침」 및 「개인정보 보호지침」을 마련하여 운영하고 있습니다.

또한 공사 외적인 정보보호 여건 및 규정 등은 상시적으로 강화되고 있으며, 이러한 지침들의 기반이 되는 법령들도 지속적으로 강화되는 추세입니다.

[개인정보 관련 언론보도]

○○○○ 2013.4.12.자 보도(개인정보유출 신고기준 강화법 발의) : “개인정보 보호법에 ‘1만 명 이상’의 개인정보가 유출됐을 때 관계기관에 신고해야 하는 범위를 정보통신망법과 같은 1건 이상하게 해서 사업자들의 혼란을 방지하고, 개인정보보호 의무를 강화

○○○○ 2013.7.30.자 보도(정부, 주민번호 유출 기업·기관 대표자 해임 권고) : 정부가 내년 8월부터 주민등록번호 유출기업과 기관에 최대 5억원의 과징금을 부과하고 대표자(CEO) 해임을 권고한다. 안전행정부는 30일 이런 내용을 골자로 한 개인정보보호법 개정안을 다음 달 초 공포하고 내년 8월부터 시행한다고 밝혔다.

[개인정보 침해 위험 요소 현황]

- 파견근로자와 같은 외부직원이 개인정보를 처리하는 경우 보안각서 미징구 등과 같은 법령준수 미흡: #건
 - 사전대비공격 프로그램 및 개인정보취급자의 개인정보를 통해 패스워드를 유추하여 비인가자 접근할 수 위험을 예방하는 가이드라인 미준수 등과 같은 지적사항: #건
- ※ 대한지적공사 개인정보영향평가 보고서('13.7.10) 참조

그러나, 위 현황과 같이 2013년도 외부기관의 공사 정보보호 체계 평가를 분석하여 보면, 정보보호를 위해 일부 개선이 필요한 사항이 있는 것을 확인할 수 있으며, 위 현황 같은 법률 미준수 사항과 개인정보 보호 가이드라인 미준수 사항들을 신속하게 개선하고 개선(교정)된 사항에 대하여 다양한 채널을 통해 재평가 하는 것이 타당합니다.

더불어 개선 시 최적화된 정보보호관리 체계 모델 수립을 통해 개선을 추진하는 노력이 필요하며, 이러한 노력의 성과는 정보보호 인증제도 (GISMS 등)를 통해 대외적인 성과를 평가 받고 인증(보증)되어야 함으로 정보보호 인증제도 도입을 위한 인프라 조성 및 기반 구축을 단계별로 로드맵을 마련하여 추진할 필요가 있습니다.

조치할 사항

○○○○부장은 ① 개인정보 보호를 위하여 추진되고 있는 다양한 프로그램 활용에 대한 체계적인 점검·평가 실시와 향후 개인별 역량과 주요 업무를 반영한 교육체계가 구축되도록 개인정보 보호 교육 프로세스 개선하시기 바랍니다.

② 「개인정보보호지침」 규정의 현행화가 미흡하여 개인정보의 수집·유출·오용·남용으로 인해 국민의 사생활의 비밀 등이 침해될 우려가 있으므로 지침 개정을 통해 금지행위 정책을 마련하시기 바랍니다.

③ 공사 정보가 적정하게 관리 및 보호된다는 것을 보증할 수 있도록 정보보호 인증제도(GISMS 등) 등과 같은 평가 체계를 마련하시기 바랍니다.

감 사 실

권 고

제 목 IT 정보시스템 이전 준비 철저

관 계 기 관 본사 ○○○○부

내 용

1. 이전 장비(소프트웨어 포함) 분류 및 평가 철저

정부는 공공기관의 수도권 집중을 억제하고 지역의 특성있는 발전을 위하여 「국가균형발전특별법」 제18조 및 같은 법시행령 제15조에 따라 수도권에 소재하고 있는 공공기관의 지방이전 정책 추진하고 있습니다. 이에 따라 우리공사도 재원조달방안을 고려하여 본사사옥신축 및 IT 시설 이전 등을 안정적으로 추진하려고 노력하고 있습니다.

또한, 정부 정책에 따른 본사 전산 장비실 현행 정보자원의 원활한 전주 사옥이전 수행을 위해 정보시스템 운영컨설팅(2013.7.10. 완료)을 실시하여 하는 등 최선의 노력을 다하고 있습니다.

그리고, IT 정보시스템 이전을 위한 이전대상 장비 조사 및 이전환경 설계를 위한 하드웨어, 스토리지, 네트워크, 회선, 소프트웨어 등 이전대상 장비를 사전 조사하고 구성내역을 분석하였으며, 시스템의 안정적인 운영 관리를 위하여 재해복구 프로세스를 포함한 전략계획을 수립하였습니다.

[재분류 권고 장비 현황]

구분	장비명	수량	적요
----	-----	----	----

네트워크 장비	백본스위치 A 외	6	재활용 또는 폐기 권고
보안장비	KLIS 방화벽 외	4	재활용 또는 폐기 권고

그러나, 위 현황과 같이 정보자원 현황을 분석한 자료를 보면, 기존 장비 중 통합 서버로의 자원 재배치에 따라 기존 랙에 배치된 서버는 재활용 또는 폐기 장비로 재분류를 권고한 장비 등이 있어, 이전 장비에 대한 전체적인 목록을 작성하고 상태 등을 표시함으로서 정보자원에 대한 효율적인 관리와 연차별 장비구입 계획 등에 반영할 필요가 있습니다.

더불어, 외부기관에 의하여 평가된 정보자원에 대하여 내부 (재)평가 등을 통해 이전 대상 장비를 확정하고 관리함으로서 이중 구입 및 불필요한 이전·활용에 따른 예산 낭비 등을 사전에 예방할 필요가 있습니다.

2. 이전 장비(소프트웨어 포함) 응급(위기)사항 대응 체계 구축 철저

IT 정보시스템의 안정적 이전 및 이전환경 설계를 위한 하드웨어, 스토리지, 네트워크, 회선, 소프트웨어 등 이전대상 장비를 사전 조사하고 구성내역을 분석하였습니다.

[이전 장비(소프트웨어 포함) 분류 미작성 현황]

- 이전 대상 장비(소프트웨어 포함) 상세목록 미작성
- 정보자원(H/W, S/W 포함)에 대하여 비상상황을 지원하는 비상연락망 등 대응 체계 미작성

그러나, 이전 전산자원 대부분 동일한 업체나 엔지니어에 의하여 관리되고 있지 않고 있어, 이전 후 개별 시스템 운영을 위해서는 개별 장비 및 시스템(배치작업 등 포함)에 대한 비상상황 발생 시 즉시 대응(조치) 할

수 있는 채널(기관·담당자 이름, 전화번호 등)을 마련할 필요가 있습니다.

조치할 사항

○○○○부장은 ① 이전 대상 장비를 구체적으로 확정하고 목록표를 작성·관리함으로써 이중 구입 등의 예산 낭비가 발생하지 않도록 이전 대상 IT 전산자원에 대한 (재)평가 등을 권고합니다.

② 전산자원에 대한 비상상황 발생 시 즉시 대응(조치) 할 수 있는 채널(기관·담당자 이름, 전화번호 등)을 파악할 수 있도록 상시적인 응급(위기) 사항 대응 체계 구축을 권고합니다.