대한지적공사

성과감사 결과보고서

❑ 감사기간 : 2014. 6. 30. ~ 7. 11.(10일간)

❑ 감사인원 : 6명

❑ 지적사항 : 7건 (통보 1, 개선 2, 권고 4)

대한지적공사

Ⅰ. 감사개요

1. 감사목적

□ 이번 감사는 공사에서 보관하고 있는 개인정보 관리 및 관련 인프라의 통제환경 진단을 통하여 내·외부의 환경변화에 적기에 대응하며 Risk를 최소화 할 수 있는 내부통제체계를 완성하기 위하여 보안 분야(IT 기반의 정보보안시스템) 진단을 위한 성과감사를 실시하였음.

2. 감사개요

□ 감 사 기 간

○ 본 감 사 : 2014. 6. 30. ~ 7. 11.(10일간)

□ 대 상 기 관 : 대한지적공사

□ 감 사 자 : 감사부장 외 5인

□ 감 사 범 위 : 본사 정보운영부 등 총 4개 부서에 대하여 보안(IT 기반의 정보보안 포함)과 관련한 업무 전반

3. 중점점검사항

□ 이번 감사는 공사가 현재 사용하고 있는 정보보안시스템 및 관련 Infra에 잠재된 위험을 식별하고, 개선안을 제시함으로써 정보시스템 부문의 통제환경 향상을 목표로 성과감사 진행 특히, 개인정보 관련 공사의 관리체계 및 사후관리에 초점을 맞춰 진행하였으며, 경영 환경을 개선하는데 노력

Ⅱ. 감사처분현황

감 사 실

개 선

제 목 보안업무 관련 지침 개선

관 계 기 관 본사 ○○○○부

내 용

공사에서는 보안업무(IT 기반의 정보보안 포함)의 적정한 운영과 업무수행에 필요한 구체적인 절차를 규정하고자 보안업무지침(예규 제58호)과 정보보안업무지침(예규 제60호)을 운영하고 있으며, 보안업무규정(대통령령) 및 동 시행규칙(대통령훈령), 국토교통부 보안업무시행세칙, 국토교통부 정보보안업무규정 등에 의거하여 공사 지침으로 제·개정되었다.

그러나 정부에서 규정한 보안업무규정(대통령령 2008. 12. 31. 개정)의 주 내용은 “비밀보호”, “신원조사”, “시설 또는 지역 등에 대한 보안조사” 등에 대한 관련 조항으로 구성되어 있는 반면 공사의 보안업무지침은 정보보안과 관련한 유사 조문들이 명시되어 있는 것을 확인 할 수 있다. 또한 보안교육 및 점검 활동 등은 정보보안업무지침과 중복되어 있어 행정력 낭비가 우려되므로 통합적인 보안 교육과 점검 활동이 필요하다.

<(표1) 보안업무지침 중복 및 유사 규정 현황>

보안업무지침(예규 제58호)	정보보안업무지침(예규 제60호)
제3조 보안심사위원회 설치 및 운영	제4조 제4항 3호 보안심사위원회 주관
제9조 사이버보안 진단의 날 시행	제12조 사이버보안 진단의 날
제43조 청년인턴 보안서약서 징구	제4조 신규직원 정보보안각서 및 퇴직직원 보안서약서 징구

	제16조 중요정보 취급자 보안서약서 징구 제40조 유지보수 인력 보안서약서 징구 제53조 원격근무자 보안서약서 징구
제44조 용역업체에 대한 보안대책	제51조 용역사업 보안관리
제45조 보안교육	제11조 정보보안교육
제47조 보안감사의 실시	제10조 정보보안 감사
제49조 보안성 검토	제19조 보안성 검토

그리고『보안업무지침』제3조에 따른 보안심의위원회의 경우『정보보안업무지침』에서 명시한 보안심의위원회와 명칭이 일치하고 있어 운영에 혼란을 초래할 수 있다. 따라서 보안심사위원회를 통합하고 기능에 맞는 분과를 설치하여 전문성을 확보할 필요가 있으며, 특히 보안성검토가 필요한 업무를 구체적으로 명시하고 절차를 명확히 정립하여 운영하는 것이 타당하다.

조치할 사항

○○○○○**장은** 『보안업무지침』과『정보보안업무지침』의 조문을 재검토하여 역할이 중복되는 사항은 통합하고 혼란을 초래할 수 있는 기능은 구체적으로 명시될 수 있도록 관련지침을 개정하시기 바랍니다.

감 사 실

개 선

제 목 홈페이지 정보공개 보안지침 개선

관 계 기 관 본사 ○○○○부, ○○부

내 용

최근 사이버 공격은 주로 웹 사이트를 공격하는 경우가 대부분이며, 개인정보가 유출된 트위터, 은행, 카드 등이 대표적인 사례이다. 이 외에도 미국 CIA나 국무성 등 주요 정부기관의 홈페이지도 해킹 공격을 당한 사례가 있는 등 웹 사이트(홈페이지)에 대한 정보보호 중요성이 커지고 있으며, 홈페이지는 기관의 단순한 홍보매체가 아닌 사이버 행정업무 및 민원업무의 주요 수단으로 자리매김하고 있어 홈페이지 시스템 관리자에 대한 정보보호 인식제고 및 보안관리 교육과 홈페이지 취약성에 대한 주기적인 평가가 필요하다.

그리고 이러한 홈페이지가 고객의 정보나 문서, 자료들이 무단게재 되어 기관의 이미지 손실은 물론이고 공사 신뢰도 또한 타격을 입게 됨으로 지속적인 보안 점검을 필요로 한다.

언론 및 외부 전문가들의 의견에 따르면 대부분 홈페이지를 통한 정보유출은 시스템 개발 또는 운영 중에 보안 사항을 소홀히 한 것에서 비롯되고 있으며, 많은 개발자가 보안관련 중요도 인식과 전문성이 부족하여 보안을 고려한 코딩을 하지 못하고 있는 데다, 홈페이지 운영자 또한 콘텐츠 관리 등 서비스에만 치중하고 보안 전문성 및 시간부족으로 보안취약점에 대한 대책을 즉시 강구하지 않음으로 인하여 발생되고 있는 겻으로 평가하고

있다.

따라서 이러한 취약점을 개선하기 위해서는 홈페이지 운영 및 관리, 게시자료 관리, 개인정보보호, 비밀번호 관리 등을 적극적으로 수행함으로써 사고가 발생하지 않도록 노력함은 물론이고 공사『정보보안지침』제30조에 따라 홈페이지 정보공개 보안지침을 수립하여야 하나, “홈페이지 정보보안 보안지침”을 미 수립하고 있다.

조치할 사항

○○○○○**장,** ○○○**장은** 기존 운영 중인 웹 사이트(홈페이지) 보안취약점에 대해 사전 점검을 실시함으로써 보안취약점을 미리 제거해 웹 서비스의 안전성 및 신뢰성을 확보하시기 바라며,『정보보안지침』제30조에 따라 홈페이지 정보공개 보안지침을 마련하시기 바랍니다.

감 사 실

권 고

제 목 비밀인가 취급 및 발급 등의 기록·관리 방법 강화 권고

관 계 기 관 본사 ○○○○실

내 용

공사에서는 『보안업무지침』제14조 내지 15조에 의거 비밀취급인가를 받은 자가 면직, 휴직, 전보, 직위해제 등을 당하였을 때에는 그 발령일자와 동시에 비밀취급인가가 해제 된 것으로 보며, 비밀취급인가증의 회수 등 필요한 조치를 취해야 한다.

또한, 비밀취급인가를 받은 자에게 비밀취급인가증(별지 제6호 서식, 이하 “인가증”이라 한다) 을 발급할 때에는 발급대장에 이를 기록하여야 하며, 인가증을 분실, 멸실 또는 훼손하였을 때에는 비밀취급인가 신청권자가 재발급 요청을 하여야 한다. 더불어 인가증을 재발급 하였을 때에는 발급대장의 비고란에 재발급일자와 재발급 사유를 명시하여야 한다.

그리고 비밀취급인가를 받은 자가 인가가 해제되었을 때에는 비밀취급인가 신청권자는 지체 없이 인가증을 회수하여 보안담당관에게 반납하여야 하며, 보안담당관은 인가증을 파기하고 그 사실을 발급대장에 기록하여야 한다.

그러나 비밀취급인가(해제) 및 비밀취급인가증 발급 등을 수기로 관리하고 있어 지역을 달리한 인사이동이나 보직 변경 등의 사유로 비밀취급인가 사항에 변동이 발생하는 경우 변경이력 사항의 기록이 누락되거나 비밀취급인가증이 발급되었으나 그 발급사항에 대한 관리가 소홀할 수 있는 우려가

있다.

따라서 전사적자원관리시스템(ERP)등과 같은 전자적인 방법으로 비밀취급인가 현황과 발급사항을 관리함으로서 업무의 효율성과 보안관리의 완전성을 확보하는 것이 타당하다.

조치할 사항

○○○○○**장은** 공사『보안업무지침』제14조 내지 15조에 따라 비밀취급인가(해제) 및 비밀취급인가증 발급 등의 보안정보를 전자적인 형태로 관리함으로서 업무의 효율성과 보안관리의 완전성을 확보하시기 바랍니다.

감 사 실

통 보

제 목 **정보보안 교육 운영 프로세스 강화**

관 계 기 관 본사 ○○○○부

내 용

『정보보안업무지침』제11조 (정보보안교육)에 따라 정보보안 교육계획을 수립하여 연 1회 이상 전 직원을 대상으로 관련 교육을 실시하여야 하며, 정보보안 교육의 효율성 제고를 위하여 자체 실정에 맞는 정보보안 교안을 작성 활용하여야 한다. 더불어 필요시 장관에게 전문 인력 및 자료 지원을 요청할 수 있다.

또한 개인정보보호법이 개정되면서 공사가 수집한 다양한 개인정보에 대한 보호대책과 더불어 “정보보안교육”이 중요한 부분을 차지하고 있다. 따라서 정보운영부에서는 정보보안교육을 전반에 대한 추진 계획 수립하여, 비밀 생산 및 관리, 보안업무 수행 시 지켜야할 절차와 직원의 보안의식 제고를 위한 규정 교육을 체계적이고 효율적으로 정보보안교육 활동을 함으로써 각종정보보안 사고를 예방하고, 사이버공격에도 대응하여야 한다. 즉, 정보보안교육이 개인정보보호법의 제정과 더불어 개인정보 유출에 대한 사전체계를 고도화하고 단계별 로드맵에 의하여 점진적으로 정교화하는 과정이 필요하다.

그런데도, 정보보안의 사각지대를 없애고 예방문화의 기반이 되는 2014년도 전 직원 정보보안교육 실시 계획이 수립되지 않는 등 체계적인 운영 및 관리가 소홀하다.

따라서 정보보안 교육에 관한 전사적인 관심 증진과 내.환경 변화에 따른 보안환경 변화를 반영한 교육 계획 수립 및 기 수립된 계획에 대해서는 피드백을 통해 실질적인 교육이 진행 될 수 있도록 교육 운영 프로세스를 강화할 필요가 있다.

조치할 사항

○○○○○**장은** 정보보안교육 계획을 수립하시기 바라며, 정보보안교육 운영 결과에 대한 피드백을 통해 실질적인 교육이 진행 될 수 있도록 교육 운영 프로세스를 강화하시기 바랍니다.

감 사 실

권 고

제 목 정보보안 감사 계획 및 점검 절차 강화 권고

관 계 기 관 본사 ○○○○부

내 용

공사에서는 『대한지적공사 정보보안업무지침』제10조(정보보안감사) 제1항에 따라 연1회 이상 자체 정보보안 감사를 실시하여야 하며, 정보보안 감사의 주체는 정보보안담당관이 되고, 수감대상기관은 본사, 지적연수원, 공간정보연구원, 본부 및 지사가 된다.

또한 『같은 지침』제10조(정보보안감사) 제3항에 따라 정보통신에 대한 보안감사 실시계획과 감사결과를 장관에게 제출하여야 한다. 그리고 해당 연도의 정보보안 감사 실시계획은 1.20.까지, 전년도 3분기부터 해당 연도 2분기까지의 정보보안감사 실시결과는 7.25.까지 제출하여야 한다.

더불어 개인정보보호법이 개정되면서 공사가 수집한 다양한 개인정보에 대한 보호대책과 “정보감사”의 중요성이 지속적으로 커지고 있다. 그러므로 정보보안 측면에서의 정보감사란 정보보호를 위한 다양한 활동 및 정책, 솔루션 등이 원활하게 운영되는지, 제대로 된 역할을 하고 있는지 검증하는 절차입니다. 따라서 개인정보보호법의 제정과 더불어 개인정보 누출에 대한 사전체계를 고도화하고 단계별 로드맵에 의하여 점진적으로 정교화하는 체계가 필요하다.

그런데도 정보보안의 사각지대를 없애고, 예방문화의 기반이 되는 정보보안감사(본사, 연구원, 연수원, 본부, 지사 대상) 계획이 감사일 현재 수

립되지 않는 등 체계적인 운영과 관리가 부족한 것으로 나타나고 있다.

조치할 사항

○○○○○**장은** 정보보안감사 계획을 수립하시기 바라며, 정보보안감사 결과에 대한 피드백을 통해 정보보안의 완전성을 확보할 수 있도록 운영 프로세스를 강화하시기 바랍니다.

감 사 실

권 고

제 목 **업무시스템 변경에 따른 보안적용 확인 절차 강화 권고**

관 계 기 관 본사 ○○○○부

내 용

공사에서는 전자문서의 암호화 및 워터마킹 그리고 출력정보 표시가 가능한 보안시스템을 구축하여 무단유출을 차단하고 이력관리가 가능하도록 DRM시스템을 도입하였다.

<(표2) 업무용시스템 DRM 미적용 현황>

구분	점검 내용	적요
전사적자원관리시스템 (ERP)	자료를 조회한 후 출력 메뉴에서 PDF로 저장하는 경우	보안 미적용
업무지원시스템 (COS)	측량접수(처리) 현황을 조회한 후 엑셀로 바로 저장하는 경우	보안 미적용
현장지원시스템 (MOS)	측량화일(GDB 등)을 추출하여 저장하는 경우	보안 미적용
고객관계관리시스템 (CRM)	민원처리 현황을 조회한 후 엑셀로 저장하는 경우	보안 미적용

그러나 위 현황 같이 현장지원시스템(MOS)에 등록된 측량 파일의 경우 사용자가 지적측량 후속업무 및 민원업무를 위하여 다운로드 받는 경우와 전사적자원관리시스템(ERP)에서 추출한 자료(보고서 형태의 자료)를 PDF 파일 형태로 다운로드 받는 경우 등에는 보안이 미적용 되고 있어 추출된 정보가 외부에 유출될 우려가 있는 등 전반적인 보안 적용에 대한 정책 수립

및 보안이 적용되고 있는 시스템에 대한 확인이 필요하다.

더불어 공사 업무용시스템에 DRM시스템이 적용되어 최상의 보안수준을 유지하고 있다 하더라도 업무용시스템(ERP, COS, MOS, CRM 등)의 업그레이드 및 시스템 변경 등의 사유가 발생되는 경우 당연히 변경된 업무용시스템에 보안적용의 이상유무를 확인하여야 하나 보안적용 여부를 확인하는 절차가 미흡하였다.

조치할 사항

○○○○○**장은** 공사가 수립한 정보보안 정책을 주기적으로 점검함으로써 업무시스템의 변경 등으로 인해 보안을 우회 할 수 있는 위험이 발생되지 않도록 업무에 철저를 기하여 주시기 바라며, 업무시스템 변경 시 보안적용을 반드시 점검하는 절차를 마련하여 보안적용을 강화하시기 바랍니다.

감 사 실

권 고

제 목 **전산실 접근 통제 강화 권고**

관 계 기 관 본사 ○○○○부

내 용

공사의 정보자산을 관리하는 전산실은 중요 정보통신시설 및 장소로 분류되어야 하며, 보호구역으로 설정 관리되어야 한다. 따라서 『대한지적공사 정보보안업무지침』제18조에 의거 보호구역은 ① 방재대책 및 외부로부터의 위해 방지대책 강구, ② 상시 이용하는 출입문은 한곳으로 정하고 이중 잠금장치 설치, ③ 출입자 인증·식별 등을 위한 출입문 보안장치 설치 및 주야간 감시대책 수립, ④ 정보시스템 안전지출 및 긴급파기 계획 등을 수립하여 한다.

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

그러나 중요 정보자산이 있는 전산실 내부는 주야간 감시가 가능하도록 5대의 CCTV가 설치되어 적정한 보안 수준을 유지하는 반면, 내·외부인의 출입이 빈번하게 발생하고 있는 전산실을 출입하기 위하여 반드시 거쳐야 하는 1차 출입문과 전산자원 모니터링실에는 출입자를 감시할 수 있는 CCTV가 미설치되어 있어 출입기록 및 감시가 소홀한 것으로 나타나고 있다.

더불어 『대한지적공사 정보보안업무지침』제18조에 따른 보호구역은 상

시 이용하는 출입문은 한곳으로 정하고 이중 잠금장치를 설치하도록 되어 있으나 1개의 보안출입통제장치만 설치되어 있어 이중화된 보안 잠금장치 설치가 요구되고 있다.

조치할 사항

○○○○○**장은** 보안구역(전산실)의 접근통제 강화를 위해 내·외부 직원의 출입이 잦은 출입문에 대한 보안을 강화하시기 바랍니다. 더불어 출입구에 CCTV 설치하는 등과 같은 접근통제 정책을 강화하시기 바랍니다.