경영유의사항 등 공개안

1. 금융회사명 : 하나생명보험㈜

2. 조치일 : 2018. 6. 27.

3. 조치내용

대상	내 용
기관	경영유의사항 2건, 개선사항 7건

4. 조치대상사실

가. 경영유의사항

(1) 개인정보 암호화 관리 철저

□ OOO솔루션을 도입하여 OOO, OOO 등 개인정보를 암호화하고 있으며, OOO을 통해 서버 내에 암호화되지 않은 개인정보를 점검하는 등 개인정보를 관리·통제하고 있으나

OOO솔루션 도입 이전에 보관된 일부 개인정보 등에 대해 암호화를 적용하지 않은 채 DB에 보관하고 있으며, OOO의 개인정보 검색대상에 일부 DB를 누락한 채 운영하여 암호화되지 않은 개인정보를 검출하지 못하는 등 개인정보 암호화 관리·통제가 다소 미흡하므로

암호화되지 않은 채 DB에 보관되는 개인정보를 즉시 암호화하고, OOO의 개인정보 검색대상을 확인하여 누락되는 DB가 발생하지 않도록 조치하는 등 개인정보 암호화 관리·통제를 강화할 필요가 있음

(2) 외부주문 업무에 대한 내부통제 강화

□ IT시스템 운영·관리업무를 외주업체(하나금융티아이)에 위탁하고 있으나

회사 내부 책임자가 외주직원이 변경 또는 개발한 고객정보 관리 등의 주요 프로그램에 대해 타당성 검토를 실시하지 않고

외주직원이 수행하고 있는 전산센터 자산 반·출입 등 인프라 관리 업무에 대한 통제방안을 마련하지 않아 보안솔루션 설치 등이 누락된 단말기를 전산실 내부에 설치하는 등 관리가 미흡하며,

외주업체와 체결한 계약에 서비스 품질수준평가 결과에 따른 패널티, 인센티브 부과 방안 등을 마련하지 않는 등 외주업체에 대한 성과평가 체계가 미흡한 한편, 개발·인프라 운영 업무매뉴얼을 외주업체가 작성·관리하게 하면서 동 내용에 대해 검토를 실시하지 않아 외주업체가 개발·인프라 운영 업무 관련 절차를 임의로 변경하고 업데이트가 적시에 이루어지지 않을 우려가 있으므로

프로그램 개발 및 인프라 관리·운영 업무에 대한 적정성 검토, 보안통제 체제 구축, 서비스 품질평가에 따른 패널티, 인센티브 부과 등 성과평가 체계 개선 및 IT운영 업무매뉴얼 관리 개선 등 IT 외부주문 업무에 대한 내부통제를 강화할 필요가 있음

나. 개선사항

(1) IT부문 자체감사 불합리

□ 전산정보부에서 IT부문에 대한 자체감사를 실시하고 있으나

형상관리시스템 계정의 적정성, 프로그램 변경관리의 적정성 등 일부 항목에 대해서만 자체감사를 수행하였을 뿐 IT보안 관련 항목에 대해서는 자체감사를 실시하지 않았고

자체감사 주기도 연 1회 실시하고 있어 즉시 조치가 필요한 미흡사항이 장기간 확인되지 않고 방치될 우려가 있으므로

IT 자체감사 시 IT보안 항목 등에 대해서도 점검할 수 있도록 자체감사 대상을 확대 운영하고, 중요 점검항목에 대해서는 감사주기를 단축하여 수행하는 등 IT 부문 자체감사를 개선하시기 바람

(2) 전산계약 업무처리 불합리

□ 내규에 의해 외주업체인 하나금융티아이와 정보처리시스템 구매 대행 계약을 수의계약 형식으로 체결하고 있으나

거래가격 등 계약의 적정성을 판단할 수 있는 세부 기준, 확인 절차 등이 마련되어 있지 않아 외주업체 임의로 불합리한 계약을 체결할 우려가 있으므로

구매대행으로 정보처리시스템 도입 계약 등을 체결할 경우 동 계약의 적정성을 판단할 수 있는 세부기준 등을 마련하는 등 전산계약 체결 방법을 개선하시기 바람

(3) 재해복구매뉴얼 및 재해복구 훈련 불철저

□ 업무연속성을 확보하기 위해 'OOO매뉴얼' 및 'OOO매뉴얼'을 마련하고, 연 1회 재해복구훈련을 실시하고 있으나

OOO매뉴얼의 내용 중 서버자원, 관련 소프트웨어, 스토리지자원 현황 등을 현행화하지 않았고, 대체사업장 IT환경 구축 상세 절차, 유지보수업체 및 대외기관 등을 포함한 비상연락망은 마련하지 않았으며,

재해복구훈련 시 OOO매뉴얼에 따라 재해복구시스템으로 자원을 할당하지 않고 평상시 환경으로 훈련을 실시하고 있어 비상시에 대비한 성능테스트 등이 미흡하므로

OOO매뉴얼에 변경된 현황 및 상세절차 등이 반영될 수 있도록 개선하고, 재해복구훈련 시 매뉴얼에 따라 재해복구시스템으로 자원을 할당하여 훈련을 실시하시기 바람

(4) 데이터베이스 운영 통제 미흡

□ OOO시스템을 사용하여 DB접속 및 사용권한 등을 통제하고, 전산원장 변경 절차를 마련·운용하고 있으나

업무부서 직원 29명에게 운영DB를 직접 조회하고 관련 명령어를 입력할 수 있는 권한을 부여하고 있어, 과다 조회 및 명령어 입력에 따른 시스템 과부하 시 운영중인 서비스가 지연처리 되는 등 영향을 미칠 우려가 있고

PC 로그인을 하는 경우 OOO시스템이 자동 로그인 되도록 운영하고 있어 타인이 PC에 무단 접근할 경우 DB까지 무단으로 접근할 우려가 있으며

관리자가 별도의 통제절차 없이 DB의 암호화된 개인정보를 복호화하여 조회할 수 있고, 전산원장 변경절차에 변경 전후내용 자동기록 및 보존 등에 대한 내용이 포함되어 있지 않으므로*

* 실제 전산원장 변경 시에는 변경 전후내용을 자동 기록하고 있음

정보조회용 시스템 구축 등을 통해 업무부서에서 운영DB를 직접 조회하는 것을 차단 또는 최소화하고, DB에 대한 접근통제를 강화하고 DB관리자의 데이터 복호화 조회 권한을 통제하는 한편, 전산원장 변경절차에 변경 전후내용 자동기록 및 보존에 대한 내용을 추가하는 등 데이터베이스 운영 통제를 개선하시기 바람

(5) 서버 접근통제 불합리

□ OOO시스템을 구축하여 서버 접속이 가능한 단말기를 제한하고 추가인증을 적용하는 등 통제 절차를 마련하고 있으나

일부 서버에 통신 내용을 평문으로 송·수신하는 접속방식을 허용하고 있어 통신 내용이 유출될 우려가 있고

일부 서버는 작업로그를 OOO시스템 등에 저장하지 않고 있으며, 치명적인 장애를 유발할 수 있는 금지 명령어 사용을 통제하지 않아 동 명령어 실행 시 장애사고 및 이에 대한 사후 추적이 곤란해질 우려가 있으며,

관리자 계정에 대해서는 동 시스템을 통하여 비밀번호의 생성규칙 및 변경 주기를 관리하고 있으나, 일반계정 비밀번호에 대해서는 별도의 관리절차가 마련되어 있지 않아 생성규칙 등을 준수하지 못할 우려가 있으므로

서버 접속 시 암호화통신을 사용하고, 서버 작업내용 기록 및 금지명령어 사용을 통제하고 일반계정에 대한 비밀번호 관리를 강화하는 등 OOO 시스템의 운영 방법을 개선하시기 바람

(6) 정보처리시스템 계정관리 미흡

□ 회사 임직원 퇴직 시 주요 업무시스템에 대한 사용자 계정을 지체없이 삭제하도록 내규를 마련·운영하고 불필요 계정에 대한 점검을 실시하고 있으나

일부 업무시스템 계정을 인사DB와 연동하지 않고, 점검주기를 다소 길게 운영하고 있어 동 시스템 계정을 가진 임직원이 퇴직하여도 계정 삭제가 즉시 이루어지지 않을 우려가 있고

회사의 전산업무 처리현황 등을 관리하는 OOO시스템의 경우 최초 사용자에게 동일한 초기 비밀번호를 부여하고 동 비밀번호를 3개월까지 사용할 수 있도록 운영하고 있으므로

업무시스템 계정을 인사DB와 연동하거나 불필요 계정에 대한 점검주기를 단축하고, OOO시스템의 초기 비밀번호를 최초 사용 즉시 변경하도록 운영하는 등 정보처리시스템 계정 관리방법을 개선하시기 바람

(7) 정보보호시스템 운영 통제 불합리

□ OOO시스템을 구축하여 내부 업무용시스템에 대해 백신 업데이트, 바이러스 감염 여부 등에 대해 모니터링하고 있으며, OOO시스템을 구축·운영하여 OOO파일에 대해 강제로 암호화하고 있으나,

인터넷 전용 단말기에 대해서는 OOO시스템이 적용되지 않아 적절한 통제가 이루어지지 않고 있으며, OOO 문서의 경우 확장자를 변경하면 암호화가 적용되지 않아 OOO시스템을 우회할 가능성이 있으므로

OOO시스템 등 정보보호시스템 운영 시 보안통제가 누락되지 않도록 개선하여 운영하시기 바람