경영유의사항 등 공개안

1. 금융기관명 : 신한캐피탈㈜

2. 조치일 : 2018. 6. 27.

3. 조치내용

대상	내용
기 관	경영유의사항 1건, 개선사항 5건

4. 조치대상사실

가. 경영유의사항

(1) 개인정보 조회권한 관리 강화

회사는 고객 개인정보를 직접 사용할 필요가 없는 OOOOO 및 OOOOO 직원에게도 개인정보 처리시스템 접근권한을 부여하는 등 개인정보 조회권한 관리가 미흡한 수준이므로

개인정보 처리시스템 접근권한을 각 업무에 필요한 최소 범위로 제한하여 업무 담당자에 따라 차등 부여하는 등 개인정보 조회권한 관리 강화 필요

나. 개선사항

(1) IT감사 사후관리 미흡

감사팀은 매년 감사계획에 따라 IT감사를 실시하고 있으며, OOOO년 ICT팀에 대한 정기감사를 실시하고 조치요구사항에 대해 조치내용 또는 조치계획 제출을 요청하였으나,

ICT팀에서 제출한 조치계획 등의 완료예정일이 명확하지 않고 조치 관련 입증자료를 제출하지 않은 사례가 있으므로

IT감사 지적사항에 대한 조치계획 등을 명확히 작성토록 하고, 조치내용에 대한 입증자료를 철저히 제출토록 하는 등 IT감사 사후관리체계 개선 필요

(2) 사용자 계정관리 미흡

회사는 사용자의 편의성을 위해 일부 OOO시스템에 통합로그인방식(SSO)을 적용하고 있고 있으나,

고객의 주요 전자금융거래를 처리하는 OOO시스템에 SSO를 적용하고 있어 사용자 아이디 및 비밀번호 입력 없이 OOO시스템에 접속 가능하고, SSO와 연계된 응용시스템 접속이 종료되어도 SSO는 O시간이 경과하여야 접속이 종료되는 등 계정관리가 미흡하므로

OOO시스템을 SSO 적용대상에서 제외하고 SSO의 접속 유효시간을 단축하는 등 SSO와 연계된 응용시스템의 계정관리 개선 필요

(3) 백업 전산자료 검증 미흡

회사는 정보처리시스템 장애 등에 대비하여 전산자료를 백업 및 소산하고 백업자료를 이용한 복구테스트를 실시하여 백업 자료에 대한 오류 발생 여부 등을 검증하고 있으나,

복구테스트 수행 주기 및 대상 등 세부기준을 마련하지 않아 OOOO년도에는 백업 복구테스트를 실시하지 않았고, 백업 복구테스트 대상을 홈페이지 관련 백업 자료에 한정하여 수행하는 등 OO업무시스템을 포함한 중요 백업자료에 대한 유효성 검증이 미흡하므로

백업 복구테스트 수행 주기 및 대상 등을 포함한 세부기준을 수립하고, 동 절차에 따라 중요 백업자료 대한 유효성 검증이 이루어질 수 있도록 개선 필요

(4) 전자금융기반시설 취약점 분석·평가 미흡

회사는 전자금융기반시설 취약점 분석·평가를 연 1회 이상(홈페이지에 대해서는 6개월에 1회 이상) 실시하고 취약점 분석·평가 결과에 따라 보완조치의 이행계획을 수립·시행하고 있으나,

동 보완조치가 적절히 이행되지 못하여 동일한 장비에서 같은 취약점이 다시 발견되는 등 장기간 보완 조치되지 않은 취약점을 통해 해킹 등 전자적 침해사고가 발생할 우려가 있으므로

취약점 보완조치 이행 및 이에 대한 사후점검을 강화하는 등 취약점이 장기간 방치되지 않도록 관련 절차 개선 필요

(5) 테스트데이터에 대한 관리 미흡

회사는 프로그램 테스트에 사용되는 이용자 정보는 테스트데이터 변환 솔루션을 통해 테스트데이터로 변환하여 개발환경으로 이관하고 있으나,

내규 「정보보호규정」에 개발환경에서 실제 운영 데이터를 사용할 수 있는 예외조항을 두고 있어 이용자 정보 보호에 취약할 우려가 있고, 동 솔루션을 통한 이용자 정보 변환·이관 작업을 별도의 통제절차 없이 주 1회 상시 수행하고 있어 테스트데이터에 대한 관리가 미흡하므로

테스트데이터 변환 신청 시 이관 대상 및 이용기간을 명시하여 책임자의 사전승인 후 변환 작업을 수행하고, 테스트 종료 후 즉시 데이터를 삭제하는 등 사후 관리가 이루어질 수 있도록 관련 절차를 수립하고 시스템 개선 필요