# 경영유의사항 등 공개안

1. 금융기관명 : 현대카드㈜

2. 조치일 : 2019. 1. 8.

3. 조치내용

| 대상 | 내용 |
|---|---|
| 기 관 | 개선사항 7건 |

4. 조치대상사실

가. 개선사항

(1) IT감사 업무 불합리

① 회사 내규「감사위원회 직무규정」에 의하면 감사실은 종합감사를 실시하고 IT부문 기능별 프로세스의 유효성 평가, 문제점 적시, 개선방안 제시 등을 포함한 감사결과 보고서를 작성·제출해야 함에도

OOOO.O.O.~OOOO.O.OO. 중 IT부문에 대한 종합감사 실시 이력은 O회에 불과하고, 동 감사결과 보고서에는 IT부문 기능별 유효성 평가 등의 내용을 포함하지 않고 지적사항에 대해서만 기술하고 있어 전체적인 IT업무에 대한 적정성을 확인하기 어려우므로

IT부문에 대한 종합감사를 정기적으로 실시하고 종합감사 결과보고시 전반적인 IT부문 기능별 유효성 평가 등의 내용을 포함하여 작성하는 등 IT부문에 대한 감사업무 개선 필요

② IT부문은 내규「IT내부관리기준서」에 따라 IT내부통제의 적정성과 IT운영을 평가·개선하기 위해 수행주기(반기/매월 등) 별 감사항목(총 O개)을 마련하고 IT자체감사를 실시하고 있으나,

동 내규에는 IT자체감사 실시 및 결과 보고 등 세부 업무절차를 반영하고 있지 않고, IT본부 외 타본부는 동 감사항목에 대한 자체감사를 실시하지 않고 별도 감사항목을 선정하여 월 O회 IT자체감사를 실시하는 등 내규와 상이하게 운영하고 있어 IT자체감사 제도를 체계적으로 운영하기 어려우므로

IT자체감사 수행절차, 감사결과 보고 및 사후관리 절차 등을 관련 내규에 반영하고 부서별 업무특성을 고려한 점검 항목을 추가·확대하여 감사를 실시하는 등 IT자체감사 업무 강화 필요

**(2) 재해복구센터 구축 및 전환훈련 실시 불합리**

① 회사는 주전산센터 장애에 대비하여 업무지속성을 확보할 수 있도록 중요 핵심 업무에 대해서 재해복구시스템을 구축·운영하고 있으나,

OOOOOO 조회 등을 위한 OOOO 및 OOOO 등 대고객 업무시스템은 재해복구시스템은 구축하지 아니하여 비상상황 발생시 고객지원 업무를 충분하게 지원하지 못할 우려가 있으므로

재해발생 시 OOOO 및 OOOO 등 대고객 업무가 지속적으로 수행될 수 있도록 재해복구시스템을 구축·운영하는 등 비상대책 강화 필요

② 재해발생 시 복구목표시간을 O시간으로 정하고, 주전산센터의 재해를 대비하여 재해복구 전환훈련을 연 O회 실시하고 있으나,

평상 시 재해복구시스템을 OOO · OOO 시스템으로 사용하고 있어 재해 발생 시 동 시스템에 할당된 자원(CPU 및 메모리 등)을 재해복구시스템으로 재할당하여야 하는데도, 재해복구 전환 훈련 시 시스템 자원 재할당 과정을 포함하지 아니하는 등 재해복구 전환훈련 계획 수립 및 운영이 다소 미흡하므로

재해 발생 시 업무지속성이 확보될 수 있도록 재해복구 훈련계획을 보완하고, 재해복구 훈련 시 실제 전환에 필요한 과정이 누락되지 않도록 하는 등 재해복구 전환훈련 개선 필요

**(3) 전산자료 백업관리 불합리**

회사는 주요 전산자료를 정기적으로 백업하여 주전산센터에 보관하고, 재해복구센터로 OOO을 활용하여 원격 복제를 실시하고 있으나,

OO OO 데이터 및 OOOO 프로그램 등을 정기 백업대상에 포함하지 않았고, 주전산센터 내에 보관하고 있는 데이터 백업테이프의 경우 내화금고가 아닌 일반 캐비넷에 보관하고 있어 화재 등 재해 발생 시 백업데이터 손실이 예상되므로

일부 누락된 OO OO 데이터 및 OOOO 프로그램 등에 대해 주기적으로 백업을 실시하고, 보관용 백업테이프를 내화금고 등 안전한 장소에 보관하는 등 전산자료 백업관리 강화 필요

**(4) 노후화 전산장비 관리 불합리**

① 회사는 전산장비의 노후화로 인해 장애사고가 발생하는 것을 방지하기 위하여 노후화된 전산장비를 폐기하고 신제품으로 교체하고 있으나,

사용이 종료된 전산장비(서버 OO대, 스토리지 O대)를 운영시스템과 분리하지 않고 내부 네트워크에 연결된 상태로 운영하고 있어 상대적으로 보안관리가 소홀한 미사용 전산장비에 의해 운영장비에 악성코드 등이 감염될 우려가 있으므로

미사용 전산장비는 운영장비와 분리하여 별도로 관리하고 폐기절차에 따라 장비를 폐기하는 등 노후화 전산장비 관리절차 강화 필요

② 서버 운영체제(OS) 총 O,OOO대 중 일부 운영체제(OOO대)에서는 제조사로부터 기술지원이 종료되어 보안패치 및 서비스 업그레이드 등의 지원을 받지 못하는 운영체제를 사용하고 있어 시스템 오류 및 장애 발생 시 신속한 대응이 어렵고, 신규 취약점을 악용한 해킹 및 악성코드 감염 등이 발생할 우려가 있으므로

기술지원이 종료된 운영체제를 업그레이드하거나 제조사와 기술지원 연장 계약을 체결하는 등 운영체제 장애발생을 미연에 방지하기 위한 구체적인 대응계획 마련·운영 필요

**(5) 서버 접근통제 관리 불합리**

회사는 서버 계정 접근권한 및 명령어 통제 등을 위해 서버접근통제솔루션을 설치하고 사용자 계정의 비밀번호를 OO마다 자동으로 변경·관리하고 있으나,

서버 관리자계정 비밀번호의 경우 서버 관리자가 OO별 수작업으로 비밀번호를 변경하면서도 비밀번호 사용 및 변경이력을 관리하기 위한 방안을 마련하지 않았고, 일부 내부사용자 서버접속의 경우 서버접근통제솔루션을 거치지 않고 서버로의 직접

접속(OOO, OOOOOO)을 허용하고 있어 서버접근통제 및 모니터링 정책을 우회할 가능성이 있으며,

서버 관리자 계정으로 전환 가능한 사용자 계정 목록을 별도 제한하지 않아 사용자 계정으로 서버에 접속한 후 계정 전환 명령어(OO)를 통해 관리자 계정으로 전환이 가능함으로써 비밀번호가 노출·공유되는 경우 권한을 부여받지 않은 사용자가 관리자 권한 작업을 수행할 우려가 있으므로

서버 관리자계정에 대한 비밀번호 관리 절차를 마련하고, IT단말기에서 서버접근통제솔루션의 통제 없이 서버로의 직접 접속을 차단하는 한편, 관리자 계정으로 전환 가능한 사용자 계정을 제한하는 등 서버 접근통제 관리 개선 필요

**(6) 문서보안 통제·관리 불합리**

회사는 사용자 단말기에 저장된 전산자료 유출을 방지하기 위하여 문서보안솔루션(DRM)을 구축하여 문서 파일(워드, 엑셀, 텍스트 파일 등)을 암호화하여 저장하고 있으나,

IT관리용 단말기에는 문서보안솔루션을 설치하지 않아 중요 내부문서가 암호화되지 않은 채 저장될 우려가 있고

기 암호화된 문서내용을 암호화되지 않은 문서로 '복사 및 붙여넣기'가 가능하여 메모장 등 텍스트 편집기를 통해 데이터를 CSV(Comma-Separated Values) 파일 등의 형태로 변환·저장하는 경우 문서 암호화가 미적용되는 취약점이 존재하므로

IT관리용 단말기에도 문서보안솔루션(DRM)을 확대 적용하고 문서암호화 통제가 누락되지 않도록 동 솔루션의 보안정책 및 기능을 강화하는 등 문서보안 통제·관리 개선 필요

**(7) 비밀번호 암호화 알고리즘 사용 불합리**

회사는 계정관리시스템에서 생성된 서버 비밀번호를 서버접근통제솔루션에서 암호화하여 보관하고 있고, 홈페이지 서버에서는 데이터베이스와의 연결에 필요한 비밀번호를 암호화하여 저장하고 있으나,

서버접근통제솔루션 및 OOOO 서버에서 비밀번호 암호화 시 보안강도가 미약한 암호화 알고리즘(OOO)를 사용하고 있어 해킹 등에 의해 OO·OO의 비밀번호가 노출될 우려가 있으므로

안전성이 낮은 암호화 알고리즘(OOO 등)이 적용된 시스템에 대하여 보안강도가 높은 암호화 알고리즘으로 강화·적용 필요