경영유의사항 · 개선사항 공개

1. 금융기관명 : 쿠콘

2. 제재조치일 : 2024. 4. 26.

3. 조치내용

대 상	내 용
기 관	경영유의사항 2건, 개선사항 5건

4. 조치대상사실

가. 경영유의사항

(1) 정보보호 전담조직 독립적 운영 강화

㈜쿠콘은 내규 ○○○○을 마련하여 정보보호 관리활동을 체계적으로 이행하기 위한 정보보호조직을 구성하고, 정보보호 최고책임자 및 정보보호 전담조직 등에게 정보보호 활동에 적합한 역할과 책임을 규정하는 등 필요한 세부사항을 정하고 있다. 이에 따라 정보보호 전담조직이 정보보호 관련 업무기획 및 정보 자산 보호와 관련된 기술적·관리적·물리적 조치 및 운영 등 정보보호 업무 전반에 대한 역할을 수행토록 하고 있다.

하지만, 회사의 네트워크 인프라 도입과 설치 등을 담당·관리하는 네트워크 운영조직에서 네트워크 장비 운영과 함께 정보보호시스템 관리업무를 일부 병행하고 있어, 업무간 이해 상충의 문제로 정보보호 관련 업무 및 정보 자산 보호가 충분히 이뤄지지 않을 우려가 있으므로, 정보보호 전담조직의 운영 방식을 개선할 필요가 있다.

<조치할 사항>

따라서 회사는 앞으로 네트워크운영부 소속의 정보보호시스템 운영인력을 정보보호 전담조직으로 분리하고, 정보보호부내 보안운영팀을 추가 신설하는

등 조직개편을 통해 정보보호 전담조직의 독립적 운영을 강화하시기 바랍니다.

(2) 내부감사 및 내규관리 등 내부통제 역량 강화 필요

회사는 임직원이 직무수행시 준수해야할 내규 ◎◎◎◎을 마련하여 자가점검, 내부품의 통제 등 내부통제 목적의 준법 감시 프로그램을 운영하고 있다.

하지만 감사 직속의 내부감사 실무조직이 설치되지 않는 등 업무전반에 대한 회사의 감사기능이 미흡해서, 전자금융업 업무 전반에 대한 실질적 내부감사 수행 내역이 없고 임직원의 직무수행에 대한 적법성 및 타당성 감사 수행에도 현실적 어려움이 있다.

또한 회사는 현재 ◇◇◇◇을 통해 ●●개의 규정 및 ◆◆개의 세칙 등을 구분하여 내규를 운영하고 있으나 내규를 전반적으로 총괄하는 부서가 없어 내규의 정기적인 개정 및 검토를 수행하는 것이 어렵고, 선불충전금 관리, 정산금 처리 등 전자금융업 관련 주요 업무에 대한 명문화된 규정이 일부 마련되어 있지 않아 업무처리 절차의 적정성을 점검하지 못하는 등 실효성 있는 내규 운영이 어렵다.

<조치할 사항>

따라서 회사는 감사 직속의 독립적인 감사 조직을 구성하고 감사 및 내규 관련 규정을 제·개정하여 IT개발·운영, 보안, 회계, 자금 등 전자금융업무 전반에 대한 일상·정기감사를 수행하시기 바랍니다.

또한 내규를 총괄하는 부서를 지정하여 내규별 담당 조직이 정기적인 개정 및 검토를 수행할 수 있도록 관리하는 등 체계적인 내규관리 시스템을 마련하시기 바랍니다.

나. 개선사항

(1) 단말기 보호대책 미흡

회사는 내규 □□□□에 따라 전산장비, 보안장비 등 회사의 정보자산과 정보시스템 운영 환경에 대한 물리적 안전성 확보를 위해 필요한 사항을 규정하고

통제구역 등 보호구역을 지정하여 구역별 보호대책을 수립·운용하고 있다.

하지만 회사는 전산센터가 아닌 본사 및 지사의 일부 공간을 통제구역으로 지정하여 해당 위치에 PC용 보안솔루션 등 임직원의 단말기 보안과 관련된 일부 정보보호시스템을 설치·운영하고 있다. 따라서 전산센터의 대·내외 반출입 통제 등 안전성 확보에 필요한 사항을 준수하기 곤란하고, 시스템 장애, 가동 중지 등 긴급사태에 대비한 백업 및 복구 절차 이행시, 해당 시스템에 대한 관리가 소홀해질 우려가 있다. 뿐만 아니라, 서로 다른 위치에 설치된 정보보호시스템 간 일관적인 보안정책 적용이 어려울 가능성이 있다.

또한 전산자료의 유출 등을 방지하기 위하여 매체제어솔루션 및 망간자료전송솔루션을 도입하여 관리책임자의 사전승인을 받은 전산자료에 한해 외부반출을 허용하고 있으나, 임원 및 부서장급 이상의 상위 책임자 일부에 대해서는 업무 편의성 등의 사유로 사후승인 절차를 운영하고 있어 비인가자 등이 해당 단말기에서 내부 전산자료를 외부로 유출할 가능성이 있다.

<조치할 사항>

따라서 회사는 안티바이러스 등 단말기 보안솔루션을 주전산센터로 이전하여 반출입통제 등 안전성을 확보하고, 본사 및 지사의 일부 공간 등 다양한 단말기 설치환경에서도 일관적인 보안정책을 적용하고, 주기적인 백업을 시행하고 복구 절차를 마련하는 등 장애 발생시 신속한 복구가 수행될 수 있도록 조치하시기 바랍니다.

또한 관리책임자에 대해서도 전산자료 반출시 사전승인 절차를 적용하여 운영하시기 바랍니다.

(2) 가맹점 정산계좌 변경시 통제 및 사후점검 불합리

회사는 ■■■■ 서비스 이용 가맹점의 정산계좌 변경 요청 시 사업부에서 공문 또는 메일로 접수 받아 이를 소비자보호실에 작업의뢰서 형태로 전자결재 상신하여 정산계좌를 변경하는 업무처리 절차를 운영하고 있다.

하지만 정산계좌 변경 권한을 가지고 있는 소비자보호실 직원은 관련부서 합의 또는 별도 책임자의 승인 없이 단독으로 정산계좌 변경이 가능하고,

정산계좌를 변경한 내역을 기록하고 있지 않아 계좌변경 절차에 대한 적정성 등에 대한 객관적인 점검이 어려워 가맹점의 정산계좌를 무단으로 변경할 가능성도 있다.

<조치할 사항>

따라서 회사는 소비자보호실에서 정산계좌 변경 시 작업의뢰서 문서번호, 일시, 작업자 등을 기록하고 관련부서 합의 및 관리 책임자의 승인을 받도록 시스템을 구축하고, 제3자가 정산계좌 변경이 가맹점의 요청에 의해서 정상적으로 수행된 것인지 여부에 대해 점검하는 등 업무절차를 개선하시기 바랍니다.

(3) 프로그램 변경통제 미흡

회사는 내규 △△△△에 따라 개발이 완료된 응용프로그램에 대해 개발요청자의 사용자테스트를 거치고, 개발자 및 요청자가 테스트를 완료하면 정보보호담당자는 소스코드 보안취약점 진단을 수행해야 한다.

하지만 개발 요청자의 사용자테스트 수행 및 이력을 남기는 절차와 정보보호담당자의 소스코드의 취약점 점검을 수행하는 구체적인 방법을 마련하지 않아 프로그램의 외부위협에 대한 안전을 담보하기 어려우므로 업무절차를 보완할 필요가 있다.

또한 회사는 내규 △△△△에 따라 개발이 완료된 응용프로그램은 운영관리자가 운영환경에 적용하고, 정보보호담당자는 운영환경에 승인된 실행파일만 존재하는지 점검해야한다.

하지만 프로그램 운영관리자를 별도로 지정하지 아니하여 응용프로그램 개발담당자가 직접 운영환경에 적용하는 것을 통제할 수 있는 수단이 부족하고, 정보보호담당자는 운영환경의 어플리케이션이 동작하는 서버에서 소스파일 등 불필요한 파일이 있는지 여부를 주기적으로 점검하지 않고 있다.

이에 따라 프로그램 운영적용의 안정성을 담보하기 어려우므로 이를 예방하기 위한 적절한 통제절차를 수립할 필요가 있다.

<조치할 사항>

따라서 회사는 사용자테스트를 수행하는 구체적인 방법 및 소스코드 보안취약점 진단을 자동화하기 위한 절차를 내규에 규정하시기 바랍니다.

또한 동일인이 여러 업무를 수행함으로 인하여 발생할 수 있는 전자금융사고를 방지하기 위해 응용프로그램 개발담당자의 운영서버 접근통제 절차를 강화하고, 운영 서버 내 불필요한 파일이 없도록 정기적으로 점검하는 절차를 마련하시기 바랍니다.

(4) 전자금융서비스 보안 불철저

회사는 내규 ▽▽▽▽에 따라 전자금융서비스의 안전성을 확보하고 공개용 웹서버가 해킹공격에 노출되지 않도록 대응 조치하는 등 각종 보안위험을 감소시키기 위한 관리적·기술적·물리적 보안기준을 수립·운용하고 있다. 이에 따라 전산센터에는 침입차단시스템(방화벽)이 도입·설치되어 있으며, 업무담당자가 보안 접속 요청시 정보보호부서가 회사 내규 ♤♤♤♤에서 정한 보안접속 원칙을 적용하여 제한적으로 보안정책을 검토·승인하고 있다.

하지만 해킹 방지 등의 목적으로 도입·운영 중인 침입방지시스템(IPS, Intrusion Prevention System)에서 ＝＝＝에 대한 해킹시도를 적절하게 탐지·방어할 수 있는 수단이 마련되어 있지 않고, 신규 해킹공격 탐지 패턴 등 중요한 업데이트 사항에 대해 보정작업을 비정기적으로 수행하는 등 사이버 침해시도 발생시 즉각적인 대응이 곤란할 가능성이 있다. 또한, 업무목적을 달성하여 현재 불필요하거나 불명확하게 설정된 보안정책이 다수 존재하는 등 방화벽 보안정책에 대한 사후관리가 미흡하다.

회사는 시스템담당자가 서버 등 정보처리시스템에 접속하는 경우 서버접근제어시스템을 통해 담당자별 접근권한 등을 사전에 통제하고 추가인증(OTP)을 적용하고 있다.

그러나, 방화벽 등 정보보호시스템 및 정보보호솔루션 접속에 대해서는 별도의 통제수단이나 절차가 마련되어 있지 않고 사후관리를 통해서 형식적인 관리자 계정현황만 파악하는 수준에 그치고 있어 체계적인 계정관리 및 접근기록 보관 등에 어려움이 예상된다.

뿐만 아니라 현재 운영중인 서버 ♠대 중 ♡대(__%), 네트워크 장비 ♥대 중 ♧대(__%), 보안시스템 ♣대 중 ⊙대(__%)가 제조사의 기술지원이 종료된 운영체제가 설치되어 있거나 노후장비로 보안패치 및 서비스 업그레이드 등의 지원을 받지 못할 가능성이 있어서 시스템 오류 및 장애 발생 시 신속한 대응에 어려움이 예상되고 신규 취약점을 악용한 해킹 및 악성코드 감염 등이 발생할 우려가 있다.

<조치할 사항>

따라서 회사는 복호화 전용시스템을 도입하여 DMZ 구간에 위치한 침입방지시스템(IPS)에서 ＝＝＝된 보안위협을 효과적으로 탐지·차단할 수 있도록 기술적 대책을 마련하고 신규공격 패턴을 주기적(월 1회)으로 업데이트하시기 바랍니다.

또한 방화벽의 보안정책관리에 대한 내용 및 절차를 회사내규에 반영하여 주기적(분기별) 점검을 통해서 불명확하거나 불필요한 정책을 비활성화 및 삭제(90일 미사용정책 비활성화, 비활성화 이후 90일 이후 삭제)하는 등 체계적으로 관리하시기 바랍니다.

한편 정보보호담당자가 시스템 관리를 위해 정보보호시스템 및 정보보호솔루션에 접근하는 경우 접근통제 절차를 마련하고, 접근제어솔루션을 통해서 접속기록을 관리하시기 바랍니다.

뿐만 아니라 기술지원이 종료된 운영체제에 대하여 업그레이드 및 서버 교체 계획을 수립하여 2024년부터 순차적으로 교체작업을 진행하시기 바랍니다.

(5) 비상대책 수립·운영 미흡

회사는 내규 ◈◈◈◈에 따라 ▣▣▣ 등 ◐개 단위업무를 대상으로 업무영향도 분석(BIA)을 실시하고, 핵심업무를 선별하여 재해복구목표설정 및 백업정책 등에 반영하고 있다.

하지만 업무영향도 평가항목에 재무적 손실 가능성과 같은 정량적 기준이 포함되지 않고, 평가 대상 업무에서 일부 대외연계서비스가 누락되는 등 업무영

향도분석 절차가 다소 미흡하다.

회사는 계좌간편결제, 기업자금관리, 대출비교, 마이데이터 등 고객의 비즈니스에 필요한 다양한 데이터를 금융회사로부터 수집하여 고객사에게 API 등의 방식으로 연결하는 데이터 플랫폼 사업과 전자금융서비스 등을 함께 영위 중에 있으며, 안정적인 지급결제 서비스를 제공하기 위해 전용회선을 이중화하여 은행, 증권사 등 다수의 금융회사와 연결하고 있다.

하지만 이중화로 구성된 전용회선이 전부 주전산센터에만 연결되어 있어 주전산센터가 중대한 장애 등 비상상황에 직면했을 때 금융회사와 재해복구센터 간 통신할 수 있는 기술적 수단이 마련되어 있지 않고, 일부 업무 시스템의 재해복구센터로의 전환시 시스템 정상 가동 여부를 확인할 수 있는 업무메뉴얼이 누락되어 있다.

한편 회사는 내규 ◑◑◑◑에 따라 백업관리대장에 기록하고 있는 ⊙개 업무에 대해서 각각 정해진 주기에 백업을 실시하여 백업자료를 매월 소산하고, ☆☆☆☆에 따라 백업한 자료에 대해서 완전성, 정확성을 정기적으로 검증하기 위해 복구테스트를 수행하여야 하며 재해복구를 위한 모의훈련을 연 1회 실시하여야 한다.

하지만 회사는 ▣▣▣, ★★★ 등 전자금융과 관련된 주요 업무에 대해서 백업 및 소산된 데이터를 이용하여 복구테스트를 수행한 사례가 없어 비상상황 발생시 시스템 운영가능 여부를 담보하기 어려운 측면이 있다.

또한 검사기간 동안 실시한 ▨차례의 비상대응훈련은 모두 핵심업무시스템에 대한 복구 테스트 없이 재해복구설비의 상태 점검 등 주관하는 정보보호부에 의한 단순 장비점검에만 국한되었고, 사업부서의 훈련 결과 검증이력이 없다. 그리고 결과보고서상 훈련과정의 기록 등 내용이 目건 모두 동일하고 과정에 대한 상세기록이 부족하여 실제 수행 여부를 확인하기 어려우며, 비상대응훈련 결과에 따른 문제점 분석을 통한 훈련절차 및 업무연속성계획을 개선하려는 노력이 부족하다.

이로 인해 회사의 비상계획이 실제 비상상황에서 재해복구목표를 준수할 수 있을지 실효성이 우려가 된다.

<조치할 사항>

따라서 회사는 업무중요도를 선정하는 과정에 사업부서가 함께 참여하여 다양한 시각을 고려하고, 분석기준에 재무적 손실 등 정량적 요소를 포함하여 평가체계를 다양화하며, 단위업무를 재파악하여 누락되는 업무가 없도록 절차를 개선하여 업무영향도분석(BIA)를 재실시하고 업무연속성계획에 반영하시기 바랍니다.

또한 회사는 주전산센터 및 재해복구센터에 각각 전용회선을 연결하여 비상상황시 금융회사와 재해복구센터간 통신할 수 있는 기술적 수단을 마련하고, ▥▥▥▥ 등 업무시스템별 정상 가동 여부를 확인할 수 있는 업무메뉴얼이 누락되지 않도록 지속 관리하시고, 재해복구 훈련시 백업 또는 소산된 자료를 이용하여 실제 복원된 자료의 정상적인 시스템 운영이 가능한지 검증하는 한편 훈련결과를 토대로 미흡사항 발견시 해당 검증절차를 보완하시기 바랍니다.