경영유의사항 · 개선사항 공개

1. 금융기관명 : 헥토파이낸셜

2. 제재조치일 : 2024. 4. 26.

3. 조치내용

대 상	내 용
기 관	경영유의사항 1건, 개선사항 4건

4. 조치대상사실

가. 경영유의사항

(1) 정보보호 전담조직 독립적 운영 강화

㈜헥토파이낸셜은 내규 ○○○○을 마련하여 정보보호 관리체계를 수립·유지하기 위한 정보보호 조직 및 정보보호위원회 등을 구성하고, 이를 관리·운영할 수 있도록 정보보호 최고책임자, 정보보호 전담부서 등에게 역할과 책임을 각각 부여하고 있다.

하지만 회사는 정보보호 조직이 회사의 서버 및 네트워크 장비 도입과 설치 등을 관리하는 인프라운영 조직과 함께 구성되어 있어 전반적인 정보보호 업무 준수여부를 감독하여야 하는 정보보호 조직의 독립적인 운영을 저해할 소지가 있고, 인프라보안팀장이 정보보호 전담부서의 장을 겸임하고 있어 인프라 및 보안간 이해상충 문제로 인해 상호견제 체계의 내부통제 기능을 상실할 가능성이 있으므로 정보보호 조직 운영방식을 개선하는 것이 바람직하다.

또한, 회사는 내규 ○○○○에 따라 정보보호시스템의 설치, 관리 및 운영방안에 관한 기준을 마련하고, 정보보호시스템 담당자의 직무를 기술하여 정보보호시스템 관리·운영과 관련된 업무활동을 세부적으로 정하고 있다.

하지만 방화벽 등 일부 정보보호시스템에 대해서는 네트워크 장비 및 전산센터

관리를 수행하는 네트워크 직무에 정보보안시스템 운영 업무를 함께 기술함에 따라 회사의 네트워크 담당자가 네트워크 구성 및 운영관리 업무를 수행하면서 정보보호시스템 구축·운영 업무를 병행하는 등 정보기술 업무와 일부 정보보호 업무를 함께 담당하고 있어 보안 관련 내부통제가 취약해질 우려가 있으므로 정보보호 직무 운영방식을 개선할 필요가 있다.

<조치할 사항>

따라서 회사는 정보보호 전담조직을 분리 운영하고, 보안전담 인력을 별도 지정하는 등 조직개편을 통해 정보보호 전담조직의 독립적 운영을 강화하시기 바랍니다.

또한 네트워크 직무에서 정보보호시스템 직무를 분리하고, 정보보호시스템 운영업무를 전담할 수 있는 보안 인력을 충원하는 등 정보보호 직무 운영방식을 보완하시기 바랍니다.

나. 개선사항

(1) 단말기 보호대책 미흡

회사는 내규 ◇◇◇◇을 마련하여 사용자 단말기의 정보보호에 필요한 표준을 제시하고 있으며, 이에 대한 보안을 유지하여 원활한 업무수행이 이뤄질 수 있도록 정보보호 최고책임자가 단말기 보안관리와 관련한 총괄을 담당하는 등 사용자별 역할과 책임 등을 명시적으로 규정하고 있다.

하지만 동 내규에 업무용 단말기 등 용도에 따른 단말기 유형을 별도로 구분하지 않고 모든 단말기에 대해 일률적인 관리지침을 적용하고 있어, 상대적으로 강화된 보호대책이 적용되는 중요 단말기와 외부 통신망과 연결된 인터넷 전용 단말기 등에 대해 차등화된 보호대책 적용의 어려움이 있다.

또한, 단말기를 통한 내부정보 유출을 방지하지 위해 정보보호 담당자가 유출의심로그에 대한 모니터링을 진행하는 등 일일 내부정보유출 점검 활동을 수행 중에 있으며, 내부 업무자료를 내부망에서 외부망으로 반출하는 경우에는 정보보안 부서장의 사전 승인을 득한 뒤 암호화하여 인터넷 전용 단말기에서 저장·관리하고 있다.

하지만 반출된 업무자료를 주기적으로 삭제하거나 인터넷 전용 단말기에서 문서편집 등의 작업을 제한하는 등의 조치를 하고 있지 않아, 저장된 내부자료가 장기간 보관될 우려가 있고 전자금융 관련 내부자료가 외부 통신망과 연결된 단말기에서 업무와 무관한 외부 인터넷 웹사이트 접속을 통해 유출될 위험이 있다.

<조치할 사항>

따라서 회사는 중요 단말기 등 용도에 맞춰 단말기 유형을 정의하고 유형별 보호대책이 마련될 수 있도록 관련 지침을 개정하시기 바랍니다.

또한, 회사는 인터넷 전용 단말기 내 저장된 내부업무자료에 대해 주기적으로 모니터링하고, 업무와 무관한 웹사이트 접속을 차단하는 등 내부정보 유출 방지를 위한 보안대책을 강화하시기 바랍니다.

(2) 고객정보 보호대책 미흡

회사는 ●● 관리자 페이지에서 이름, 휴대폰번호 등 개인정보에 대해서는 마스킹 처리를 하고 있으며, 내부직원이 해당 페이지를 조회하는 경우 접속내역을 자동으로 기록·관리하고 있다.

하지만 고객정보가 포함된 데이터를 조회하여 단말기에 저장하는 경우에 대해서는 다운로드 사유 등을 자동화된 방식으로 기록하지 않고 개인정보보호담당자가 수기로 서버 로그 등을 확인하여 적정성을 점검하는 등 업무 절차가 미비하여 업무 목적 이외의 불필요한 개인정보 조회 행위에 대한 적시 대응이 곤란하고 접속 이력에 대한 사후 관리에 어려움이 예상된다.

<조치할 사항>

따라서 회사는 임직원이 고객의 개인정보를 포함한 데이터 다운로드 시 다운로드 사유 등을 포함한 기록을 관리할 수 있도록 통제 절차를 강화하시기 바랍니다.

(3) 일괄작업 통제 절차 미흡

회사는 가맹점 정산업무 등 총 ◆◆◆개의 일괄작업을 통해 각각 특정 주기로 데이터를 삽입, 갱신하거나 파일을 생성하고 있다. 수행 후 결과는 알람기능을 통해 작업담당자와 책임자가 실시간으로 확인하여 오류에 즉시 대응하고 결과기록을 매월 점검하고 있다.

하지만 일괄 작업에 대한 사전 승인 절차가 없어 응용 프로그램 개발담당자가 서버계정으로 접속하여 직접 등록·수행·폐기함에 따라 책임자에 대한 사전 보고 없이 작업을 진행할 우려가 있고, 일괄작업 수행 중 발생한 오류내역 및 발생원인, 조치내역 등의 이력이 체계적으로 관리되지 않고 있다.

<조치할 사항>

따라서 회사는 응용프로그램 개발 담당자가 일괄작업 스케쥴러에 작업을 직접 등록·변경·삭제 할 수 있는 환경을 적절하게 통제하고 오퍼레이터가 작업요청서에 의해서만 수행하도록 절차를 개선하시기 바랍니다.

또한 일괄작업의 내용, 작업자, 처리시간, 처리결과, 오류 및 조치내역 등의 이력을 관리하고 실행할 수 있는 도구를 도입하여 모든 일괄작업에 적용하고, 오류 발생시 발생 일시, 발생 내용(원인), 해결 내용 등을 기록한 오류관리대장을 작성하여 전자결재를 통한 관리자 승인 절차를 마련하는 등 업무처리 방안을 개선하시기 바랍니다.

(4) 비상대책 수립·운영 불합리

회사는 내규 △△△△를 마련하여, 업무연속성 적용범위를 회사와 관련된 금융서비스, IT인프라, 인력 등 직·간접적으로 관련된 모든 부분으로 정하고, 비상상황에도 회사의 비즈니스가 지속적으로 수행될 수 있도록 정보시스템에 대한 재해복구 및 업무연속성 확보대책을 마련하고 있다. 또한, 회사는 동 내규에 따라 주전산센터의 전자금융업무 관련 서버 등 전산장비를 이중화하여 운영하며 주전산센터와 재해복구센터를 이원화하여 각각 운영 중에 있다.

하지만, 주전산센터가 아닌 본사 사무공간 내 별도의 장소에서 설치·운영되고 있는 ■■■■시스템 등 회사의 경영지원과 관련된 일부 시스템에 대해

서는 주전산센터에 준하는 이중화·이원화가 되어 있지 않아, 실제 비상상황 발생시 업무연속성 확보가 어려워질 우려가 있다. 또한, ▲▲▲▲시스템의 재해복구 메뉴얼이 부재하는 등 재해복구계획이 일부 현행화되지 않아 재해복구목표를 달성하지 못할 우려가 있다. 뿐만 아니라, 주전산센터의 이중화된 회선 중 백업회선에 대해 일부 보안장비가 구성되지 않아 백업회선으로 전환되어 있는 동안 외부 위협에 노출될 수 있다.

한편 회사는 내규 ▽▽▽▽를 마련하여 비상시에 핵심업무의 백업자료를 활용하기 위해 백업관리대장을 통해 내용을 기록 관리하고 이를 정기적으로 검토하며, △△△△에 따라 비상대응훈련 중 재해복구 및 장애대응 훈련을 연 1회 실시하고 있고, 침해사고 대응·복구 훈련으로 연 1회 악성메일 모의훈련을 실시하고 있다.

하지만 회사는 DB 등의 백업자료를 활용한 복구 테스트는 주기적으로 수행하지 않고 있어서 외부의 침해공격(랜섬웨어 등)을 받아 데이터가 소실되는 경우 등 백업자료를 실제 업무에 활용해야 할 때 사전 테스트 부족으로 인해 복구목표시점을 준수하지 못할 우려가 있고, 비상대응훈련 종류에 웹시스템을 대상으로 한 DDoS공격대응훈련 등이 포함되어 있지 않아 다양한 외부 공격에 대응하기 위해서는 절차를 개선할 필요가 있다.

또한 회사는 내규 △△△△에 의거 재해·장애로부터 업무의 연속성을 확보하고 핵심 업무를 식별하기 위해 업무영향분석(BIA)을 실시하여 업무시스템을 크게 4가지(▼, ♠, ♥, ♣)로 분류하고 업무중요도 등의 기준으로 핵심업무를 선정하며 이를 「업무연속성계획」에 포함하였다.

하지만 업무연속성계획을 주관하는 인프라보안팀 외 협업부서의 참여가 부족하여 ★★★★ 웹시스템 등이 업무영향분석 대상에서 누락된 사례가 있는 등 세부 절차가 일부 미흡하다.

이에 따라 재해로 인해 해당 업무가 중단될 경우 복구목표시점(RTO)·복구목표지점(RPO) 등 업무영향분석 결과를 기반으로 수행하는 세부 복구절차가 부재하여 체계적으로 업무를 복구하지 못할 우려가 있다.

<조치할 사항>

따라서 회사의 경영지원과 관련된 시스템 등을 전산센터로 이전하거나 비상상황 발생시 적극 대응이 가능하도록 전산센터에 준하는 관리를 하고, 주전산센터(◈◈◈◈)의 백업회선으로 전환되는 상황을 고려하여 백업회선에 대한 보안을 강화하기 위해 침입방지시스템(IPS), 웹방화벽(WAF)을 설치·운영하며, 재해복구 메뉴얼을 적기에 현행화하시기 바랍니다.

또한 업무영향분석을 주관하는 인프라보안팀 외 협업부서가 함께 참여하여 다양한 시각을 고려하고, 단위업무를 재파악하여 대상에서 누락되는 업무가 없도록 절차를 개선하는 등 개선한 절차를 적용한 업무영향도분석을 재실시하여 「업무연속성계획」에 반영하시기 바랍니다.