경영유의사항 등 공개안

1. 금융회사명 : 산은캐피탈㈜

2. 제재조치일 : 2017. 8. 14.

3. 조치내용

대상	내 용
기관	경영유의사항 1건, 개선사항 3건

4. 조치대상사실

가. 경영유의사항

(1) 정보유출 방지대책 강화

A) 내부망과 외부망을 분리하고 있어 자료전송시 OOO 시스템을 이용하여 책임자 승인 후 자료를 전송하고 있으나,

OOO 관련 계정의 권한 부여 및 회수 절차가 마련되어 있지 않아 각부서의 부서장이 OOO의 승인권한을 임의로 부서원들에게 부여 및 회수가 가능하도록 운영하고 있어 책임자급이 아닌 직원의 승인만으로 외부로 자료유출이 가능하므로,

OOO 관련 계정의 권한 부여 및 회수 절차를 마련하고, 동 절차에 따라 내부통제담당자가 OOO 승인권한을 부여 및 회수 할 수 있도록 관련절차를 마련할 필요

B) 개인정보 유출 방지를 위해 OOO 시스템을 운영하고 있으며, PC에 파일을 저장시 개인정보가 검색될 경우 자동으로 해당파일을 중앙서버로 별도 격리처리하고 다시 PC로 다운로드시 책임자 승인을 받도록 하고 있으나,

파일에 OOO가 있는 경우만 개인정보가 검출될 수 있도록 설정되어 있고, 일부 개인정보가 포함된 파일이 미검출되거나 검출기준에 부합하지 않을 경우 책임자 승인 없이 파일 반출이 가능하며,

내부업무시스템을 통해 고객정보가 포함된 문서를 승인절차 없이 PC에 다운로드 및 화면 캡쳐가 가능하여 암호화되지 않은 고객 정보가 유출될 우려가 있으므로,

OOO의 검출기준에 OOO 등을 포함하고, 개인PC에 고객정보 보관시 암호화하여 저장 및 관리 하며, 내부업무시스템을 통한 고객정보 다운로드 및 화면캡쳐시 책임자 승인을 거치도록 하는 등 개인정보 유출 방지 대책을 강화할 필요

C) 불법 사이트 차단을 위해 유해사이트 차단 솔루션을 사용하고 있고, 메일 송수신을 위해 사내용 메일과 인터넷용 외부메일로 분리하여 사용하고 있으나,

메신저 기능이 있는 SNS 및 상용메일이 인터넷 PC에서 사용가능한 상태이고, 외부로 메일 발송시 본문내용 및 첨부파일에 개인정보를 검출하는 기능이 없어 승인되지 않은 개인정보 포함 파일이 외부로 반출될 우려가 있으므로,

불필요한 SNS기능 및 상용메일은 차단하고, 외부로 메일 발송시 개인정보포함 파일의 경우 책임자 승인을 거쳐 발송 될 수 있도록 절차를 개선할 필요

D) 출력물 보안을 위해 DRM을 도입·운영하여 좌측하단 출력물에 일자, 시간, 사번을 출력하고 있으며 고객업무 처리를 위해 OOO를 사용하고 있으나,

출력물 중앙에 워터마크가 없고 고객정보가 포함된 OOO 등의 파일을 책임자 승인 없이 OOO를 통해 송신 할 수 있는 등 출력물 통제가 미흡하므로,

출력물 중앙에 워터마크를 포함하고 OOO를 통해 고객정보가 포함된 문서를 발송할 경우 책임자 승인을 거치도록 절차를 마련할 필요

나. 개선사항

(1) 홈페이지 서버보안 강화

고객 대상으로 제공하는 산은캐피탈 카드 홈페이지는 웹(WEB) 서비스 구간에서 데이터 송수신 시 통신구간 암호화를 적용 하고 있으나

웹응용서버(WAS)를 DMZ구간에서 웹서버와 공동으로 운영하고 있어 외부 해킹으로 인한 웹응용서버의 침해사고 발생 시 정보유출의 위험이 있으므로

웹응용서버와 웹서버를 분리하여 웹서버는 중립구간(DMZ)에 배치하고 웹응용서버

(WAS)는 내부 네트워크에 배치하는 등 웹서버보안 대책을 강화할 필요

(2) 프로그램 개발 및 관리 절차 강화

회사내규인 OOO에 시스템 개발 및 프로그램 폐기 등의 절차가 정의되어 있으며, 프로그램 신규 개발 및 변경시 형상관리시스템을 통하여 프로그램 변경 전후 내역 등을 기록 관리를 하고 있으나

내규에 프로그램 개발, 변경, 테스트, 승인 등의 절차가 구체적으로 명시되어 있지 않아 업무수행이 일관되게 이루어지지 않고 있으므로

프로그램 변경절차, 개발자 테스트 및 업무소관부서(현업)테스트 결과 기록·관리, 프로그램 운영서버 배포절차, IT지원실 자체작업의 전산처리요청서 관리, 홈페이지 형상관리시스템 적용 등 프로그램 개발 및 변경 관련 내규를 개선하고 동 절차에 따라 프로그램을 개발 및 관리할 필요

(3) 데이터베이스 통제 및 변경 절차 강화

전산원장변경은 전산처리 작업요청서(PSR)를 접수 받아 처리하고 있으며, 데이터베이스에 대한 접근계정, 접근일시, 수정작업시 변경 전후내역 등을 기록하고 있으나,

OOO와 OOO가 하나의 주전산기에 구축되어 있어 OOO과 동일한 계정으로 OOO에 접근이 가능하고 OOO 명령어 실행권한이 세분화 되어있지 않아 권한별로 통제가 이루어지지 않고 있으며

여신원부 및 회계전표 등 전산원장 외에 OOO 등에 대한 데이터 변경 작업은 전산처리 작업요청서(PSR) 및 책임자 승인 등의 전산원장 변경절차를 적용하지 않고 담당자가 데이터베이스 변경문을 책임자 승인 없이 실행하고 있어 책임자가 데이터베이스 명령문 및 변경내역의 정당성 여부를 사전에 검증할 수 없으므로,

OOO과 OOO계정을 분리하여 관리하고, OOO명령어에 대한 권한을 세분화하며, 여신원부 및 회계전표 등 전산원장 외에 OOO 등에 대한 데이터 변경작업에 대해서도 전산원장 변경절차를 준수 할 수 있도록 변경작업 적용대상을 확대하고, 책임자 승인 후 OOO 변경문을 실행할 수 있도록 관련절차를 개선할 필요