Privacy Report 2018.01

SOMANSA

전자금융거래법고시 전자금융감독규정 2절~6절
〈전자금융거래의 안전성확보&이용자 보호규정〉①

2016.10월 개정시행 전자금융감독규정 원문보기 | 2017. 5월 발간 전자금융감독규정 해설서 원문보기

적용대상 〈금융회사〉 〈전자금융업자〉의 모든 〈전자금융거래〉

〈전자금융거래〉

〈금융회사〉 or 〈전자금융업자〉가 전자적장치로 금융상품제공 & 이용자가 〈금융회사〉 or 〈전자금융업자〉 종사자와 대면or의사소통 없이 자동화거래

〈전산자료〉 중 중요정보는 개인정보(특히 고유식별정보, 개인신용정보)

전자금융거래에 사용하는 모든 데이터 〈전산자료〉

금융회사

전자금융업자

핀테크, 비트코인 등 금융플랫폼이 혁신되면서 범위 확대 중

(법적인 정의)
전자화폐, 전자자금이체, 직불전자지급수단, 선불전자지급수단 전자지급결제대행업자 등

전자금융보조업자 (전자금융거래의 수탁자) (동일한 안전조치 기준 적용)

전자금융거래와 관련하여 전자금융보조업자의 고의나 과실은 금융회사 or 전자금융업자의 고의나 과실로 본다.

▣ 금융회사 및 전자금융업자와 직접 계약을 체결하고 관련된 업무를 수행하는 사업자는 전자금융보조업자로 분류하여야 하나

- 이들 사업자와 재위탁 계약을 체결한 사업자들 중 전자금융거래와 직접적인 관련이 없는 단순 콜센터, DM 발송 업체 등은 제외
- 내부에 상주하지 않는 콜센터, 쇼핑몰, 외부통신회선 관리, IDC 등도 전자금융보조업자의 범위에 포함되지 않음

서비스 형태	주요업체
VAN사업자	KICC, KSNet, KMPS 등
ATM관리 아웃소싱업체	NICE, 한네트, 웹캐시, 노틸러스효성 등
자금이체대행 PG	금융결제원 등
전자고지납부업체	한국인터넷빌링, 금융결제원 등
결제중계시스템 운영자	금융결제원, 한국예탁결제원 등
공동수탁기관	KOSCOM, 저축은행중앙회 등

출처) 전자금융감독규정 해설서 18page

전체구성

2절. 인력조직예산 (8)
인력&조직운용(5) 인력&예산(2) 인력&예산규정 미이행시 공시규정(1)

3절. 시설 (25)
건물(6) 전원 공조 등 설비(7) 전산실(12)

개인정보 중심규정

4절. IT부문 (69)
단말기보호(4) 전산자료보호대책(20) 〈정보처리시스템〉보호대책(10) 비중요〈정보처리시스템〉보호대책(5) 해킹등방지대책(11) 악성코드감염방지대책(4) 공개용웹서버관리대책(10) IP주소관리대책(5)

5절. IT부문 내부통제 (72)
계획서(2) 교육(3) 계약(9) 감리(4) 비상대책(10) 비상대응훈련(3) 성능관리(1) 직무분리(8) 전산원장통제(5) 거래통제(2) 프로그램통제(10) 일괄작업에 대한 통제(5) 암호프로그램&키관리통제(2) 내부사용자PW관리(3) 이용자PW관리(5)

6절. 전자금융업무 (18)
전자금융거래(5) 이용자주의사항공지(4) 자체보안성심의(8) 인증방법사용기준(1)

전자금융거래법고시 전자금융감독규정 2절~6절

〈전자금융거래의 안전성확보&이용자 보호규정〉의 4대 의의

의의 1 가장 기술중심적인 법으로 금융플랫폼혁신의 중심이 되는 법

핀테크, 인터넷은행, 비트코인, 월렛, 간편결제, 크라우드펀딩 등 금융플랫폼이 혁신되면서 전자금융거래의 범위가 확대

전자금융업무의 범위는 전자금융거래의 대중화, 다양화 및 이용자 보호 등을 고려할 때 광의의 개념으로 보는 것이 타당함

- 따라서 인터넷을 통한 신용정보, 자산보유 또는 거래내역 조회 서비스 제공도 전자금융업무에 해당함

출처) 전자금융감독규정해설서 10page

의의 2 가장 구체적으로 CEO의무, 조직, 예산을 규정

〈CEO의무〉
임직원의 보안법규 위반시 제재기준 & 절차를 마련,운영
정보보호위원회의 심의 · 의결사항을 준수

〈조직〉 IT인력은 총 임직원 수의 100분의 5 이상, 정보보호인력은 IT인력의 100분의 5 이상

〈예산〉 정보보호예산은 IT부문예산 100분의 7 이상

의의 3 세계금융의 메카 뉴욕의 금융규정 〈NYCRR500〉보다 10년을 선도

2007.1.1 시행 전자금융거래법		2017.3.1 시행 NYCRR500
금융기관 & 전자금융업자 & **수탁자**	적용대상	뉴욕주 모든 금융기관 & **제3자 제공자**
전자금융거래에 사용되는 **데이터및 데이터가 포함된 정보시스템**	보호대상	금융거래에 사용되는 **데이터 및 데이터가 포함된 정보시스템**
개인정보를 포함한 〈전산자료〉로 광범위	보호데이터	**개인정보를 포함한 〈비공개정보〉로 광범위**
금감원 , 금융위의 감사	사전규제	〈보안준수확인서〉를 뉴욕금융감독기관에 제출

의의 4 개인정보 측면에서 라이프사이클에 따른 〈현황파악〉 〈접근통제& 접속기록관리〉 〈유출통제〉를 가장 중시한 법

개인정보 중심규정

제4절. IT부문 (69)
단말기보호(4) 전산자료보호대책(20) 〈정보처리시스템〉보호대책(10) 비중요〈정보처리시스템〉보호대책(5) 해킹등방지대책(11) 악성코드감염방지대책(4) 공개용웹서버관리대책(10) IP주소관리대책(5)

데이터

전자금융감독규정의 데이터 〈전산자료〉 보호대책(20)
정의) 전산장비에 의해 입력 · 보관 · 출력된 자료, 자료가 입 · 출력된 〈매체〉를 포함

데이터가 포함된 정보 시스템

DB,서버단 — 엔드포인트 — 네트워크

〈정보처리시스템〉보호대책(10)

〈비중요정보 처리시스템〉보호대책(5)

단말기 보호규정(4)

해킹 등 방지대책(11)
악성코드 감염방지대책(4)
공개용웹서버 관리대책(10)
IP주소 관리대책(5)

가장 개인정보와 밀접한 규정
1페이지로 보는 4절 IT부문 of 〈전자금융거래의 안전성확보&이용자 보호규정〉

핵심은 라이프사이클에 따른 데이터
〈현황파악〉〈접근통제 & 접속기록관리〉〈유출통제〉

전산자료

현황파악

〈전산자료〉 보유현황관리
&책임자 지정 · 운영

중요도에 따라
〈전산자료〉 정기백업

접근통제 & 접속기록관리

〈전산자료〉 입력 · 출력 · 열람시 접근권한 통제

외부자에게 ID 부여시 최소권한 할당 & 통제장치

ID,PW개인별 부여,
〈전산자료〉 등록 · 변경 · 폐기를 체계적관리

유출통제

〈전산자료〉 & 전산장비의
반출 · 반입을 통제

전산자료가 포함된 정보시스템

DB, 서버단	엔드포인트	유출경로(네트워크,매체, 출력물)

현황파악

〈정보처리시스템〉

〈정보자산중요도평가기준〉수립

→〈중요정보처리시스템〉 지정
(고유식별정보와 개인신용정보가 있는 경우
〈중요정보처리시스템〉임)

→〈중요정보처리시스템〉 내역은
정보보호위원회심의를 거쳐
금감원에 제출

〈단말기〉

〈중요단말기〉지정, 보호대책강화

단말기에 이용자정보 등
주요정보 보관금지
(불가피할 경우 보관사유,
기간&PW 등을 책임자승인)

〈공개용웹서버〉

DMZ구간내에 이용자정보 등
주요정보 저장 & 관리금지
(거래로그 관리목적시
예외로 하되 반드시 암호화저장)

접근통제 & 접속기록관리

〈정보처리시스템〉

〈정보처리시스템〉 가동기록은
1년 이상 보존,
접속성공여부와 상관없이
다음 자동기록 · 유지
1.〈정보처리시스템〉접속일시, 접속자 & 접근을 확인할 수 있는 접근기록
2.〈전산자료〉사용일시, 사용자 & 자료의 내용을 확인할 수 있는 접근기록
3.〈정보처리시스템〉내 〈전산자료〉처리내용을 확인할 수 있는 로그인, 액세스로그 등 접근기록

(5회 내에서) 규정이상의 접속오류시
〈정보처리시스템〉 접속제한

이용자중요원장에
직접 접근/조회/수정/삭제/삽입시
작업자 & 작업내용을 5년보존

〈단말기〉

단말기를 통한
이용자정보 조회시
다음을
〈정보처리시스템〉에
자동기록&
1년이상 보존

사용자, 사용일시,
변경 · 조회내용,
접속방법

〈유해사이트〉

단말기에서 음란, 도박 등 비업무프로그램 or 인터넷접근에 대한 통제대책 마련

내부 · 외부 IP의 인터넷 접속내용을 1년 이상 별도로 기록 · 보관

유출통제(출력물 매체)

단말기에서 〈매체〉 & 휴대용전산장비
접근을 통제(유출, 악성코드 방지목적)

〈전산자료〉 출력시 접근권한통제

망분리 예외상황시 단말기와 네트워크보안을 강화해야 함

망분리 대체

단말기보안강화

단말기 〈전산자료〉
암호화 저장

PC사용자의
관리자권한 제거,
승인된 프로그램만
설치/실행토록
대책수립

메일보안강화

메일을 통한
〈전산자료〉 외부전송시
정보유출탐지/차단/
사후모니터링 수립

본문과 첨부파일 포함하여
메일을 통한
악성코드 감염 예방 대책

외부망보안강화

외부망을 통한
〈전산자료〉 외부전송시
정보유출탐지/차단/
사후모니터링 수립

지능형 해킹(APT)
차단대책 수립

원격접속통제

원격접속시

모든 작업내역 기록
매일 이상여부 점검
책임자가 확인실행

Privacy Report 2018.01

SOMANSA

전자금융거래법고시 전자금융감독규정 2절~6절
〈전자금융거래의 안전성확보&이용자 보호규정〉②

2016.10월 개정시행 전자금융감독규정 원문보기 | 2017. 5월 발간 전자금융감독규정 해설서 원문보기

전체구성

제2절. 인력조직예산 (8)
인력&조직운용(5) 인력&예산(2) 인력&예산규정 미이행시 공시규정(1)

제3절. 시설 (25)
건물(6) 전원 공조 등 설비(7) 전산실(12)

개인정보 중심규정

제4절. IT부문 (69)
단말기보호(4) 전산자료보호대책(20) 〈정보처리시스템〉보호대책(10) 비중요〈정보처리시스템〉보호대책(5)
해킹등방지대책(11) 악성코드감염방지대책(4) 공개용웹서버관리대책(10) IP주소관리대책(5)

제5절. IT부문 내부통제 (72)
계획서(2) 교육(3) 계약(9) 감리(4) 비상대책(10) 비상대응훈련(3) 성능관리(1)
직무분리(8) 전산원장통제(5) 거래통제(2) 프로그램통제(10) 일괄작업에 대한 통제(5)
암호프로그램&키관리통제(2) 내부사용자PW관리(3) 이용자PW관리(5)

제6절. 전자금융업무 (18)
전자금융거래(5) 이용자주의사항공지(4)
자체보안성심의(8) 인증방법사용기준(1)

4절 IT부문

조	전자금융감독규정 내용	전자금융감독규정 해설서 내용		기술적 보호조치
12조 단말기 보호 대책	1. 업무담당자 이외 사람이 단말기를 무단으로 조작하지 못하도록 조치	단말기 접근통제	로그인 PW 설정	
			일정시간 사용중지시 화면보호기능 설정 & PW 재입력,	Privacy-i
			취급자 지정	
	2. 〈정보처리시스템〉 접속단말기에 대해 정당한 사용자 여부를 확인할 수 있는 기록유지	〈정보처리시스템〉 사용자의 정당성 확인을 위해 사용자인가 정보조회가 가능하도록 조치		DB-i
	3. 〈강화된 보호대책〉이 적용되는 〈중요단말기〉지정	〈중요단말기〉 : 〈정보처리시스템〉 or DB에 직접 접근가능한 단말기		Privacy-i
		〈강화된 보호대책〉 : 외부반출금지, 인터넷접속금지, 그룹웨어접속금지		망분리 WebKeeper
	4. 단말기에서 〈매체〉 & 휴대용 전산장비 접근을 통제 (유출, 악성코드방지목적)	외주개발직원의 단말기에도 동일수준의 접속통제를 적용		Privacy-i (Media Control)
		용도에 따라 USB 쓰기/읽기 기능 차단		
		USB 사용시 책임자의 사전 승인		
		보안 정책에 따른 USB 관리 기록		

제4절 IT부문

조	전자금융감독규정 내용		전자금융감독규정 해설서 내용		기술적 보호조치
13조 전산자료 보호 대책	① 전산자료의 유실파괴 방지	1. ID, PW를 개인별로 부여, 등록 · 변경 · 폐기를 체계적관리	퇴직, 계약종료시 사용자계정 삭제 삭제가 불가능할시 PW & 실사용자 이름변경		
			모든 계정은 실사용자가 확인될 수 있도록 등록관리, 변경내용 세부내역을 기록관리		
		2. 외부사용자 ID 부여시 최소권한 할당& 적절한 통제장치	계약종료시 해당시스템 접속이 차단되도록 통제장치마련		DB-i WAS-i App-i Privacy-i Server-i
		3. 〈전산자료〉 보유현황관리 책임자 지정 · 운영	-	• 권한구분 (읽기쓰기변경삭제등) • 권한에 따라 접근자료 한정 • 〈중요자료〉 변경삭제권한은 최소한 부여	
		4. 〈전산자료〉의 입력 · 출력 · 열람시 사용자 업무별로 접근권한을 통제	고객정보 & 금융거래 정보에 대한 조회는 업무상 관련성이 없는 경우에는 엄격히 제한		
		5. 〈전산자료〉 & 전산장비의 반출 · 반입을 통제	반출입사항을 기록관리		
			반출된 〈전산자료〉는 목적외사용이 되지 않도록 함		
			반출된 〈전산자료〉는 사용완료 후 즉시 회수 or 파기조치		
			노트북 or PC 반출시, 〈중요자료〉수록여부 확인		
			외부반입 PC or 보조기억장치 내에 악성코드, 해킹프로그램 수록여부 확인		
		6. 비상대비, 〈전산자료〉 안전지출& 긴급파기계획 수립 · 운용	〈매체〉는 보유현황, 사용자, 사용용도 등 파악을 위해 관리대장으로 관리		Privacy-i
		7.정기적으로 〈매체〉 보유현황 & 관리실태를 점검하고 책임자 확인	〈매체〉 파기는 매체에 수록된 정보의 복구가 불가능하도록 완전 파기 조치함		
		8. 중요도에 따라 〈전산자료〉를 정기백업, 원격 안전지역에 소산, 백업내역을 기록 · 관리	(전산센터시스템의) 데이터 & 프로그램이 완전파괴된 경우에도 시스템 정상복구가 가능한 수준으로 백업 & 관리		
			백업자료(매체)는 식별이 용이하도록 보유현황관리		
			전산센터로부터 원격지에 보관		
			법을 고려하여 소산대상 & 보존기간 결정 프로그램&시스템프로그램과 관련문서(매뉴얼,설계서)포함		
			소산장소는 환경유지&정기점검 및 접근통제 필요		
		9. 주요 백업 〈전산자료〉정기검증	주요 백업 〈전산자료〉는 비상사태 발생시 복구를 위해 사용될 수 있도록 〈전산자료〉의 무결성 등을 정기적으로 점검		
		10. 이용자정보 조회 출력 통제 — 테스트시 이용자정보 사용금지	-	법인인 이용자정보는 테스트목적, 기간, 정보항목 등을 사전고지 후 동의얻어 사용가능	Privacy-i Server-i DB-i
		10. 이용자정보 조회 출력 통제 — 사용이 불가피한 경우 (부하테스트 등) 변환사용& 테스트종료시 즉시삭제	고객인적사항, 금융거래정보 등 이용자정보가 포함된 조회나 출력시 이용자가 노출되지 않도록 이용자식별정보를 통제 (마스킹 등)		

제4절 IT부문

<table>
<tr><th>조</th><th colspan="3">전자금융감독규정 내용</th><th>전자금융감독규정 해설서 내용</th><th>기술적
보호조치</th></tr>
<tr><td rowspan="8">13조

전산
자료
보호
대책</td><td rowspan="4">①

전
산
자
료
의

유
실
파
괴

방
지</td><td>11.
〈정보처리
시스템〉
가동기록
1년 이상
보존</td><td colspan="2">● 계정계, 정보계, 업무서버, 네트워크 장비 등 정보처리시스템의 가동기록3)은 전산기기의 가동, 업무처리와 관련하여 주전산기 또는 서버에 접속한 일시, 접속자 및 접근을 확인할 수 있는 접근 기록과 전산자료를 사용한 일시, 사용자 및 자료의 내용 등을 확인할 수 있는 접근 기록 등이 자동기록 되도록 하고 1년 이상 보존(제1항 제11호, 제4항)
– (예) 시스템 로그, 콘솔로그 등

3) 시스템 가동기록은 시스템이 최초 가동된 시각, 시스템 자원(CPU, 메모리, 디스크 등) 상태기록, 시스템 장애상태 등을 확인할 수 있는 기록을 의미하고, 접근기록은 정보시스템에 사용자가 접근한 기록으로 접근시간, 접근ID, 접근IP, 작업내용, 처리결과 등을 의미
출처) 전자금융감독규정 해설서 18page</td><td rowspan="8">DB-i
WAS-i
App-i</td></tr>
<tr><td colspan="2">12. 5회 내 범위에서 횟수 이상의
접속오류 발생시
〈정보처리시스템〉 접속제한</td><td>〈정보처리시스템〉 접속에 실패한
접근시도 기록유지

5회이내 반복발생시
시스템사용을 제한하고 중점점검</td></tr>
<tr><td colspan="2">13. 단말기에 이용자정보 등
주요정보 보관금지
(불가피 할 경우 보관사유,기간,
관리PW 등을 정하여
책임자승인을 거쳐 보관).

단말기 공유금지</td><td>이용자정보가 없는 단말기도
이용자 정보보다 넓은 개념인
〈전산자료〉보호를 위해 공유금지</td></tr>
<tr><td colspan="2">14. 전출 · 퇴직 등 인사조치시 지체없이
계정 삭제, 사용 중지, 공동계정 변경</td><td>이전 계정&권한으로 〈정보처리시스템〉에
접속할 수 없도록 통제</td></tr>
<tr><td colspan="3">② ID 공동사용이 불가피할 경우
개인별사용내역을 기록 · 관리</td><td>공동사용계정(예: UNIX의 “root)은
추후에 추적&확인할 수 있도록
사용자 IP, 접근시간 등
개인별사용내역을 기록유지</td></tr>
<tr><td colspan="3">③ 단말기를 통한 이용자정보 조회시 사용자,
사용일시, 변경 · 조회내용, 접속방법을
〈정보처리시스템〉에 자동기록 & 1년 이상 보존</td><td>추후에 추적&확인이 가능해야 함</td></tr>
<tr><td colspan="2">④ 〈정보처리시스템〉
가동기록시
접속성공과
상관없이
다음을 자동기록</td><td>1. 〈정보처리시스템〉 접근기록 :
접속일시, 접속자 및 접근을 확인할 수 있는 접근기록
2. 전산자료 접근기록 : 전산자료를 사용한 일시,
사용자 및 전산자료의 내용을 확인할 수 있는 접근기록
3. 〈정보처리시스템〉 내 전산자료의 처리 내용을 확인할 수
있는 접근기록 : 사용자 로그인, 액세스로그 등</td><td></td></tr>
<tr><td colspan="3">⑤ 〈정보처리시스템〉관리자 대상
적절한 통제장치 마련/운용
(책임자가 이중확인&모니터링)</td><td>〈정보처리시스템〉 관리자가
전산원장, 이용자정보 등 주요정보가 저장된
〈정보처리시스템〉에 대한 중요작업 수행시
책임자가 이중확인
&작업수행내역 정기적 모니터링</td></tr>
</table>

제4절 IT부문

조	전자금융감독규정 내용	전자금융감독규정 해설서 내용	기술적 보호조치
14조 정보처리시스템 보호대책	1. 운영매뉴얼 작성 (구동, 조작방법, 명령어사용법, 운용순서, 장애조치 & 연락처 등)	〈정보처리시스템〉 & 주요프로그램에 대한 운영매뉴얼을 지정장소(전산실 & 재해복구센터)에 보관 & 관리	
		〈정보처리시스템〉 & 프로그램 등 주요프로그램 변경시 최신상태 유지	
	2. 유지보수 정기실시(DBMS · OS · 웹프로그램 등 주요 프로그램 대상) 〈유지보수관리대장〉 작성 · 보관 (작업일, 작업내용, 작업결과 등 기록)	〈정보처리시스템〉 & 주요 프로그램(DBMS, 운영체제, Web & WAS 서버 등)은 장애 예방을 위해 정기적으로 유지보수	
		외부업체가 유지보수시 중요정보가 유출되지 않도록 주의하고 유지보수 내용을 기록한 유지보수 관리대장을 작성보관	
	3. 〈장애상황기록부〉 작성 · 보관 (장애일시, 장애내용 & 조치사항 등)	〈정보처리시스템〉의 장애예방을 위해 시스템의 모든 장애 발생은 장애상황기록부에 기록관리	
	4. 〈정보처리시스템〉 정상작동여부 확인을 위한 모니터링시스템 구축 (자원상태의 감시, 경고 & 제어)	시스템의 정상작동여부 확인이 가능하도록 시스템의 자원 상태를 감시하고, 장애 등 이상징후 발생시 경고 & 제어가 가능한 모니터링시스템을 구축	
	5. 시스템 통합, 전환 & 재개발 통제절차 준수	통합,전환, 재개발시 〈정보처리시스템〉 운영에 지장을 초래하지 않도록 사전검증을 실시하는 등 통제절차를 마련하여 운영	
	6. 〈정보처리시스템〉 책임자 지정 · 운영	〈정보처리시스템〉 책임자는 해당 〈정보처리시스템〉에 문제가 발생하지 않도록 운영, 유지보수, 보안관리 등의 시스템 관리업무 총괄	
	7. 긴급&중요 패치사항 (운영체계, 시스템 유틸리티 등)은 즉시 패치실행	〈정보처리시스템〉책임자는 주요SW에 대한 patch발표여부를 주기적으로 확인 →발표시 테스트시스템에 우선 적용 →운영에 지장을 초래하지 않을 경우 즉시 실운영시스템에 적용	
	8. OS & 설정내용 등을 정기백업, 원격 안전지역에 소산, 백업자료는 1년 이상 기록 · 관리	비상시 신속하게 정상복구가 가능하도록 〈정보처리시스템〉의 OS & 설정내용 등을 정기적으로 백업, 원격안전지역에 소산, 백업자료는 정기적검증을 실시하며 1년 이상 보관	
	9. OS 계정으로 로그인시 계정 & PW 이외에 별도의 추가인증 시행	〈정보처리시스템〉의 OS 계정에 대한 보안강화를 위하여 로그인시 계정 & 비밀 번호 이외의 별도 안전한 추가인증 절차를 반드시 시행하고, OS 계정의 작업 수행에 대한 이상징후 발생시 필요한 통제 조치가 즉시 시행될 수 있도록 모니터링 체계수립	
	10. OS계정 사용권한, 접근기록, 작업내역 상시 모니터링체계 수립. 이상징후 발생시 통제조치 즉시 시행		
14조의2 비중요정보처리시스템 지정	① 〈정보자산중요도 평가기준〉 자체수립 후 〈비중요정보 처리시스템〉 지정	〈비중요정보 처리시스템〉으로 지정가능한 경우: 클라우드컴퓨팅 등을 이용하기 위하여 고유식별정보 &개인신용정보를 제외한 정보를 처리하는 시스템	Privacy-i Server-i
		〈비중요정보 처리시스템〉으로 지정가능한 경우: 고유식별정보와 개인신용정보를 비식별화조치한 경우	
		〈비중요정보 처리시스템〉 지정시 적용되지 않는 규정(제11조제11호 & 제12호, 제15조제1항제5호) & 전자금융감독규정시행세칙 제2조의2(망분리 예외 적용시) 등을 모두 준수할 경우 비중요〈정보처리시스템〉의 지정 없이 클라우드컴퓨팅 서비스 이용이 가능	
	② 〈비중요정보 처리시스템〉 지정시 (제8조의2에 따라) 〈정보보호위원회〉의 심의 · 의결을 거침		
	③ 〈비중요정보 처리시스템〉 지정일로부터 7일 이내에 〈보고서〉 (정보자산중요도 평가기준, 지정 결과, 관리 방안 등을 포함) 를 금감원에 제출		
	④ 금감원장은 〈보고서〉 검토결과, 적합하지 않다고 판단되는 경우에는 개선 · 보완을 요구할 수 있다.		
	⑤ 〈비중요정보 처리시스템〉만 위치한 전산실은 전산실관련규정(11조 11호 & 12호, 15조 1항 5호) 비적용	전산실 & 재해복구센터의 국내 설치(제11조제11호), 무선통신망의 설치 금지 (제11조제12호) & 전산센터 물리적망분리(제15조제1항제5호) 규정의 적용을 받지 않을 수 있음	

제4절 IT부문

조	전자금융감독규정 내용, 전자금융감독규정해설서내용 (이하 [해]), 전자금융감독규정시행세칙내용 (이하 [시])		기술적 보호조치
15조 해킹등방지대책	① 〈정보처리시스템〉& 정보통신망 해킹방지	1. 해킹사고방지를 위한 〈정보보호시스템〉 설치 & 운영 [해] 침입차단&탐지, 암호화프로그램 등 정보보호시스템을 설치 & 운영 대내외에서 〈정보처리시스템〉접속시 정보보호시스템을 우회접속하지 못하도록 보안정책적용	
		2. 해킹대비〈정보보호시스템〉프로그램은 긴급&중요패치에 대하여 즉시 패치 [해] 시스템프로그램의 보안취약점개선 등 긴급하고 중요한 사항은 즉시 보정작업 실시	
		망분리 예외 1 **본점, 영업점 단말기** 3. 내부통신망과 연결된 내부업무용시스템은 외부망과 분리・차단 [시] 2조의 2① 업무상 특정 외부기관과 연결시 포트를 한정 [해] 내부통신망과 연결된 본점 영업점 PC,프린터 등 주변 기기는 물리적 or 논리적 망분리 업무상 불가피한 경우 내부망의 서버에서 특정 외부기관과의 연결가능	망분리 대체 정보보호 통제
		4. 내부통신망 파일 배포기능은 통합 & 최소화운영, 배포시 무결성검증 수행	
		망분리 예외2 5. 전산실내 〈정보처리시스템〉과 〈정보처리시스템〉에 직접 접속하는 중요단말기는 외부망과 물리적분리 **중요단말기** 하단 〈중요단말기〉 망분리 예외규정 전자금융 감독규정 시행세칙 2조의 2 참고	망분리 대체 정보보호 통제
	② 〈정보보호시스템〉 설치 운영시 준수사항	2. 최소한의 Port와 기능만을 적용, 업무목적외 기능 & 프로그램 제거	
		3. 〈보안정책 승인,적용,등록, 변경, 삭제이력〉을 기록・보관	
		4. 원격관리금지. 불가피한 경우 전용회선(VPN 포함)사용, 〈원격접속보안대책〉 수립・운영	
		5. 〈정보보호시스템〉 작동상태를 주기적 점검	
		6. 시스템 장애, 가동중지 등 긴급사태에 대비하여 〈백업 & 복구절차〉 등을 수립・시행	

전자금융감독규정 해설서 내용

망분리 대체 정보보호 통제		기술적 보호조치
메일시스템 보안	메일을 통한 〈전산자료〉 외부전송 시 정보유출 탐지,차단,사후 모니터링 대책 수립	Network DLP
	본문과 첨부파일 포함하여 메일을 통한 악성코드 감염 예방 대책 수립	
외부망 보안	외부망을 통해 〈전산자료〉 외부전송 시 정보유출 탐지, 차단, 사후 모니터링 대책 수립	Network DLP
	지능형 해킹(APT)차단 대책 수립	
단말기 보안	PC 사용자의 관리자 권한 제거 – 승인된 프로그램만 설치,실행토록 대책 수립	
	단말기 전산 자료 암호화 저장	Privacy-i
원격접속통제	원격접속 기준 및 절차가 포함된 보안정책 수립	
	불법 원격접속을 방지하기 위한 사용자인증, 암호화 등의 보안대책을 수립	
	원격접속은 승인받은 사전 등록자에 한하여 허용하며 원격접속관리기록부를 기록보관	WebKeeper
	원격에서 접속하는 외부 단말기와 내부 업무용 시스템 구간의 암호화 통신	
	원격접속 사용자는 ID,PW 이외에 추가 인증수단을 적용	
	원격에서 접속하는 외부 단말기의 악성코드 감염 예방 대책 수립적용	
	원격접속 가능한 내부 업무용시스템의 접근통제 수립적용	
	원격접속하여 수행한 모든 작업 내역 기록하고 매일 이상여부 점검 실시 및 책임자가 확인	WebKeeper

〈중요단말기〉 망분리 예외규정 전자금융 감독규정 시행세칙 2조의 2

1. 정보처리업무를 국외 전산센터에 위탁처리시, 국외소재 전산센터는 물리적 망분리 이외 방법으로 망분리 가능	
2. 업무상 외부통신망과 연결이 불가피한 다음의 정보처리시스템 (필요한 포트에 한하여 연결)	가. 전자금융업무의 처리를 위하여 특정 외부기관과 데이터를 송수신하는 정보처리시스템
	나. DMZ구간 내 정보처리시스템과 실시간으로 데이터를 송수신하는 내부통신망의 정보처리시스템 [해] DMZ내 인터넷뱅킹 등 공개서버(Web서버)와 내부서버(WAS) 연결
	다. 다른 계열사와 공동으로 사용하는 정보처리시스템 [해] 계열사와 공동사용하는 인트라넷, 이메일, 회계시스템과 내부서버연결
3. 전자금융감독규정 23조의 비상대책에 따라 원격 접속이 필요한 경우 비상시 제한적으로 외부망에서 내부망으로 원격 접속 가능	
4. 전산실 내에 위치한 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기와 외부통신망과의 연결구간	

특정 외부기관의 범위

- 행정안전부, 금융협회, 금융결제원, 예탁결제원, 코스콤, 금융보안원, 공인인증기관 등의 정부 또는 금융 유관기관
- 그 외 업무상 연결이 필요한 전자금융보조업자

제4절 IT부문

조	전자금융감독규정 내용		전자금융감독규정 해설서 내용	기술적 보호조치
16조 악성코드 감염 방지 대책	① 악성코드 감염방지대책 수립・운용 1. 응용프로그램 사용시 악성코드검색 프로그램 으로 진단 & 치료 후 사용 2. 악성코드 검색 & 치료프로그램은 최신상태유지 3. 악성코드 감염대비 복구절차를 마련 4. 〈중요단말기〉는 감염여부 매일 점검		- 출처, 경로,제작자가 불명확한 응용프로그램은 진단 후 사용 - 필요시 악성코드검색서버 설치, 외부메일 사전검색체계 구축 - 단말기,서버군의 감염여부 정기점검 실시 & 기록 보관 - 악성코드 검색프로그램의 정기적업데이트 예약설정 - 실시간 감시 기능을 이용하여 〈정보처리시스템〉 보호	백신 WebKeeper
	② 악성코드 감염 발견시 확산 및 피해 최소화를 위하여 필요한 조치를 신속하게 취하여야 한다		- 악성코드 감염신고 연락체계 구축 - 악성코드감염시스템의 사용중지 or 내부망에서 분리 - 악성코드 검색 & 치료 프로그램을 이용하여 악성코드 치료 - 확산방지를 위해 사용자에게 관련사실 &보안조치 즉시 전달 - 감염재발방지를 위해 원인분석 & 예방조치 수행	
17조 〈공개용 웹서버〉 관리 대책	① 대책	1. 내부통신망과 분리, "DMZ구간"에 설치, 네트워크 & 웹접근제어 실시	외부 유해트래픽이 웹서버를 경유해서 내부네트워크로 침입이 불가능하도록 침입차단시스템 구성	
		2. 업무관련자만 접속할 수 있도록 제한, ID・PW 이외에 추가인증수단 적용		
		3. 제공서비스를 제외한 다른 서비스 & 시험/개발 도구 등의 사용을 제한	웹서버에 반영하기 위한 프로그램 변경, 수정,테스트는 반드시 별도 개발,테스트서버에서 실시	
		4. DMZ구간내에 이용자 정보 등 주요정보 저장 & 관리금지 (거래로그 관리목적시 예외로하되 반드시 암호화저장)		WAS-i Server-i
	② 게재내용	1. 게시자료에 대한 사전 내부통제 실시	업무종류, 내용 등에 대하여 포괄적으로 적용 게시자료의 개인정보포함여부에 대한 내부통제절차 실시	
		2. 무기명 or 가명에 의한 게시 금지	책임관계 명확화	
		3. 홈페이지 자료게시 담당자 지정・운용	자료게시는 지정된 담당자로 제한	
		4. 개인정보 유출 & 위/변조방지 보안조치	개인정보 등 중요정보가 유출, 위변조 되지 않도록 게시기간만료정보 삭제 개인식별정보는 마스킹하여 게재, 화면위변조방지조치	Server-i
	③ 삭제			
	④ 〈공개용 웹서버〉가 해킹공격에 노출되지 않도록 대응조치		주기점검, 대응조치 마련하여 비인가자접근 or 서버내 고객정보 유출 & 웹서버의 비정상적인 동작을 야기하는 공격에 대응	
	⑤ 단말기에서 음란, 도박 등 비업무프로그램 or 인터넷접근에 대한 통제대책 마련		직원들이 단말기로 음란, 도박 등 업무와 관련이 없는 인터넷 사이트에 접근할 경우 동 사이트를 통하여 스파이웨어, 바이러스 등 악성코드에 감염되고 내부 통신망을 통해 조직 내에 전파될 우려가 있으므로 불필요한 사이트의 접근통제대책을 강구	WebKeeper

제4절 IT부문

조	전자금융감독규정 내용		전자금융감독규정 해설서 내용	기술적 보호조치
18조 IP 주소 관리 대책	대책	1. 내부통신망은 사설IP주소 사용 등으로 보안강화, 내부 IP주소 체계의 외부유출금지	사설주소체계를 사용하고, 공인IP를 제외하여 구성. 외부접속시 NAT기능으로 사설주소체계를 공인주소로 변환	
		2. 개인별로 내부IP주소를 부여하여 유지・관리	반드시 개인별로 부여, 가능한 고정IP를 부여. 업무담당자가 개인별로 IP를 부여하고 개인별 IP 부여 & 변경현황을 기록관리할 경우 DHCP방식도 가능	
		3. 내부・외부 IP의 인터넷접속내용을 1년 이상 별도로 기록・보관	내부직원이 인터넷접속시 기록보관항목 접속일시, 출발지 & 목적지 IP, 접속포트(Port), 사설IP 주소 등	WebKeeper
		4. 업무 (예 〈정보처리시스템〉 운영, 개발, 외부직원) 별로 네트워크를 분리하여 IP사용. (네트워크분리가 어렵다고 금감원장이 정하는 경우에 한해) 업무별로 접근권한을 분리하여 IP 사용가능	각 네트워크별 업무특성에 따른 적절한 접근권한 통제 등 보안정책을 적용하여 보안 강화	
		5. 내부통신망은 다른 기관 내부통신망과 분리하여 사용	다른 기관이 침입차단시스템을 우회하여 금융회사 & 전자금융업자의 내부망에 접속하는 것 금지	

전자금융감독규정 항목보기

제2절. 인력조직예산 (8)
인력&조직운용(5) 인력&예산(2) 인력&예산규정 미이행시 공시규정(1)

제3절. 시설 (25)
건물(6) 전원 공조 등 설비(7) 전산실(12)

제4절. IT부문 (69)
단말기보호(4) 전산자료보호대책(20) 〈정보처리시스템〉보호대책(10) 비중요〈정보처리시스템〉보호대책(5)
해킹등방지대책(11) 악성코드감염방지대책(4) 공개용웹서버관리대책(10) IP주소관리대책(5)

제5절. IT부문 내부통제 (72)
계획서(2) 교육(3) 계약(9) 감리(4) 비상대책(10) 비상대응훈련(3) 성능관리(1)
직무분리(8) 전산원장통제(5) 거래통제(2) 프로그램통제(10) 일괄작업에 대한 통제(5)
암호프로그램&키관리통제(2) 내부사용자PW관리(3) 이용자PW관리(5)

제6절. 전자금융업무 (18)
전자금융거래(5) 이용자주의사항공지(4)
자체보안성심의(8) 인증방법사용기준(1)

제2절 인력, 조직 & 예산

조		내용
8 인력, 조직, 예산	①인력/조직 운용	1. 〈정보처리시스템〉 & 전자금융업무 관련 전담 조직 확보
		2. 외부주문계약 체결시 계약검토 & 자체통제를 위한 내부조직과 인력 확보
		3.전산인력의 자질향상 & 예비요원 양성을 위한 교육 & 연수프로그램 운영
		4. 〈CIO의무〉 임직원의 보안법규준수여부를 정기점검→ CEO보고
		5. 〈CEO의무〉 임직원의 보안법규 위반시 제재기준 & 절차를 마련,운영
	②인력/예산	1. IT인력은 총 임직원수의 100분의 5 이상, 정보보호인력은 IT인력의 100분의 5 이상
		2. 정보보호예산을 IT부문 예산의 100분의 7 이상이 되도록 할 것
	③ 제②항 미이행시 사유&이용자보호에 미치는 영향을 사업연도 종료 후 1달이내에 홈페이지 등에 공시	
8조의2 정보보호위원회 운영	① 중요 정보보호에 관한 사항을 심의 · 의결하는 〈정보보호위원회〉를 설치 운영	
	② 위원회의 장은 CIO, 위원은 정보보호 or 전산운영 & 개발 or 준법업무 관련부서장 등으로 구성	
	③ 심의/의결 사항	1. (법 제21조제4항에 따른) 〈IT부문계획서〉
		2. (법 21조②의) 〈전자금융거래의 안정성 확보 & 이용자 보호를 위한 전략 & 계획〉 수립
		3. (법 제21조의3에서 정한) 〈취약점 분석 · 평가 결과 & 보완조치〉의 이행계획
		4. 전산보안사고 & 전산보안관련규정위반자의 처리
		5. 기타 〈정보보호위원회〉의 장이 정보보안업무 수행에 필요하다고 정한 사항
	④ CIO는 〈정보보호위원회〉 심의 · 의결사항을 CEO에게 보고	
	⑤ CEO는 특별한 사정이 없는 한 정보보호위원회의 심의 · 의결사항을 준수	

전자금융감독규정 항목보기

제3절 시설

조	내용
9 건물	1. 건물 출입구는 경비원에 의하여 통제하고 〈출입통제 보안대책〉을 수립 · 운용
	2. 비상시 대피를 위한 비상계단 & 정전대비 유도등 설치
	3. 번개, 과전류 등 고전압으로 인한 전산장비 & 통신장비 등의 피해 예방을 위하여 피뢰설비 설치
	4. 서버, 스토리지등 전산장비 & 통신장비 등의 중량을 감안한 적재하중 안전대책을 수립 · 운용
	5. 화재예방안전대책 수립 · 운용 : 소화기&자동소화설비, 배연설비설치 등
	6. 화재, 침수, 진동피해 발생지역 등은 제외
10 전원, 공조 등 설비	1. 전원실, 공조실 등 주요 설비시설에 자물쇠 등 출입통제장치를 설치
	2. 전원, 공조, 방재 & 방범 설비에 대한 적절한 감시제어시스템을 갖출 것
	3. 전산실의 전력공급 중단에 대비하여 자가발전설비를 갖출 것
	4. 전력공급장애 시 전력선 대체가 가능하도록 복수회선을 설치, 전력공급의 연속성을 위한 무정전전원장치(UPS) 설치
	5. 과전류차단기, 누전경보기 등을 설치, 정전압정주파수장치(CVCF)를 갖출 것
	6. 전산실 전원 & 공조 설비는 설비부분과 분리설치, 공조설비점검을 위한 압력계, 온도계 등을 갖출 것
	7. 전산실에 24시간 동안 적정한 온도 & 습도를 유지하기 위해서 자동제어 항온 · 항습기 설치
11 전산실 등	1. 화재 · 수해 등의 재해 & 외부 위해(危害) 방지대책을 수립 · 운용할 것
	2. 상시출입문은 한곳으로 지정, 사전등록자에게만 허용, 그 외 출입자는 책임자승인을 받아 출입, 출입자관리기록부 작성
	3. 그 외 출입자가 출입시에는 무인감시카메라 or 출입자동기록시스템 등 조치를 취하여 사후 확인이 가능하도록 할 것
	4. 출입문은 이중 안전장치로 보호하며 외벽이 유리인 경우 유리창문을 통하여 접근할 수 없도록 조치할 것
	5. 침수로 인한 장애가 발생하지 않도록 외벽과 전산장비와의 거리를 충분히 유지하고 이중바닥설치 등 방안을 강구할 것
	6. 적정수준의 온도 · 습도를 유지하기 위하여 온도 · 습도 자료 자동기록장치 & 경보장치 설치 등 적절한 조치를 취할 것
	7. 케이블이 안전하게 유지되도록 전용 통로관 설치 등 적절한 보호조치를 강구할 것
	8. 정전에 대비하여 조명설비 & 휴대용손전등을 비치할 것
	9. IDC 등 다수기관이 공동이용하는 장소에 〈정보처리시스템〉을 설치하는 경우 미승인자가 접근하지 못하도록 접근통제
	10. 보호구역으로 관리 — 가. 전산센터 & 재해복구센터 나. 〈전산자료〉 보관실 다. 〈정보보호시스템〉 설치장소 라. 보안관리가 필요한 〈정보처리시스템〉 설치장소
	11. 국내에 본점을 둔 금융회사의 전산실 & 재해복구센터는 국내에 설치할 것
	12. 무선통신망을 설치하지 아니할 것

전자금융감독규정 항목보기

제5절 IT부문 내부통제

조	내용	
19조 IT부문 계획서 제출	① 금융위에 〈IT부문계획서〉를 제출해야 하는 금융회사 or 전자금융업자는 〈장 · 단기 IT부문계획〉 매년 수립 · 운용	
	② 금융위원장은 금감원장으로 하여금 〈IT부문계획서〉의 적정성 등을 평가한 후 관련보고서를 제출하게함	
19조의2 정보보호 교육계획 수립 시행	① CPO는 매년 교육계획을 수립 · 시행	1. 임원 : 3시간 이상(단, CIO는 6시간 이상)
		2. 일반직원 : 6시간 이상
		3. IT부문업무 담당 직원 : 9시간 이상
		4. 정보보호업무 담당 직원 : 12시간 이상
	② CEO는 정보보호교육을 실시한 이후 대상 임직원에 대해 평가를 실시	
	③ ①의 교육프로그램 개발과 정보보호교육은 정보보호 전문 교육기관에 위탁할 수 있다.	
20조 〈정보처리시스템〉 구축 & 전자금융거래 관련 사업추진	1.영향이 크거나 부서장전결금액 이상의 사업추진시 사전에 타당성검토실시	
	2. 〈정보처리시스템〉 신규 · 통합 · 전환 · 재개발 등 사업에 대하여 비용대비효과분석 실시	
	3. 타당성 검토와 비용 대비 효과분석 결과는 전산운영위원회 등 독립적인 조직의 승인	
	4. 〈정보처리시스템〉의 안전성과 신뢰성을 확보하기 위하여 분석 · 설계 단계부터 보안대책을 강구	
21조 〈정보처리시스템〉 구축 & 전자금융거래 관련 계약	1. 적합한 업체를 공정하게 선정하기 위하여 객관적인 〈업체 선정 기준 & 절차〉를 마련 · 운용할 것	
	2. 〈정보처리시스템〉의 안전성&신뢰성확보를 위해 〈업체 선정 기준 & 절차〉에 정보보안 포함	
	3. 공정하고 합리적인 〈예정가격 산출 기준〉을 수립 · 적용할 것	
	4. 〈계약서 작성 기준〉을 수립 · 운용(계약금액, 구축완료일자, 납품방법 & 대금지급방법 등)	
	5. 구매,개발제품의 소유권, 저작권,지적재산권 등의 귀속관계를 명확히 하여 사후분쟁을 막을 것	
	6. 납품, 개발이 완료된 SW 등에 대하여 공급업체 파산 등 〈비상사태대비대책〉을 마련 · 운용할 것	
	7. 검수는 개발자, 계약자 등 이해당사자를 배제하여 공정하게 실시할 것	
	8. 계약 미이행사유가 발생하였거나 계약조항을 변경할 경우에는 검사부서의 승인을 받을 것	
	9. 내부감사규정에 따라 감사가 정한 금액 이상의 계약에 대하여는 자체감사실시or 검사부서의 승인	
22조 〈정보처리시스템〉 감리	정보처리시스템 〈감리 지침〉 작성 · 운용	1. 목적 & 대상, 시스템 감리인, 감리시기 & 계획 등 일반기준
		2. 기획, 개발 & 운용의 감리 실시 기준
		3. 지적사항 & 개선사항 등 감리 후 보고 기준
		4. 전자금융업무와 관련된 외부주문 등에 대한 감리 기준

제5절 IT부문 내부통제

조	내용	
23조 비상대책 등의 수립/운용	① 긴급상황시 〈업무지속성 확보대책〉 수립 · 준수	1. 상황별 대응절차 2. 백업 or 재해복구센터를 활용한 재해복구계획 3. 비상대응조직의 구성 & 운용 4. 입력대행, 수작업 등의 조건 & 절차 5. 모의훈련의 실시 6. 유관기관&관련업체 비상연락체제 구축 7. 보고 & 대외통보의 범위와 절차
	② 〈업무지속성 확보대책〉에는 비상사태 대비 안전대책 반영.	1. 파업시 비상지원인력 확보 · 운영
		2. 〈정보처리시스템〉 운영에 대한 〈비상지원인력 or 외부 전문업체 활용방안〉을 수립 · 운영
		3. 비상지원인력이 업무가능한 수준으로 〈전산시스템 운영지침서〉, 〈사용자매뉴얼〉 작성 & 유지
		4. 담당자 부재시에도 비상지원 인력이 업무를 수행할 수 있도록 비상지원인력에 대한 연수 실시
	③ ①의 규정에 따른 〈업무지속성 확보대책〉의 실효성 · 적정성 등을 매년 1회 이상 점검, 최신상태로 유지, 관리	
	④ 「국가위기관리기본지침」에 따라 금융위가 지정한 금융회사는 금융위「금융전산분야위기대응실무매뉴얼」에 따라 〈위기대응행동매뉴얼〉수립 · 준수, 금융위에 알림	
	⑤ 금융위가 별도로 지정하지 아니한 금융회사 or 전자금융업자는 자연 재해, 인적 재해, 기술적 재해, 전자적 침해 등으로 인한 전산시스템의 마비 방지와 신속한 복구를 위한 〈비상대책〉을 수립 · 운영	
	⑥ 〈위기대응행동매뉴얼〉(④에 따른) or 〈비상대책〉(⑤에 따른)에는 〈업무지속성 확보대책〉(①에 따른) 반영	
	⑦ 중앙처리장치, 데이터저장장치 등 주요 전산장비에 대하여 이중화 or 예비장치 확보	
	⑧ 다음 금융회사는 재해복구센터를 주 전산센터와 일정거리 이상 떨어진 안전한 장소에 구축 · 운용	1. 은행 2.한국산업은행, 중소기업은행, 농협은행, 수산업협동조합중앙회의 신용사업부문 3.투자매매업자 · 투자중개업자 4.증권금융회사 & 한국예탁결제원 5.거래소 6.신용카드업자 7.보험요율산출기관 8.상호저축은행중앙회 9.신용협동조합중앙회 10.보험회사
제24조 비상 대응훈련 실시	① 〈행동매뉴얼〉〈비상대책〉에 따라 비상대응훈련 연 1회 실시, 금융위에 결과보고. 〈재해복구전환훈련〉을 포함하여 실시할 수 있다.	
	② 금융위는 금융회사 or 전자금융업자를 선별하여 〈금융분야 합동비상대응훈련〉을 실시	
	③ 금융위는 〈합동비상대응훈련〉때, 다음 기관에게 지원요청가능	1."국가정보원(국가사이버안전센터)" 2."경찰청(사이버테러대응센터)" 3. 침해사고대응기관 4. 금융위가 필요하다고 인정하는 기관
25조 성능관리	장애예방 & 성능최적화를 위하여 〈정보처리시스템〉 사용현황 & 추이분석 등을 정기실시	
26조 직무의 분리	1. 프로그래머와 오퍼레이터	5. 업무운영자와 내부감사자
	2. 응용프로그래머와 시스템프로그래머	6. 내부인력과 전자금융보조업자 & 유지보수업자 등을 포함한 외부인력
	3. 시스템보안관리자와 시스템프로그래머	7. IT부문인력과 정보보호인력
	4. 〈전산자료〉관리자와 그밖의 업무담당자	8. 그 밖에 내부통제관련 직무분리가 요구되는 경우
제27조 전산 원장 통제	① 장애 or 오류 등에 의한 전산원장의 변경을 위하여 별도의 변경절차를 수립 · 운용	
	② ①의 포함사항 – 변경대상 & 방법, 변경권한자 지정, 변경 전후내용 자동기록 & 보존, 변경내용의 정당여부에 대한 제3자확인	
	③ 대차대조표 등 중요자료의 계상액과 각종 보조부 · 거래기록 · 전산원장파일의 계상액에 대한 상호일치여부를 전산시스템을 통하여 주기적으로 확인	
	④ ③확인 결과 불일치가 발견시 원인 & 조치 내용을 〈전산자료〉의 형태로 5년간 보존	
	⑤ 이용자중요원장에 직접 접근, 조회 · 수정 · 삭제 · 삽입하는 경우 작업자 & 작업내용기록을 5년보존	

제5절 IT부문 내부통제

조	내용		
제28조 거래 통제 등	①사고위험도높은 거래는 책임승인거래로 처리하는 등 전산시스템에 의한 이중확인이 가능하도록 함		
	② 전산원장, 주요or이용자정보저장 〈정보처리시스템〉에 대한 중요작업 수행시 책임자가 이중확인		
29조 프로그램 통제	〈프로그램 등록/변경/폐기절차〉를 수립/운용	1. 적용대상 프로그램 종류 & 등록 · 변경 · 폐기 방법을 마련	
		2. 프로그램 변경 전후 내용을 기록 · 관리	
		3. 프로그램 등록 · 변경 · 폐기내용의 정당성에 대해 제3자의 검증을 받을 것	
		4. 변경 필요시 해당 프로그램을 개발 or 테스트 시스템으로 복사 후 수정할 것	
		5. 프로그램에 대한 접근은 업무담당자에 한정할 것	
		6. 처리정보의 기밀성 · 무결성 · 가용성을 고려, 테스트 & 책임자승인 후 운영시스템적용	
		7. 반출, 실행프로그램의 생성 & 운영시스템 등록은 해당프로그램 담당자 외의 자가 수행	
		8. OS, DBMS 등의 시스템 프로그램도 응용프로그램과 동일수준으로 관리	
		9. 유지보수에 필요한 문서 작성 · 관리 (설명서, 입 · 출력 레코드 설명서, 프로그램목록 & 지침서 등)	
		10. 전자금융거래 전산프로그램은 〈정보처리시스템〉에 설치 전에 자체보안성검증 실시	
30조 일괄작업에 대한 통제	1. 일괄작업은 작업요청서에 의한 책임자의 승인을 받은 후 수행		
	2. 일괄작업은 최대한 자동화하여 오류를 최소화		
	3. 일괄작업 수행 과정에서 오류가 발생하였을 경우 반드시 책임자의 확인을 받을 것		
	4. 모든 일괄작업의 작업내용을 기록 · 관리할 것		
	5. 책임자는 일괄작업 수행자의 주요업무 관련 행위를 모니터링할 것		
31조 암호프로그램 &키관리 통제	① 암호프로그램에 대하여 담당자 지정, 담당자 이외의 이용 통제 & 원시프로그램(source program) 별도 보관 등을 준수하여 유포 & 부당 이용이 발생하지 않도록 하여야 한다		
	② 암호 & 인증시스템에 적용되는 키에 대하여 주입 · 운용 · 갱신 · 폐기에 대한 절차 & 방법을 마련하여 안전관리		
32조 내부사용자 PW관리	내부사용자 PW유출 방지를 위하여 다음을 〈정보처리 시스템〉에 반영	1. 담당업무 외에는 열람 & 출력을 제한할 수 있는 접근자의 PW를 설정하여 운영	
		2. PW는 다음 각 목의 사항을 준수	가. ID, 생년월일, 주민번호, 전화번호를 포함하지 않은 숫자와 영문자 & 특수문자 등을 혼합하여 8자리 이상으로 설정 & 분기별 1회 이상 변경
			나. PW 보관 시 암호화
			다. 시스템마다 관리자 PW를 다르게 부여
		3. PW입력 시 5회 이내에서 미리 정한 횟수 이상의 입력오류가 연속발생시 즉시 해당 PW를 이용하는 접속을 차단하고 본인 확인절차를 거쳐 PW를 재부여 or 초기화	
33조 이용자 PW관리	① 〈정보처리시스템〉 & 〈전산자료〉에 보관하고 있는 이용자의 PW를 암호화하여 보관하며 동 PW를 조회할 수 없도록 하여야 한다. 다만, PW의 조회가 불가피하다고 인정되는 경우에는 그 조회사유 · 내용 등을 기록 · 관리		
	② 이용자의 PW 유출을 방지하기 위하여 다음 각 호의 사항을 〈정보처리 시스템〉에 반영	1. 주민번호, 동일숫자, 연속숫자 등 제3자가 쉽게 유추할 수 있는 PW 등록불가	
		2. 통신용 PW와 계좌원장 PW를 구분해서 사용	
		3. 5회 이내에서 미리 정한 횟수 이상의 입력오류 발생시 즉시 해당 PW이용거래를 중지, 본인확인절차를 거친 후 PW 재부여 & 거래 재개 (이체 PW 등 동일PW가 다양한 전자금융거래에 공통으로 이용시, 입력오류 횟수는 이용되는 모든 전자금융거래를 통산)	
		4. 금융회사가 이용자로부터 받은 PW는 거래전표, 계좌개설신청서 등에 기재하지 말고 핀패드(PIN pad) 등 보안장치를 이용하여 입력받을 것	

전자금융감독규정 항목보기

제6절 전자금융업무

조	내용	
34조 전자금융거래	1. 전자금융거래는 암호화통신 (예외-전용선+자체보안성심의 실시, 전화 등 암호화가 불가능한 경우)	
	2. 전자금융사고 예방을 위하여 비대면 전자금융거래를 허용하지 않는 계좌 개설, 이용자가 문자 & 이메일통지 요청시, 서비스를 제공할 수 있도록 시스템을 갖출 것	
	3. 전자금융거래에 사용되는 접근〈매체〉 발급시 실명확인 후 교부	
	4. 거래인증수단 채택시 안전성, 보안성, 이용편의성 등을 충분히 고려할 것	
	5. 전자금융거래프로그램(거래전문포함)의 위·변조 여부 등 무결성을 검증할 수 있는 방법을 제공	
35조 이용자 유의사항 공지	전자금융거래의 안전한 수행을 위하여 이용자에게 다음 공지	1. PW 유출위험 & 관리에 관한 사항
		2. 금융기관 or 전자금융업자가 제공하고 있는 이용자 보호제도에 관한 사항
		3. 해킹·피싱 등 전자적 침해 방지에 관한 사항
		4. 본인확인절차를 거쳐 PW변경이 가능하도록 〈정보처리시스템〉 구축, 같은 PW 재사용하지 않도록 할 것
36조 자체 보안성 심의	①다음 경우 금감원기준에 따라 〈자체 보안성심의〉	1. 정보통신망으로 이용자대상 신규 전자금융업무를 수행
		2. 복수의 금융회사 or 전자금융업자가 공동으로 전자금융거래 관련 표준을 제정
	② 〈자체 보안성심의〉 후 ①항 각 호를 수행한 날부터 7일 이내에 〈자체 보안성심의 결과보고서〉를 금감원에 제출. (예외 - ①항 1호에 따른 경우+ 과거 1년간 전자금융사고 미발생기관 + 금감원기준에 해당할 경우)	
	③ 금감원장은 〈자체 보안성심의 결과보고서〉 검토결과, 개선·보완을 요구할 수 있다	
	④ 다음 기관은 〈자체 보안성심의 결과보고서〉 미제출 가능	1. 「우체국예금·보험에 관한 법률」에 의한 체신관서
		2. 「새마을금고법」에 의한 새마을금고 & 새마을금고중앙회
		3. 「한국수출입은행법」에 따른 한국수출입은행
		4. 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관
37조 인증방법 사용기준	전자금융거래의 종류,성격,위험수준 등을 고려하여 안전한 인증방법을 사용하여야 한다.	