전자금융감독규정 일부개정고시안

전자금융감독규정 일부를 다음과 같이 개정한다.

제5조제1항 각 호 외의 부분 중 “다음”을 “전자금융거래 규모, 전자금융사고 발생 건수 등을 고려하여 다음”으로, “이상이어야”를 “이상으로 설정해야”로 하고, 같은 항 제2호 중 “「금융위원회의 설치 등에 관한 법률」 제38조제8호”를 “「금융위원회의 설치 등에 관한 법률」 제38조제2호(다만, 명의개서대행업무를 수행하는 회사는 제외)의 회사 중 자산이 2조원 이상인 회사, 같은 법 제38조제8호”로 하며, 같은 항 제3호 중 “회사 :”를 “회사 중 자산이 2조원 미만인 회사 :”로 하고, 같은 항 제4호 본문 중 “1억원”을 “2억원”으로 하며, 같은 항 제5호 중 “법 제28조제2항제1호 및 제2호”를 “법 제28조제2항제1호”로 하고, 같은 항 제6호를 제8호로 하며, 같은 항에 제6호를 다음과 같이 신설하고, 같은 항 제8호(종전의 제6호) 중 “중”을 “: 2억원(단,”으로, “전자금융업자 : 10억원”을 “전자금융업자는 10억원)”으로 하며, 같은 항에 제9호부터 제11호까지를 각각 다음과 같이 신설하고, 같은 항 제7호를 다음과 같이 하며, 같은 항에 제12호를 다음과 같이 신설한다.

6. 법 제28조제2항제2호의 전자금융업자 : 2억원

9. 시행령 제15조제3항제1호의 전자금융업자 : 2억원

10. 시행령 제15조제3항제2호의 전자금융업자 : 2억원

11. 법 제28조제1항의 전자금융업자 : 2억원

7. 법 제28조제2항제3호의 전자금융업자 : 2억원

12. 제1호부터 제11호에 2개 이상 해당하는 회사는 각 호의 금액의 합계액으로 한다. 다만 제5호부터 제11호의 합계액이 15억원을 초과하는 경우에는 제5호부터 제11호의 합계액을 15억원으로 한다.

제5조제2항 중 “제1항”을 “전자금융거래 규모, 전자금융사고 발생 건수 등을 고려하여 제1항”으로 한다.

제7조 각 호 외의 부분 중 “제8조 부터 제37조”를 “제8조부터 제36조 및 제37조의5”로 하고, 같은 조 제1호 중 “조직”을 “조직, 교육”으로 하며, 같은 조 제3호 중 “전산자료, 정보처리시스템 및 정보통신망”을 “전산자료 및 정보처리시스템”으로 하고, 같은 조 제4호를 제8호로 하며, 같은 조에 제4호부터 제7호까지를 각각 다음과 같이 신설한다.

4. 해킹, 악성코드 감염 등 정보보호부문

5. 정보처리시스템 및 전자금융거래 관련 사업 부문

6. 비상대책 등 업무지속성부문

7. 전산원장통제, 프로그램 통제 등 정보기술부문 내부통제

제3장제2절의 제목 “인력, 조직 및 예산 부문”을 “인력, 조직, 교육 및 예산 부문”으로 한다.

제8조제1항제3호를 다음과 같이 하고, 같은 항 제4호 및 제5호를 각각 제5호 및 제6호로 하며, 같은 항에 제4호를 다음과 같이 신설한다.

3. 정보보호최고책임자는 임직원의 정보보호역량 강화를 위하여 매년 교육계획을 수립·시행하여야 한다.

4. 최고경영자는 전년도 교육계획 시행 결과를 평가하고 그 결과를 금년도 교육계획에 반영해야 한다.

제8조제1항제5호(종전의 제4호) 중 “임직원이 정보보안 관련법규가 준수되고”를 “임직원의 정보보안 관련법규를 준수하고”로, “점검결과를”을 “점검결과 및 보완계획을”로 하고, 같은 조 제2항 각 호 외의 부분을 다음과 같이 한다.

금융회사 또는 전자금융업자는 정보기술 및 정보보호 분야별 전문성을 갖춘 인력과 충분한 예산을 확보해야 한다.

제8조제2항제1호 및 제2호를 각각 삭제하고, 같은 조 제3항 및 제4항을 각각 삭제한다.

제8조의2제4항 중 “한다”를 “하며, 전자금융거래의 안전성 및 신뢰성에 중대한 영향을 미치는 심의·의결사항에 대해서는 이사회에 보고 하여야 한다”로 한다.

제9조부터 제11조까지를 각각 다음과 같이 한다.

제9조(건물에 관한 사항) 금융회사 또는 전자금융업자는 전산실이 위치한 건물에 관하여 안전대책 및 출입통제 보안대책을 수립·운용해야 한다.

1. 삭제

2. 삭제

3. 삭제

4. 삭제

5. 삭제

6. 삭제

제10조(전원, 공조 등 설비에 관한 사항) 금융회사 또는 전자금융업자는 전산실이 위치한 건물의 전원, 공조 등 설비의 안전성을 위한 기준을 수립 · 준수해야 한다.

1. 삭제

2. 삭제

3. 삭제

4. 삭제

5. 삭제

6. 삭제

7. 삭제

제11조(전산실 등에 관한 사항) 금융회사 또는 전자금융업자는 전산실에 관하여 다음 각 호의 사항을 포함한 대책을 수립·준수하여야 한다.

1. 국내에 본점을 둔 금융회사 또는 전자금융업자의 전산실 및 재해복구센터는 국내에 설치할 것 단, 제50조제2항에 따라 등록한 국외 사이버몰을 위한 전자지급 결제대행업자는 제외

2. 무선통신망을 설치하지 아니할 것

3. 그 밖에 재해 및 위해방지, 출입·접근통제 등 전산실의 안전 및 보안에 관한 사항

4. 삭제

5. 삭제

6. 삭제

7. 삭제

8. 삭제

9. 삭제

10. 삭제

11. 삭제

12. 삭제

제12조제1호를 다음과 같이 하고, 같은 조 제3호 중 “금지”를 “금지, 정기적인 악성코드 감염여부 확인”으로 하며, 같은 조 제4호 중 “정보유출,”을 “정보유출 및”으로, “및 휴대용 전산장비에”를 “등에”로 한다.

1. 단말기는 인가된 사용자만 사용할 수 있도록 관리할 것

제13조제1항제1호를 다음과 같이 하고, 같은 항 제2호를 삭제하며, 같은 항 제3호를 제2호로 하고, 같은 항 제4호를 삭제하며, 같은 항 제5호부터 제11호까지를 각각 제3호부터 제9호까지로 하고, 같은 항 제4호(종전의 제6호) 중 “보조기억매체 등 전산자료”를 “전산자료”로 하며, 같은 항 제9호(종전의 제11호) 중 “1년”을 “금융감독원장이 정하는 사항을 접속의 성공여부와 상관없이 자동적으로 기록·유지하고 1년”으로 하고, 같은 항 제12호를 삭제하며, 같은 항 제13호 및 제14호를 각각 제10호 및 제11호로 하고, 같은 항 제11호(종전의 제14호) 중 “사용자 계정”을 “사용자 계정”으로 하며, 같은 조 제2항 중 “제1항제1호의 사용자계정”을 “사용

자계정”으로 한다.

1. 사용자 인증 수단을 개인별로 부여하고 접근권한은 최소한으로 부여하는 등 적절한 접근권한 관리 및 통제 절차를 수립·운용할 것

제13조제3항 및 제4항을 각각 삭제하고, 같은 조 제5항을 제3항으로 한다.

제14조 각 호 외의 부분 중 “위하여”를 “위하여 운영매뉴얼, 유지보수관리대장, 책임자명부 및 장애상황기록부 등”으로 하고, 같은 조 제1호를 다음과 같이 하며, 같은 조 제2호 및 제3호를 각각 삭제하고, 같은 조 제4호 및 제5호를 각각 제2호 및 제3호로 하며, 같은 조 제2호(종전의 제4호) 중 “가능한”을 “가능하도록”으로 하고, 같은 조 제6호를 삭제하며, 같은 조 제7호 및 제8호를 각각 제4호 및 제5호로 하고, 같은 조 제4호(종전의 제7호) 중 “운영체계, 시스템 유틸리티 등의 긴급”을 “긴급”으로 하며, 같은 조 제9호를 삭제하고, 같은 조 제10호를 제6호로 하며, 같은 호(종전의 제10호) 중 “정보처리시스템 운영체제(Operating System)”를 “정보처리시스템의 운영체제(Operating System) 계정으로 로그인(Log in)할 경우 이중인증 절차를 시행하고,”로, “수립하고”를 “수립하며”로 한다.

1. 다음 각 목을 작성·보관 할 것

가. 주요 정보처리시스템에 대한 운영매뉴얼

나. 주요 정보처리시스템에 대한 정기적인 유지보수 실시 내용을 기록한 유지보수관리대장

다. 정보처리시스템에 대한 책임자명부 및 장애상황기록부

제14조의2제3항 중 “제37조의4제1항”을 “제37조의6제1항”으로 하고, 같은 조 제4항 각 호 외의 부분 중 “발생 사유, 관련 자료 및 대응계획을 첨부하여 금융감독원장에게 보고하여야 한다”를 “금융감독원장에게 보고하여야 하고, 관련 서류를 최신상태로 유지하여야 한다”로 하며, 같은 항 제1호 중 “체결하는”을 “체결하거나, 기존 클라우드컴퓨팅서비스 이용계약을 통해 신규 업무를 처리하는”으로 하고, 같은 조 제5항 각 호 외의 부분을 다음과 같이 한다.

제4항의 보고에 관한 양식, 첨부서류 등에 관해서는 금융감독원장이 정하는 바에 따른다.

제14조의2제5항제1호부터 제6호까지를 각각 삭제하고, 같은 조 제6항을 삭제하며, 같은 조 제7항부터 제9항까지를 각각 제6항부터 제8항까지로 하고, 같은 조 제7항(종전의 제8항) 본문 중 “제11조제11호 및 제12호”를 “제11조제1호 및 제2호”로 하며, 같은 항 단서 중 “제11조제12호”를 “제11조제2호”로 한다.

제15조 앞에 절 번호 및 제목을 다음과 같이 신설한다.

제5절 정보보호부문

제15조제1항제3호가목 및 같은 항 제5호가목 중 “적용한 경우에 한한다”를 각각 “적용하고 정보보호위원회가 승인한 경우에 한한다.”로 하고, 같은 조 제2항 각 호 외의 부분 중 “정보보호시스템을 설치·운영하는 경우에는 다음 각 호의”를 “정보보호시스템의 안전한 운영을 위하여 금융감독원장이 정하는”으로 하며, 같은 항 제2호부터 제6호까지를 각각 삭

제하고, 같은 조 제4항 중 “침해행위로 인한 피해 발생시 즉시 대처할 수 있도록 적절한 대책을 마련”을 “침해의 예방, 피해 최소화 및 신속한 복구를 위한 대책을 수립·운용”으로 하며, 같은 조 제6항제3호를 다음과 같이 하고, 같은 항 제4호를 삭제하며, 같은 조에 제7항을 다음과 같이 신설한다.

3. 무선통신망에 인가되지 않은 정보처리시스템 및 단말기의 접속을 차단하여야 하며, 비인가 무선접속장비(Access Point: AP) 설치·접속여부, 중요 정보 노출여부를 주기적으로 점검할 것

⑦ 금융회사 또는 전자금융업자는 단말기에서 음란, 도박 등 업무와 무관한 프로그램 또는 인터넷 사이트에 접근하는 것에 대한 통제대책을 마련하여야 한다.

제16조 및 제17조를 각각 다음과 같이 한다.

제16조(악성코드 감염 방지대책) 금융회사 또는 전자금융업자는 악성코드 감염·확산 방지, 피해 최소화 및 복구를 위한 대책을 수립·준수하여야 한다.

제17조(홈페이지 등 공개용 웹서버 관리대책) 금융회사 또는 전자금융업자는 공개용 웹서버의 안전한 관리를 위하여 다음 각 호를 포함한 적절한 대책을 수립·운용하여야 한다.

1. 공개용 웹서버를 내부통신망과 분리하여 내부통신망과 외부통신망 사이의 독립된 통신망(이하 “DMZ구간”이라 한다)에 설치하고 네트워크 및 웹 접근제어 수단으로 보호할 것

2. 공개용 웹서버에 접근할 수 있는 사용자계정은 업무관련자만 접속할 수 있도록 제한하고 이중 인증수단을 적용할 것

3. 공개용 웹서버에서 제공하는 서비스를 제외한 다른 서비스 및 시험·개발 도구 등의 사용을 제한하고, DMZ구간 내에 이용자 정보 등 주요 정보를 저장 및 관리하지 아니할 것(다만, 거래로그를 관리하기 위한 경우에는 예외로 하되 이 경우 반드시 암호화하여 저장·관리하여야 한다)

4. 금융회사 또는 전자금융업자는 공개용 웹서버에 자료 게시 절차·내용에 관한 내부통제 방안과 개인정보 유출 및 위·변조를 방지하기 위한 보안조치 방안을 수립·운용하여야 한다.

제18조 각 호 외의 부분 중 “다음 각 호를 포함하여”를 “주소 체계·할당·관리 등에 대한 내용을 포함한”으로, “수립·운용”을 “수립·운용하고, 내부 IP주소 및 외부 IP주소의 인터넷 접속내용을 1년 이상 별도로 기록·보관”으로 하고, 같은 조 제1호부터 제5호까지를 각각 삭제한다.

제19조 앞에 “제5절 정보기술부문 내부통제”를 삭제한다.

제19조를 제36조의2로 하고, 같은 조(종전의 제19조) 제1항 중 “한다”를 “하며, 정보기술부문 계획서 제출에 관한 세부적인 절차, 양식 등에 관해서는 금융감독원장이 정하는 바에 따른다”로 한다.

제19조의2를 삭제한다.

제20조 앞에 절 번호 및 제목을 다음과 같이 신설한다.

제6절 사업부문

제20조 및 제21조를 각각 다음과 같이 한다.

제20조(정보처리시스템 구축 및 전자금융거래 관련 사업 추진) 금융회사 또는 전자금융업자는 정보처리시스템 및 전자금융거래와 관련된 사업 추진에 대한 내부통제 기준을 수립·준수하여야 한다.

1. 삭제
2. 삭제
3. 삭제
4. 삭제

제21조(정보처리시스템 구축 및 전자금융거래 관련 계약) 금융회사 또는 전자금융업자는 정보처리시스템 구축 및 전자금융거래와 관련된 계약 체결시에 정보처리시스템의 안전성·신뢰성 및 계약의 공정성이 확보될 수 있도록 체결·이행·감사 등에 관한 내용을 포함한 내부통제 절차를 수립·운용해야 한다.

1. 삭제
2. 삭제
3. 삭제
4. 삭제
5. 삭제
6. 삭제
7. 삭제

8. 삭제

9. 삭제

제22조 각 호 외의 부분 중 “위하여 다음 각 호의 사항을 포함한”을 “위한”으로 하고, 같은 조 제1호부터 제4호까지를 각각 삭제한다.

제23조 앞에 절 번호 및 제목을 다음과 같이 신설한다.

제7절 업무지속성 부문

제26조를 제3장제2절제8조의3으로 하고, 같은 조(종전의 제26조) 각 호 외의 부분 중 “다음 각 호의 업무에 대하여 직무를 분리·운영”을 “정보기술부문의 내부통제를 위한 직무분리 기준을 수립·운용”으로 하며, 같은 조 제1호부터 제8호까지를 각각 삭제한다.

제23조제1항에 제8호를 다음과 같이 신설한다.

8. 비상지원인력의 확보 및 운영

제23조제2항을 삭제하고, 같은 조 제8항에 제6호의2를 다음과 같이 신설하며, 같은 항 제8호 중 “상호저축은행중앙회”를 “상호저축은행중앙회 및 자체 전산시스템을 구축하여 운영하는 상호저축은행”으로 하고, 같은 항에 제11호를 다음과 같이 신설한다.

6의2. 「여신전문금융업법」에 의한 시설대여업자, 할부금융업자, 신기술사업금융업자(다만, 시행령 제11조의3제1항에 해당하는 회사에 한한다.)

11. 「전자금융거래법」에 의한 전자금융업자(다만, 연간 전자금융거래 총액이 2조원 이상인 회사에 한한다.)

제24조제3항제1호 중 “「정부조직법」 제15조”를 “「정부조직법」 제17조”로 하고, 같은 항 제2호를 다음과 같이 한다.

2. 「국가경찰과 자치경찰의 조직 및 운영에 관한 법률」 제12조에 따른 “경찰청(사이버수사국)“

제26조 앞에 절 번호 및 제목을 다음과 같이 신설한다.

제8절 정보기술부문 내부통제

제31조, 제32조 및 제33조를 각각 제19조, 제19조의2 및 제34조의3으로 한다.

제19조(종전의 제31조)제2항 중 “인증시스템에 적용되는 키”를 “인증시스템 등에 적용되는 키(Key)(프로그램 진위 및 무결성 확인에 사용되는 암호 또는 인증시스템 등에 적용되는 키를 포함한다.)”로 한다.

제19조의2(종전의 제32조)의 제목 “(내부사용자 비밀번호 관리)”를 “(사용자 인증수단 관리)”로 하고, 같은 조 각 호 외의 부분 중 “내부사용자의 비밀번호”를 “비밀번호, 생체정보 등 사용자 인증수단”으로, “다음 각 호의 사항을 정보처리시스템에 반영”을 “인증수단의 발급·보관·주기적 변경 및 인증오류 발생시 처리 절차 등을 포함한 관리방안을 수립·준수”로 하며, 같은 조 제1호부터 제3호까지를 각각 삭제한다.

제27조제1항 중 “변경절차”를 “통제절차”로 한다.

제29조 및 제30조를 각각 다음과 같이 한다.

제29조(프로그램 통제) 금융회사 또는 전자금융업자는 프로그램 등록·변경·폐기 등에 관하여 금융감독원장이 정하는 사항을 포함한 절차

를 수립·운용하여야 한다.

1. 삭제

2. 삭제

3. 삭제

4. 삭제

5. 삭제

6. 삭제

7. 삭제

8. 삭제

9. 삭제

10. 삭제

제30조(일괄작업에 대한 통제) 금융회사 또는 전자금융업자는 안전하고 체계적인 일괄작업(batch)의 수행을 위한 절차를 수립·준수하여야 한다.

1. 삭제

2. 삭제

3. 삭제

4. 삭제

5. 삭제

제34조의3(종전의 제33조)제2항 각 호 외의 부분 중 “반영”을 “반영하고 이를 준수”로 하고, 같은 항 제1호를 다음과 같이 하며, 같은 항 제2호를

삭제하고, 같은 항 제3호 및 제5호를 각각 제2호 및 제3호로 하며, 같은 항 제2호(종전의 제3호) 중 “5회 이내의 범위에서 미리”를 “미리”로 하고, 같은 항 제4호를 다음과 같이 한다.

1. 제3자가 쉽게 유추할 수 없는 비밀번호 작성규칙 및 등록·변경 절차를 수립·운영할 것

4. 이용자 비밀번호 변경 시 본인확인 절차를 수행할 것

제34조 앞에 “제6절 전자금융업무”를 삭제한다.

제34조 앞에 절 번호 및 제목을 다음과 같이 신설한다.

제9절 전자금융업무

제34조제4호를 삭제하고, 같은 조 제5호를 제4호로 한다.

제35조 각 호 외의 부분 중 “다음 각 호의 사항을 준수하도록”을 “필요한 사항을”로 하고, 같은 조 제1호부터 제4호까지를 각각 삭제한다.

제36조제2항 본문 중 “7일”을 “30일”로 하고, 같은 조 제4항제3호를 삭제하며, 같은 항 제4호를 제3호로 한다.

제37조를 제34조의2로 한다.

제37조의2 앞에 절 번호 및 제목을 다음과 같이 신설한다.

제10절 취약점 분석 및 사고 대응 등

제37조의4를 제37조의6으로 하고, 같은 조(종전의 제37조의4) 제3항을 다음과 같이 하며, 제37조의4를 다음과 같이 신설한다.

③ 금융위원장은 제37조의4 및 제37조의5제3항에 따라 보고받은 내용으로서 전자적 침해행위가 원인이거나 원인으로 의심되는 경우 사고

조사 및 피해확산 방지를 위해 침해사고대응기관을 포함하여 침해사고조사단을 구성·운영할 수 있다.

제37조의4(침해사고 통지의 방법) 금융회사 및 전자금융업자는 법 제21조의5에 따른 침해사고가 발생한 사실을 안 때에는 지체 없이 사고 내용, 사고에 따른 영향 등을 <별지 7호 서식>에 기재하여 금융위원회에 보고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여서는 아니된다.

제37조의5를 삭제하고, 제73조를 제37조의5로 한다.

제37조의5(종전의 제73조)제1항 각 호 외의 부분을 다음과 같이 한다.

금융회사 및 전자금융업자는 정보기술부문 및 전자금융과 관련된 사고에 관하여 다음 각 호를 준수하여야 한다.

제37조의5(종전의 제73조) 제1항제1호 및 제2호를 각각 다음과 같이 하고, 같은 항 제3호 및 제4호를 각각 삭제하며, 같은 조 제2항 중 “제1항”을 “제1항제2호”로 하고, 같은 조 제3항 중 “제1항에”를 “제1항제2호에”로, “하며, 제1항제3호에 따른 사고 발생시에는 제37조의4제1항 각 호에 따른 침해사고대응기관에도 알려야 한다”를 “한다”로 하며, 같은 조 제4항 중 “제1항”을 “제1항제2호”로, “절차”를 “대상, 절차”로 한다.

1. 사고의 유형 분류, 처리단계, 조치방법, 영향도 및 심각도 평가 방법 등이 포함된 절차를 마련·운영
2. 금융감독원장이 정하는 사이버보안 사고가 발생한 경우에는 지체없이 금융감독원장에게 보고

제60조제5항 중 “제37조의4제1항”을 “제37조의6제1항”으로 한다.

별표 1 및 별표 2를 각각 삭제한다.

별표 3 나목5)의 기호(*) 중 “제37조의”를 “제34조의2”로 한다.

부 칙

제1조(시행일) 이 규정은 고시한 날부터 시행한다. 다만, 제5조, 제8조의2 및 제23조제8항의 개정규정은 이 규정 고시 이후 6개월이 경과한 날부터 시작한다.

신·구조문대비표

현 행	개 정 안
제5조(전자금융사고 책임이행을 위한 보험 등의 가입에 관한 기준) ① 금융회사 또는 전자금융업자가 법 제9조제4항에 따라 전자금융사고 책임이행을 위한 보험 또는 공제에 가입하는 경우 보상한도는 다음 각 호에서 정하는 금액 이상이어야 한다.	제5조(전자금융사고 책임이행을 위한 보험 등의 가입에 관한 기준) ① ---------- ---------- ---------- ---------- ---------- 전자금융거래 규모, 전자금융사고 발생 건수 등을 고려하여 다음 --- 이상으로 설정해야 ---.
1. (생 략)	1. (현행과 같음)
2. 「금융위원회의 설치 등에 관한 법률」 제38조제8호의 회사, 「전자금융거래법」 제2조제3호나목(신용카드업자에 한한다) 및 다목의 회사, 「전자금융거래법 시행령」 제2조제1호의 회사, 「은행법」에 따른 지방금융회사 및 같은 법 제58조에 의해 인가를 받은 외국금융회사의 국내지점 : 10억원	2. 「금융위원회의 설치 등에 관한 법률」 제38조제2호(다만, 명의개서대행업무를 수행하는 회사는 제외)의 회사 중 자산이 2조원 이상인 회사, 같은 법 제38조제8호--------- ---------- ---------- ---------- ---------- ----
3. 「금융위원회의 설치 등에 관한 법률」 제38조제2호(다	3. ---------- ----------

만, 명의개서대행업무를 수행하는 회사는 제외)의 회사 : 5억원	-- 회사 중 자산이 2조원 미만인 회사 : ---
4. 제1호 부터 제3호 이외의 금융회사 : 1억원. 다만, 제1호 부터 제3호 이외의 금융회사들이 관련 법령에 의해 당해 금융회사를 구성원으로 하는 금융회사를 통해 전자금융거래 관련 정보기술부문의 주요 부분을 공동으로 이용하는 경우, 정보기술부문의 주요부문을 제공하는 금융회사가 공동 이용 금융회사 전체의 사고를 보장하는 내용으로 제2호의 금액(시행령 제2조제5호의 금융회사는 제1호의 금액) 이상의 보험 또는 공제에 가입하면 공동 이용 금융회사는 본 호의 보험 또는 공제에 가입한 것으로 본다.	4. ---------------------------- 2억원. ---.
5. 법 제28조제2항제1호 및 제2호의 전자금융업자 : 2억원	5. 법 제28조제2항제1호------------------------------
<신 설>	6. 법 제28조제2항제2호의 전자금융업자 : 2억원

6. 법 제28조제2항제4호의 전자금융업자 중 제1호 또는 제2호에 속하는 금융회사가 발급한 신용카드, 직불카드 등 거래지시에 사용되는 접근매체의 정보를 저장하는 전자금융업자 : 10억원	8. ---------- ------ : 2억원(단, ---------- ---------- ---------- ---------- ---------- ---------- 전자금융업자는 10억원)
<신 설>	9. 시행령 제15조제3항제1호의 전자금융업자 : 2억원
<신 설>	10. 시행령 제15조제3항제2호의 전자금융업자 : 2억원
<신 설>	11. 법 제28조제1항의 전자금융업자 : 2억원
7. 제5호, 제6호 이외의 전자금융업자 : 1억원	7. 법 제28조제2항제3호의 전자금융업자 : 2억원
<신 설>	12. 제1호부터 제11호에 2개 이상 해당하는 회사는 각 호의 금액의 합계액으로 한다. 다만 제5호부터 제11호의 합계액이 15억원을 초과하는 경우에는 제5호부터 제11호의 합계액을 15억원으로 한다.
② 금융회사 또는 전자금융업자가 전자금융사고 책임이행을 위한 준비금을 적립하는 경우에는 제1항 각 호에서 정한 금액 이	② ---------- ---------- ---------- 전자금융거래 규모, 전자금융사

상의 금액을 보유하고 책임이행이 신속히 이루어질 수 있도록 준비금 관리 및 지급에 관한 내부 절차를 수립하여 운영하여야 한다.	고 발생 건수 등을 고려하여 제1항 ----------.
③·④ (생 략)	③·④ (현행과 같음)
제7조(전자금융거래 종류별 안전성 기준) 법 제21조제2항의 “금융위원회가 정하는 기준”이라 함은 다음 각 호의 내용에 관하여 제8조 부터 제37조에서 정하는 기준을 말한다.	제7조(전자금융거래 종류별 안전성 기준) ---------- 제8조부터 제36조 및 제37조의5----------.
1. 인력, 조직 및 예산 부문	1. --- 조직, 교육 ------
2. (생 략)	2. (현행과 같음)
3. 단말기, 전산자료, 정보처리시스템 및 정보통신망 등 정보기술부문	3. ----- 전산자료 및 정보처리시스템 --------
<신 설>	4. 해킹, 악성코드 감염 등 정보보호부문
<신 설>	5. 정보처리시스템 및 전자금융거래 관련 사업 부문
<신 설>	6. 비상대책 등 업무지속성부문
<신 설>	7. 전산원장통제, 프로그램 통제 등 정보기술부문 내부통제
4. (생 략)	8. (현행 제4호와 같음)
제2절 인력, 조직 및 예산 부문	제2절 인력, 조직, 교육 및

	예산 부문
제8조(인력, 조직 및 예산) ① 금융회사 또는 전자금융업자는 인력 및 조직의 운용에 관하여 다음 각 호의 사항을 준수하여야 한다.	제8조(인력, 조직 및 예산) ① ---------- ---------- ---------- ---.
1.·2. (생 략)	1.·2. (현행과 같음)
3. 전산인력의 자질향상 및 예비요원 양성을 위한 교육 및 연수프로그램을 운영할 것	3. 정보보호최고책임자는 임직원의 정보보호역량 강화를 위하여 매년 교육계획을 수립·시행하여야 한다.
<신 설>	4. 최고경영자는 전년도 교육계획 시행 결과를 평가하고 그 결과를 금년도 교육계획에 반영해야 한다.
4. 정보보호최고책임자는 임직원이 정보보안 관련법규가 준수되고 있는지 정기적으로 점검하고 그 점검결과를 최고경영자에게 보고할 것	5. ---------- 임직원의 정보보안 관련법규를 준수하고 ---------- ------- 점검결과 및 보완계획을 ----------
5. (생 략)	6. (현행 제5호와 같음)
② 금융회사 또는 전자금융업자는 인력 및 예산에 관하여 다음 각 호의 사항을 준수하도록 노력하여야 한다.	② 금융회사 또는 전자금융업자는 정보기술 및 정보보호 분야별 전문성을 갖춘 인력과 충분한 예산을 확보해야 한다.
1. 정보기술부문 인력은 총 임	<삭 제>

직원수의 100분의 5 이상, 정보보호인력은 정보기술부문 인력의 100분의 5 이상이 되도록 할 것	
2. 정보보호예산을 정보기술부문 예산의 100분의 7 이상이 되도록 할 것	<삭 제>
③ 제2항 각 호의 사항을 이행하지 못하는 금융회사 또는 전자금융업자는 그 사유 및 이용자 보호에 미치는 영향 등을 설명한 자료를 해당 금융회사 또는 전자금융업자가 운영하는 홈페이지 등을 통해 매 사업연도 종료 후 1개월 이내에 공시하여야 한다. 다만, 허가, 등록 또는 인가를 마친 후 1년이 지나지 않은 금융회사 또는 전자금융업자는 공시하지 아니할 수 있다. <단서신설 2016. 10. 5.>	<삭 제>
④ 제2항제1호의 인력에 관한 기준은 <별표 1>과 같으며, 제2항제2호의 예산에 관한 기준은 <별표 2>와 같다.	<삭 제>
제8조의2(정보보호위원회 운영)	제8조의2(정보보호위원회 운영)
① ~ ③ (생 략)	① ~ ③ (현행과 같음)

④ 정보보호최고책임자는 정보보호위원회 심의·의결사항을 최고경영자에게 보고하여야 한다.	④ ---------- 하며, 전자금융거래의 안전성 및 신뢰성에 중대한 영향을 미치는 심의·의결사항에 대해서는 이사회에 보고 하여야 한다.
⑤ (생 략)	⑤ (현행과 같음)
제9조(건물에 관한 사항) 금융회사 또는 전자금융업자는 전산실이 위치한 건물에 관하여 다음 각 호의 사항을 준수하여야 한다.	제9조(건물에 관한 사항) 금융회사 또는 전자금융업자는 전산실이 위치한 건물에 관하여 안전대책 및 출입통제 보안대책을 수립·운용해야 한다.
1. 건물 출입구는 경비원에 의하여 통제하고 출입통제 보안대책을 수립·운용할 것	1. 삭제
2. 비상시 대피를 위한 비상계단 및 정전대비 유도등을 설치할 것	2. 삭제
3. 번개, 과전류 등 고전압으로 인한 전산장비 및 통신장비 등의 피해 예방을 위하여 피뢰설비를 갖출 것	3. 삭제
4. 서버, 스토리지(Storage) 등 전산장비 및 통신장비 등의 중량을 감안한 적재하중 안전	4. 삭제
	5. 삭제
	6. 삭제

대책을 수립·운용할 것 5. 화재발생 시 조기진압을 위한 소화기 및 자동소화설비 등을 갖추고, 화재전파방지를 위한 배연설비설치 등 화재예방 안전대책을 수립·운용할 것 6. 화재발생 위험이 높은 지역, 상습 침수지역 및 진동피해 발생지역 등 외부환경에 의하여 전산장비 등이 영향을 받을 수 있는 지역은 제외할 것	
제10조(전원, 공조 등 설비에 관한 사항) 금융회사 또는 전자금융업자는 전산실이 위치한 건물의 전원, 공조 등 설비에 관하여 다음 각 호의 사항을 준수하여야 한다. 1. 전원실, 공조실 등 주요 설비 시설에 자물쇠 등 출입통제장치를 설치할 것 2. 전원, 공조, 방재 및 방범 설비에 대한 적절한 감시제어시스템을 갖출 것 3. 전산실의 전력공급 중단에 대비하여 자가발전설비를 갖	제10조(전원, 공조 등 설비에 관한 사항) 금융회사 또는 전자금융업자는 전산실이 위치한 건물의 전원, 공조 등 설비의 안전성을 위한 기준을 수립·준수해야 한다. 1. 삭제 2. 삭제 3. 삭제 4. 삭제 5. 삭제 6. 삭제 7. 삭제

출 것 4. 전력공급 장애 시 전력선 대체가 가능하도록 복수회선을 설치하고 전력공급의 연속성 유지를 위한 무정전전원장치(Uninterruptible Power Supply : UPS)를 갖출 것 5. 과전류, 누전에 의한 장애 방지를 위하여 과전류차단기, 누전경보기 등을 설치하고 일정한 전압 및 주파수 유지를 위한 정전압정주파수장치(Constant Voltage Constant Frequency : CVCF)를 갖출 것 6. 전산실에 공급되는 전원 및 공조 설비는 부하가 큰 설비 부분과 분리하여 설치하고 공조 설비 상태 점검을 위한 압력계, 온도계 등을 갖출 것 7. 전산실에 24시간 동안 적정한 온도 및 습도를 유지하기 위해서 자동제어 항온·항습기를 갖출 것	
제11조(전산실 등에 관한 사항) 금융회사 또는 전자금융업자는 전산실에 관하여 다음 각 호의	제11조(전산실 등에 관한 사항) 금융회사 또는 전자금융업자는 전산실에 관하여 다음 각 호의

사항을 준수하여야 한다. 1. 화재·수해 등의 재해 및 외부 위해(危害) 방지대책을 수립·운용할 것 2. 상시 출입문은 한 곳으로 정하며 상시 출입은 업무와 직접 관련이 있는 사전 등록자에 한하여 허용하고, 그 밖의 출입자에 대하여는 책임자의 승인을 받아 출입하도록 하며 출입자 관리기록부를 기록·보관할 것 3. 상시 출입이 허용된 자 이외의 출입자의 출입사항에 대하여는 전산실의 규모 및 설치장소 등을 감안하여 무인감시카메라 또는 출입자동기록시스템 설치 등 적절한 조치를 취하여 사후 확인이 가능하도록 할 것 4. 출입문은 이중 안전장치로 보호하며 외벽이 유리인 경우 유리창문을 통하여 접근할 수 없도록 조치할 것 5. 천정·바닥·벽의 침수로 인한 정보처리시스템의 장애가	사항을 포함한 대책을 수립·준수하여야 한다. 1. 국내에 본점을 둔 금융회사 또는 전자금융업자의 전산실 및 재해복구센터는 국내에 설치할 것 단, 제50조제2항에 따라 등록한 국외 사이버몰을 위한 전자지급 결제대행업자는 제외 2. 무선통신망을 설치하지 아니할 것 3. 그 밖에 재해 및 위해방지, 출입·접근통제 등 전산실의 안전 및 보안에 관한 사항 4. 삭제 5. 삭제 6. 삭제 7. 삭제 8. 삭제 9. 삭제 10. 삭제 11. 삭제 12. 삭제

발생하지 않도록 외벽과 전산장비와의 거리를 충분히 유지하고 이중바닥설치 등 방안을 강구할 것 6. 적정수준의 온도·습도를 유지하기 위하여 온도·습도 자료 자동기록장치 및 경보장치 설치 등 적절한 조치를 취할 것 7. 케이블이 안전하게 유지되도록 전용 통로관 설치 등 적절한 보호조치를 강구할 것 8. 정전에 대비하여 조명설비 및 휴대용손전등을 비치할 것 9. 집적정보통신시설(Internet Data Center : IDC) 등과 같이 다수의 기관이 공동으로 이용하는 장소에 정보처리시스템을 설치하는 경우에는 미승인자가 접근하지 못하도록 적절한 접근통제 대책을 마련할 것 10. 다음 각 목의 중요 시설 및 지역을 보호구역으로 설정 관리할 것 가. 전산센터 및 재해복구센	

터 나. 전산자료 보관실 다. 정보보호시스템 설치장소 라. 그 밖에 보안관리가 필요하다고 인정되는 정보처리 시스템 설치장소 11. 국내에 본점을 둔 금융회사의 전산실 및 재해복구센터는 국내에 설치할 것 12. 무선통신망을 설치하지 아니할 것	
제12조(단말기 보호대책) 금융회사 또는 전자금융업자는 단말기 보호를 위하여 다음 각 호의 사항을 준수하여야 한다.	제12조(단말기 보호대책) ----------.
1. 업무담당자 이외의 사람이 단말기를 무단으로 조작하지 못하도록 조치할 것	1. 단말기는 인가된 사용자만 사용할 수 있도록 관리할 것
2. (생 략)	2. (현행과 같음)
3. 외부 반출, 인터넷 접속, 그룹웨어 접속의 금지 등 강화된 보호대책이 적용되는 중요단말기를 지정할 것	3. ---------- 금지, 정기적인 악성코드 감염여부 확인 ----------
4. 정보유출, 악성코드 감염 등을 방지할 수 있도록 단말기에서 보조기억매체 및 휴대용	4. 정보유출 및 ---------- 등에 ----

전산장비에 접근하는 것을 통제할 것	----------
제13조(전산자료 보호대책) ① 금융회사 또는 전자금융업자는 전산자료의 유출, 파괴 등을 방지하기 위하여 다음 각 호를 포함한 전산자료 보호대책을 수립·운용하여야 한다.	제13조(전산자료 보호대책) ① ----------
1. 사용자계정과 비밀번호를 개인별로 부여하고 등록·변경·폐기를 체계적으로 관리할 것	1. 사용자 인증 수단을 개인별로 부여하고 접근권한은 최소한으로 부여하는 등 적절한 접근권한 관리 및 통제 절차를 수립·운용할 것
2. 외부사용자에게 사용자계정을 부여하는 경우 최소한의 작업권한만 할당하고 적절한 통제장치를 갖출 것	<삭 제>
3. (생 략)	2. (현행 제3호와 같음)
4. 전산자료의 입력·출력·열람을 함에 있어 사용자의 업무별로 접근권한을 통제할 것	<삭 제>
5. (생 략)	3. (현행 제5호와 같음)
6. 비상시에 대비하여 보조기억매체 등 전산자료에 대한 안전지출 및 긴급파기 계획을 수립·운용할 것	4. ----------여 전산자료----------

7. ~ 10. (생 략)	5. ~ 8. (현행 제7호부터 제10호까지와 같음)
11. 정보처리시스템의 가동기록은 1년 이상 보존할 것	9. ---------- -- 금융감독원장이 정하는 사항을 접속의 성공여부와 상관없이 자동적으로 기록·유지하고 1년 ---
12. 정보처리시스템 접속 시 5회 이내의 범위에서 미리 정한 횟수 이상의 접속 오류가 발생하는 경우 정보처리시스템의 사용을 제한할 것	<삭 제>
13. (생 략)	10. (현행 제13호와 같음)
14. 사용자가 전출·퇴직 등 인사조치가 있을 때에는 지체 없이 해당 사용자 계정 삭제, 계정 사용 중지, 공동 사용 계정 변경 등 정보처리시스템에 대한 접근을 통제할 것	11. ---------- ---------- ------- 사용자계정 ------ ---------- ---------- ----------
② 제1항제1호의 사용자계정의 공동 사용이 불가피한 경우에는 개인별 사용내역을 기록·관리하여야 한다.	② 사용자계정---------- ---------- ---------- --------
③ 금융회사 또는 전자금융업자는 단말기를 통한 이용자 정보 조회 시 사용자, 사용일시, 변경	<삭 제>

·조회내용, 접속방법이 정보처리시스템에 자동적으로 기록되도록 하고, 그 기록을 1년 이상 보존하여야 한다.	
④ 제1항제11호의 정보처리시스템 가동기록의 경우 다음 각 호의 사항이 접속의 성공여부와 상관없이 자동적으로 기록·유지되어야 한다.	<삭 제>
1. 정보처리시스템에 접속한 일시, 접속자 및 접근을 확인할 수 있는 접근기록	
2. 전산자료를 사용한 일시, 사용자 및 자료의 내용을 확인할 수 있는 접근기록	
3. 정보처리시스템내 전산자료의 처리 내용을 확인할 수 있는 사용자 로그인, 액세스 로그 등 접근기록	
⑤ (생 략)	③ (현행 제5항과 같음)
제14조(정보처리시스템 보호대책) 금융회사 또는 전자금융업자는 정보처리시스템의 안전한 운영을 위하여 다음 각 호를 포함한 보호대책을 수립·운용하여야 한다.	제14조(정보처리시스템 보호대책) ---------- ---------- -- 위하여 운영매뉴얼, 유지보수관리대장, 책임자명부 및 장애상황기록부 등 ----------

	---.
1. 주요 정보처리시스템에 대한 구동, 조작방법, 명령어 사용법, 운용순서, 장애조치 및 연락처 등 시스템 운영매뉴얼을 작성할 것	1. 다음 각 목을 작성·보관 할 것 가. 주요 정보처리시스템에 대한 운영매뉴얼 나. 주요 정보처리시스템에 대한 정기적인 유지보수 실시 내용을 기록한 유지보수관리대장 다. 정보처리시스템에 대한 책임자명부 및 장애상황기록부
2. 데이터베이스관리시스템(Database Management System : DBMS)·운영체제·웹프로그램 등 주요 프로그램에 대하여 정기적으로 유지보수를 실시하고, 작업일, 작업내용, 작업결과 등을 기록한 유지보수관리대장을 작성·보관할 것	<삭 제>
3. 정보처리시스템의 장애발생시 장애일시, 장애내용 및 조치사항 등을 기록한 장애상황기록부를 상세하게 작성·보관할 것	<삭 제>
4. 정보처리시스템의 정상작동	2. ----------

여부 확인을 위하여 시스템 자원 상태의 감시, 경고 및 제어가 가능한 모니터링시스템을 갖출 것	---------- ---------- -- 가능하도록 ---------- --------
5. (생 략)	3. (현행 제5호와 같음)
6. 정보처리시스템의 책임자를 지정·운영할 것	<삭 제>
7. 정보처리시스템의 운영체계, 시스템 유틸리티 등의 긴급하고 중요한 보정(patch)사항에 대하여는 즉시 보정 작업을 할 것	4. ---------- 긴급----- ---------- ---------- ---------- ---
8. (생 략)	5. (현행 제8호와 같음)
9. 정보처리시스템의 운영체제(Operating System) 계정으로 로그인(Log in)할 경우 계정 및 비밀번호 이외에 별도의 추가인증 절차를 의무적으로 시행할 것	<삭 제>
10. 정보처리시스템 운영체제(Operating System) 계정에 대한 사용권한, 접근 기록, 작업내역 등에 대한 상시 모니터링체계를 수립하고, 이상 징후 발생 시 필요한 통제 조치를 즉시 시행할 것	6. 정보처리시스템의 운영체제(Operating System) 계정으로 로그인(Log in)할 경우 이중 인증 절차를 시행하고, --- 수립하며---------- ------

제14조의2(클라우드컴퓨팅서비스 이용절차 등) ①·② (생 략)	제14조의2(클라우드컴퓨팅서비스 이용절차 등) ①·② (현행과 같음)
③ 금융회사 또는 전자금융업자는 제1항제2호의 평가를 직접 수행하거나 제37조의4제1항의 침해사고대응기관이 수행한 평가 결과를 활용할 수 있다.	③ ---------- 제37조의6제1항----------
④ 금융회사 또는 전자금융업자는 다음 각 호의 어느 하나에 해당하는 사유가 발생한 날로부터 3개월 이내에 발생 사유, 관련 자료 및 대응계획을 첨부하여 금융감독원장에게 보고하여야 한다.	④ ---------- 금융감독원장에게 보고하여야 하고, 관련 서류를 최신상태로 유지하여야 한다.
1. 클라우드컴퓨팅서비스 이용계약을 신규로 체결하는 경우	1. ---------- 체결하거나, 기존 클라우드컴퓨팅서비스 이용계약을 통해 신규 업무를 처리하는 ---
2. ~ 4. (생 략)	2. ~ 4. (현행과 같음)
⑤ 제4항에 따라 금융감독원장에게 보고할 경우 첨부해야 하는 서류는 다음 각 호와 같다.	⑤ 제4항의 보고에 관한 양식, 첨부서류 등에 관해서는 금융감독원장이 정하는 바에 따른다.
1. 「금융회사의 정보처리 업무 위탁에 관한 규정」 제7조제1	<삭 제>

항 각 호에 관한 서류	
2. 제1항제1호에 따른 업무의 중요도 평가 기준 및 결과	<삭 제>
3. 제1항제2호에 따른 클라우드컴퓨팅서비스 제공자의 건전성 및 안전성 등에 대한 평가 결과	<삭 제>
4. 제1항제3호에 따른 업무 연속성 계획 및 안전성 확보조치에 관한 사항	<삭 제>
5. 제2항에 따른 정보보호위원회 심의·의결 결과	<삭 제>
6. <별표 2의5>의 계약서 주요 기재사항을 포함한 클라우드컴퓨팅서비스 이용계약서	<삭 제>
⑥ 클라우드컴퓨팅서비스를 이용하는 금융회사 또는 전자금융업자는 제4항에 따른 보고의무와 관계없이 제5항 각호에 따른 서류를 최신상태로 유지하여야 하며, 금융감독원장의 요청이 있을 경우 이를 지체 없이 제공하여야 한다.	<삭 제>
⑦ (생 략)	⑥ (현행 제7항과 같음)
⑧ 제1항의 절차를 거친 클라우드컴퓨팅서비스 제공자의 정보	⑦ ----------

처리시스템이 위치한 전산실에 대해서는 제11조제11호 및 제12호, 제15조제1항제5호를 적용하지 아니한다. 다만, 금융회사 또는 전자금융업자(전자금융거래의 안전성 및 신뢰성에 중대한 영향을 미치지 않는 외국금융회사의 국내지점, 제50조의2에 따른 국외 사이버몰을 위한 전자지급결제대행업자는 제외한다)가 고유식별정보 또는 개인신용정보를 클라우드컴퓨팅서비스를 통하여 처리하는 경우에는 제11조제12호를 적용하고, 해당 정보처리시스템을 국내에 설치하여야 한다. <단서신설 2018. 12. 21., 개정 2022. 11. 23.>	---------- ------ 제11조제1호 및 제2호- ---------- --------. ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- --제11조제2호---------- ---------- ----------.
⑨ (생 략)	⑧ (현행 제9항과 같음)
<신 설>	제5절 정보보호부문
제15조(해킹 등 방지대책) ① 금융회사 또는 전자금융업자는 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해행위로부터 방지하기 위하여 다음 각 호의 대책을 수립·운용하여야 한다.	제15조(해킹 등 방지대책) ① --- ---------- ---------- ---------- ---------- ----------.
1.·2. (생 략)	1.·2. (현행과 같음)

3. 내부통신망과 연결된 내부 업무용시스템은 인터넷(무선통신망 포함) 등 외부통신망과 분리·차단 및 접속 금지. 다만, 다음 각 목의 경우에는 그러하지 아니하다.	3. ----------.
가. 이용자의 고유식별정보 또는 개인신용정보를 처리하지 않는 연구·개발 목적의 경우(단, 금융회사 또는 전자금융업자가 자체 위험성 평가를 실시한 후 금융감독원장이 정한 망분리 대체 정보보호통제를 적용한 경우에 한한다)	가. ---------- 적용하고 정보보호위원회가 승인한 경우에 한한다.----
나. (생 략)	나. (현행과 같음)
4. (생 략)	4. (현행과 같음)
5. 전산실 내에 위치한 정보처리시스템과 해당 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기에 대해서는 인터넷 등 외부통신망으로부터 물리적으로 분리할 것. 다만, 다음 각 목의 경	5. ----------. ----------

우에는 그러하지 아니하다.	----------.
가. 이용자의 고유식별정보 또는 개인신용정보를 처리하지 않는 연구·개발 목적의 경우(단, 금융회사 또는 전자금융업자가 자체 위험성 평가를 실시한 후 금융감독원장이 정한 망분리 대체 정보보호통제를 적용한 경우에 한한다)	가. ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- 적용하고 정보보호위원회가 승인한 경우에 한한다.----
나. (생 략)	나. (현행과 같음)
② 제1항제1호의 규정에 따른 정보보호시스템을 설치·운영하는 경우에는 다음 각 호의 사항을 준수하여야 한다.	② ---------- 정보보호시스템의 안전한 운영을 위하여 금융감독원장이 정하는 ----------.
1. 삭 제	
2. 최소한의 서비스번호(port)와 기능만을 적용하고 업무목적 이외의 기능 및 프로그램을 제거할 것	<삭 제>
3. 보안정책의 승인·적용 및 보안정책의 등록, 변경 및 삭제에 대한 이력을 기록·보관할 것	<삭 제>

4. 정보보호시스템 원격관리를 금지할 것. 다만, 원격관리가 불가피한 경우 전용회선(전용회선과 동등한 보안수준을 갖춘 가상의 전용회선을 포함한다) 사용, 접근통제 등을 포함한 원격 접속 보안 대책을 수립·운영할 것	<삭 제>
5. 정보보호시스템의 작동 상태를 주기적으로 점검할 것	<삭 제>
6. 시스템 장애, 가동중지 등 긴급사태에 대비하여 백업 및 복구 절차 등을 수립·시행할 것	<삭 제>
③ (생 략)	③ (현행과 같음)
④ 금융회사 또는 전자금융업자는 해킹 등 전자적 침해행위로 인한 피해 발생시 즉시 대처할 수 있도록 적절한 대책을 마련하여야 한다.	④ ---------- 침해의 예방, 피해 최소화 및 신속한 복구를 위한 대책을 수립·운용----------.
⑤ 삭 제	
⑥ 금융회사 또는 전자금융업자는 무선통신망을 설치·운용할 때에는 다음 각 호의 사항을 준수하여야 한다.	⑥ ----------.
1.·2. (생 략)	1.·2. (현행과 같음)

3. 금융회사 내부망에 연결된 정보처리 시스템이 지정된 업무 용도와 사용 지역(zone) 이외의 무선통신망에 접속하는 것을 차단하기 위한 차단시스템을 구축하고 실시간 모니터링체계를 운영할 것	3. 무선통신망에 인가되지 않은 정보처리시스템 및 단말기의 접속을 차단하여야 하며, 비인가 무선접속장비(Access Point: AP) 설치·접속여부, 중요정보 노출여부를 주기적으로 점검할 것
4. 비인가 무선접속장비(Access Point : AP) 설치·접속여부, 중요 정보 노출여부를 주기적으로 점검할 것	<삭 제>
<신 설>	⑦ 금융회사 또는 전자금융업자는 단말기에서 음란, 도박 등 업무와 무관한 프로그램 또는 인터넷 사이트에 접근하는 것에 대한 통제대책을 마련하여야 한다.
제16조(악성코드 감염 방지대책) ① 금융회사 또는 전자금융업자는 악성코드 감염을 방지하기 위하여 다음 각 호를 포함한 대책을 수립·운용하여야 한다.	제16조(악성코드 감염 방지대책) 금융회사 또는 전자금융업자는 악성코드 감염·확산 방지, 피해 최소화 및 복구를 위한 대책을 수립·준수하여야 한다.
1. 응용프로그램을 사용할 때에는 악성코드 검색프로그램 등으로 진단 및 치료 후 사용할 것	

2. 악성코드 검색 및 치료프로그램은 최신상태로 유지할 것 3. 악성코드 감염에 대비하여 복구 절차를 마련할 것 4. 제12조제3호에 따른 중요 단말기는 악성코드 감염여부를 매일 점검할 것 ② 금융회사 또는 전자금융업자는 악성코드 감염이 발견된 경우 악성코드 확산 및 피해를 최소화하기 위하여 필요한 조치를 신속하게 취하여야 한다.	
제17조(홈페이지 등 공개용 웹서버 관리대책) ① 금융회사 또는 전자금융업자는 공개용 웹서버의 안전한 관리를 위하여 다음 각 호를 포함한 적절한 대책을 수립·운용하여야 한다. 1. 공개용 웹서버를 내부통신망과 분리하여 내부통신망과 외부통신망사이의 독립된 통신망(이하 “DMZ구간”이라 한다)에 설치하고 네트워크 및 웹 접근제어 수단으로 보호할 것 2. 공개용 웹서버에 접근할 수	제17조(홈페이지 등 공개용 웹서버 관리대책) 금융회사 또는 전자금융업자는 공개용 웹서버의 안전한 관리를 위하여 다음 각 호를 포함한 적절한 대책을 수립·운용하여야 한다. 1. 공개용 웹서버를 내부통신망과 분리하여 내부통신망과 외부통신망사이의 독립된 통신망(이하 “DMZ구간”이라 한다)에 설치하고 네트워크 및 웹 접근제어 수단으로 보호할 것 2. 공개용 웹서버에 접근할 수

있는 사용자계정은 업무관련자만 접속할 수 있도록 제한하고 아이디·비밀번호 이외에 추가 인증수단을 적용할 것	있는 사용자계정은 업무관련자만 접속할 수 있도록 제한하고 이중 인증수단을 적용할 것
3. 공개용 웹서버에서 제공하는 서비스를 제외한 다른 서비스 및 시험·개발 도구 등의 사용을 제한할 것	3. 공개용 웹서버에서 제공하는 서비스를 제외한 다른 서비스 및 시험·개발 도구 등의 사용을 제한하고, DMZ구간 내에 이용자 정보 등 주요 정보를 저장 및 관리하지 아니할 것(다만, 거래로그를 관리하기 위한 경우에는 예외로 하되 이 경우 반드시 암호화하여 저장·관리하여야 한다)
4. DMZ구간 내에 이용자 정보 등 주요 정보를 저장 및 관리하지 아니할 것(다만, 거래로그를 관리하기 위한 경우에는 예외로 하되 이 경우 반드시 암호화하여 저장·관리하여야 한다)	4. 금융회사 또는 전자금융업자는 공개용 웹서버에 자료 게시 절차·내용에 관한 내부통제 방안과 개인정보 유출 및 위·변조를 방지하기 위한 보안조치 방안을 수립·운용하여야 한다.
② 금융회사 또는 전자금융업자는 공개용 웹서버에 게재된 내용에 대하여 다음 각 호의 사항을 준수하여야 한다.	
1. 게시자료에 대한 사전 내부통제 실시	
2. 무기명 또는 가명에 의한 게시 금지	
3. 홈페이지에 자료를 게시하는 담당자의 지정·운용	

4. 개인정보의 유출 및 위·변조를 방지하기 위한 보안조치 ③ 삭제 ④ 금융회사 또는 전자금융업자는 공개용 웹서버가 해킹공격에 노출되지 않도록 대응 조치하여야 한다. ⑤ 금융회사 또는 전자금융업자는 단말기에서 음란, 도박 등 업무와 무관한 프로그램 또는 인터넷 사이트에 접근하는 것에 대한 통제대책을 마련하여야 한다.	
제18조(IP주소 관리대책) 금융회사 또는 전자금융업자는 정보제공자 주소(이하 “IP주소”라 한다)의 안전한 사용을 위하여 다음 각 호를 포함하여 적절한 대책을 수립·운용하여야 한다.	제18조(IP주소 관리대책) ---------- 주소 체계·할당·관리 등에 대한 내용을 포함한 ---------- 수립·운용하고, 내부 IP주소 및 외부 IP주소의 인터넷 접속내용을 1년 이상 별도로 기록·보관---.
1. 내부통신망에서 사용하는 IP주소의 경우 사설 IP주소 사용 등으로 보안을 강화하며	<삭 제>

내부 IP주소체계의 외부유출을 금지할 것	
2. 개인별로 내부 IP주소를 부여하여 유지·관리할 것	<삭 제>
3. 내부 IP주소 및 외부 IP주소의 인터넷 접속내용을 1년 이상 별도로 기록·보관할 것	<삭 제>
4. 정보처리시스템의 운영담당, 개발담당 및 외부직원 등 업무 특성별로 네트워크를 적절하게 분리하여 IP주소를 사용할 것. 다만, 외부직원 등과의 공동작업 수행 등 네트워크의 분리가 어렵다고 금융감독원장이 정하는 경우에는 업무특성별로 접근권한을 분리하여 IP주소를 사용할 수 있다.	<삭 제>
5. 내부통신망은 다른 기관 내부통신망과 분리하여 사용할 것	<삭 제>
제5절 정보기술부문 내부통제	<삭 제>
제19조(정보기술부문 계획서 제출 절차 등) ① 시행령 제11조의2에 따라 금융위원회에 정보기술부문 계획서를 제출해야 하는 금융회사 또는 전자금융업자는	제36조의2(정보기술부문 계획서 제출 절차 등) ① ---------- ---------- ---------- ----------

현실적이고 실현 가능한 장·단기 정보기술부문 계획을 매년 수립·운용하여야 한다.	---------- ---------- ---------- 하며, 정보기술부문 계획서 제출에 관한 세부적인 절차, 양식 등에 관해서는 금융감독원장이 정하는 바에 따른다.
② (생 략)	② (현행과 같음)
제19조의2(정보보호 교육계획의 수립 시행) ① 정보보호최고책임자는 임직원의 정보보호역량 강화를 위하여 필요한 교육프로그램을 개발하고, 다음 각 호의 기준에 따라 매년 교육계획을 수립·시행하여야 한다. 1. 임원 : 3시간 이상(단, 정보보호최고책임자는 6시간 이상) 2. 일반직원 : 6시간 이상 3. 정보기술부문업무 담당 직원 : 9시간 이상 4. 정보보호업무 담당 직원 : 12시간 이상 ② 최고경영자는 정보보호교육을 실시한 이후 대상 임직원에 대해 평가를 실시하여야 한다. ③ 제1항의 교육프로그램 개발	<삭 제>

과 정보보호교육은 정보보호 전문 교육기관에 위탁할 수 있다. <신 설>	
제20조(정보처리시스템 구축 및 전자금융거래 관련 사업 추진) 금융회사 또는 전자금융업자는 정보처리시스템 및 전자금융거래와 관련된 사업을 추진하는 경우에 다음 각 호의 사항을 준수하여야 한다. 1. 조직에 미치는 영향이 크거나 내부직무전결기준에 따라 부서장 전결 금액 이상의 사업 추진 시에는 사전에 충분한 타당성 검토를 실시할 것 2. 정보처리시스템의 신규 사업 및 통합·전환·재개발 등과 같은 주요 추진사업에 대하여 비용 대비 효과분석을 실시할 것 3. 타당성 검토와 비용 대비 효과분석 결과는 전산운영위원회 등 독립적인 조직의 승인을 받을 것 4. 정보처리시스템의 안전성과 신뢰성을 확보하기 위하여 분	제6절 사업부문 제20조(정보처리시스템 구축 및 전자금융거래 관련 사업 추진) 금융회사 또는 전자금융업자는 정보처리시스템 및 전자금융거래와 관련된 사업 추진에 대한 내부통제 기준을 수립·준수하여야 한다. 1. 삭제 2. 삭제 3. 삭제 4. 삭제

석·설계 단계부터 보안대책을 강구할 것	
제21조(정보처리시스템 구축 및 전자금융거래 관련 계약) 금융회사 또는 전자금융업자는 정보처리시스템 구축 및 전자금융거래와 관련된 계약 체결 시에 다음 각 호의 사항을 준수하여야 한다.	제21조(정보처리시스템 구축 및 전자금융거래 관련 계약) 금융회사 또는 전자금융업자는 정보처리시스템 구축 및 전자금융거래와 관련된 계약 체결시에 정보처리시스템의 안전성·신뢰성 및 계약의 공정성이 확보될 수 있도록 체결·이행·감사 등에 관한 내용을 포함한 내부통제 절차를 수립·운용해야 한다.
1. 적합한 업체를 공정하게 선정하기 위하여 객관적인 업체 선정 기준 및 절차를 마련·운용할 것	1. 삭제
2. 정보처리시스템의 안전성과 신뢰성을 확보하기 위하여 제1호에 따른 기준 및 절차의 내용에는 정보보안 관련 사항을 포함할 것	2. 삭제
3. 공정하고 합리적인 예정가격 산출 기준을 수립·적용할 것	3. 삭제
4. 계약금액, 구축완료일자, 납품방법 및 대금지급방법 등 계약이행에 필요한 내용을 포함한 계약서 작성 기준을 수립·운용할 것	4. 삭제
5. 구매 또는 개발한 제품의 소	5. 삭제
	6. 삭제
	7. 삭제
	8. 삭제
	9. 삭제

유권, 저작권 및 지적재산권 등의 귀속관계를 명확히 하여 사후 분쟁이 발생하지 않도록 할 것 6. 납품 또는 개발이 완료된 소프트웨어 등에 대하여 공급업체 파산 등 비상사태에 대비한 대책을 마련·운용할 것 7. 검수는 개발자, 계약자 등 이해당사자를 배제하여 공정하게 실시할 것 8. 계약조항을 이행하지 못하는 사유가 발생하였거나 계약조항을 변경할 경우에는 검사부서의 승인을 받을 것 9. 내부감사규정에 따라 감사가 정한 금액 이상의 계약에 대하여는 자체 감사를 실시하거나 검사부서의 승인을 받을 것	
제22조(정보처리시스템 감리) 금융회사 또는 전자금융업자는 정보처리시스템의 안전성 및 효율성 확보를 위하여 다음 각 호의 사항을 포함한 정보처리시스템 감리 지침을 작성·운용하여야	제22조(정보처리시스템 감리) -- ---------- ---------- ------- 위한 ---------- ---------- ----------

한다.	---.
1. 목적 및 대상, 시스템 감리인, 감리시기 및 계획 등 일반기준	<삭 제>
2. 기획, 개발 및 운용의 감리 실시 기준	<삭 제>
3. 지적사항 및 개선사항 등 감리 후 보고 기준	<삭 제>
4. 전자금융업무와 관련된 외부주문등에 대한 감리 기준	<삭 제>
<신 설>	제7절 업무지속성 부문
제23조(비상대책 등의 수립·운용) ① 금융회사 또는 전자금융업자는 장애·재해·파업·테러 등 긴급한 상황이 발생하더라도 업무가 중단되지 않도록 다음 각 호의 내용을 포함한 업무지속성 확보방안을 수립·준수하여야 한다.	제23조(비상대책 등의 수립·운용) ① ----------.
1. ~ 7. (생 략)	1. ~ 7. (현행과 같음)
<신 설>	8. 비상지원인력의 확보 및 운영
② 제1항에 따른 업무지속성 확보대책에는 비상사태에 대비한 다음 각 호의 안전대책이 반영되어야 한다.	<삭 제>

1. 파업 시 핵심전산업무 종사자의 근무지 이탈에 따른 정보처리시스템의 마비를 방지하기 위하여 비상지원인력을 확보·운영할 것 2. 비상사태 발생 시에도 정보처리시스템의 마비를 방지하고 신속히 원상복구가 될 수 있도록 정보처리시스템 운영에 대한 비상지원인력 또는 외부 전문업체를 활용하는 방안을 수립·운영할 것 3. 비상지원인력이 사용법을 충분히 이해하고 업무운용이 가능한 수준으로 전산시스템 운영지침서, 사용자매뉴얼 등을 쉽고 자세하게 작성하고 최신 상태로 유지할 것 4. 핵심전산업무 담당자 부재 시에도 비상지원 인력이 업무를 수행할 수 있도록 비상지원인력에 대한 연수를 실시할 것	
③ ~ ⑦ (생 략)	③ ~ ⑦ (현행과 같음)
⑧ 다음 각 호의 금융회사는 시스템 오류, 자연재해 등으로 인	⑧ ----------

한 전산센터 마비에 대비하여 업무지속성을 확보할 수 있도록 적정 규모·인력을 구비한 재해복구센터를 주전산센터와 일정 거리 이상 떨어진 안전한 장소에 구축·운용하여야 한다.	---------- ---------- ---------- ---------- ---------- ----------.
1. ~ 6. (생 략)	1. ~ 6. (현행과 같음)
<신 설>	6의2. 「여신전문금융업법」에 의한 시설대여업자, 할부금융업자, 신기술사업금융업자(다만, 시행령 제11조의3제1항에 해당하는 회사에 한한다.)
7. (생 략)	7. (현행과 같음)
8. 「상호저축은행법」에 의한 상호저축은행중앙회	8. ---------- 상호저축은행중앙회 및 자체 전산시스템을 구축하여 운영하는 상호저축은행
9.·10. (생 략)	9.·10. (현행과 같음)
<신 설>	11. 「전자금융거래법」에 의한 전자금융업자(다만, 연간 전자금융거래 총액이 2조원 이상인 회사에 한한다.)
⑨·⑩ (생 략)	⑨·⑩ (현행과 같음)
제24조(비상대응훈련 실시) ①·② (생 략)	제24조(비상대응훈련 실시) ①·② (현행과 같음)
③ 금융위원회는 제2항의 규정	③ ----------

에 따른 합동비상대응훈련을 실시할 때, 다음 각 호의 기관에게 지원을 요청할 수 있다.	----------.
1. 「정부조직법」 제15조에 따른 “국가정보원(국가사이버안전센터)”	1. 「정부조직법」 제17조----------
2. 「경찰법」 제2조에 따른 “경찰청(사이버테러대응센터)”	2. 「국가경찰과 자치경찰의 조직 및 운영에 관한 법률」 제12조에 따른 "경찰청(사이버수사국)"
3.·4. (생 략)	3.·4. (현행과 같음)
④ (생 략)	④ (현행과 같음)
제26조(직무의 분리) 금융회사 또는 전자금융업자는 다음 각 호의 업무에 대하여 직무를 분리·운영하여야 한다.	제8조의3(직무의 분리) ---------- 정보기술부문의 내부통제를 위한 직무분리 기준을 수립·운용----------.
1. 프로그래머와 오퍼레이터	<삭 제>
2. 응용프로그래머와 시스템프로그래머	<삭 제>
3. 시스템보안관리자와 시스템프로그래머	<삭 제>
4. 전산자료관리자(librarian)와 그 밖의 업무 담당자	<삭 제>
5. 업무운영자와 내부감사자	<삭 제>
6. 내부인력과 전자금융보조업	<삭 제>

자 및 유지보수업자 등을 포함한 외부인력	
7. 정보기술부문인력과 정보보호인력	<삭 제>
8. 그 밖에 내부통제와 관련하여 직무의 분리가 요구되는 경우	<삭 제>
<신 설>	제8절 정보기술부문 내부통제
제27조(전산원장 통제) ① 금융기관 또는 전자금융업자는 장애 또는 오류 등에 의한 전산원장의 변경을 위하여 별도의 변경절차를 수립·운용하여야 한다.	제27조(전산원장 통제) ① ---------- 통제절차----------.
② ~ ⑤ (생 략)	② ~ ⑤ (현행과 같음)
제29조(프로그램 통제) 금융회사 또는 전자금융업자는 다음 각 호의 사항을 포함한 프로그램 등록·변경·폐기 절차를 수립·운용하여야 한다.	제29조(프로그램 통제) 금융회사 또는 전자금융업자는 프로그램 등록·변경·폐기 등에 관하여 금융감독원장이 정하는 사항을 포함한 절차를 수립·운용하여야 한다.
1. 적용대상 프로그램 종류 및 등록·변경·폐기 방법을 마련할 것	1. 삭제
2. 프로그램 변경 전후 내용을 기록·관리할 것	2. 삭제
3. 프로그램 등록·변경·폐기	3. 삭제
	4. 삭제
	5. 삭제

내용의 정당성에 대해 제3자의 검증을 받을 것 4. 변경 필요시 해당 프로그램을 개발 또는 테스트 시스템으로 복사 후 수정할 것 5. 프로그램에 대한 접근은 업무담당자에 한정할 것 6. 운영시스템 적용은 처리하는 정보의 기밀성·무결성·가용성을 고려하여 충분한 테스트 및 관련 책임자 승인 후 실시할 것 7. 프로그램 반출, 실행프로그램의 생성 및 운영시스템 등록은 전산자료 관리자 등 해당 프로그램 담당자 이외의 자가 수행할 것 8. 운영체제, 데이터베이스관리 프로그램 등의 시스템 프로그램도 응용프로그램과 동일한 수준으로 관리할 것 9. 프로그램 설명서, 입·출력 레코드 설명서, 프로그램 목록 및 사용자·운영자지침서 등 프로그램 유지보수에 필요한 문서를 작성·관리할 것	6. 삭제 7. 삭제 8. 삭제 9. 삭제 10. 삭제

10. 전자 금융거래에 사용되는 전산프로그램은 실제 업무를 처리하는 정보처리시스템에 설치하기 전에 자체 보안성 검증을 실시할 것	
제30조(일괄작업에 대한 통제) 금융회사 또는 전자금융업자는 안전하고 체계적인 일괄작업(batch)의 수행을 위하여 다음 각 호의 사항을 준수하여야 한다.	제30조(일괄작업에 대한 통제) 금융회사 또는 전자금융업자는 안전하고 체계적인 일괄작업(batch)의 수행을 위한 절차를 수립·준수하여야 한다.
1. 일괄작업은 작업요청서에 의한 책임자의 승인을 받은 후 수행할 것	1. 삭제
2. 일괄작업은 최대한 자동화하여 오류를 최소화할 것	2. 삭제
3. 일괄작업 수행 과정에서 오류가 발생하였을 경우 반드시 책임자의 확인을 받을 것	3. 삭제
4. 모든 일괄작업의 작업내용을 기록·관리할 것	4. 삭제
5. 책임자는 일괄작업 수행자의 주요업무 관련 행위를 모니터링할 것	5. 삭제
제31조(암호프로그램 및 키 관리 통제) ① (생 략)	제19조(암호프로그램 및 키 관리 통제) ① (현행과 같음)
② 금융회사 또는 전자금융업자	② ----------

는 암호 및 인증시스템에 적용되는 키에 대하여 주입·운용·갱신·폐기에 대한 절차 및 방법을 마련하여 안전하게 관리하여야 한다.	-------- 인증시스템 등에 적용되는 키(Key)(프로그램 진위 및 무결성 확인에 사용되는 암호 또는 인증시스템 등에 적용되는 키를 포함한다.)--------.
제32조(내부사용자 비밀번호 관리) 금융회사 또는 전자금융업자는 내부사용자의 비밀번호 유출을 방지하기 위하여 다음 각 호의 사항을 정보처리시스템에 반영하여야 한다.	제19조의2(사용자 인증수단 관리) ---------- 비밀번호, 생체정보 등 사용자 인증수단 ---- 인증수단의 발급·보관·주기적 변경 및 인증오류 발생시 처리 절차 등을 포함한 관리방안을 수립·준수---.
1. 담당업무 외에는 열람 및 출력을 제한할 수 있는 접근자의 비밀번호를 설정하여 운영할 것	<삭 제>
2. 비밀번호는 다음 각 목의 사항을 준수할 것	<삭 제>
가. 비밀번호는 이용자 식별부호(아이디), 생년월일, 주민등록번호, 전화번호를 포함하지 않은 숫자와 영문자 및 특수문자 등을 혼합하여 8자리 이상으로 설	

정하고 분기별 1회 이상 변경 나. 비밀번호 보관 시 암호화 다. 시스템마다 관리자 비밀번호를 다르게 부여	
3. 비밀번호 입력 시 5회 이내의 범위에서 미리 정한 횟수 이상의 입력오류가 연속하여 발생한 경우 즉시 해당 비밀번호를 이용하는 접속을 차단하고 본인 확인절차를 거쳐 비밀번호를 재부여하거나 초기화 할 것	<삭 제>
제33조(이용자 비밀번호 관리) ① (생 략) ② 금융회사 또는 전자금융업자는 이용자의 비밀번호 유출을 방지하기 위하여 다음 각 호의 사항을 정보처리시스템에 반영하여야 한다.	제34조의3(이용자 비밀번호 관리) ① (현행과 같음) ② ---------- 반영하고 이를 준수----------.
1. 주민등록번호, 동일숫자, 연속숫자 등 제3자가 쉽게 유추할 수 있는 비밀번호의 등록 불가	1. 제3자가 쉽게 유추할 수 없는 비밀번호 작성규칙 및 등록·변경 절차를 수립·운영할 것
2. 통신용 비밀번호와 계좌원장	<삭 제>

비밀번호를 구분해서 사용	
3. 5회 이내의 범위에서 미리 정한 횟수 이상의 비밀번호 입력 오류가 발생한 경우 즉시 해당 비밀번호를 이용하는 거래를 중지시키고 본인 확인절차를 거친 후 비밀번호 재부여 및 거래 재개(이체 비밀번호 등 동일한 비밀번호가 다양한 형태의 전자금융거래에 공통으로 이용되는 경우, 입력 오류 횟수는 이용되는 모든 전자금융거래에 대하여 통산한다)	2. 미리 ----------
4. 금융회사가 이용자로부터 받은 비밀번호는 거래전표, 계좌개설신청서 등에 기재하지 말고 핀패드(PIN pad) 등 보안장치를 이용하여 입력 받을 것	4. 이용자 비밀번호 변경 시 본인확인 절차를 수행할 것
5. (생 략)	3. (현행 제5호와 같음)
제6절 전자금융업무	<삭 제>
<신 설>	제9절 전자금융업무
제34조(전자금융거래 시 준수사항) 금융회사 또는 전자금융업자는 전자금융거래와 관련하여	제34조(전자금융거래 시 준수사항) ----------

다음 각 호의 사항을 준수하여야 한다.	----------.
1. ~ 3. (생 략)	1. ~ 3. (현행과 같음)
4. 거래인증수단 채택시 안전성, 보안성, 이용편의성 등을 충분히 고려할 것	<삭 제>
5. (생 략)	4. (현행 제5호와 같음)
제35조(이용자 유의사항 공지) 금융회사 또는 전자금융업자는 전자금융거래의 안전한 수행을 위하여 이용자에게 다음 각 호의 사항을 준수하도록 공지하여야 한다.	제35조(이용자 유의사항 공지) ---------- ---------- ---------- 필요한 사항을 ---------- ---.
1. 비밀번호 유출위험 및 관리에 관한 사항	<삭 제>
2. 금융기관 또는 전자금융업자가 제공하고 있는 이용자 보호제도에 관한 사항	<삭 제>
3. 해킹·피싱 등 전자적 침해 방지에 관한 사항	<삭 제>
4. 본인확인 절차를 거쳐 비밀번호 변경이 가능하도록 정보처리시스템을 구축하고 비밀번호 변경 시 같은 번호를 재사용하지 않도록 할 것	<삭 제>
제36조(자체 보안성심의) ① (생	제36조(자체 보안성심의) ① (현

략)	행과 같음)
② 금융회사 또는 전자금융업자는 제1항에 따른 심의(이하 “자체 보안성심의”라 한다)를 마친 후 제1항 각 호의 행위를 수행한 날로부터 7일 이내에 금융감독원장이 정하는 자체 보안성심의 결과보고서를 금융감독원에 제출하여야 한다. 다만, 제1항제1호에 따른 보안성심의의 경우 신규 전자금융업무가 제공 또는 시행된 날을 기준으로 과거 1년 이내에 전자금융사고가 발생하지 않은 기관으로서 금융감독원장이 정하는 기준에 해당하는 금융회사 또는 전자금융업자는 그러하지 아니하다.	② ---------- 30일 ----------.
③ (생 략)	③ (현행과 같음)
④ 제2항 및 제3항에도 불구하고 다음 각 호의 기관은 제1항제1호에 따른 자체 보안성심의 결과보고서의 제출을 하지 아니할 수 있다.	④ ----------.
1.·2. (생 략)	1.·2. (현행과 같음)
3. 「한국수출입은행법」에 따른 한국수출입은행	<삭 제>

4. (생 략)	3. (현행 제4호와 같음)
제37조 (생 략)	제34조의2 (현행 제37조와 같음)
<신 설>	제10절 취약점 분석 및 사고 대응 등
<신 설>	제37조의4(침해사고 통지의 방법) 금융회사 및 전자금융업자는 법 제21조의5에 따른 침해사고가 발생한 사실을 안 때에는 지체 없이 사고 내용, 사고에 따른 영향 등을 <별지 7호 서식>에 기재하여 금융위원회에 보고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여서는 아니된다.
제37조의4(침해사고대응기관 지정 및 업무범위 등) ①·② (생략)	제37조의6(침해사고대응기관 지정 및 업무범위 등) ①·② (현행과 같음)
③ 금융위원장은 침해사고대응기관을 포함하여 침해사고조사단을 구성할 수 있다.	③ 금융위원장은 제37조의4 및 제37조의5제3항에 따라 보고받은 내용으로서 전자적 침해행위가 원인이거나 원인으로 의심되는 경우 사고 조사 및 피해확산 방지를 위해 침해사고대응기관을 포함하여 침해사고조사단을 구성·운영할 수 있다.
④ ~ ⑦ (생 략)	④ ~ ⑦ (현행과 같음)

제37조의5(정보보호최고책임자의 업무) 정보보호최고책임자는 정보보안점검의 날을 지정하고, 임직원이 금융감독원장이 정하는 정보보안 점검항목을 준수했는지 여부를 매월 점검하고, 그 점검 결과 및 보완 계획을 최고경영자에게 보고하여야 한다.	<삭 제>
제60조(외부주문등에 대한 기준) ① ~ ④ (생 략) ⑤ 금융회사 또는 전자금융업자는 제14조의2제1항제2호에 따른 평가를 위하여 제37조의4제1항 각 호의 어느 하나에 해당하는 기관에 지원을 요청할 수 있다.	제60조(외부주문등에 대한 기준) ① ~ ④ (현행과 같음) ⑤ ---------- 제37조의6제1항 ----------.
제73조(정보기술부문 및 전자금융 사고보고) ① 금융회사 및 전자금융업자는 다음 각 호와 관련된 중대한 사고가 발생한 경우에는 지체 없이 금융감독원장에게 보고하여야 한다. 1. 정보처리시스템 또는 통신회선 등의 장애로 10분 이상 전산업무가 중단 또는 지연된 경우	제37조의5(정보기술부문 및 전자금융 사고보고) ① 금융회사 및 전자금융업자는 정보기술부문 및 전자금융과 관련된 사고에 관하여 다음 각 호를 준수하여야 한다. 1. 사고의 유형 분류, 처리단계, 조치방법, 영향도 및 심각도 평가 방법 등이 포함된 절차를 마련·운영

2. 전산자료 또는 프로그램의 조작과 관련된 금융사고가 발생한 경우	2. 금융감독원장이 정하는 사이버보안 사고가 발생한 경우에는 지체없이 금융감독원장에게 보고
3. 전자적 침해행위로 인해 정보처리시스템에 사고가 발생하거나 이로인해 이용자가 금전적 피해를 입었다고 금융회사 또는 전자금융업자에게 통지한 경우	<삭 제>
4. 법 제9조제1항의 규정에서 정하는 사고	<삭 제>
② 금융회사 및 전자금융업자는 제1항에 따른 사고보고를 고의로 지연하거나 숨긴 자에 대하여 소정절차에 따라 징계 등 필요한 조치를 취하여야 한다.	② ----------제1항제2호----------.
③ 금융감독원장은 제1항에 따라 보고 받은 내용을 지체 없이 금융위원장에게 보고하여야 하며, 제1항제3호에 따른 사고 발생시에는 제37조의4제1항 각 호에 따른 침해사고대응기관에도 알려야 한다.	③ ---------- 제1항제2호에 ---------- 한다.
④ 제1항의 사고보고와 관련하여 사고보고 절차 및 방법 등	④ 제1항제2호---------- 대상, 절차 ------

세부사항은 금융감독원장이 정하는 바에 따른다.	----------.

<별표 2의3> <전문개정>

클라우드컴퓨팅서비스 이용과 관련한 업무 연속성 계획(제14조의2 관련)

금융회사 또는 전자금융업자는 클라우드서비스에 대해 예상치 못한 재해 또는 사고 발생 시 업무 연속성에 미칠 수 있는 영향을 파악하고, 데이터 백업, 재해복구 및 침해 사고대응 훈련계획, 출구전략 등을 포함한 업무 연속성 계획을 수립하여 이행하여야 한다. 다만, 제14조의2제1항제1호에 따라 중요업무로 분류된 경우 필수 사항과 추가 사항을 모두 준수하여야 하고, 비중요업무로 분류된 경우 필수 사항만을 준수할 수 있다.

1. 데이터 백업 등 장애 대비	필수 사항 (전자금융감독규정상 규율사항)	- 제13조제1항제4호, 제13조제1항제6호내지7호, 제14조제1호내지3호, 제14조제5호, 제50조제1항제3호
	추가 사항	- 클라우드서비스와 관련된 중요 설정파일, 가상시스템 이미지 등을 데이터 백업 대상에 포함
2. 이중화 또는 예비장치 확보 등	필수 사항 (전자금융감독규정상 규율사항)	- 제23조제3항, 제23조제7항
	추가 사항	- 클라우드 서비스 제공과 관련된 지리적 특성, 동시 장애 발생 가능성 등을 고려하여 중복 설계 및 구성
3. 훈련 및 사고 관리	필수 사항 (전자금융감독규정상 규율사항)	- 제15조제4항, 제23조제1항, 제23조제3항내지6항, 제23조제8항내지10항, 제24조제1항내지4항, 제37조의6제5항
	추가 사항	- 훈련 및 사고관리 계획에 클라우드서비스 제공자의 역할, 책임, 비상연락망 등을 포함
4. 비상대책 수립	필수 사항 (전자금융감독규정상 규율사항)	- 제23조제5항
	추가 사항	- 계약 변경, 파산 등과 같은 중대한 상황 발생에

		대비한 공급 대체 방안, 업무 복구 가능성 식별 등 출구전략 수립

<별표 2의4> <전문개정>

클라우드컴퓨팅서비스 이용과 관련한 안전성 확보조치(제14조의2 관련)

클라우드서비스 관련 보안사고의 예방을 위해 계정관리, 접근통제 등 필수 보안 통제가 구현되도록 안전성 확보조치 방안을 수립하여 이행하여야 한다. 다만, 제14조의2제1항제1호에 따라 중요업무로 분류된 경우 필수 사항과 추가 사항을 모두 준수하여야 하고, 비중요업무로 분류된 경우 필수 사항만을 준수할 수 있다.

1.계정관리	필수 사항 (전자금융감독 규정상 규율사항)	- 제13조1제1항제1호, 제13조제1항제11호, 제13조제2항, 제14조제6호, 제17조제2호
	추가 사항	- 클라우드 관리 콘솔에 접근하는 관리자 계정에 대한 이중인증 등 강화된 보안조치 적용
2. 접근통제	필수 사항 (전자금융감독 규정상 규율사항)	- 제13조제1항제2호내지제3호, 제13조제3항, 제19조의2
	추가 사항	- 클라우드시스템 접근 절차를 문서화하고 관리 콘솔 관리자 계정의 경우 별도로 분리된 단말에서만 접근하도록 조치
3. 네트워크 보안	필수 사항 (전자금융감독 규정상 규율사항)	- 제15조제1항제3호, 제15조제6항제1호, 제17조제1호, 제18조
	추가 사항	- 시스템간 연계 및 클라우드서비스 내 주요 통신 채널에 대한 암호화 적용
4. 금융회사 등의	필수 사항 (전자금융감독	- 제12조제1호내지제4호, 제15조제1항제5호, 제34조제1호, 제60조제1항제5호

내부시스템과 클라우드 시스템 연계	규정상 규율사항)	
	추가 사항	- 내부시스템과 클라우드 시스템 간 연계되는 데이터의 식별 및 관리
5. 암호화 및 키 관리	필수 사항 (전자금융감독 규정상 규율사항)	- 제19조, 제34조의3제1항, 개인정보보호법ㆍ신용정보보호법ㆍ정보통신망법 등 관계법령에 따른 정보
	추가 사항	- 클라우드서비스 제공자 등 외부자의 키접근 가능성 등을 고려하여 키의 수명주기별 보안 관리 방안 수립
6. 로깅	필수 사항 (전자금융감독 규정상 규율사항)	- 제13조제1항제9호, 제18조, 제25조
	추가 사항	- 클라우드 관리 콘솔 관리자 등 주요 계정에 대한 활동 내역 로깅 및 주기적 검토
7. 가상 환경 보안	필수 사항 (전자금융감독 규정상 규율사항)	- 해당사항 없음
	추가 사항	- 가상 이미지 템플릿을 최신 상태로 유지하고, 이미지 무결성 등 보안사항을 주기적으로 점검
8. 보안 모니터링 및 취약점 분석·평가	필수 사항 (전자금융감독 규정상 규율사항)	- 제14조제1호, 제14조제4호, 제15조제1항제1호 내지제2호, 제15조제2항내지제3항, 제16조, 제37조의2
	추가 사항	- 클라우드서비스 내 주요 변경 사항에 대한 실시간 경보 설정 및 모니터링 실시
		- 주요 정보처리시스템의 경우 침해사고 대응기관의 통합보안관제 적용
9. 인적보안	필수 사항 (전자금융감독 규정상 규율사항)	- 제8조제1항제2호

	추가 사항	- 클라우드서비스 제공자 및 클라우드서비스 운영을 위탁받은 관리형 서비스 제공자 등의 권한과 책임을 식별하고 관리

<별지 제7호 서식>

<table>
<tr><td colspan="7">1. 기본 사항</td></tr>
<tr><td>보고자</td><td>금융회사명</td><td></td><td>보고 담당자
(부서명/성명)</td><td></td><td>연락처
(전화/이메일)</td><td></td></tr>
<tr><td>보고일시</td><td colspan="6"></td></tr>
<tr><td>보고형태</td><td colspan="6">☐ 최초 ☐ 중간 ☐ 종결</td></tr>
<tr><td colspan="7">2. 침해사고 발생 정보</td></tr>
<tr><td>공격 대상</td><td colspan="6">☐ 내부망 시스템 ☐ DMZ 구간 시스템 ☐ 기타( ) ☐ 미상(파악 중)</td></tr>
<tr><td>공격 방법</td><td colspan="6">☐ 악성코드(웹쉘, 랜섬웨어, 바이러스 등) ☐ 서비스 거부 (DDoS 공격 등)
☐ 보안취약점 해킹 ☐ 무단 접속 및 조작 ☐ 공급망 보안 침해(연계기관 해킹 등)
☐ 기타( ) ☐ 미상(파악 중)</td></tr>
<tr><td>최초 인지 경로</td><td colspan="6">☐ 금융회사 ☐ 외부( ) ☐ 고객(민원인) ☐ 기타( )</td></tr>
<tr><td>사고인지 일시</td><td colspan="2"></td><td>사고발생 일시</td><td colspan="3"></td></tr>
<tr><td>사고 지속시간</td><td colspan="2"></td><td>사고종료 일시</td><td colspan="3"></td></tr>
<tr><td>사고 발생 업무(시스템 등)</td><td colspan="2"></td><td>사고 발생 업무 중요도</td><td colspan="3">☐ 높음 ☐ 보통 ☐ 낮음</td></tr>
<tr><td>사고 내용
(현상 및 결과)</td><td colspan="6"></td></tr>
<tr><td>초동 조치사항</td><td colspan="6"></td></tr>
<tr><td colspan="7">3. 침해사고 영향</td></tr>
<tr><td>침해사고 결과
(복수 선택)</td><td colspan="6">☐ 시스템 및 서비스 중단(중단시간:)
☐ 정보유출(유출된 정보: / 유출량:)
※ 개인정보, 소스코드, 암호화 키, 인증서 등
☐ 주요 정보 조작(조작된 정보:)
☐ 금전적 손실(금액:)
☐ 기타 ( )
☐ 미상 (파악 중)</td></tr>
<tr><td>업무 연계 영향
(타기관 파급 등)</td><td colspan="6"></td></tr>
<tr><td colspan="7">4. 침해사고 대응 및 복구 (종결 보고 시 작성)</td></tr>
<tr><td>사고 해소 일시</td><td colspan="6"></td></tr>
<tr><td>처리 결과
(후속조치 등)</td><td colspan="6"></td></tr>
<tr><td>사고발생 원인</td><td colspan="6"></td></tr>
<tr><td>재발방지 대책</td><td colspan="6"></td></tr>
<tr><td colspan="7">[선택 입력사항] 금융회사 공격자 정보 제공</td></tr>
<tr><td>공격 방법</td><td colspan="6"></td></tr>
<tr><td>공격자 IP</td><td colspan="2"></td><td>Domain 정보</td><td colspan="3"></td></tr>
<tr><td>공격자 이메일</td><td colspan="6"></td></tr>
<tr><td>악성코드 정보
(해시 값 등)</td><td colspan="6"></td></tr>
<tr><td>상세내용</td><td colspan="6"></td></tr>
</table>