전자금융감독규정

[시행 2023. 1. 1.] [금융위원회고시 제2022-44호, 2022. 11. 23., 일부개정]

금융위원회(금융안전과), 02-2100-2943

제1조(목적) 이 규정은 「전자금융거래법」(이하 "법"이라 한다) 및 동법 시행령(이하 "시행령"이라 한다)에서 금융위원회에 위임한 사항과 그 시행에 필요한 사항 및 다른 법령에 따라 금융감독원의 검사를 받는 기관의 정보기술부문 안전성 확보 등을 위하여 필요한 사항을 규정함을 목적으로 한다.

제1장 총칙

제2조(정의) 이 규정에서 사용하는 용어의 정의는 다음과 같다.

1. "전산실"이라 함은 전산장비, 통신 및 보안장비, 전산자료 보관 및 출력장비가 설치된 장소를 말한다.
2. "전산자료"라 함은 전산장비에 의해 입력・보관・출력되어 있는 자료를 말하며 그 자료가 입력・출력되어 있는 자기테이프, 디스크, 디스켓, 콤팩트디스크(CD) 등 보조기억매체를 포함한다.
3. "정보처리시스템"이라 함은 전자금융업무를 포함하여 정보기술부문에 사용되는 하드웨어(hardware)와 소프트웨어(software)를 말하며 관련 장비를 포함한다.
4. "정보기술부문"이라 함은 컴퓨터 등 정보처리능력을 가진 장치를 이용하여 정보를 수집・가공・저장・검색・송신 또는 수신을 행하는 금융회사 또는 전자금융업자의 업무, 인력, 시설 및 조직을 말한다.<개정 2013. 12. 3.>
5. "정보보호" 또는 "정보보안"이라 함은 컴퓨터 등 정보처리능력을 가진 장치를 이용하여 수집・가공・저장・검색・송신 또는 수신되는 정보의 유출・위변조・훼손 등을 방지하기 위하여 기술적・물리적・관리적 수단을 강구하는 일체의 행위를 말하며 사이버안전을 포함한다.
6. "정보보호시스템"이라 함은 정보처리시스템내 정보를 유출・위변조・훼손하거나 정보처리시스템의 정상적인 서비스를 방해하는 행위로부터 정보 등을 보호하기 위한 장비 및 프로그램을 말한다.
7. "해킹"이라 함은 접근을 허가받지 아니하고 전자금융기반시설에 불법적으로 침투하거나 허가받지 아니한 권한을 불법적으로 갖는 행위 또는 전자금융기반시설을 공격하거나 해를 끼치는 행위를 말한다.<개정 2013. 12. 3.>
8. "컴퓨터악성코드"(이하 "악성코드"라 한다)라 함은 컴퓨터에서 이용자의 허락 없이 스스로를 복사하거나 변형한 뒤 정보유출, 시스템 파괴 등의 작업을 수행하여 이용자에게 피해를 주는 프로그램을 말한다.<개정 2013. 12. 3.>
9. "공개용 웹서버"라 함은 인터넷 이용자들이 웹페이지를 자유롭게 보고 웹서비스(월드 와이드 웹을 이용한 서비스를 말한다)를 이용할 수 있게 해주는 프로그램이 실행되는 장치를 말한다.<개정 2013. 12. 3.>
10. "정보통신망"(이하 "통신망"이라 한다)이라 함은 유・무선, 광선 등 정보통신 수단에 의하여 부호・문자・음향・영상 등을 처리・저장 및 송・수신할 수 있는 정보통신 조직형태를 말한다.<개정 2013. 12. 3.>

11. 삭제<2013. 12. 3.>

제3조(전자금융보조업자의 범위) 법 제2조제5호에서 "금융위원회가 정하는 자"라 함은 다음 각 호의 어느 하나에 해당하는 자를 말한다.

1. 정보처리시스템을 통하여「여신전문금융업법」상 신용카드업자의 신용카드 승인 및 결제 그 밖의 자금정산에 관한 업무를 지원하는 사업자
2. 정보처리시스템을 통하여 은행업을 영위하는 자의 자금인출업무, 환업무 및 그 밖의 업무를 지원하는 사업자
3. 전자금융업무와 관련된 정보처리시스템을 해당 금융회사 또는 전자금융업자를 위하여 운영하는 사업자<개정 2013. 12. 3.>
4. 제1호 부터 제3호의 사업자와 제휴, 위탁 또는 외부주문(이하 "외부주문등"이라 한다)에 관한 계약을 체결하고 정보처리시스템을 운영하는 사업자

제2장 전자금융거래 당사자의 권리와 의무

제4조(확인에 필요한 구체적인 거래내용) 시행령 제7조제4항제6호에서 "금융위원회가 정하여 고시하는 사항"이란 다음 각 호를 말한다.

1. 법 제8조에 따른 오류정정 요구사실 및 처리결과에 관한 사항
2. 전자금융거래 신청, 조건변경에 관한 내용

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.<개정 2013. 12. 3.>

1.「금융위원회의 설치 등에 관한 법률」제38조제1호(다만,「은행법」에 의한 지방금융회사 및 같은 법 제58조에 의해 인가를 받은 외국금융회사의 국내지점은 제외한다) 및 제7호의 회사,「전자금융거래법 시행령」제2조제2호의 회사 : 20억원<개정 2013. 12. 3.>
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<개정 2013. 12. 3.>
3.「금융위원회의 설치 등에 관한 법률」제38조제2호(다만, 명의개서대행업무를 수행하는 회사는 제외)의 회사 : 5억원<개정 2013. 12. 3.>
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 주요부분을 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 본호의 보험 또는 공제에 가입한 것으로 본다.<개정 2013. 12. 3.>

5. 법 제28조제2항제1호 및 제2호의 전자금융업자 : 2억원

6. 법 제28조제2항제4호의 전자금융업자 중 제1호 또는 제2호에 속하는 금융회사가 발급한 신용카드, 직불카드 등 거래지시에 사용되는 접근매체의 정보를 저장하는 전자금융업자 : 10억원<개정 2016. 10. 5.>

7. 제5호, 제6호 이외의 전자금융업자 : 1억원 <종전의 제6호에서 이동>

② 금융회사 또는 전자금융업자가 전자금융사고 책임이행을 위한 준비금을 적립하는 경우에는 제1항 각 호에서 정한 금액 이상의 금액을 보유하고 책임이행이 신속히 이루어질 수 있도록 준비금 관리 및 지급에 관한 내부 절차를 수립하여 운영하여야 한다.<개정 2013. 12. 3., 2016. 10. 5.>

③ 금융회사 또는 전자금융업자가 보험 또는 공제 가입과 준비금 적립을 병행하는 경우 보험 또는 공제의 보상한도는 제1항에서 정한 금액에서 준비금 적립액을 차감한 금액 이상으로 한다.<개정 2013. 12. 3.>

④ 제1항 부터 제3항의 규정은 전자금융업무를 취급하지 않는 금융회사에 대하여는 적용하지 아니한다.<개정 2013. 12. 3.>

제6조(추심이체 출금 동의의 방법 등) ① 시행령 제10조제1호에서 "금융위원회가 정하여 고시하는 전자문서"라 함은 다음 각 전자문서을 말한다.

1.「전자서명법」제2조제2호에 따른 전자서명으로 다음 각 목의 요건을 구비된 전자서명을 한 전자문서<개정 2016. 6. 30.>

가. 전자서명을 생성하기 위하여 이용하는 전자적 정보(이하 "전자서명생성정보"라함)가 본인에게 유일하게 속할 것

나. 전자서명 당시 본인이 전자서명생성정보를 지배・관리하고 있을 것

다. 전자서명이 있은 후에 당해 전자서명에 대한 변경여부를 확인할 수 있을 것

라. 전자서명이 있은 후에 당해 전자문서의 변경여부를 확인할 수 있을 것

2.「전자서명법」제2조제2호에 따른 전자서명으로 다음 각 목의 요건을 구비된 전자서명을 한 전자문서

가. 서명 전 실명증표를 통해 본인확인

나. 전자문서가 생성된 이후 서명자가 지급인 본인임을 확인 가능

다. 전자서명 및 전자문서에 대한 위변조 여부 확인이 가능

라. 전자문서를 고객에게 전송한 이후 고객이 취소할 수 있는 충분한 기간 부여

3. 삭제<2015. 3. 18.>

② 시행령 제10조제1호 및 제2호에서 "금융위원회가 정하는 방법"이라 함은 다음 각 호의 방법을 말한다.

1. 전화 녹취

2. 음성응답 시스템(Audio Response System : ARS)

③ 지급인(출금계좌의 실지명의인을 포함한다)이 출금의 동의를 해지하는 경우에도 제1항 및 제2항의 규정을 준용한다.<개정 2015. 6. 24.>

④ 금융회사・전자금융업자 또는 수취인은 제1항 각 호의 출금 동의의 방법을 운용함에 있어 다음 각 호의 어느 하나에 해당하는 사실을 확인하여야 한다.<개정 2013. 12. 3.>

1. 지급인과 추심이체 출금계좌 실지명의인이 동일인인 사실
2. 지급인과 추심이체 출금계좌 실지명의인이 동일인이 아닐 경우에는 지급인이 당해 계좌에서 출금할 수 있는 권한을 보유하고 있는 사실

제6조의2(정보보호최고책임자의 지정대상) ① 시행령 제11조의3제1항 후단에서 "금융위원회가 정하여 고시하는 상시 종업원 수의 산정방식"이란 「소득세법」에 따른 원천징수의무자가 근로소득세를 원천징수한 자를 말한다.

② 시행령 <별표 1>의제3호나목 단서에서 "금융위원회가 정하여 고시하는 산정방식"이란 「소득세법」에 따른 원천징수의무자가 근로소득세를 원천징수한 자를 말한다.

제3장 전자금융거래의 안전성 확보 및 이용자 보호

제1절 통칙

제7조(전자금융거래 종류별 안전성 기준) 법 제21조제2항의 "금융위원회가 정하는 기준"이라 함은 다음 각 호의 내용에 관하여 제8조 부터 제37조에서 정하는 기준을 말한다.

1. 인력, 조직 및 예산 부문<개정 2013. 12. 3.>
2. 건물, 설비, 전산실 등 시설 부문
3. 단말기, 전산자료, 정보처리시스템 및 정보통신망 등 정보기술부문
4. 그 밖에 전자금융업무의 안전성 확보를 위하여 필요한 사항

제2절 인력, 조직 및 예산 부문

제8조(인력, 조직 및 예산) ① 금융회사 또는 전자금융업자는 인력 및 조직의 운용에 관하여 다음 각 호의 사항을 준수하여야 한다.<개정 2013. 12. 3.>

1. 정보처리시스템 및 전자금융업무 관련 전담 조직을 확보할 것
2. 외부주문등에 관한 계약을 체결하는 때에는 계약내용의 적정성을 검토하고 자체적으로 통제가 가능하도록 회사내부에 조직과 인력을 갖출 것
3. 전산인력의 자질향상 및 예비요원 양성을 위한 교육 및 연수프로그램을 운영할 것
4. 정보보호최고책임자는 임직원이 정보보안 관련법규가 준수되고 있는지 정기적으로 점검하고 그 점검결과를 최고경영자에게 보고할 것<신설 2013. 12. 3.>
5. 최고경영자는 임직원이 정보보안 관련법규를 위반할 경우 그 제재에 관한 세부기준 및 절차를 마련하여 운영할 것<신설 2013. 12. 3.>

② 금융회사 또는 전자금융업자는 인력 및 예산에 관하여 다음 각 호의 사항을 준수하도록 노력하여야 한다.<개정 2013. 12. 3.>

1. 정보기술부문 인력은 총 임직원수의 100분의 5 이상, 정보보호인력은 정보기술부문 인력의 100분의 5 이상이 되도록 할 것

2. 정보보호예산을 정보기술부문 예산의 100분의 7 이상이 되도록 할 것<개정 2013. 12. 3.>

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.>

④ 제2항제1호의 인력에 관한 기준은 <별표 1>과 같으며, 제2항제2호의 예산에 관한 기준은 <별표 2>와 같다.

제8조의2(정보보호위원회 운영) ① 금융회사 또는 전자금융업자는 중요 정보보호에 관한 사항을 심의·의결하는 정보보호위원회를 설치 운영하여야 한다.

② 정보보호위원회의 장은 정보보호최고책임자로 하며, 위원은 정보보호업무 관련 부서장, 전산운영 및 개발 관련 부서장, 준법업무 관련 부서의 장 등으로 구성한다.

③ 정보보호위원회는 다음 각 호의 사항을 심의·의결한다.

1. 법 제21조제4항에 따른 정보기술부문 계획서에 관한 사항
2. 법 제21조의2제4항제1호에 관한 사항<개정 2015. 6. 24.>
3. 법 제21조의3에서 정한 취약점 분석·평가 결과 및 보완조치의 이행계획에 관한 사항
4. 전산보안사고 및 전산보안관련 규정 위반자의 처리에 관한 사항
5. 제14조의2제1항의 클라우드컴퓨팅서비스의 이용에 관한 사항<신설 2022. 11. 23.>
6. 기타 정보보호위원회의 장이 정보보안업무 수행에 필요하다고 정한 사항<개정 2022. 11. 23.>

④ 정보보호최고책임자는 정보보호위원회 심의·의결사항을 최고경영자에게 보고하여야 한다.

⑤ 최고경영자는 특별한 사정이 없는 한 정보보호위원회의 심의·의결사항을 준수하여야 한다.

제3절 시설부문

제9조(건물에 관한 사항) 금융회사 또는 전자금융업자는 전산실이 위치한 건물에 관하여 다음 각 호의 사항을 준수하여야 한다.<개정 2013. 12. 3.>

1. 건물 출입구는 경비원에 의하여 통제하고 출입통제 보안대책을 수립·운용할 것
2. 비상시 대피를 위한 비상계단 및 정전대비 유도등을 설치할 것<개정 2013. 12. 3.>
3. 번개, 과전류 등 고전압으로 인한 전산장비 및 통신장비 등의 피해 예방을 위하여 피뢰설비를 갖출 것
4. 서버, 스토리지(Storage) 등 전산장비 및 통신장비 등의 중량을 감안한 적재하중 안전대책을 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.<개정 2013. 12. 3.>

1. 전원실, 공조실 등 주요 설비시설에 자물쇠 등 출입통제장치를 설치할 것
2. 전원, 공조, 방재 및 방범 설비에 대한 적절한 감시제어시스템을 갖출 것
3. 전산실의 전력공급 중단에 대비하여 자가발전설비를 갖출 것
4. 전력공급 장애 시 전력선 대체가 가능하도록 복수회선을 설치하고 전력공급의 연속성 유지를 위한 무정전전원장치(Uninterruptible Power Supply : UPS)를 갖출 것<개정 2013. 12. 3.>
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 설비부분과 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 사항을 준수하여야 한다.<개정 2013. 12. 3.>

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 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 재해복구센터
    나. 전산자료 보관실
    다. 정보보호시스템 설치장소
    라. 그 밖에 보안관리가 필요하다고 인정되는 정보처리시스템 설치장소
11. 국내에 본점을 둔 금융회사의 전산실 및 재해복구센터는 국내에 설치할 것<개정 2016. 6. 30.>
12. 무선통신망을 설치하지 아니할 것

제4절 정보기술부문

제12조(단말기 보호대책) 금융회사 또는 전자금융업자는 단말기 보호를 위하여 다음 각 호의 사항을 준수하여야 한다.<개정 2013. 12. 3.>

1. 업무담당자 이외의 사람이 단말기를 무단으로 조작하지 못하도록 조치할 것<개정 2015. 2. 3.>
2. 정보처리시스템에 접속하는 단말기에 대해 정당한 사용자인가의 여부를 확인할 수 있는 기록을 유지할 것<개정 2015. 2. 3.>
3. 외부 반출, 인터넷 접속, 그룹웨어 접속의 금지 등 강화된 보호대책이 적용되는 중요단말기를 지정할 것<개정 2013. 12. 3., 2015. 2. 3.>
4. 정보유출, 악성코드 감염 등을 방지할 수 있도록 단말기에서 보조기억매체 및 휴대용 전산장비에 접근하는 것을 통제할 것<개정 2015. 2. 3.>
5. 삭제<2015. 2. 3.>

제13조(전산자료 보호대책) ① 금융회사 또는 전자금융업자는 전산자료의 유출, 파괴 등을 방지하기 위하여 다음 각 호를 포함한 전산자료 보호대책을 수립·운용하여야 한다.<개정 2013. 12. 3.>

1. 사용자계정과 비밀번호를 개인별로 부여하고 등록·변경·폐기를 체계적으로 관리할 것
2. 외부사용자에게 사용자계정을 부여하는 경우 최소한의 작업권한만 할당하고 적절한 통제장치를 갖출 것
3. 전산자료의 보유현황을 관리하고 책임자를 지정·운영할 것
4. 전산자료의 입력·출력·열람을 함에 있어 사용자의 업무별로 접근권한을 통제할 것
5. 전산자료 및 전산장비의 반출·반입을 통제할 것
6. 비상시에 대비하여 보조기억매체 등 전산자료에 대한 안전지출 및 긴급파기 계획을 수립·운용할 것<개정 2013. 12. 3.>
7. 정기적으로 보조기억매체의 보유 현황 및 관리실태를 점검하고 책임자의 확인을 받을 것
8. 중요도에 따라 전산자료를 정기적으로 백업하여 원격 안전지역에 소산하고 백업내역을 기록·관리할 것
9. 주요 백업 전산자료에 대하여 정기적으로 검증할 것
10. 이용자 정보의 조회·출력에 대한 통제를 하고 테스트 시 이용자 정보 사용 금지(다만, 법인인 이용자 정보는 금융감독원장이 정하는 바에 따라 이용자의 동의를 얻은 경우 테스트 시 사용 가능하며, 그 외 부하 테스트 등 이용자 정보의 사용이 불가피한 경우 이용자 정보를 변환하여 사용하고 테스트 종료 즉시 삭제하여야 한다)<개정 2013. 12. 3., 2016. 10. 5.>
11. 정보처리시스템의 가동기록은 1년 이상 보존할 것
12. 정보처리시스템 접속 시 5회 이내의 범위에서 미리 정한 횟수 이상의 접속 오류가 발생하는 경우 정보처리시스템의 사용을 제한할 것
13. 단말기에 이용자 정보 등 주요정보를 보관하지 아니하고, 단말기를 공유하지 아니할 것(다만, 불가피하게 단말기에 보관할 필요가 있는 경우 보관사유, 보관기간 및 관리 비밀번호 등을 정하여 책임자의 승인을 받아야

한다)

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<개정 2013. 12. 3.>

② 제1항제1호의 사용자계정의 공동 사용이 불가피한 경우에는 개인별 사용내역을 기록·관리하여야 한다.

③ 금융회사 또는 전자금융업자는 단말기를 통한 이용자 정보 조회 시 사용자, 사용일시, 변경·조회내용, 접속방법이 정보처리시스템에 자동적으로 기록되도록 하고, 그 기록을 1년 이상 보존하여야 한다.<개정 2013. 12. 3.>

④ 제1항제11호의 정보처리시스템 가동기록의 경우 다음 각 호의 사항이 접속의 성공여부와 상관없이 자동적으로 기록·유지되어야 한다.

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 금융회사 또는 전자금융업자는 단말기와 전산자료의 접근권한이 부여되는 정보처리시스템 관리자에 대하여 적절한 통제장치를 마련·운용하여야 한다. 다만, 정보처리시스템 관리자의 주요 업무 관련 행위는 책임자가 제28조제2항에 따라 이중확인 및 모니터링을 하여야 한다.<개정 2013. 12. 3.>

제14조(정보처리시스템 보호대책) 금융회사 또는 전자금융업자는 정보처리시스템의 안전한 운영을 위하여 다음 각 호를 포함한 보호대책을 수립·운용하여야 한다.<개정 2013. 12. 3.>

1. 주요 정보처리시스템에 대한 구동, 조작방법, 명령어 사용법, 운용순서, 장애조치 및 연락처 등 시스템 운영매뉴얼을 작성할 것
2. 데이터베이스관리시스템(Database Management System : DBMS)·운영체제·웹프로그램 등 주요 프로그램에 대하여 정기적으로 유지보수를 실시하고, 작업일, 작업내용, 작업결과 등을 기록한 유지보수관리대장을 작성·보관할 것
3. 정보처리시스템의 장애발생 시 장애일시, 장애내용 및 조치사항 등을 기록한 장애상황기록부를 상세하게 작성·보관할 것
4. 정보처리시스템의 정상작동여부 확인을 위하여 시스템 자원 상태의 감시, 경고 및 제어가 가능한 모니터링시스템을 갖출 것
5. 시스템 통합, 전환 및 재개발 시 장애 등으로 인하여 정보처리시스템의 운영에 지장이 초래되지 않도록 통제절차를 마련하여 준수할 것
6. 정보처리시스템의 책임자를 지정·운영할 것
7. 정보처리시스템의 운영체계, 시스템 유틸리티 등의 긴급하고 중요한 보정(patch)사항에 대하여는 즉시 보정작업을 할 것
8. 중요도에 따라 정보처리시스템의 운영체제 및 설정내용 등을 정기 백업 및 원격 안전지역에 소산하고 백업자료는 1년 이상 기록·관리할 것
9. 정보처리시스템의 운영체제(Operating System) 계정으로 로그인(Log in)할 경우 계정 및 비밀번호 이외에 별도의 추가인증 절차를 의무적으로 시행할 것<신설 2013. 12. 3.>

10. 정보처리시스템 운영체제(Operating System) 계정에 대한 사용권한, 접근 기록, 작업 내역 등에 대한 상시 모니터링체계를 수립하고, 이상 징후 발생 시 필요한 통제 조치를 즉시 시행할 것<신설 2013. 12. 3.>

제14조의2(클라우드컴퓨팅서비스 이용절차 등) ① 금융회사 또는 전자금융업자는「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」제2조제3호에 따른 클라우드컴퓨팅서비스를 이용하고자 하는 경우 다음 각 호의 절차를 수행하여야 한다.<개정 2018. 12. 21.>

1. 다음 각 목의 기준에 따른 이용업무의 중요도 평가<개정 2022. 11. 23.>
   가. 규모, 복잡성 등 클라우드컴퓨팅서비스를 통해 처리되는 업무의 특성<신설 2022. 11. 23.>
   나. 클라우드컴퓨팅서비스 제공자로부터 제공받는 서비스가 중단될 경우 미치는 영향<신설 2022. 11. 23.>
   다. 전자적 침해행위 발생 시 고객에게 미치는 영향<신설 2022. 11. 23.>
   라. 여러 업무를 같은 클라우드컴퓨팅서비스 제공자에게 위탁하는 경우 해당 클라우드컴퓨팅서비스 제공자에 대한 종속 위험<신설 2022. 11. 23.>
   마. 클라우드컴퓨팅서비스 이용에 대한 금융회사 또는 전자금융업자의 내부통제 및 법규 준수 역량<신설 2022. 11. 23.>
   바. 그 밖에 금융감독원장이 정하여 고시하는 사항<신설 2022. 11. 23.>
2. 클라우드컴퓨팅서비스 제공자의 건전성 및 안전성 등에 대한 평가(단, 제1호의 평가를 통해 비중요업무로 분류된 업무에 대해서는 <별표 2의2>의 평가항목 중 필수항목만 평가할 수 있다.)<개정 2022. 11. 23.>
3. 클라우드컴퓨팅서비스 이용과 관련한 업무 연속성 계획 및 안전성 확보조치의 수립・시행(단, 제1호의 평가를 통해 비중요업무로 분류된 업무에 대해서는 <별표 2의3> 및 <별표 2의4>의 필수 사항만 수립・시행할 수 있다.)<개정 2022. 11. 23.>

② 금융회사 또는 전자금융업자는 제1항 각 호에 따른 평가결과, 업무연속성 계획 및 안전성 확보조치에 대하여 제8조의2에 따른 정보보호위원회의 심의・의결을 거쳐야 한다.<개정 2018. 12. 21., 2022. 11. 23.>

③ 금융회사 또는 전자금융업자는 제1항제2호의 평가를 직접 수행하거나 제37조의4제1항의 침해사고대응기관이 수행한 평가 결과를 활용할 수 있다.<개정 2018. 12. 21, 2022. 11. 23.>

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.<신설 2018. 12. 21., 개정 2022. 11. 23.>

1. 클라우드컴퓨팅서비스 이용계약을 신규로 체결하는 경우<신설 2022. 11. 23.>
2. 클라우드컴퓨팅서비스 제공자의 합병, 분할, 계약상 지위의 양도, 재위탁 등 중대한 변경사항이 발생한 경우<개정 2022. 11. 23.>
3. 클라우드컴퓨팅서비스 제공자가 서비스품질의 유지, 안전성 확보 등과 관련한 중요 계약사항을 이행하지 아니한 경우<개정 2022. 11. 23.>
4. 제1항제2호 또는 제3호에 관한 중대한 변경사항이 발생한 경우<개정 2022. 11. 23.>

⑤ 제4항에 따라 금융감독원장에게 보고할 경우 첨부해야 하는 서류는 다음 각 호와 같다.<신설 2018. 12. 21., 개정 2022. 11. 23.>

1.「금융회사의 정보처리 업무 위탁에 관한 규정」제7조제1항 각 호에 관한 서류

2. 제1항제1호에 따른 업무의 중요도 평가 기준 및 결과<개정 2022. 11. 23.>

3. 제1항제2호에 따른 클라우드컴퓨팅서비스 제공자의 건전성 및 안전성 등에 대한 평가 결과<신설 2022. 11. 23.>

4. 제1항제3호에 따른 업무 연속성 계획 및 안전성 확보조치에 관한 사항<개정 2022. 11. 23.>

5. 제2항에 따른 정보보호위원회 심의·의결 결과<개정 2022. 11. 23.>

6. <별표 2의5>의 계약서 주요 기재사항을 포함한 클라우드컴퓨팅서비스 이용계약서<신설 2022. 11. 23.>

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.<신설 2018. 12. 21., 개정 2022. 11. 23.>

⑦ 금융감독원장은 제4항에 따라 제출한 보고 서류가 누락되거나, 중요도 평가 또는 업무연속성계획·안전성 확보조치 등이 충분하지 않다고 판단하는 경우에는 금융회사 또는 전자금융업자에 대하여 개선·보완을 요구할 수 있다.<개정 2018. 12. 21., 2022. 11. 23.>

⑧ 제1항의 절차를 거친 클라우드컴퓨팅서비스 제공자의 정보처리시스템이 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.>

⑨ 그 밖에 금융회사 또는 전자금융업자의 클라우드컴퓨팅서비스 이용에 대해서는「금융회사의 정보처리 업무 위탁에 관한 규정」에 따른다.<신설 2018. 12. 21.>

제15조(해킹 등 방지대책) ① 금융회사 또는 전자금융업자는 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해행위로부터 방지하기 위하여 다음 각 호의 대책을 수립·운용하여야 한다.

1. 해킹 등 전자적 침해행위로 인한 사고를 방지하기 위한 정보보호시스템 설치 및 운영

2. 해킹 등 전자적 침해행위에 대비한 시스템프로그램 등의 긴급하고 중요한 보정(patch)사항에 대하여 즉시 보정작업 실시

3. 내부통신망과 연결된 내부 업무용시스템은 인터넷(무선통신망 포함) 등 외부통신망과 분리·차단 및 접속 금지. 다만, 다음 각 목의 경우에는 그러하지 아니하다.<개정 2013. 12. 3., 2022. 11. 23.>

   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)<신설 2022. 11. 23.>

   나. 업무상 불가피한 경우로서 금융감독원장의 확인을 받은 경우<신설 2022. 11. 23.>

4. 내부통신망에서의 파일 배포기능은 통합 및 최소화하여 운영하고, 이를 배포할 경우에는 무결성 검증을 수행할 것<신설 2013. 12. 3.>

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 경우에는 그러하지 아니하다.<신설 2013. 12. 3., 개정 2015. 2. 3., 2022. 11. 23.>

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)<신설 2022. 11. 23.>

나. 업무상 불가피한 경우로서 금융감독원장이 인정하는 경우<신설 2022. 11. 23.>

② 제1항제1호의 규정에 따른 정보보호시스템을 설치・운영하는 경우에는 다음 각 호의 사항을 준수하여야 한다.

1. 삭제<2015. 3. 18.>
2. 최소한의 서비스번호(port)와 기능만을 적용하고 업무목적 이외의 기능 및 프로그램을 제거할 것
3. 보안정책의 승인・적용 및 보안정책의 등록, 변경 및 삭제에 대한 이력을 기록・보관할 것
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 <개정 2016. 10. 5.>
5. 정보보호시스템의 작동 상태를 주기적으로 점검할 것<신설 2016. 10. 5>
6. 시스템 장애, 가동중지 등 긴급사태에 대비하여 백업 및 복구 절차 등을 수립・시행할 것 <종전의 제5호에서 이동>

③ 제1항 각 호의 정보보호시스템에 대하여 책임자를 지정・운영하여야 하며, 운영결과는 1년 이상 보존하여야 한다.

④ 금융회사 또는 전자금융업자는 해킹 등 전자적 침해행위로 인한 피해 발생시 즉시 대처할 수 있도록 적절한 대책을 마련하여야 한다.<개정 2013. 12. 3.>

⑤ 삭제<2013. 12. 3.>

⑥ 금융회사 또는 전자금융업자는 무선통신망을 설치・운용할 때에는 다음 각 호의 사항을 준수하여야 한다.<개정 2013. 12. 3.>

1. 무선통신망 이용 업무는 최소한으로 국한하고 법 제21조의2에 따른 정보보호최고책임자의 승인을 받아 사전에 지정할 것
2. 무선통신망을 통한 불법 접속을 방지하기 위한 사용자인증, 암호화 등 보안대책을 수립할 것
3. 금융회사 내부망에 연결된 정보처리 시스템이 지정된 업무 용도와 사용 지역(zone) 이외의 무선통신망에 접속하는 것을 차단하기 위한 차단시스템을 구축하고 실시간 모니터링체계를 운영할 것<개정 2015. 2. 3.>
4. 비인가 무선접속장비(Access Point : AP) 설치・접속여부, 중요 정보 노출여부를 주기적으로 점검할 것

제16조(악성코드 감염 방지대책) ① 금융회사 또는 전자금융업자는 악성코드 감염을 방지하기 위하여 다음 각 호를 포함한 대책을 수립・운용하여야 한다.<개정 2013. 12. 3.>

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<개정 2015. 2. 3.>

② 금융회사 또는 전자금융업자는 악성코드 감염이 발견된 경우 악성코드 확산 및 피해를 최소화하기 위하여 필요한 조치를 신속하게 취하여야 한다.<개정 2013. 12. 3.>

제17조(홈페이지 등 공개용 웹서버 관리대책) ① 금융회사 또는 전자금융업자는 공개용 웹서버의 안전한 관리를 위하여 다음 각 호를 포함한 적절한 대책을 수립·운용하여야 한다.<개정 2013. 12. 3.>

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<개정 2015. 2. 3.>
3. 공개용 웹서버에서 제공하는 서비스를 제외한 다른 서비스 및 시험·개발 도구 등의 사용을 제한할 것
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)

② 금융회사 또는 전자금융업자는 공개용 웹서버에 게재된 내용에 대하여 다음 각 호의 사항을 준수하여야 한다.<개정 2013. 12. 3.>

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<2013. 12. 3.>

④ 금융회사 또는 전자금융업자는 공개용 웹서버가 해킹공격에 노출되지 않도록 대응 조치하여야 한다.<개정 2013. 12. 3., 2015. 2. 3.>

⑤ 금융회사 또는 전자금융업자는 단말기에서 음란, 도박 등 업무와 무관한 프로그램 또는 인터넷 사이트에 접근하는 것에 대한 통제대책을 마련하여야 한다.<개정 2013. 12. 3.>

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.<개정 2013. 12. 3.>

1. 내부통신망에서 사용하는 IP주소의 경우 사설 IP주소 사용 등으로 보안을 강화하며 내부 IP주소체계의 외부유출을 금지할 것
2. 개인별로 내부 IP주소를 부여하여 유지·관리할 것
3. 내부 IP주소 및 외부 IP주소의 인터넷 접속내용을 1년 이상 별도로 기록·보관할 것
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 경우

에는 업무특성별로 접근권한을 분리하여 IP주소를 사용할 수 있다.<개정 2015. 6. 24.>

5. 내부통신망은 다른 기관 내부통신망과 분리하여 사용할 것

제5절 정보기술부문 내부통제

제19조(정보기술부문 계획서 제출 절차 등) ① 시행령 제11조의2에 따라 금융위원회에 정보기술부문 계획서를 제출해야 하는 금융회사 또는 전자금융업자는 현실적이고 실현 가능한 장·단기 정보기술부문 계획을 매년 수립·운용하여야 한다.<개정 2013. 12. 3.>

② 금융위원장은 금융감독원장으로 하여금 정보기술부문 계획서의 적정성 등을 평가한 후 관련보고서를 제출하게 할 수 있다.<신설 2013. 12. 3.>

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 개발과 정보보호교육은 정보보호 전문 교육기관에 위탁할 수 있다.

제20조(정보처리시스템 구축 및 전자금융거래 관련 사업 추진) 금융회사 또는 전자금융업자는 정보처리시스템 및 전자금융거래와 관련된 사업을 추진하는 경우에 다음 각 호의 사항을 준수하여야 한다.<개정 2013. 12. 3.>

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 분석·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.<개정 2013. 12. 3.>

1. 적합한 업체를 공정하게 선정하기 위하여 객관적인 업체 선정 기준 및 절차를 마련·운용할 것
2. 정보처리시스템의 안전성과 신뢰성을 확보하기 위하여 제1호에 따른 기준 및 절차의 내용에는 정보보안 관련 사항을 포함할 것
3. 공정하고 합리적인 예정가격 산출 기준을 수립·적용할 것

4. 계약금액, 구축완료일자, 납품방법 및 대금지급방법 등 계약이행에 필요한 내용을 포함한 계약서 작성 기준을 수립·운용할 것
5. 구매 또는 개발한 제품의 소유권, 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 한다.<개정 2013. 12. 3.>

1. 목적 및 대상, 시스템 감리인, 감리시기 및 계획 등 일반기준
2. 기획, 개발 및 운용의 감리 실시 기준
3. 지적사항 및 개선사항 등 감리 후 보고 기준
4. 전자금융업무와 관련된 외부주문등에 대한 감리 기준

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.<개정 2013. 12. 3., 2016. 10. 5.>

1. 상황별 대응절차
2. 백업 또는 재해복구센터를 활용한 재해복구계획
3. 비상대응조직의 구성 및 운용
4. 입력대행, 수작업 등의 조건 및 절차
5. 모의훈련의 실시
6. 유관기관 및 관련업체와의 비상연락체제 구축
7. 보고 및 대외통보의 범위와 절차 등

② 제1항에 따른 업무지속성 확보대책에는 비상사태에 대비한 다음 각 호의 안전대책이 반영되어야 한다.

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 최신상태로 유지할 것

4. 핵심전산업무 담당자 부재 시에도 비상지원 인력이 업무를 수행할 수 있도록 비상지원인력에 대한 연수를 실시할 것

③ 금융회사 또는 전자금융업자는 제1항의 규정에 따른 업무지속성 확보대책의 실효성・적정성 등을 매년 1회 이상 점검하여 최신상태로 유지하고 관리하여야 한다.<개정 2013. 12. 3.>

④「국가위기관리기본지침」에 따라 금융위원회가 지정한 금융회사는 금융위원회의「금융전산분야위기대응실무매뉴얼」에 따라 위기대응행동매뉴얼(이하 "행동매뉴얼"이라 한다)을 수립・준수하고 이를 금융위원회에 알려야 한다.<개정 2013. 12. 3., 2016. 10. 5.>

⑤ 금융위원회가 별도로 지정하지 아니한 금융회사 또는 전자금융업자는 자연 재해, 인적 재해, 기술적 재해, 전자적 침해 등으로 인한 전산시스템의 마비 방지와 신속한 복구를 위한 비상대책을 수립・운영하여야 한다.<개정 2013. 12. 3., 2016. 10. 5.>

⑥ 제4항에 따른 행동매뉴얼 또는 제5항에 따른 비상대책에는 제1항의 규정에 따른 업무지속성 확보대책이 반영되어야 한다.

⑦ 금융회사 또는 전자금융업자는 중앙처리장치, 데이터저장장치 등 주요 전산장비에 대하여 이중화 또는 예비장치를 확보하여야 한다.<개정 2013. 12. 3.>

⑧ 다음 각 호의 금융회사는 시스템 오류, 자연재해 등으로 인한 전산센터 마비에 대비하여 업무지속성을 확보할 수 있도록 적정 규모・인력을 구비한 재해복구센터를 주전산센터와 일정거리 이상 떨어진 안전한 장소에 구축・운용하여야 한다.<개정 2013. 12. 3., 2015. 6. 24.>

1.「은행법」에 의해 인가를 받아 설립된 은행(다만,「은행법」제58조에 의해 인가를 받은 외국금융회사의 국내지점은 제외한다)<개정 2013. 12. 3.>
2.「한국산업은행법」에 의한 한국산업은행,「중소기업은행법」에 의한 중소기업은행,「농업협동조합법」에 의한 농협은행,「수산업협동조합법」에 의한 수산업협동조합중앙회의 신용사업부문<개정 2013. 12. 3.>
3.「자본시장과 금융투자업에 관한 법률」에 의한 투자매매업자・투자중개업자(다만,「자본시장과 금융투자업에 관한 법률」제12조에 의해 인가를 받은 외국 투자매매업자・투자중개업자의 지점 등은 제외한다)
4.「자본시장과 금융투자업에 관한 법률」에 의한 증권금융회사 및 한국예탁결제원
5.「자본시장과 금융투자업에 관한 법률」에 의한 거래소<개정 2013. 12. 3.>
6.「여신전문금융업법」에 의한 신용카드업자(다만, 법인신용카드 회원에 한하여 신용카드업을 영위하는 자는 제외한다)
7.「보험업법」에 의한 보험요율산출기관
8.「상호저축은행법」에 의한 상호저축은행중앙회
9.「신용협동조합법」에 의한 신용협동조합중앙회
10.「보험업법」에 의한 보험회사

⑨ 제8항 각 호의 금융회사는 업무별로 업무지속성 확보의 중요도를 분석하여 핵심업무를 선정하여야 하며, 업무별 복구목표시간을 정하여야 한다. 이 경우 핵심업무의 복구목표시간은 3시간 이내로 하되,「보험업법」에 의한 보험회사의 핵심업무의 경우에는 24시간 이내로 한다.<신설 2015. 6. 24.>

⑩ 제8항의 규정에 따른 재해복구센터를 운영하는 금융회사는 매년 1회 이상 재해복구센터로 실제 전환하는 재해복구전환훈련을 실시하여야 한다. , <종전의 제9항에서 이동 2015. 6. 24.> <개정 2013. 12. 3.>

제24조(비상대응훈련 실시) ① 금융회사 또는 전자금융업자는 제23조제4항에 따른 행동매뉴얼 또는 같은 조 제5항에 따른 비상대책에 따라 연 1회의 비상대응훈련을 실시하고 그 결과를 금융위원회에 보고하여야 한다. 이때, 제23조제10항에 따른 재해복구전환훈련을 포함하여 실시할 수 있다.<개정 2013. 12. 3., 2016. 6. 30.>

② 금융위원회는 금융분야의 비상대응능력을 강화하기 위하여 금융회사 또는 전자금융업자를 선별하여 금융분야 합동비상대응훈련을 실시할 수 있다.<개정 2013. 12. 3.>

③ 금융위원회는 제2항의 규정에 따른 합동비상대응훈련을 실시할 때, 다음 각 호의 기관에게 지원을 요청할 수 있다.

1.「정부조직법」제15조에 따른 "국가정보원(국가사이버안전센터)"

2.「경찰법」제2조에 따른 "경찰청(사이버테러대응센터)"

3. 침해사고대응기관<개정 2013. 12. 3.>

4. 그밖에 비상대응훈련의 실효성 확보를 위하여 금융위원회가 필요하다고 인정하는 기관

④ 금융회사 또는 전자금융업자는 제1항 및 제2항에 따른 의무의 이행을 위하여 전자금융보조업자에게 협조를 요청할 수 있다.<신설 2018. 12. 21.>

제25조(정보처리시스템의 성능관리) 금융회사 또는 전자금융업자는 정보처리시스템의 장애예방 및 성능의 최적화를 위하여 정보처리시스템의 사용 현황 및 추이 분석 등을 정기적으로 실시하여야 한다.<개정 2013. 12. 3.>

제26조(직무의 분리) 금융회사 또는 전자금융업자는 다음 각 호의 업무에 대하여 직무를 분리・운영하여야 한다. <개정 2013. 12. 3.>

1. 프로그래머와 오퍼레이터

2. 응용프로그래머와 시스템프로그래머

3. 시스템보안관리자와 시스템프로그래머

4. 전산자료관리자(librarian)와 그 밖의 업무 담당자

5. 업무운영자와 내부감사자

6. 내부인력과 전자금융보조업자 및 유지보수업자 등을 포함한 외부인력

7. 정보기술부문인력과 정보보호인력

8. 그 밖에 내부통제와 관련하여 직무의 분리가 요구되는 경우

제27조(전산원장 통제) ① 금융기관 또는 전자금융업자는 장애 또는 오류 등에 의한 전산원장의 변경을 위하여 별도의 변경절차를 수립・운용하여야 한다.

② 제1항의 절차에는 변경 대상 및 방법, 변경 권한자 지정, 변경 전후내용 자동기록 및 보존, 변경내용의 정당여부에 대한 제3자 확인 등이 포함되어야 한다.

③ 금융회사 또는 전자금융업자는 대차대조표 등 중요 자료의 계상액과 각종 보조부・거래기록・전산원장파일의 계상액에 대한 상호일치 여부를 전산시스템을 통하여 주기적으로 확인하여야 한다.<개정 2013. 12. 3.>

④ 금융회사 또는 전자금융업자는 제3항에 따른 확인 결과 불일치가 발견된 때에는 그 원인 및 조치 내용을 전산자료의 형태로 5년간 보존하여야 한다.<개정 2013. 12. 3.>

⑤ 금융회사 또는 전자금융업자는 이용자 중요원장에 직접 접근하여 중요원장을 조회・수정・삭제・삽입하는 경우에는 작업자 및 작업내용 등을 기록하여 5년간 보존하여야 한다.<개정 2013. 12. 3.>

제28조(거래통제 등) ① 금융회사 또는 전자금융업자는 사고위험도가 높은 거래에 대하여는 책임자 승인거래로 처리토록 하는 등 전산시스템에 의한 이중확인이 가능하도록 하여야 한다.<개정 2013. 12. 3.>

② 금융회사 또는 전자금융업자는 전산원장, 주요정보 또는 이용자 정보 등이 저장된 정보처리시스템에 대한 중요작업 수행 시 책임자가 이중확인을 해야 한다.<개정 2013. 12. 3.>

제29조(프로그램 통제) 금융회사 또는 전자금융업자는 다음 각 호의 사항을 포함한 프로그램 등록・변경・폐기 절차를 수립・운용하여야 한다.<개정 2013. 12. 3.>

1. 적용대상 프로그램 종류 및 등록・변경・폐기 방법을 마련할 것
2. 프로그램 변경 전후 내용을 기록・관리할 것
3. 프로그램 등록・변경・폐기내용의 정당성에 대해 제3자의 검증을 받을 것
4. 변경 필요시 해당 프로그램을 개발 또는 테스트 시스템으로 복사 후 수정할 것<개정 2013. 12. 3.>
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 해당프로그램 담당자 이외의 자가 수행할 것
8. 운영체제, 데이터베이스관리프로그램 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
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.<개정 2013. 12. 3.>

1. 일괄작업은 작업요청서에 의한 책임자의 승인을 받은 후 수행할 것
2. 일괄작업은 최대한 자동화하여 오류를 최소화할 것
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

제31조(암호프로그램 및 키 관리 통제) ① 금융회사 또는 전자금융업자는 암호프로그램에 대하여 담당자 지정, 담당자 이외의 이용 통제 및 원시프로그램(source program) 별도 보관 등을 준수하여 유포 및 부당 이용이 발생하지

않도록 하여야 한다.<개정 2013. 12. 3.>

② 금융회사 또는 전자금융업자는 암호 및 인증시스템에 적용되는 키에 대하여 주입・운용・갱신・폐기에 대한 절차 및 방법을 마련하여 안전하게 관리하여야 한다.<개정 2013. 12. 3.>

제32조(내부사용자 비밀번호 관리) 금융회사 또는 전자금융업자는 내부사용자의 비밀번호 유출을 방지하기 위하여 다음 각 호의 사항을 정보처리시스템에 반영하여야 한다.<개정 2013. 12. 3.>

1. 담당업무 외에는 열람 및 출력을 제한할 수 있는 접근자의 비밀번호를 설정하여 운영할 것
2. 비밀번호는 다음 각 목의 사항을 준수할 것
   가. 비밀번호는 이용자 식별부호(아이디), 생년월일, 주민등록번호, 전화번호를 포함하지 않은 숫자와 영문자 및 특수문자 등을 혼합하여 8자리 이상으로 설정하고 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

제33조(이용자 비밀번호 관리) ① 금융회사 또는 전자금융업자는 정보처리시스템 및 전산자료에 보관하고 있는 이용자의 비밀번호를 암호화하여 보관하며 동 비밀번호를 조회할 수 없도록 하여야 한다. 다만, 비밀번호의 조회가 불가피하다고 인정되는 경우에는 그 조회사유・내용 등을 기록・관리하여야 한다.<개정 2013. 12. 3.>

② 금융회사 또는 전자금융업자는 이용자의 비밀번호 유출을 방지하기 위하여 다음 각 호의 사항을 정보처리시스템에 반영하여야 한다.<개정 2013. 12. 3.>

1. 주민등록번호, 동일숫자, 연속숫자 등 제3자가 쉽게 유추할 수 있는 비밀번호의 등록 불가
2. 통신용 비밀번호와 계좌원장 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, 입력오류 횟수는 이용되는 모든 전자금융거래에 대하여 통산한다)
4. 금융회사가 이용자로부터 받은 비밀번호는 거래전표, 계좌개설신청서 등에 기재하지 말고 핀패드(PIN pad) 등 보안장치를 이용하여 입력 받을 것<개정 2013. 12. 3.>
5. 신규 거래, 비밀번호 변경, 이체 신청과 같이 비밀번호를 등록・사용하는 경우 사전에 신청서 등에 기입하지 않고, 핀패드 등 보안장치를 이용하거나 이용자가 사후에 전자적 장치를 이용하여 직접 입력하는 방식으로 운영할 것

제6절 전자금융업무

제34조(전자금융거래 시 준수사항) 금융회사 또는 전자금융업자는 전자금융거래와 관련하여 다음 각 호의 사항을 준수하여야 한다.

1. 전화 등 거래수단 성격상 암호화가 불가능한 경우를 제외한 전자금융거래는 암호화 통신을 할 것(다만, 전용선을 사용하는 경우로서 제36조의 규정에 따라 자체 보안성심의를 실시한 경우에는 그러하지 아니하다)
2. 전자금융사고를 예방하기 위하여 비대면 전자금융거래를 허용하지 않는 계좌 개설, 중요거래정보에 대한 문자메시지 및 이메일(e-mail) 통지 등의 서비스를 이용자가 요청하는 경우, 동 서비스를 제공할 수 있도록 시스템을 갖출 것
3. 전자금융거래에 사용되는 접근매체를 발급받기 위해서는 반드시 실명확인 후 교부할 것.
4. 거래인증수단 채택시 안전성, 보안성, 이용편의성 등을 충분히 고려할 것
5. 금융회사 또는 전자금융업자는 전자금융거래에서 이용자에게 제공하거나 거래를 처리하기 위한 전자금융거래 프로그램(거래전문포함)의 위·변조 여부 등 무결성을 검증할 수 있는 방법을 제공할 것

② 삭제

제35조(이용자 유의사항 공지) 금융회사 또는 전자금융업자는 전자금융거래의 안전한 수행을 위하여 이용자에게 다음 각 호의 사항을 준수하도록 공지하여야 한다.<개정 2013. 12. 3.>

1. 비밀번호 유출위험 및 관리에 관한 사항
2. 금융기관 또는 전자금융업자가 제공하고 있는 이용자 보호제도에 관한 사항
3. 해킹·피싱 등 전자적 침해 방지에 관한 사항
4. 본인확인 절차를 거쳐 비밀번호 변경이 가능하도록 정보처리시스템을 구축하고 비밀번호 변경 시 같은 번호를 재사용하지 않도록 할 것

제36조(자체 보안성심의) ① 금융회사 또는 전자금융업자는 다음 각 호의 행위를 하고자 하는 경우 금융감독원장이 정하는 기준과 절차에 따라 보안성심의를 실시하여야 한다.<개정 2016. 6. 30.>

1. 정보통신망을 이용하여 이용자를 대상으로 신규 전자금융업무를 수행
2. 복수의 금융회사 또는 전자금융업자가 공동으로 전자금융거래 관련 표준을 제정

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.

③ 금융감독원장은 제2항에 따라 제출받은 자체 보안성심의 결과보고서를 검토한 결과, 보안수준이 충분하지 않다고 인정되는 경우에는 금융회사 또는 전자금융업자에 대하여 개선·보완을 요구할 수 있다.

④ 제2항 및 제3항에도 불구하고 다음 각 호의 기관은 제1항제1호에 따른 자체 보안성심의 결과보고서의 제출을 하지 아니할 수 있다.

1.「우체국예금·보험에 관한 법률」에 의한 체신관서
2.「새마을금고법」에 의한 새마을금고 및 새마을금고중앙회
3.「한국수출입은행법」에 따른 한국수출입은행

4.「공공기관의 운영에 관한 법률」제4조에 따른 공공기관

제37조(인증방법 사용기준) 금융회사 또는 전자금융업자는 전자금융거래의 종류·성격·위험수준 등을 고려하여 안전한 인증방법을 사용하여야 한다.<개정 2015. 3. 18.>

제37조의2(전자금융기반시설의 취약점 분석·평가 주기, 내용 등) ① 전자금융기반시설의 취약점 분석·평가는 총자산이 2조원 이상이고, 상시 종업원 수(「소득세법」에 따른 원천징수의무자가 근로소득세를 원천징수한 자를 기준으로 한다. 이하 같다) 300명 이상인 금융회사 또는 전자금융업자이거나「수산업협동조합법」,「산림조합법」,「신용협동조합법」,「상호저축은행법」및「새마을금고법」에 따른 중앙회의 경우 연 1회 이상(홈페이지에 대해서는 6개월에 1회 이상) 실시하여야 한다.

② 금융회사 및 전자금융업자는 취약점 분석·평가를 위하여 정보보호최고책임자(정보보호최고책임자가 없는 경우 최고경영자가 지정한다)를 포함하여 5인 이상으로 자체전담반을 구성하여야 하며, 구성원 중 100분의 30 이상은「정보보호산업의 진흥에 관한 법률 시행규칙」제8조의 정보보호 전문서비스 기업 지정기준에서 정한 고급 기술인력 이상의 자격을 갖춘 자이어야 한다. 다만, 제37조의3제1항에 따른 평가전문기관에 위탁하는 경우에는 자체전담반을 구성하지 아니할 수 있다.<개정 2016. 6. 30.>

③ 제1항에 따른 금융회사 및 전자금융업자 이외의 자의 경우 연 1회 이상(홈페이지에 대해서는 6개월에 1회 이상) 실시하되 자체전담반을 구성하지 아니할 수 있다. 이 경우 취약점 분석·평가의 내용은 금융감독원장이 정한다.

④ 금융회사 및 전자금융업자는 해당 주기 내에 평가 대상 시설과 평가기간을 나누어 평가할 수 있다.

⑤ 금융회사 또는 전자금융업자는 취약점 분석·평가에 따라 이행계획을 수립·시행하여야 하며 다음 각 호의 사항을 준수하여야 한다.

1. 취약점 분석·평가 결과에 따른 취약점의 제거 또는 이에 상응하는 조치의 시행
2. 취약점의 제거 또는 이에 상응하는 조치가 불가한 경우에는 최고경영자 승인을 득할 것
3. 이행계획의 시행 결과는 최고경영자에게 보고할 것

⑥ 금융회사 또는 전자금융업자는 제1항 또는 제3항에 따른 의무의 이행을 위하여 전자금융보조업자에게 협조를 요청할 수 있다.<신설 2018. 12. 21.>

제37조의3(전자금융기반시설의 취약점 분석·평가 전문기관의 지정 등) ① 전자금융기반시설의 취약점 분석·평가를 위한 평가전문기관은 다음 각 호의 자로 한다.

1.「정보통신기반 보호법」제16조에 따라 금융분야 정보공유·분석센터로 지정된 자
2.「정보보호산업의 진흥에 관한 법률」제23조에 따라 지정된 정보보호전문서비스 기업<개정 2016. 6. 30.>
3. 침해사고대응기관
4. 금융위원장이 지정하는 자

② 금융회사 및 전자금융업자는 시행령 제11조의5제3항에 따른 전자금융기반시설의 취약점 분석·평가 결과보고서를 금융위원장에게 제출하여야 하며, 금융감독원장은 결과보고서를 분석하여 매분기 1개월 이내에 금융위원장에게 보고하여야 한다.

③ 금융위원장은 취약점 분석·평가 결과보고서에 근거하여 필요시 금융회사 및 전자금융업자에 대하여 개선·보완을 요구할 수 있다.

제37조의4(침해사고대응기관 지정 및 업무범위 등) ① 침해사고에 대응하기 위한 침해사고대응기관은 다음 각 호의 자로 한다.

1. 금융보안원<개정 2015. 3. 18.>
2. 삭제<2015. 3. 18.>
3. 금융위원장이 지정한 자

② 침해사고대응기관은 다음 각 호의 업무를 수행한다.

1. 침해사고에 관한 정보의 수집·전파를 위한 정보공유체계의 구축
2. 침해사고의 예보·경보 발령내용의 전파
3. 침해사고의 원인분석과 신속한 대응 및 피해 확산방지를 위해 필요한 조치
4. 금융회사 및 전자금융업자와 관련된 해킹 등 전자적 침해행위 정보를 탐지·분석하여 즉시 대응 조치를 하기 위한 기구(이하 "금융권 통합 보안관제센터"라 한다)의 운영<신설 2016. 10. 5.>
5. 금융회사 및 전자금융업자의 침해사고 예방, 대응을 위한 자율기준의 마련 및 운영<신설 2018. 12. 21.>

③ 금융위원장은 침해사고대응기관을 포함하여 침해사고조사단을 구성할 수 있다.

④ 금융위원장은 제2항에 따른 침해사고 긴급대응을 위한 침해사고대응기관의 업무 수행 또는 제3항에 따른 침해사고 원인분석 및 긴급조치를 위하여 금융회사 및 전자금융업자, 전자금융보조업자에 협조를 요청할 수 있다.<개정 2016. 10. 5.>

⑤ 금융회사 및 전자금융업자는 침해사고에 대한 대응능력 확보를 위하여 연 1회 이상 침해사고 대응 및 복구훈련 계획을 수립·시행하여야 하며 그 계획 및 결과를 침해사고대응기관의 장에게 제출하여야 한다. 다만 다음 각 호의 어느 하나에 해당하는 금융회사는 그러하지 아니한다.<개정 2016. 10. 5.>

1. 법 제2조제3호가목의 금융회사 중 신용협동조합
2. 법 제2조제3호다목·라목의 금융회사
3. 시행령 제2조제4호부터 제6호까지의 조합
4. 시행령 제5조제2항의 요건을 충족한 금융회사

⑥ 금융위원장은 침해사고대응기관의 장으로 하여금 침해사고 대응·복구 및 훈련결과를 점검하고 보완이 필요하다고 판단되는 경우 개선·보완을 요구할 수 있다.

⑦ 금융위원장은 침해사고대응기관의 장으로 하여금 시행령 제11조의6제1항제4호에 따른 보안취약점 통보를 위하여 금융회사 및 전자금융업자가 사용하고 있는 소프트웨어에 대한 조사·분석을 실시하게 할 수 있다.

[시행일 : 금융보안원이 성립한 날] 제37조의4제1항<신설 2016. 10. 5.>

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.[[본조신설 2015. 2. 3.]]]

제38조(금융위원회가 정하는 보관자료 및 거래기록 등) 시행령 제12조제1항제2호다목에서 "금융위원회가 정하여 고시하는 거래기록"이라 함은 제4조제1호의 기록을 말한다.

제39조(전자지급수단의 이용한도) 시행령 제13조제2항 부터 제4항에 따라 금융위원회가 정하는 전자지급수단의 구체적인 이용한도는 <별표 3>과 같다.

제40조(약관교부 방법 등) ① 전자금융업무를 수행하는 금융회사 및 전자금융업자는 전자금융거래와 관련한 약관(이하 "약관"이라 한다)을 별도로 마련하여야 한다.<개정 2013. 12. 3.>

② 금융회사 또는 전자금융업자는 이용자와 전자금융거래의 계약을 체결함에 있어 이용자의 요청이 있는 경우 전자문서의 전송(전자우편을 이용한 전송을 포함한다), 모사전송, 우편 또는 직접 교부의 방식으로 전자금융거래 약관의 사본을 이용자에게 교부하여야 한다.<개정 2013. 12. 3.>

③ 금융회사 또는 전자금융업자는 이용자와 전자금융거래의 계약을 체결함에 있어 이용자가 약관의 내용에 대한 설명을 요청하는 경우 다음 각 호의 어느 하나의 방법으로 이용자에게 약관의 중요내용을 설명하여야 한다.<개정 2013. 12. 3.>

1. 약관의 중요내용을 이용자에게 직접 설명
2. 약관의 중요내용에 대한 설명을 전자적 장치를 통하여 이용자가 알기 쉽게 표시하고 이용자로부터 해당 내용을 충분히 인지하였다는 의사표시를 전자적 장치를 통하여 수령

④ 금융회사 또는 전자금융업자는 약관을 변경하는 때에는 그 시행일 1월 전에 변경되는 약관을 해당 전자금융거래를 수행하는 전자적 장치(해당 전자적 장치에 게시하기 어려울 경우에는 이용자가 접근하기 용이한 전자적 장치로서 당해 금융회사등이 지정하는 대체장치를 포함한다. 이하 이 조에서 같다)에 게시하고 이용자에게 통지하여야 한다. 다만, 이용자가 이의를 제기할 경우 금융회사 또는 전자금융업자는 이용자에게 적절한 방법으로 약관 변경내용을 통지하였음을 확인해 주어야 한다.<개정 2013. 12. 3.>

⑤ 금융회사 또는 전자금융업자가 법령의 개정으로 인하여 긴급하게 약관을 변경한 때에는 변경된 약관을 전자적 장치에 최소 1월 이상 게시하고 이용자에게 통지하여야 한다.<개정 2013. 12. 3.>

제41조(약관 제정 또는 변경에 따른 보고 등) ① 법 제25조제1항 단서에서 "금융위원회가 정하는 경우"란 다음 각 호와 같다.

1. 이용자의 권익을 확대하거나 의무를 축소하기 위한 약관의 변경
2. 금융감독원장에게 보고된 약관의 내용과 동일하거나 유사한 약관의 제정 또는 변경
3. 그 밖에 이용자의 권익이나 의무에 불리한 영향이 없는 경우로서 금융감독원장이 정하는 약관의 제정 또는 변경

② 금융회사 또는 전자금융업자가 전자금융거래 약관을 제정 또는 변경하고자 하는 경우에는 해당 약관 및 약관 내용을 이해하는데 필요한 관련서류를 시행예정일 45일 전까지 금융감독원장에게 제출하여야 한다. 이 경우 약관 및 관련서류는 전자문서로 제출할 수 있다.<개정 2013. 12. 3.>

③ 금융감독원장은 제2항의 규정에 따라 제출받은 약관을 심사하고 건전한 금융거래질서의 유지를 위하여 약관 내용의 변경이 필요하다고 인정하는 경우 해당 금융회사 또는 전자금융업자에 대하여 약관의 변경을 권고할 수

있다.<개정 2013. 12. 3.>

④ 제3항의 규정에 따라 변경권고를 받은 금융회사 또는 전자금융업자는 권고의 수락여부를 금융감독원장에게 보고하여야 한다.<개정 2013. 12. 3.>

제4장 전자금융업의 허가와 등록 및 업무

제1절 허가 및 등록의 대상과 절차

제42조(총발행잔액의 산정방법 등) ① 시행령 제15조제5항에 따른 선불전자지급수단 발행 시 총발행잔액은 등록신청일이 속하는 사업연도의 직전 사업연도 1분기(직전 사업연도 1분기말 이후에 사업을 개시한 경우에는 사업개시한 날이 속하는 분기를 말한다)부터 등록신청일 직전 분기까지 각 분기말 미상환 발행잔액의 단순평균으로 한다. 다만, 사업기간이 3월 미만인 경우에는 등록신청일 직전 월말 미상환 발행잔액으로 한다.

② 법 제28조제3항제1호다목에 따라 금융위원회에 등록하지 아니하고 선불전자지급수단을 발행하는 자는 매분기말 기준으로 선불전자지급수단의 미상환잔액을 평가하여 이를 시행령 제15조제6항에 따른 지급보증, 상환보증보험 또는 공제에 반영하여야 한다.

제42조의2(거래금액 기준) ① 법 제30조제3항제1호에서 "금융위원회가 정하는 기준"이라 함은 당해 전자금융업에 대한 분기별 결제대행금액(이용자가 지급한 재화 및 용역의 매출총액), 결제대금예치금액 또는 전자고지결제금액이 30억원 이하에 해당하는 경우를 말한다.

② 법 제30조제4항에서 "금융위원회가 정하는 기한"이라 함은 신고한 때로부터 6월 이내를 말한다.

③ 등록 자본금 초과시 신고와 관련한 절차 및 방법 등 세부사항은 금융감독원장이 정하는 바에 따른다.

제43조(허가등 절차의 구분) 다음 각 호의 허가 또는 인가(이하 "허가등"이라 한다)의 절차는 허가등 사항에 대한 사전심사 및 확실한 실행을 위하여 허가등의 이전에 예비적으로 행하는 의사표시(이하 "예비허가등"이라 한다)와 허가등으로 구분한다.

1. 법 제28조제1항의 규정에 의한 전자화폐의 발행 및 관리 업무의 허가
2. 법 제45조에 의한 합병 등의 인가

제44조(예비허가등) ① 예비허가등을 신청하고자 하는 자는 금융감독원장이 정하는 바에 따라 <별지 제3호 서식>에 따른 관련 신청서 및 첨부서류를 금융위원회에 제출하여야 한다.

② 금융위원회는 예비허가등의 심사를 위하여 필요하다고 인정하는 때에는 예비허가등의 신청에 대하여 이해관계인의 의견을 요청할 수 있고, 금융시장에 중대한 영향을 미칠 우려가 있다고 판단되는 경우 공청회를 개최할 수 있다.

③ 금융위원회는 제2항의 규정에 의하여 접수된 의견 중 신청인에게 불리한 의견에 대하여는 신청인에게 소명하도록 기한을 정하여 통보할 수 있다.

④ 금융감독원장은 예비허가등의 신청내용에 대한 진위여부를 확인하고 이해관계인, 일반인 및 관계기관 등으로부터 제시된 의견을 감안하여 신청내용이 관련 법령과 이 장 제2절에서 규정하는 허가등 세부기준에 부합되는지

여부를 심사하여야 한다.

⑤ 금융감독원장은 사업계획의 타당성을 평가하기 위하여 평가위원회를 구성·운영할 수 있으며 신청내용의 확인, 발기인 및 경영진과의 면담 등을 위하여 실지조사를 실시할 수 있다.

⑥ 금융위원회는 예비허가등의 신청에 대하여 관련 법령과 이 장 제2절에서 규정하는 허가의 세부기준을 감안하여 예비허가등의 여부를 결정한다.

⑦ 금융위원회는 예비허가등 시에 조건을 붙일 수 있으며 예비허가등을 거부하는 경우 이를 서면으로 신청인에게 통보하여야 한다.

⑧ 금융위원회는 합병, 영업양도 등 구조조정 및 이용자보호 등을 위하여 신속한 처리가 필요하거나 예비허가등의 신청 시 허가등의 요건을 갖추었다고 판단되는 때에는 예비허가등의 절차를 생략할 수 있다.

제45조(허가등) ① 신청인은 예비허가등의 내용 및 조건을 이행한 후 금융감독원장이 정하는 바에 따라 <별지 제4호 서식>에 따른 관련 신청서 및 첨부서류를 금융위원회에 제출하여야 한다.

② 금융위원회는 허가등의 신청에 대하여 관련 법령과 이 장 제2절에서 규정하는 허가의 세부기준에 따라 심사하여 허가여부를 결정한다.

③ 허가등에는 조건을 붙일 수 있으며 허가를 거부하는 경우에는 이를 서면으로 신청인에게 통보하여야 한다.

④ 금융위원회는 예비허가등의 내용 및 조건의 이행여부를 확인하기 위하여 실지조사를 실시할 수 있으며, 신청인은 이에 적극 협조하여야 한다.

⑤ 신청인은 예비허가등 또는 허가등 시에 부과된 조건이 있는 경우 그 이행상황을 이행기일 경과 후 지체 없이 금융위원회에 보고하여야 한다.

제46조(보완서류 등의 제출) 금융위원회는 예비허가등 또는 허가등의 심사 시 보완서류 등의 추가자료가 필요한 경우 신청인에게 기한을 정하여 그 자료의 제출을 요구할 수 있다.

제47조(허가등 사실의 공고) 금융위원회는 허가등의 신청을 승인한 경우에는 지체 없이 그 내용을 관보에 공고하고 인터넷 등을 이용하여 일반인들에게 알려야 한다.

제48조(등록) ① 법 제28조 및 제29조에 따라 등록을 신청하고자 하는 자는 금융감독원장이 정하는 바에 따라 <별지 제5호 서식>에 따른 등록신청서를 금융감독원에 제출하여야 하며 금융감독원장은 등록신청일로부터 20일 이내에 서면으로 등록여부를 통지한다. 다만, 제3항의 실지조사에 걸린 기간은 통지기간에 산입하지 아니한다.

② 금융감독원장은 신청인의 등록 신청에 대하여 이 장 제2절의 심사기준에 따라 등록 여부를 결정한다.

③ 금융감독원장은 등록의 내용 및 조건의 이행여부를 확인하기 위한 실지조사를 실시할 수 있다.

④ 금융감독원장은 등록 신청을 수리한 경우에는 지체 없이 그 내용을 관보에 공고하고 인터넷 등을 이용하여 일반인들에게 알려야 한다.

제49조(기재가 생략되는 출자자의 범위) 시행령 제20조제1항제3호에서 "금융위원회가 정하여 고시하는 소액출자자"라 함은 허가 또는 등록대상 전자금융업자가 되고자 하는 법인의 의결권 있는 발행주식총수의 100분의 1 이하의 주식을 소유하는 자를 말한다.

제2절 허가 및 등록의 세부요건

제50조(인력 및 물적 시설 세부요건) ① 법 제28조 및 제29조에 따라 허가를 받거나 등록을 하고자 하는 자는 인력과 물적 시설에 대한 다음 각 호의 요건을 모두 갖추어야 한다.<개정 2013. 12. 3.>

1. 신청 당시 전산업무 종사 경력이 2년 이상인 임직원을 5명 이상 확보하고 있거나 허가・등록 시점에 확보 가능할 것
2. 전자금융업을 원활히 영위하는데 필요한 전산기기를 갖출 것<개정 2018. 12. 21.>
3. 전산장애 발생 시 전산자료 손실에 대비한 백업(backup)장치를 구비할 것
4. 전자금융업의 원활한 영위를 위한 각종 프로그램을 갖출 것<개정 2018. 12. 21.>
5. 전산자료 보호 등을 위한 적절한 정보처리시스템 관리방안을 확보하고 정보보호시스템 등 감시운영체제를 구축할 것
6. 전산실 등의 구조 및 내장, 설비 등의 안전성을 확보하고 적절한 보안대책을 수립할 것

② 국외에서 주로 영업하는 국외 사이버몰("국외 사이버몰"이란 컴퓨터 등과 정보통신설비를 이용하여 재화 등을 거래할 수 있도록 설정된 가상의 영업장으로서 운용자의 사무소가 국외에 있는 경우를 말한다. 이하 같다)에서의 상거래에 수반한 전자지급결제대행업을 영위할 목적으로 전자금융업을 등록하고자 하는 자는 제50조제1항의 규정에도 불구하고 다음 각 호의 요건을 모두 충족한 경우 등록할 수 있다.<신설 2013. 12. 3.>

1. 국외에 소재한 계열사(「금융회사의 정보처리 및 전산설비 위탁에 관한 규정」 제2조제3항의 "계열사"를 말한다. 이하 같다)와 이용계약을 체결하였고, 계열사의 인력 및 물적 시설이 제50조제1항 각 호의 세부요건을 충족할 것
2. 제1호의 규정에도 불구하고 전자금융업을 등록하고자 하는 자는 신청 당시 법령 준수업무와 이용자 민원처리 업무를 담당할 3명 이상의 임직원(전산업무 종사 경력이 2년 이상인 임직원 1명을 포함하여야 한다)은 직접 확보하고 있거나 등록시점에 확보 가능할 것
3. 신청 당시 계열사의 인력 또는 물적시설을 통해 5개국 이상의 국가에서 전자지급결제대행업무가 수행되고 있을 것

③ 제2항에 따라 등록을 하려는 자가 계열사의 인력 또는 물적시설의 이용계약을 체결하는 경우에는 「금융회사의 정보처리 및 전산설비 위탁에 관한 규정」을 적용한다. 다만, 동 규정의 제7조는 적용하지 아니한다. ,<신설 2013. 12. 3.> <개정 2016. 6. 30.>

제50조의2(국외 사이버몰을 위한 전자지급결제대행업) ① 제50조제2항에 따라 등록하고자 하는 경우 시행령 제20조제2항제8호에 따라 다음 각 호의 서류를 제출하여야 한다.

1. 「금융회사의 정보처리 및 전산설비 위탁에 관한 규정」 제7조제1항 각 호의 서류
2. 등록신청자 및 계열사의 수탁업무 수행 과정에서의 법・시행령 및 이 규정 등 준수에 대한 확약서
3. 신청 시점에 전자지급결제대행업무를 수행하고자 하는 국외 사이버몰에 대한 다음 각 목의 사항(해당 국가의 법령 등에서 이와 유사한 것으로 인정되는 사항을 포함한다)을 기재한 서류

가.「전자상거래 등에서의 소비자보호에 관한 법률」제10조제1항 각 호의 서류

나. 신청일 직전연도에 사이버몰에서 체결된 전자상거래 중 국내에 소재한 소비자와 사업자 간 거래의 비중

② 제50조제2항에 따라 등록을 한 자는 국외에서 주로 영업하는 국외 사이버몰을 통한 상거래에 대해서만 전자지급결제대행업을 영위하여야 한다.

③ 금융감독원장은 국외에서 주로 영업하는 국외 사이버몰의 판단기준 등 필요한 사항을 정할 수 있다.

제51조(재무건전성 세부기준 및 계산방법 등) ① 시행령 제18조제1항 및 제2항에 따라 금융위원회가 정하는 재무건전성 기준은 다음 각 호와 같다.

1. 시행령 제18조제1항의 규정에 따른 기관 중「금융산업의 구조개선에 관한 법률」제2조제1호의 금융회사에 해당하는 기관은 그 기관의 설립・운영 등에 관한 법령상 경영개선권고, 경영개선요구 또는 경영개선명령 등의 요건이 되는 재무기준에 해당하지 아니할 것<개정 2013. 12. 3.>
2. 제1호 이외의 경우에는 다음 각 목의 요건을 충족할 것
   가. 시행령 제18조제1항의 규정에 따른 금융회사 중「금융산업의 구조개선에 관한 법률」제2조제1호의 금융회사에 해당하지 않는 기관은 자기자본 대비 부채총액의 비율이 100분의 200 이내일 것. 다만, 금융회사 업무의 성격 및 재무 구조 등을 감안할 때 부채비율 기준을 적용하지 아니하고,「금융산업의 구조 개선에 관한 법률」제2조제1호 각 목 중 어느 하나의 금융회사(이하 "기준 금융회사"라 한다)의 재무건전성 기준을 적용하는 것이 적절하다고 금융위원회가 승인하는 경우에는, 기준 금융회사의 설립, 운영 등에 관한 법령에 따라 산출한 재무 비율이 같은 법령상의 경영개선권고, 경영개선요구 또는 경영개선명령 등의 요건이 되는 기준에 해당하지 아니할 것<개정 2013. 12. 3.>
   나. 법 제28조제1항에 따른 허가대상 전자금융업일 경우에는 자기자본 대비 부채총액의 비율이 100분의 180 이내일 것
   다. 법 제28조제2항 및 제29조에 따른 등록대상 전자금융업일 경우에는 자기자본・출자총액 또는 기본재산 대비 부채총액의 비율이 100분의 200 이내일 것

② 제1항제2호의 부채비율은 신청일이 속하는 사업연도의 직전 사업연도말 대차대조표(최근 대차대조표를 사용하고자 하는 경우에는 신청일 최근 분기말 대차대조표 또는 회계법인의 확인을 받은 신청일 최근 월말 대차대조표) 상의 자기자본 및 부채총액을 이용하여 산출한다. 이 경우 전자화폐・선불전자지급수단의 미상환잔액 및 전자자금이체・전자지급결제대행・결제대금예치・전자고지결제・「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제2조제10호에 따른 통신과금서비스 등의 업무를 영위하는 자가 이용자와의 거래 관계에서 일시 보관하는 금액(이하 "미정산 잔액"이라 한다)은 부채총액에서 차감한다.<개정 2015. 6. 24., 2016. 10. 5.>

③ 제1항에도 불구하고 다음 각 호의 요건을 갖춘 신청인의 재무건전성 기준은 자기자본 대비 부채총액의 비율이 100분의 1500 이내일 것으로 한다.

1. 정부등이 자본금・출자총액 또는 기본재산의 100분의 10 이상을 소유하고 있거나 출자하고 있을 것
2. 신청인의 사업 수행이 곤란하게 되는 경우 정부등이 해당 사업을 인수할 것을 확약하는 등 그 사업의 연속성에 대하여 정부등이 보장하고 있을 것

3. 사업 개시 후 5년 이내 제1항의 재무건전성 기준을 충족하는 것을 내용으로 하는 실현가능한 재무구조개선계획을 수립하여 관련서류와 함께 제출할 것

제52조(사업계획에 관한 요건) 법 제28조에 따라 허가를 받고자 하는 자의 사업계획은 다음 각 호의 요건을 모두 갖추어야 한다.

1. 영업개시 후 3년간 추정재무제표 및 수익전망이 전자화폐 내지 선불전자지급수단 발행업계의 과거 수익상황 등에 비추어 타당성이 있고 그 내용이 해당 신청회사의 영업계획에 부합할 것
2. 전자화폐 발행업을 원활히 영위하는데 필요한 이용자 확보계획이 구체적이고 타당하며 실현가능성이 있을 것
3. 영위하고자 하는 영업의 내용이 법령에 위반되지 아니하고 투자자보호나 건전한 금융질서를 저해할 우려가 없을 것

제53조(주요출자자에 관한 요건) 주요출자자(시행령 제18조제3항에 따른 주요출자자를 말한다)는 <별표 4>에서 정한 요건을 충족하여야 한다.

제54조(허가 및 등록신청 결격자) 법 제32조제4호의 규정에서 "금융위원회가 정하는 자"라 함은「신용정보의 이용 및 보호에 관한 법률」제25조 제2항 제1호의 종합신용정보집중기관에 다음 각호 중 어느하나의 신용정보가 등록된 자를 말한다.

1. 어음・수표 거래정지처분 또는 부도거래정보
2. 대출금 등의 용도 외 유용 사실
3. 부정한 방법으로 대출을 받는 등 금융거래질서를 문란하게 한 사실

제55조(신청에 따른 등록말소 및 이용자 보호조치) ① 법 제34조에 따라 등록의 말소를 신청하고자 하는 전자금융업자는 <별지 제6호 서식>에 따른 등록말소신청서를 금융위원회에 제출하여야 한다.

② 법 제34조에 따라 등록의 말소를 신청하고자 하는 전자금융업자는 신청 이전에 이용자 보호조치 계획을 금융위원회에 제출하여야 한다.

③ 금융위원회는 제1항의 전자금융업자가 제출한 계획이 이용자 보호에 충분하지 않은 경우에 그 보완을 요구할 수 있다.

제3절 전자금융업의 업무

제56조(전자화폐 발행업자의 겸업가능 업무) 시행령 제22조제1항제3호에서 "금융위원회가 정하여 고시하는 업무"란 다음 각 호의 어느 하나에 해당하는 업무를 말한다.

1. 전자화폐 발행 및 관리를 위한 가맹점의 모집
2. 전자화폐 발행 및 관리를 위한 인터넷 홈페이지의 운영 및 이를 통한 통신판매 중개

제57조(수수료 및 준수사항 등의 고지방법) 법 제38조제3항 각 호의 사항은 다음 각 호의 방법 중 제1호의 방법을 포함한 둘 이상의 방법으로 가맹점에게 알려야 한다.

1. 가맹점에의 개별 통보
2. 전국적으로 보급되는 일간신문에의 공고
3. 해당 금융회사 또는 전자금융업자 영업장 및 인터넷 홈페이지에의 게시<개정 2013. 12. 3.>

제5장 전자금융업무의 감독

제58조(금융회사의 정보기술부문 실태평가 등) ① 금융감독원장은 금융회사의 정보기술부문의 건전성 여부를 감독하여야 한다.<개정 2013. 12. 3.>

② 금융감독원장은 업무의 성격 및 규모, 정보기술부문에 대한 의존도 등을 감안하여 <별표 5>에 규정된 금융회사(이하 이 조에서 '은행등'이라 한다)에 대하여 검사를 통해 정보기술부문 운영 실태를 평가하고 그 결과를 경영실태평가 등 감독 및 검사업무에 반영하여야 한다.<개정 2013. 12. 3.>

③ 제2항에 의한 실태평가는 1등급(우수), 2등급(양호), 3등급(보통), 4등급(취약), 5등급(위험)의 5단계 등급으로 구분한다.

④ 금융감독원장은 제2항에 따른 정보기술부문 실태평가 결과 종합등급이 4등급인 경우에는 해당 은행등에게 이의 개선을 위한 확약서 제출을 요구할 수 있으며, 종합등급이 5등급이거나 직전 정보기술부문 실태평가 결과에 비해 평가등급이 2등급 이상 하향된 경우에는 취약점 개선대책의 수립·이행을 내용으로 하는 양해각서를 체결할 수 있다.

⑤ 제4항의 확약서는 대표자의 승인을 받아 제출하고, 양해각서는 해당 은행등의 이사회 재적이사 전원의 서명을 받아 체결한다.

⑥ 금융감독원장은 확약서 또는 양해각서의 이행상황을 점검하여 그 이행이 미흡하다고 판단되는 경우에는 확약서를 다시 제출받거나 양해각서를 다시 체결할 수 있다.

⑦ 확약서 또는 양해각서의 효력발생일자, 이행시한 및 이행상황 점검주기는 각 확약서 또는 양해각서에서 정한다. 다만, 이행상황 점검주기를 따로 정하지 않은 경우 은행등은 매분기 익월말까지 분기별 이행상황을 금융감독원장에게 보고하여야 한다.

⑧ 제2항에 따른 정보기술부문 실태평가 결과는 경영실태평가 세부 평가항목 중 경영관리 또는 위험관리 항목의 평가비중에서 최소 100분의 20 이상 반영되어야 하며, 금융감독원장은 정보기술부문 실태평가 결과가 4등급 이하인 은행등에 대해 경영실태평가 2등급 이상으로 평가할 수 없다.

⑨ 제2항에 의한 정보기술부문의 실태평가를 위한 세부 사항은 금융감독원장이 정한다.

제59조(검사결과의 보고방법) 금융감독원장은 법 제39조제5항에 따른 결과보고를 하는 경우 「금융기관 검사 및 제재에 관한 규정」 제3장부터 제4장을 준용한다.<개정 2013. 12. 3.>

제60조(외부주문등에 대한 기준) ① 금융회사 또는 전자금융업자는 전자금융거래를 위한 외부주문등의 경우에는 다음 각 호의 사항을 준수하여야 한다.<개정 2013. 12. 3.>

1. 외부주문등에 의한 정보처리시스템의 개발업무에 사용되는 업무장소 및 전산설비는 내부 업무용과 분리하여 설치·운영<개정 2015. 2. 3.>

2. 금융회사와 이용자 간 암호화정보 해독 및 원장 등 중요 데이터 변경 금지<개정 2013. 12. 3.>
3. 계좌번호, 비밀번호 등 이용자 금융정보 무단보관 및 유출 금지
4. 접근매체 위・변조, 해킹, 개인정보유출 등에 대비한 보안대책 수립
5. 금융회사와 전자금융보조업자 간의 접속은 전용회선(전용회선과 동등한 보안수준을 갖춘 가상의 전용회선을 포함한다)을 사용<개정 2013. 12. 3., 2016. 10. 5.>
6. 정보처리시스템 장애 등 서비스 중단에 대비한 비상대책 수립
7. 외부주문등의 입찰・계약・수행・완료 등 각 단계별로 금융감독원장이 정하는 보안관리방안을 따를 것<개정 2015. 2. 3.>
8. 업무지속성을 위한 중요 전산자료의 백업(backup)자료 보존 및 백업설비 확보 등 백업대책 수립
9. 정보관리의 취약점을 최소화하고 보안유지를 위한 내부통제방안을 수립・운용하고, 통제는 제8조제1항제2호의 조직에서 수행<개정 2015. 2. 3.>
10. 전자금융보조업자에 대한 재무건전성을 연1회 이상 평가하여 재무상태 악화에 따른 도산에 대비하고 전자금융보조업자의 주요 경영활동에 대해 상시 모니터링을 실시
11. 전자금융보조업자가 제공하는 서비스의 품질수준을 연1회 이상 평가할 것
12. 전자금융보조업자가 사전 동의 없이 다시 외부주문등 계약을 체결하거나 계약업체를 변경하지 못하도록 하고, 사전 동의시 해당 계약서에 제7호의 사항을 기재하도록 통제<개정 2016. 6. 30.>
13. 업무수행인력에 대하여 사전 신원조회 실시(이 경우 신원보증보험 증권 징구로 갈음할 수 있다) 또는 대표자의 신원보증서 징구, 인력변경시 인수인계에 관한 사항 등을 포함한 업무수행인력 관리방안 수립<개정 2018. 12. 21.>
14. 외부주문등은 자체 보안성검토 및 정기(금융감독원장이 정하는 중요 점검사항에 대해서는 매일) 보안점검 실시<개정 2015. 2. 3.>

② 금융회사 또는 전자금융업자는 제1항제10호 및 제11호의 평가결과를 금융감독원장에게 보고하여야 한다.<개정 2013. 12. 3.>

③ 금융감독원장은 제2항의 규정에 따른 평가결과 보고를 접수하고, 그 평가실시 여부를 제58조제2항의 규정에 따른 정보기술부문 실태평가에 반영할 수 있다.

④ 법 제40조제6항 단서에서 "금융위원회가 인정하는 경우"란 전자금융거래정보의 보호와 관련된 전산장비・소프트웨어에 대한 개발・운영 및 유지관리 업무를 재위탁하는 경우로서 다음 각 호의 사항을 준수하는 경우를 말한다.

1. 재수탁업자가 재위탁된 업무를 처리함에 있어 금융거래 정보의 변경이 필요한 경우에는 위탁회사 또는 원수탁업자의 개별적 지시에 따라야 하며, 위탁회사 또는 원수탁업자는 변경된 정보가 지시 내용에 부합하는지 여부를 확인하여야 함
2. 위탁업무와 관련된 이용자의 금융거래정보는 위탁회사의 전산실 내에 두어야 함. 다만, 재수탁업자가 이용자의 이용자 정보를 어떠한 경우에도 알지 못하도록 위탁회사 또는 원수탁업자가 금융거래정보를 처리하여 제공한 경우에는 위탁회사의 관리・통제 하에 재수탁회사 등 제3의 장소로 이전 가능함

⑤ 금융회사 또는 전자금융업자는 제14조의2제1항제2호에 따른 평가를 위하여 제37조의4제1항 각 호의 어느 하나에 해당하는 기관에 지원을 요청할 수 있다.

[본항신설 2015. 2. 3.]

[시행일 : 2015. 4. 16.] 제60조제1항제1호・7호・14호 및 제4항<신설 2018. 12. 21.>

제61조(전자금융보조업자 자료제출 기준) ① 금융감독원장은 전자금융보조업자에 대해 외부주문등과 관련한 계약서, 계약서 부속자료 및 그 밖의 전자금융업무와 관련한 자료 등을 직접 요구할 수 있다.

② 제1항에 따른 자료제출 요구시 전자금융보조업자는 특별한 이유가 없는 한 자료제출에 응하여야 한다.

제62조(업무보고서의 제출) ① 법 제42조에 따라 금융회사 및 전자금융업자는 금융감독원장이 정하는 바에 따라 업무보고서를 금융감독원장에게 제출하여야 한다. 다만, 법 제2조제1호에 따른 전자금융업무를 하지 아니하는 금융회사는 그러하지 아니하다. , <단서신설 2015. 2. 3.><개정 2013. 12. 3.>

② 제1항에 따른 업무보고서 제출은 정보통신망(「정보통신망 이용 촉진 및 정보보호 등에 관한 법률」 제2조의 규정에 의한 정보통신망을 말한다)을 이용한 전자문서의 방법에 의할 수 있다.

③ 제1항의 업무보고서 제출에 관한 세부적인 절차, 양식 등에 관해서는 금융감독원장이 별도로 정한다.

제63조(전자금융업자 경영지도기준) ① 법 제42조제2항에 따른 구체적인 경영지도기준은 다음과 같다.

1. 법 제30조 및 시행령 제17조에 따른 허가나 등록요건 상 최소자본금・출자총액 또는 기본재산 기준을 항상 충족할 것
2. 총자산에서 총부채를 감한 자기자본이 항상 0을 초과할 것
3. 미상환잔액 대비 자기자본 비율은 100분의 20 이상일 것(전자화폐 및 선불전자지급수단 발행자에 한한다)
4. 총자산 대비 투자위험성이 낮은 자산의 비율은 100분의 10 이상으로 유지하거나 미정산 잔액 대비 투자위험성이 낮은 자산의 비율을 100분의 100 이상으로 유지할 것. 단, 법 제28조제1항의 규정에 따라 허가를 받은 전자금융업자 및 법 제28조제2항제3호의 규정에 따라 등록을 한 전자금융업자는 제외한다. 이 때 투자위험성이 낮은 자산은 <별표 6>와 같다.<개정 2016. 10. 5.>
5. 유동성 비율은 다음 각 목과 같이 유지할 것
   가. 법 제28조제1항의 규정에 따라 허가를 받은 전자금융업자 : 100분의 60 이상
   나. 법 제28조제2항제3호의 규정에 따라 등록을 한 전자금융업자 : 100분의 50 이상
   다. 그 밖의 등록대상 전자금융업자 : 100분의 40 이상

② 제1항에서 정하는 비율의 구체적 산정기준은 금융감독원장이 정한다.

③ 금융감독원장은 제1항의 경영지도비율이 악화될 우려가 있거나 경영상 취약부문이 있다고 판단되는 전자금융업자에 대하여 이의 개선을 위한 계획 또는 약정서를 제출토록 하거나 해당 전자금융업자와 경영개선협약을 체결할 수 있다. 다만, 제64조 부터 제66조까지의 규정에 의한 경영개선권고, 경영개선요구 또는 경영개선명령을 받고 있는 전자금융업자의 경우에는 그러하지 아니하다.

제64조(경영개선권고) ① 금융위원회는 법 제28조제1항의 규정에 따라 허가를 받은 전자금융업자가 다음 각 호의 어느 하나에 해당되는 경우에는 해당 전자금융업자에 대하여 필요한 조치를 이행하도록 권고하여야 한다.

1. 제63조제1항제3호의 미상환잔액 대비 자기자본 비율이 100분의 20 미만인 경우
2. 거액의 금융사고 또는 부실채권의 발생으로 제1호의 기준에 해당될 것이 명백하다고 판단되는 경우

② 제1항에서 정하는 필요한 조치라 함은 다음 각 호의 일부 또는 전부에 해당하는 조치를 말한다.

1. 인력 및 조직운영의 개선
2. 경비절감
3. 고정자산투자, 신규업무영역에의 진출 및 신규출자의 제한
4. 부실자산의 처분
5. 자본금의 증액 또는 감액
6. 이익배당의 제한
7. 특별대손충당금의 설정

③ 금융위원회는 제1항에 의한 권고를 하는 경우 해당 전자금융업자 및 관련 임원에 대하여 주의 또는 경고조치를 취할 수 있다.

제65조(경영개선요구) ① 금융위원회는 법 제28조제1항의 규정에 따라 허가를 받은 전자금융업자가 다음 각 호의 어느 하나에 해당되는 경우에는 해당 전자금융업자에 대하여 필요한 조치를 이행하도록 요구하여야 한다.

1. 제63조제1항제3호의 미상환잔액 대비 자기자본 비율이 100분의 10 미만인 경우
2. 거액의 금융사고 또는 부실채권의 발생으로 제1호의 기준에 해당될 것이 명백하다고 판단되는 경우
3. 제64조제1항의 규정에 의해 경영개선권고를 받은 전자금융업자가 경영개선계획의 주요사항을 이행하지 않아 제69조제8항의 규정에 의해 이행촉구를 받았음에도 이를 이행하지 아니하는 경우

② 제1항에서 정하는 필요한 조치라 함은 다음 각 호의 일부 또는 전부에 해당하는 조치를 말한다.

1. 조직의 축소
2. 위험자산의 보유제한 및 처분
3. 자회사의 정리
4. 임원진 교체 요구
5. 영업의 일부정지
6. 합병, 제3자 인수, 영업의 전부 또는 일부 양도계획의 수립
7. 제64조제2항에서 정하는 사항

제66조(경영개선명령) ① 금융위원회는 법 제28조제1항의 규정에 따라 허가를 받은 전자금융업자가 다음 각 호의 어느 하나에 해당하는 경우에는 해당 전자금융업자에 대해 필요한 조치를 이행하도록 명령하여야 한다.

1. 제63조제1항제3호의 미상환잔액 대비 자기자본 비율이 100분의 5 미만인 경우
2. 제65조제1항의 규정에 의해 경영개선요구를 받은 전자금융업자가 경영개선계획의 주요사항을 이행하지 않아 제69조제8항의 규정에 의해 이행촉구를 받았음에도 이를 이행하지 아니하거나 이행이 곤란하여 정상적인 경영이 어려울 것으로 인정되는 경우

② 제1항에서 정하는 필요한 조치라 함은 다음 각 호의 일부 또는 전부에 해당하는 조치를 말한다. 다만, 영업의 전부정지, 영업의 전부양도, 계약의 전부이전 또는 주식의 전부소각의 조치는 제1항제1호의 기준에 미달하고 건

전한 전자금융거래질서나 이용자의 권익을 해할 우려가 현저하다고 인정되는 경우에 한한다.

1. 주식의 전부 또는 일부 소각
2. 임원의 직무집행 정지 및 관리인의 선임
3. 6월 이내의 영업의 정지
4. 계약의 전부 또는 일부의 이전
5. 제65조제2항에서 정하는 사항

제67조(이유제시 등) 제64조 부터 제66조의 조치를 하는 경우 금융위원회는 해당 전자금융업자에게 그 근거와 이유를 제시하여야 한다.

제68조(적기시정조치의 유예) 제64조제1항, 제65조제1항 및 제66조제1항 각 호의 어느 하나에 해당하는 전자금융업자가 자본의 확충 또는 자산의 매각 등을 통하여 단기간 내에 그 기준에 해당되지 않을 수 있다고 판단되는 경우 또는 이에 준하는 사유가 있다고 인정되는 경우에는 금융위원회는 일정기간동안 조치를 유예할 수 있다.

제69조(경영개선계획 제출 및 평가 등) ① 제64조 부터 제66조에 의해 경영개선권고, 경영개선요구 또는 경영개선명령을 받은 전자금융업자는 동 조치를 받은 후 2월의 범위 내에서 금융위원회가 정하는 기한 내에 해당 조치의 내용이 반영된 계획(이하 "경영개선계획"이라 한다)을 금융감독원장에게 제출하여야 한다.

② 금융위원회는 제64조 부터 제66조에 의해 경영개선권고, 경영개선요구 또는 경영개선명령을 받은 전자금융업자가 제1항에 의해 제출한 계획에 대하여 1월 이내에 승인여부를 결정하여야 한다. 다만, 제3항의 규정에 의한 경영평가위원회의 심의가 지연되는 경우에는 15일 이내에서 그 기한을 초과할 수 있다.

③ 금융감독원장은 제2항의 금융위원회의 승인여부 결정 이전에 해당 계획에 대하여 외부 전문가로 구성된 경영평가위원회의 심의를 거치도록 하여야 한다. 다만, 긴급을 요하거나 심의의 실익이 크지 아니하다고 금융감독원장이 인정하는 경우에는 그러하지 아니하다.

④ 제3항에 의해 경영평가위원회가 사전심의를 하는 경우에는 해당 전자금융업자를 출석시켜 의견을 청취할 수 있다.

⑤ 금융위원회는 제64조에 의해 경영개선권고를 받은 전자금융업자가 제1항의 규정에 의해 제출한 계획의 타당성이 인정되지 않을 경우 동 계획을 불승인하고, 제65조제2항 각 호의 일부 또는 전부에 해당하는 조치를 요구하며, 동 조치내용이 반영된 계획을 일정기간 내에 제출하도록 하여 승인여부를 결정한다.

⑥ 금융위원회는 제5항의 규정에 의해 제출한 계획 또는 제65조에 의해 경영개선요구를 받은 전자금융업자가 제1항의 규정에 의해 제출한 계획의 타당성이 인정되지 않을 경우 동 계획을 불승인한다. 이 경우 금융위원회는 제65조제2항 각 호의 일부 또는 전부에 해당하는 조치를 요구하고, 동 조치내용이 반영된 계획을 일정기간 내에 제출토록 하여야 하며 동 계획의 타당성이 인정되지 않을 경우에는 제66조제2항에서 규정한 조치의 일부 또는 전부를 이행하도록 명령하여야 한다.

⑦ 금융위원회는 제6항의 규정에 의해 제출된 계획 또는 제66조에 의해 경영개선명령을 받은 전자금융업자가 제1항의 규정에 의해 제출한 계획의 타당성이 인정되지 않을 경우 동 계획을 불승인한다. 이 경우 금융위원회는 제71조 각 호의 일부 또는 전부에 해당하는 조치를 할 수 있다.

⑧ 제2항의 규정에 따라 경영개선계획을 승인받은 전자금융업자는 매분기말 익월 10일까지 동 계획의 분기별 이행실적을 금융감독원장에게 제출하여야 하며, 금융감독원장은 그 이행실적이 미흡하거나 관련제도의 변경 등 여건변화로 인하여 이행이 곤란하다고 판단되는 경우에는 경영개선계획의 수정요구, 일정기간 내 이행촉구 등 필요한 조치를 취할 수 있다.

⑨ 제8항의 규정에 따라 금융감독원장이 경영개선권고, 경영개선요구 또는 경영개선명령을 받은 전자금융업자의 경영개선계획의 주요사항을 수정 요구하거나 일정기간 내 이를 이행토록 촉구하는 경우에는 그 내용을 금융위원회에 사전 보고하여야 한다.

⑩ 제8항의 규정에 따라 전자금융업자가 경영개선계획의 주요사항을 수정하여 제출한 경우에는 제2항부터 제7항을 준용할 수 있다.

⑪ 제3항의 경영평가위원회의 구성・운영과 관련된 세부사항은 금융감독원장이 정한다.

제70조(경영개선계획 이행기간 등) ① 제64조에 의하여 경영개선권고를 받은 전자금융업자의 경영개선계획 이행기간은 승인일로부터 6월 이내로 한다.

② 제65조에 의하여 경영개선요구를 받은 전자금융업자의 경영개선계획 이행기간은 승인일로부터 1년 이내로 한다. 이 경우 제64조에 의하여 경영개선권고를 받은 전자금융업자가 경영개선계획 이행 중 경영개선요구를 받은 경우의 이행기간은 경영개선권고에 따른 경영개선계획의 승인일로부터 1년 이내로 한다.

③ 제69조제8항에 의하여 금융감독원장으로부터 경영개선계획의 수정요구 또는 일정기간 내 이행촉구를 받은 경우에는 제1항과 제2항의 기간을 초과할 수 있다. 다만, 그 초과기간은 제1항 또는 제2항에서 정하는 기간 이내이어야 한다.

④ 제66조에 의하여 경영개선명령을 받은 전자금융업자의 경영개선계획의 이행기간은 금융위원회가 정한다.

⑤ 제64조 부터 제66조까지의 규정에 의해 경영개선권고, 경영개선요구 또는 경영개선명령을 받은 전자금융업자가 자본 확충 또는 부실채권정리 등 경영개선계획의 주요사항을 조기에 달성하여 경영상태가 현저히 개선된 경우에는 금융위원회는 권고, 요구 또는 명령한 조치의 내용을 완화하거나 그 이행을 면제할 수 있다.

⑥ 제64조 부터 제66조까지의 규정에 의해 경영개선권고, 경영개선요구 또는 경영개선명령을 받은 전자금융업자의 경영개선계획 이행기간이 만료되어 경영상태가 충분히 개선되었다고 인정되는 경우에는 금융위원회는 당초의 조치가 종료되었음을 통지하여야 하며, 경영상태가 제64조제1항, 제65조제1항 또는 제66조제1항에 해당하는 경우에는 동 조항에 따라 별도의 경영개선권고, 경영개선요구 또는 경영개선명령을 하여야 한다.

제71조(경영개선계획의 불이행에 따른 조치) 금융위원회는 제66조에 의하여 경영개선명령을 받은 전자금융업자가 제70조에 의한 이행기한 내에 경영개선계획의 주요사항을 이행하지 아니하여 경영정상화가 이루어지지 아니하였다고 판단되는 경우 해당 전자금융업자에 대하여 다음 각 호의 일부 또는 전부에 해당하는 조치를 할 수 있다.

1. 제66조제2항에서 정한 조치
2. 허가의 취소
3. 임원의 해임 권고
4. 그 밖에 이용자 보호를 위하여 필요한 조치

제72조(과징금 수납기관 및 납부서식 등) ① 시행령 제27조제1항의 규정에 의하여 금융위원회가 과징금의 납부를 통지하는 경우에는 <별지 제2호 서식>에 따른다.

② 시행령 제27조제2항에 따른 수납기관은 은행법에 의한 금융회사와 우체국으로 한다.

제72조의2(과징금 과오납에 따른 환급가산금 이율) 금융위원장은 「은행법」제8조에 따라 은행업 인가를 받은 국내 은행의 1년 만기 정기예금 이자율을 감안하여 환급가산금 이자율을 정하여야 한다.[[본조신설 2013. 12. 3.]]]

제6장 보칙

제73조(정보기술부문 및 전자금융 사고보고) ① 금융회사 및 전자금융업자는 다음 각 호와 관련된 중대한 사고가 발생한 경우에는 지체 없이 금융감독원장에게 보고하여야 한다.<개정 2013. 12. 3., 2015. 2. 3.>

1. 정보처리시스템 또는 통신회선 등의 장애로 10분 이상 전산업무가 중단 또는 지연된 경우
2. 전산자료 또는 프로그램의 조작과 관련된 금융사고가 발생한 경우
3. 전자적 침해행위로 인해 정보처리시스템에 사고가 발생하거나 이로인해 이용자가 금전적 피해를 입었다고 금융회사 또는 전자금융업자에게 통지한 경우<개정 2013. 12. 3.>
4. 법 제9조제1항의 규정에서 정하는 사고

② 금융회사 및 전자금융업자는 제1항에 따른 사고보고를 고의로 지연하거나 숨긴 자에 대하여 소정절차에 따라 징계 등 필요한 조치를 취하여야 한다.<개정 2013. 12. 3.>

③ 금융감독원장은 제1항에 따라 보고 받은 내용을 지체 없이 금융위원장에게 보고하여야 하며, 제1항제3호에 따른 사고 발생시에는 제37조의4제1항 각 호에 따른 침해사고대응기관에도 알려야 한다.<개정 2015. 2. 3.>

④ 제1항의 사고보고와 관련하여 사고보고 절차 및 방법 등 세부사항은 금융감독원장이 정하는 바에 따른다.

[시행일 : 2015. 4. 16.] 제73조제1항・제3항 및 제4항<신설 2015. 2. 3.>

제74조(위탁업무의 처리 결과 보고) 금융감독원장은 시행령 제30조의 규정에 따라 금융위원회로부터 위탁받은 업무의 처리 결과를 매분기 금융위원회에 보고하여야 한다.

제75조(규제의 존속기한 및 재검토) ① 금융위원회는 「행정규제기본법」 제8조・제19조의2 및 「훈령・예규 등의 발령 및 관리에 관한 규정」(대통령훈령 제248호)에 따라 이 고시에 대하여 2019년 1월 1일을 기준으로 매 3년이 되는 시점(매 3년째의 12월 31일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.<개정 2013. 12. 31., 2018. 12. 21.>

② 제8조제2항은 2020년 1월 1일까지 효력을 가진다.<신설 2015. 2. 3.>

부칙 <제2022-44호,2022.11.23.>

제1조(시행일) 이 규정은 2023년 1월 1일부터 시행한다.