전자금융감독규정시행세칙

[시행 2025. 2. 5.] [금융감독원세칙 , 2025. 2. 3., 일부개정]

제1장 총칙
제1조(목적)
제2조(정의)
제2장 전자금융거래 안전성 확보 등
제2조의2(정보처리시스템 가동기록)
제2조의3(망분리 적용 예외)
제2조의4(클라우드컴퓨팅서비스의 보고)
제2조의5(법인 이용자 정보의 사용에 대한 동의)
제2조의6(정보보호시스템 운영)
제2조의7(프로그램 통제)
제3조(자체 보안성심의 기준 등)
제3조의2(정보기술부문 계획서 제출)
제4조삭 제
제5조삭 제
제6조삭 제
제7조삭 제
제7조의2(전자금융기반시설의 취약점 분석·평가의 내용)
제7조의3삭 제
제7조의4(정보기술부문 사고보고)
제8조(약관의 제정 또는 변경)
제8조의2(국외에서 주로 영업하는 국외 사이버몰의 판단기준)
제8조의3(거래금액 기준 초과시 신고 등)
제3장 정보기술부문 실태평가 등
제9조(정보기술부문 실태평가 방법 등)
제9조의2(외부주문등에 대한 기준)
제10조(업무보고서의 제출)
제11조(경영지도비율 산정기준)
제4장 보칙
제12조삭 제

전자금융감독규정시행세칙

[시행 2025. 2. 5.] [금융감독원세칙 , 2025. 2. 3., 일부개정]

금융감독원(디지털금융총괄국), 02-3145-7126

제1장 총칙

제1조(목적) 이 세칙은 「전자금융거래법」(이하 "법"이라 한다) 및 동법 시행령(이하 "시행령"이라 한다)과 「전자금융감독규정」(이하 "규정"이라 한다)에서 금융감독원장(이하 "감독원장"이라 한다)에게 위임한 사항과 그 시행에 필요한 사항을 규정함을 목적으로 한다.

[전문개정 2012. 05. 24.]

제2조(정의) 이 세칙에서 별도로 정하지 아니한 용어는 법・시행령・규정에서 정하는 바에 따른다.

[전문개정 2012. 05. 24.]

제2장 전자금융거래 안전성 확보 등

제2조의2(정보처리시스템 가동기록) 규정 제13조제1항제9호에 따라 감독원장이 정하는 사항은 다음 각 호와 같다.

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

[본조신설 2025. 2. 3.]

제2조의3(망분리 적용 예외) ① 규정 제15조제1항제3호나목에서 감독원장의 확인을 받은 경우란 다음 각 호와 같다.<개정 2020. 11. 6., 2022. 12. 29.>

1. 내부 통신망에 연결된 단말기가 업무상 필수적으로 외부기관과 연결해야 하는 경우(다만, 이 경우 필요한 서비스번호(port)에 한하여 특정 외부기관과 연결할 수 있다).
2. 규정 제12조의 보안대책을 적용한 단말기에서 전용회선과 동등한 보안수준을 갖춘 통신망을 이용하여 외부망으로부터 내부 업무용시스템으로 원격접속 하는 경우

② 규정 제15조제1항제5호나목에서 감독원장이 인정하는 경우란 다음 각 호와 같다.<개정 2022. 12. 29.>

1. 「금융회사의 정보처리 업무 위탁에 관한 규정」에 따라 정보처리 업무를 국외 소재 전산센터에 위탁하여 처리하는 경우(다만, 해당 국외 소재 전산센터에 대해서는 물리적 방식 외의 방법으로 망을 분리하여야 하며, 이 경우에도 국내 소재 전산센터 및 정보처리시스템 등은 물리적으로 망을 분리하여야 한다)
2. 업무상 외부통신망과 연결이 불가피한 다음의 정보처리시스템(다만, 필요한 서비스번호(port)에 한하여 연결할 수 있다)

가. 전자금융업무의 처리를 위하여 특정 외부기관과 데이터를 송수신하는 정보처리시스템

나. DMZ구간 내 정보처리시스템과 실시간으로 데이터를 송수신하는 내부통신망의 정보처리시스템

다. 다른 계열사(「금융회사의 정보처리 업무 위탁에 관한 규정」 제2조제3항의 "계열사"를 말한다)와 공동으로 사용하는 정보처리시스템

3. 규정 제23조의 비상대책에 따라 원격 접속이 필요한 경우

4. 전산실 내에 위치한 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기와 외부통신망과의 연결 구간, 규정 제15조제1항제3호의 내부 업무용 시스템과의 연결 구간을 각각 차단한 경우<신설 2016. 5. 12.>

③ 제1항 및 제2항의 규정은 금융회사 또는 전자금융업자가 자체 위험성 평가를 실시한 후 별표 7에서 정한 망분리 대체 정보보호통제를 적용하고 정보보호위원회가 승인한 경우에 한하여 적용한다.

[종전의 제2조의2에서 이동]

제2조의4(클라우드컴퓨팅서비스의 보고) ① 규정 제14조의2제4항에 따라 감독원장에게 보고하는 양식은 별지 제6호서식에 따른다.<개정 2022. 12. 29., 2025. 2. 3.>

② 규정 제14조의2제4항 및 제5항에 따라 감독원장에게 보고할 경우 첨부해야 하는 서류는 다음 각 호와 같다.

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

2. 규정 제14조의2제1항제1호에 따른 업무의 중요도 평가 기준 및 결과

3. 규정 제14조의2제1항제2호에 따른 클라우드컴퓨팅서비스 제공자의 건전성 및 안전성 등에 대한 평가 결과

4. 규정 제14조의2제1항제3호에 따른 업무 연속성 계획 및 안전성 확보조치에 관한 사항

5. 규정 제14조의2제2항에 따른 정보보호위원회 심의·의결 결과

6. 규정 별표 2의5의 계약서 주요 기재사항을 포함한 클라우드컴퓨팅서비스 이용계약서

[종전의 제2조의3에서 이동]

제2조의5(법인 이용자 정보의 사용에 대한 동의) 규정 제13조제1항제8호에 따라 동의를 얻는 경우 다음 각 호의 사항을 정보주체에게 사전에 알려야 한다.

1. 테스트의 목적 및 기간

2. 사용되는 이용자 정보의 항목

3. 테스트 기간 중 정보유출 방지를 위한 통제 계획

4. 테스트 종료 후 테스트에 사용된 이용자 정보의 파기 계획

[종전의 제2조의4에서 이동]

제2조의6(정보보호시스템 운영) 규정 제15조제2항에 따라 감독원장이 정하는 사항은 다음 각 호와 같다.

1. 최소한의 서비스번호(port)와 기능만을 적용하고 업무목적 이외의 기능 및 프로그램을 제거할 것

2. 보안정책의 승인, 적용, 등록, 변경 및 삭제에 대해 기록·보관하고 적용된 보안정책의 적정성을 주기적으로 점검할 것

3. 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·운용할 것

4. 정보보호시스템의 정상 작동 여부 확인을 위하여 시스템 상태의 감시, 경고가 가능하도록 모니터링시스템을 갖추고 시스템 장애, 가동중지 등 긴급사태에 대비하여 백업 및 복구 절차 등을 수립·운용할 것

[본조신설 2025. 2. 3.]

제2조의7(프로그램 통제) 규정 제29조에 따라 감독원장이 정하는 사항은 다음 각 호와 같다.

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
5. 프로그램에 대한 접근은 업무담당자에 한정하고, 적절한 접근권한(읽기・쓰기・실행 등 포함) 설정 및 중요 조작에 대한 책임자 사전 승인 등 통제절차를 수립・운용할 것
6. 프로그램 반출, 실행프로그램의 생성 및 운영시스템 적용은 해당 프로그램 담당자 이외의 자가 수행할 것
7. 운영시스템 적용은 처리하는 정보의 기밀성・무결성・가용성 및 전자금융거래의 안전성과 신뢰성이 훼손되지 않도록 충분한 테스트 및 관련 책임자 승인 후 실시할 것
8. 운영체제, 데이터베이스관리프로그램 등의 시스템 프로그램도 응용프로그램과 동일한 수준으로 관리할 것
9. 프로그램 설명서, 프로그램 목록 및 사용자・운영자 지침서 등 프로그램 유지보수에 필요한 문서를 작성・관리할 것
10. 전자금융거래에 사용되는 프로그램은 도입・분석・설계 단계에서부터 안전성과 신뢰성을 확보할 수 있는 대책을 마련하고, 운영시스템 적용 전에 동 대책이 반영되었는지 충분히 검증하고 적용할 것

[본조신설 2025. 2. 3.]

제3조(자체 보안성심의 기준 등) ① 규정 제36조제1항에 따른 감독원장이 정하는 기준과 절차란 다음 각 호를 말한다.

1. 정보통신망을 이용하여 신규전자금융업무를 수행하는 경우 별표 1의 기준에 따라 보안성심의를 실시한 후 정보보호최고책임자의 승인을 받을 것
2. 공동으로 전자금융거래 관련 표준을 제정하는 경우 별표 1의2의 기준에 따라 보안성심의를 실시할 것(다만, 이 경우 특정 금융회사 또는 전자금융업자가 다른 금융회사등을 대표하여 규정 제36조제2항에 따른 자체 보안성심의 결과보고서를 제출할 수 있음).<개정 2014. 3. 31., 2016. 7. 27.>

② 금융회사 또는 전자금융업자가 규정 제36조제2항에 따라 제출하는 자체 보안성심의 결과보고서의 양식은 제1항제1호의 경우 별지 제3호서식에, 제1항제2호의 경우 별지 제4호서식에 각각 따른다.<개정 2014. 3. 31., 2016. 7. 27.>

③ 금융회사 또는 전자금융업자는 제1항에 따른 자체 보안성심의를 수행함에 있어 필요한 경우 규정 제37조의6제1항의 침해사고대응기관,「정보통신기반보호법」제16조제1항의 정보공유・분석센터 등 외부기관에 보안대책의 적정성 여부 등에 대한 검토를 의뢰할 수 있다.<신설 2014. 3. 31.>

④ 규정 제36조제2항 단서에서 "금융감독원장이 인정하는 기준"이란 다음 각 호에서 정하는 요건을 충족하는 것을 말한다.<신설 2016. 5. 12.>

1. 전자금융업자 : 법 제28조에 따라 금융위원회로부터 허가를 받았거나 금융위원회에 등록한 날 및 전자금융업무를 신규로 수행한 날로부터 1년이 경과하였을 것.

2. 금융회사 : 전자금융업무를 신규로 수행한 날로부터 1년이 경과하였을 것

제3조의2(정보기술부문 계획서 제출) 규정 제36조의2제1항에 따라 제출하는 정보기술부문계획서의 양식은 별지 제8호 서식에 따른다.

제4조 삭제 <2015. 9. 17.>

제5조 삭제 <2015. 9. 17.>

제6조 삭제 <2015. 9. 17.>

제7조 삭제 <2015. 9. 17.>

제7조의2(전자금융기반시설의 취약점 분석·평가의 내용) 규정 제37조의2제3항에 따라 감독원장이 정하는 취약점 분석·평가의 내용은 별표 3과 같다.<신설 2014. 3. 31., 개정 2022. 12. 29.>

제7조의3 삭제 <2025. 2. 3.>

제7조의4(정보기술부문 사고보고) ① 규정 제37조의5제4항에 따라 감독원장이 정하는 사고보고 대상은 다음 각 호와 같다.<신설 2025. 2. 3.>

1. 정보처리시스템 또는 통신회선 등의 장애로 인하여 다음 각 목 중 하나에 해당하는 사고가 발생한 경우
   가. 전자금융업무 지연·중단 시간이 30분 이상인 경우
   나. 전자금융업무 지연·중단 시간이 10분 이상이고 해당 전자금융서비스 가입자가 1만명 이상인 경우
2. 전산자료 또는 프로그램의 조작 및 오류와 관련된 사고가 발생한 경우
3. 전자적 침해행위로 인해 정보처리시스템에 사고가 발생하거나 이로 인해 이용자가 금전적 피해를 입었다고 금융회사 또는 전자금융업자에게 통지한 경우
4. 법 제9조제1항의 규정에서 정하는 사고가 발생한 경우

② 제1항에도 불구하고 다음 각 호에 해당하는 경우는 사고보고 대상에서 제외한다.<신설 2025. 2. 3.>

1. 제1항제1호에 해당하는 사고 중 영업점 내 장애의 경우 1개 영업점에 국한된 전자금융업무 중단·지연
2. 제1항제1호에 해당하는 사고 중 이용자에게 단순 정보 제공을 위한 공개용 웹서버 등의 장애 또는 금융상품 및 서비스와 무관한 장애
3. 법 제9조제1항제1호 또는 제3호의 사고가 발생하였으나 사고금액이 100만원 미만인 경우

③ 금융회사 및 전자금융업자는 제1항의 사고가 발생한 경우 별지 제2호서식 별첨1에 따라 지체 없이 보고하여야 하며, 정당한 사유없이 그 사실을 안 때부터 24시간을 경과하여서는 아니된다. 다만, 법 제9조제1항제1호의 사고 중 사고금액이 3억원 미만인 사고의 경우 매월 발생한 사고를 익월 15일까지 별지 제2호서식 별첨2에 따라 일괄 보고할 수 있다. <제1항에서 이동 2025. 2. 3.><개정 2014. 3. 31., 2017. 9. 5., 2025. 2. 3.>

④ 제3항에 따른 사고보고는 최초보고, 중간보고 및 종결보고로 구분한다. <제2항에서 이동 2025. 2. 3.>

1. 최초보고 : 사고를 인지 또는 발견한 때로부터 24시간 이내에 전자금융사고대응시스템(Electronic Financial Accident Response System : EFARS)으로 보고한다. 단, 전산장애, 금융정보교환망 미연결 등 부득이한 경우에는 서면, 팩시밀리 또는 유선으로 보고할 수 있으며, 이 경우에 전자금융사고대응시스템(EFARS)으로 보고가능

한 즉시 전자금융사고대응시스템(EFARS)으로 보고한다.<개정 2015. 4. 8., 2025. 2. 3.>

2. 중간보고 : 제1호의 최초보고 후 사고내용을 보완할 필요가 있는 경우에는 즉시 중간보고를 하여야 하며, 제3호의 조치완료 시까지 2월 이상 소요될 경우에는 인지·발견일로부터 2월 이내 및 종결 시까지 매 6월마다 제1호의 방법에 따라 보고한다. 다만, 최초보고 후 조치완료 시까지 2월 미만이 소요될 경우에는 중간보고를 생략할 수 있다.<개정 2017. 9. 5.>

3. 종결보고 : 사고발생 원인 파악 및 조치, 재발방지 대책 마련 등이 완료(사고금액에 대한 배상책임이 있는 경우에는 배상조치까지 포함)되어 정상적인 업무를 수행하게 된 때 제1호의 방법에 따라 보고한다. 다만, 최초보고 시 조치가 이미 완료된 경우에는 종결보고를 생략할 수 있다.<개정 2017. 9. 5., 2025. 2. 3.>

⑤ 감독원장은 금융회사 및 전자금융업자 정보기술부문의 사고보고 등을 전담할 비상연락 담당자를 회사별로 지정할 수 있다. <제3항에서 이동 2025. 2. 3.><개정 2014. 3. 31., 2015. 4. 8.>

⑥ 금융회사 및 전자금융업자는 비상연락 담당자가 제5항에 따라 지정되거나 변경된 경우에는 제4항제1호에서 정한 보고방법에 따라 감독원장에게 즉시 보고하여야 한다. <제4항에서 이동 2025. 2. 3.><개정 2014. 3. 31., 2015. 4. 8.>

⑦ 감독원장은 제4항에 따라 보고 받은 내용이 제1항제3호의 사고 발생인 경우에는 규정 제37조의6제1항 각 호에 따른 침해사고대응기관에도 알려야 한다.<신설 2025. 2. 3.>

[종전의 제12조에서 이동]

제8조(약관의 제정 또는 변경) ① 규정 제41조제1항제3호에 따른 감독원장이 정하는 약관의 제정 또는 변경이란 다음 각 호의 어느 하나를 말한다.

1. 법령의 개정 또는 금융위원회의 명령에 따른 약관의 변경
2. 이용자의 권익이나 의무사항을 제외한 사항으로서 단순히 업무편의를 위한 약관의 변경
3. 사업자단체의 표준약관을 원용하는 약관의 제정 또는 변경

② 금융회사 또는 전자금융업자가 제1항에 따라 약관을 제정하거나 변경하는 경우에는 당해 약관과 약관내용을 이해하는 데 필요한 관련서류를 별지 제7호서식에 따라 감독원장에게 보고한다.<신설 2021. 2. 25.>

③ 법 제25조제2항에 따라 변경권고를 받은 전자금융업자는 해당 권고를 받은 날로부터 10영업일 이내에 해당 권고의 수락여부 및 수정된 약관(수락한 경우에 한함)을 감독원장에게 보고하여야 한다. 다만, 감독원장이 따로 기간을 정한 경우에는 그러하지 아니하다.<신설 2021. 2. 25.>

제8조의2(국외에서 주로 영업하는 국외 사이버몰의 판단기준) 규정 제50조의2제3항에 따라 감독원장은 국외에서 주로 영업하는 국외 사이버몰을 판단하는데 있어 다음 각 호의 사항 등을 고려한다.<신설 2014. 3. 31.>

1. 사이버몰 운용자의 사무소, 인적·물적 시설의 소재지
2. 사이버몰에서 이루어지는 상거래 대상 국가의 수
3. 사이버몰에 대한 국외 감독당국, 규제기관의 감독·규제여부
4. 사이버몰에서 체결된 전자상거래 중 국내에 소재한 소비자와 사업자간 거래의 비중
5. 규정 제50조의2제2항에 따른 제한을 회피하기 위한 사이버몰 여부

제8조의3(거래금액 기준 초과시 신고 등) ① 법 제30조제3항제1호에 해당하는 전자금융업자는 분기별 거래 총액(결제대행금액, 결제대금예치금액 또는 전자고지결제금액)이 규정 제42조의2제1항에 따른 거래금액 기준을 초과한

경우 해당 분기 종료 후 45일 이내에 별지 제5호서식에 따라 감독원장에게 초과 내역 및 자본금 증액 계획을 신고하여야 한다.

② 제1항에 따른 신고를 마친 자는 법 제30조제4항에 따른 자본금 요건을 갖춘 후, 신고한 때부터 6개월 이내에 자본금 납입 증명서류 등 관련 서류를 감독원장에게 제출하여야 한다.

제3장 정보기술부문 실태평가 등

제9조(정보기술부문 실태평가 방법 등) ① 규정 제58조에 따른 정보기술부문 실태평가는 검사기준일 현재 평가대상기관의 정보기술부문 실태를 IT감사, IT경영, 시스템 개발・도입・유지 보수, IT서비스 제공 및 지원, IT보안 및 정보보호의 부문별로 구분 평가하고 부문별 평가결과를 감안하여 종합평가한다.<개정 2014. 3. 31.>

② 제1항의 규정에 따른 부문별 세부 평가 항목은 별표 4와 같다.<개정 2014. 3. 31.>

③ 규정 제58조제3항의 평가등급별 정의는 별표 5와 같다.<개정 2014. 3. 31.>

제9조의2(외부주문등에 대한 기준) ① 규정 제60조제1항제7호에 따라 감독원장이 정하는 보안관리방안은 별표 5-2와 같다.

② 규정 제60조제1항제14호에 따라 감독원장이 정하는 중요 점검사항은 별표 5-3과 같다.<신설 2015. 4. 8.>

제10조(업무보고서의 제출) ① 금융회사 또는 전자금융업자는 규정 제62조에 따른 업무보고서를 분기말 현재로 작성하여 매분기 종료 후 45일 이내에 감독원장에게 제출하여야 한다.<개정 2014. 3. 31.>

② 업무보고서 양식 및 기재사항은 별지 제1호서식에 따른다.

제11조(경영지도비율 산정기준) 규정 제63조제2항에 따른 경영지도비율의 구체적 산정기준은 별표 6과 같다.<개정 2014. 3. 31.>

[전문개정 2012. 05. 24.]

제4장 보칙

제12조 삭제

부칙 <제호,2025.2.3.>

제1조(시행일) 이 세칙은 2025년 2월 5일부터 시행한다.

[별표 1] 자체 보안성심의 기준
[별표 1의2] 자체 보안성 심의 기준
[별표 2] 삭제
[별표 3] 전자금융기반시설의 취약점 분석·평가의 내용
[별표 3의2] 삭제

[별표 4] 정보기술부문 실태평가 부문별 평가항목
[별표 5] 평가등급별 정의
[별표 5의2] 보안관리방안
[별표 5의3] 중요 점검사항
[별표 6] 경영지도비율 산정기준
[별표 7] 망분리 대체 정보보호통제
[별지 1] 업무보고서
[별지 2] 정보기술부문 및 전자금융 사고보고서
[별지 3] 자체 보안성심의 결과보고서(신규 전자금융서비스)
[별지 4] 자체 보안성심의 결과보고서(공동 표준안)
[별지 5] 전자금융 거래금액 기준 초과 신고서
[별지 6] 클라우드컴퓨팅서비스 이용업무 지정/변경 보고
[별지 7] 약관 제정(변경)보고
[별지 8] 정보기술부문 연간 계획서