전자금융감독규정시행세칙

[시행 2023. 1. 1.] [금융감독원세칙 , 2022. 12. 29., 일부개정]

금융감독원(디지털금융혁신국), 02-3145-7124

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 망분리 적용 예외・자체 보안성심의 기준 등

제2조의2 (망분리 적용 예외) ① 규정 제15조제1항제3호나목에서 금융감독원장의 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 금융감독원장이 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」 제2조 제3항의 "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 7>에서 정한 망분리 대체 정보보호통제를 적용하고 정보보호위원회가 승인한 경우에 한하여 적용한다.

제2조의3 (클라우드컴퓨팅서비스의 보고) 규정 제14조의2제4항에 따라 감독원장에게 보고하는 양식은 별지 제6호 서식에 따른다.<개정 2022. 12. 29.>[[본조신설 2016. 11. 10.]]]

제2조의4 (법인 이용자 정보의 사용에 대한 동의) 규정 제13조 제1항 제10호에 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

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

1. 정보통신망을 이용하여 신규전자금융업무를 수행하는 경우 <별표 1>의 기준에 따라 보안성심의를 실시한 후 정보보호최고책임자의 승인을 받을 것
2. 공동으로 전자금융거래 관련 표준을 제정하는 경우 <별표 1의2>의 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 제3호 서식에, 제1항제2호의 경우 별지 제4호 서식에 각각 따른다.<개정2014. 3. 31., 2016. 7. 27.>

③ 금융회사 또는 전자금융업자는 제1항에 따른 자체 보안성심의를 수행함에 있어 필요한 경우 규정 제37조의4제1항의 침해사고대응기관,「정보통신기반보호법」제16조제1항의 정보공유・분석센터 등 외부기관에 보안대책의 적정성 여부 등에 대한 검토를 의뢰할 수 있다.<신설 2014. 3. 31.>

④ 규정 제36조 제2항 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

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(정보보호최고책임자의 업무) 규정 제37조의5에 따라 감독원장이 정하는 정보보안 점검항목은 별표 3-2와 같다.<신설 2015. 4. 8.>

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 제7호 서식에 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 제5호 서식에 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 평가대상 기관의 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(정보기술부문 사고보고) ① 금융회사 및 전자금융업자는 규정 제73조에 따른 정보기술부문 및 전자금융 사고가 발생한 경우 별지 제2호서식 별첨1에 따라 즉시 보고하여야 한다. 다만, 규정 제73조제1항제4호의 사고 중 사고금액이 3억원 미만인 사고의 경우 매월 발생한 사고를 익월 15일까지 별지 제2호서식 별첨2에 따라 일괄 보고할 수 있다.<개정 2014. 3. 31., 2017. 9. 5.>

② 제1항에 따른 사고보고는 최초보고, 중간보고 및 종결보고로 구분한다.

1. 최초보고 : 사고를 인지 또는 발견한 즉시 감독원의 전자금융사고 대응시스템(Electronic Financial Accident Response System : EFARS), 서면, 팩시밀리 또는 전화로 보고하되, 전화로 보고한 경우에는 즉시 전자금융사고 대응시스템, 서면 또는 팩시밀리로 보고한다.<개정 2015. 4. 8.>
2. 중간보고 : 제1호의 즉시보고 후 사고내용 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, 즉시보고 후 조치완료 시까지 2월 미만이 소요될 경우에는 중간보고를 생략할 수 있다.<개정 2017. 9. 5.>
3. 종결보고 : 사고금액에 대한 배상조치가 완료되거나 사고조치 등이 완료되어 정상적인 업무를 수행하게 된 때 제1호의 방법에 따라 보고한다. 다만, 최초보고 시 조치가 이미 완료된 경우에는 종결보고를 생략할 수 있다.

<개정 2017. 9. 5.>

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

④ 금융회사 및 전자금융업자는 비상연락 담당자가 제3항에 따라 지정되거나 변경된 경우에는 제2항제1호에서 정한 보고방법에 따라 감독원장에게 즉시 보고하여야 한다.<개정 2014. 3. 31., 2015. 4. 8.>

부칙 <제호,2022.12.29.>

이 세칙은 2023년 1월 1일부터 시행한다.

<별표 1> 자체 보안성심의 기준 <개정 2015.9.17>

	심의기준
1	거래 당사자 인증
2	거래정보의 기밀성 및 무결성
3	정보처리시스템 보호대책
4	고객 단말기 보호대책
5	정보유출 방지대책
6	이상금융거래 방지대책
7	시스템 가용성 확보 및 비상대책
8	시스템 설치장소에 대한 물리적 접근통제

※ 전자금융업무 유형에 따라 자체적으로 심의기준 추가·수정 가능

<별표 1의2> 자체 보안성 심의 기준 <신설 2016.7.27>

	심의기준
1	컴플라이언스 준수
2	사용자 접근성
3	호환성 지원
4	서비스 품질 보장(안정성)
5	불필요한 기능 제거(간결성)
6	표준화 그룹 체계 관리

※ 공동 표준안의 유형에 따라 자체적으로 심의기준 추가 · 수정

<별표 3> 전자금융기반시설의 취약점 분석·평가의 내용

평가 부문	평가 항목
관리적 보안	- 정보보호 정책 - 정보보호 조직 및 인력 - 내부통제 - 정보보호 교육 및 훈련 - 자산관리 - 업무연속성 관리 - 사고관리 - 정보시스템 도입·개발·유지보수
물리적 보안	- 전산설비 보안 - 전산센터 보안
기술적 보안	- 인터넷 전자금융 보안 - 모바일 전자금융 보안 - 접근통제 - 전산자료 보안 - 서버 보안 - 데이터베이스 보안 - 웹 서비스 보안 - 단말기 보안 - 네트워크 보안 - 정보보호시스템 보안

<별표 3-2> 정보보안 점검항목 <신설 2015.4.8>

	점검항목
전산실	상시출입자외 출입자에 대한 책임자 승인 및 출입자관리기록부 기록·보관 여부
	무인감시카메라 또는 출입자동기록시스템 등의 정상 작동 여부
단말기	업무담당자 이외의 단말기 무단조작 금지 조치 여부
	정보처리시스템 접속 단말기의 정당한 사용자인가를 확인할 수 있는 기록 유지 여부
	중요 단말기의 외부 반출 금지 여부
	중요 단말기의 인터넷 접속 금지 여부
	중요 단말기의 그룹웨어 접속 금지 여부
	단말기에서 보조기억매체 및 휴대용 전산장비 접근 통제 여부
전산자료	개인별 사용자계정과 비밀번호 부여 여부
	사용자계정과 비밀번호 등록·변경·폐기의 체계적 관리 여부
	이용자 정보 조회·출력 통제 여부
	테스트시 이용자 정보 사용 금지 및 불가피한 경우 이용자정보를 변환하여 사용하고 테스트 종료 즉시 삭제 여부
	단말기에 이용자 정보 등 주요정보 보관을 금지하고 불가피한 경우 책임자의 승인을 받고 있는지 여부
	단말기 공유 금지 여부
	전산자료 및 전산장비의 반출·반입 통제 여부
	사용자 인사 조치시 지체 없이 해당 사용자계정 삭제, 계정 사용 중지, 공동 사용 계정 변경 등 정보처리시스템 접근을 통제하고 있는지 여부
정보처리시스템	내부통신망의 비인가 전산장비·무선통신 접속 통제 여부
해킹 등 방지대책	해킹 등을 방지하기 위한 정보보호시스템의 정상 작동 여부
	정보보호시스템에 최소한의 서비스번호와 기능만을 적용하고 있는지 여부
	정보보호시스템에 업무목적이외 기능 및 프로그램 제거 여부
	정보보호시스템의 원격관리 금지 여부
	시스템프로그램 등 긴급하고 중요한 보정사항에 대한 즉시 보정작업 실시 여부
	무선통신망 이용 업무에 대한 승인 및 사전 지정 여부
악성코드	악성코드 검색 및 치료프로그램의 최신상태 유지 여부
	중요 단말기의 악성코드 감염여부를 매일 점검하고 있는지 여부
공개용 웹서버	사용자계정에 아이디·비밀번호 이외 추가 인증수단 적용 여부
	DMZ구간 내 이용자 정보 등 주요정보를 저장, 관리하지 않는지 여부
내부사용자 비밀번호	접근자 비밀번호 설정·운영 여부
	비밀번호 보관시 암호화 여부
이용자 비밀번호 관리	정보처리시스템 및 전산자료에 보관하고 있는 이용자 비밀번호 암호화 보관 여부
이용자 유의사항	비밀번호 유출위험 및 관리에 관한 사항의 공지 여부
	제공하고 있는 이용자보호 제도에 관한 사항의 공지 여부
	해킹·피싱 등 전자적 침해방지에 관한 사항의 공지 여부
전자금융 사고보고	전자적 침해행위에 대한 보고 및 조치 여부

<별표 4> 정보기술부문 실태평가 부문별 평가항목

평가 부문	평가 항목
1. IT 감사	- IT감사조직 및 요원 - IT감사 실시 내용 - IT감사 사후관리 및 기타
2. IT 경영	- IT부서 조직 및 요원 - IT관련 내규(규정, 지침, 절차, 편람 등) - IT계획 및 방향제시 - 비상계획 - 경영정보시스템(MIS) 등 - IT 인력 및 예산의 적정성
3. 시스템 개발, 도입 및 유지보수	- 시스템 개발, 도입 및 유지보수 관련 조직 및 요원 - 시스템 개발, 도입 및 유지보수 관련 내규(규정, 지침, 절차 등) - 시스템 개발, 도입, 유지보수 현황 - 내부통제용 시스템, 시스템통합 등
4. IT서비스 제공 및 지원	- IT서비스 제공/지원 관련 조직 및 요원 - IT서비스 제공/지원 관련 내규(규정, 지침, 절차 등) - 시설 및 장비 - 운영통제 - 통신망 - 최종사용자 컴퓨팅 - 전자금융거래 등
5. IT보안 및 정보보호	- IT보안 절차 - IT보안 리스크 평가 - IT보안 및 정보보호 전략 - IT보안 통제 구현 - IT보안 모니터링

<별표 5> 평가등급별 정의

가. IT 감사 부문에 대한 평가등급별 정의

평가등급	정 의
1 등급 (우수:Strong)	감사업무가 독립적으로 정확하게 이루어지고 감사내용 및 결과처리가 적절하며 특별한 문제점이 없어 감독상 주의를 기울일 필요가 거의 없음
2 등급 (양호:Satisfactory)	감사업무가 독립적으로 비교적 정확하게 이루어지나 감사내용 및 결과처리에 경미한 문제점이 있어 감독상 최소의 주의를 요함
3 등급 (보통:Less than satisfactory)	감사활동의 독립성과 감사내용 및 감사결과처리가 다소 미흡하여 개선이 요망되며 업무의 정확성 및 적시성이 부족하여 적정수준의 감독이 요구됨
4 등급 (취약:Deficient)	감사활동의 독립성과 감사내용 및 감사결과처리가 현저하게 미흡하고 업무수행이 부적절하여 적절한 통제 및 시정이 요구됨
5 등급 (위험:Critically deficient)	감사활동 및 감사결과처리가 크게 미흡하여 감사업무 전반에 대한 신뢰성이 없음

나. IT 경영 부문에 대한 평가등급별 정의

평가등급	정 의
1 등급 (우수:Strong)	경영전략 및 비상대책이 우수하고 이를 효율적으로 추진할 수 있는 조직과 경영정보시스템 등이 적절히 구축되어 정보기술부문의 취약점이나 문제점에 대해 효과적으로 대응할 수 있음
2 등급 (양호:Satisfactory)	경영전략 및 비상대책이 양호하고 이를 추진하는 조직과 경영정보시스템 등이 비교적 효율적으로 구축되어 정보기술부문의 취약점이나 문제점에 대해 적절히 대응할 수 있음
3 등급 (보통:Less than satisfactory)	경영전략 및 비상대책이 다소 미흡하고 이를 추진하는 조직과 경영정보시스템 등에 대한 개선이 요망되며 정보기술부문의 취약점이나 문제점에 대한 대응이 약간 부족함
4 등급 (취약:Deficient)	경영전략 및 비상대책 및 이를 추진하는 조직과 경영정보시스템 등이 전반적으로 부족하여 이에 대한 개선이 요망됨
5 등급 (위험:Critically deficient)	경영전략 및 비상대책 및 이를 추진하는 조직과 경영정보시스템 등이 전반적으로 크게 부족하여 긴급대책이 요구됨

다. 시스템 개발, 도입 및 유지보수 부문에 대한 평가등급별 정의

평가등급	정 의
1 등급 (우수:Strong)	시스템이 효율적으로 구축되고 사용목적에 부합하며 시스템 및 프로그램의 변경과정에 대한 효과적인 통제제도 등이 수립되어 있음
2 등급 (양호:Satisfactory)	시스템이 비교적 효율적으로 구축되고 시스템 및 프로그램의 변경과정에 대한 통제제도 등이 건전하나 사용목적에 다소 부합하지 않고 경미한 문제점이 발견됨
3 등급 (보통:Less than satisfactory)	시스템에 일부 결함이 발견되고 시스템 및 프로그램의 변경과정에 대한 통제제도 등이 다소 미흡하며 사용목적에 부합하기 위해서는 개선이 요망됨
4 등급 (취약:Deficient)	시스템이 심각한 취약점을 내포하고 사용목적에 부합하지 않으며 시스템 및 프로그램의 변경과정에 대한 통제제도가 미흡하여 금융회사의 건전성에 손해를 초래할 우려가 있음
5 등급 (위험:Critically deficient)	시스템과 시스템 및 프로그램의 변경과정에 대한 통제제도가 극히 취약하며 중대한 결함을 갖고 있고 사용목적을 전혀 고려하지 못하여 금융회사의 존립이 위태로움

라. IT 서비스 제공 및 지원 부문에 대한 평가등급별 정의

평가등급	정 의
1 등급 (우수:Strong)	IT 서비스 부문이 효율적이고 일상적인 운영상황에 특별한 문제점이 없음
2 등급 (양호:Satisfactory)	IT 서비스 부문이 비교적 효율적이고 일상적인 운영상황에 경미한 문제점이 있으나 정상적인 운영과정에서 적절히 대응할 수 있음
3 등급 (보통:Less than satisfactory)	IT 서비스 부문의 효율성이 다소 미흡하고 일상적인 운영상의 취약점이나 문제점에 대한 대응이 부족하여 개선이 요구됨
4 등급 (취약:Deficient)	IT 서비스 부문의 효율성이 취약하고 일상적인 운영상의 취약점이나 문제점이 현저하게 드러나 동 부문의 안전성 및 건전성에 위험을 초래할 가능성이 큼
5 등급 (위험:Critically deficient)	IT 서비스 부문이 비효율적이고 일상적인 운영상의 취약점이나 문제점이 크게 심각하여 동 부문의 안전성 및 건전성 확보가 위태로움

마. IT보안 및 정보보호 부문에 대한 평가등급별 정의

평가등급	정 의
1 등급 (우수:Strong)	IT보안 및 정보보호가 우수하고 이를 효율적으로 추진할 수 있는 조직과 정보보호시스템 등이 적절히 구축되어 보안부문의 취약점이나 문제점에 대해 효과적으로 대응할 수 있음
2 등급 (양호:Satisfactory)	IT보안 및 정보보호가 양호하고 이를 추진하는 조직과 정보보호시스템 등이 비교적 효율적으로 구축되어 보안부문의 취약점이나 문제점에 대해 적절히 대응할 수 있음
3 등급 (보통:Less than satisfactory)	IT보안 및 정보보호가 다소 미흡하고 이를 추진하는 조직과 정보보호시스템 등에 대한 개선이 요망되며 보안부문의 취약점이나 문제점에 대한 대응이 약간 부족함
4 등급 (취약:Deficient)	IT보안 및 정보보호를 추진하는 조직과 이를 지원하는 정보보호시스템 등이 전반적으로 부족하여 이에 대한 개선이 요망됨
5 등급 (위험:Critically deficient)	IT보안 및 정보보호를 추진하는 조직과 이를 추진하는 정보보호시스템 등이 전반적으로 크게 부족하여 긴급대책이 요구됨

바. 종합평가등급의 정의

평가등급	정 의
1 등급 (우수:Strong)	- 전자금융업무와 정보기술부문 전반에 걸쳐 운영상태가 건전하며 정상적인 감독상의 주의만 요구됨 - 약간의 적출사항은 있으나 그 정도가 경미하여 통상적인 방법으로 해결이 가능함
2 등급 (양호:Satisfactory)	- 전자금융업무와 정보기술부문 전반에 걸쳐 운영상태가 근본적으로 건전하나, 약간의 취약점을 내포하고 있으며 필요시 제한된 범위내의 감독조치가 요구됨
3 등급 (보통:Less than satisfactory)	- 전자금융업무와 정보기술부문 전반에 걸쳐 즉각적인 시정을 요하는 다양한 취약점을 내포하고 있어 이를 시정하기 위해 통상적인 수준 이상의 감독상의 주의가 요구됨
4 등급 (취약:Deficient)	- 전자금융업무와 정보기술부문 전반에 걸쳐 즉각적인 시정을 요하는 다양한 취약점을 내포하고 있어 감독당국의 면밀한 주의 및 문제점을 시정하기위한 조치가 필요함 - 전자금융업무와 정보기술부문 전반에 걸친 취약점이 심각하여 장래 동 업무처리 자체가 위험하게 될 가능성이 있으므로 감독당국의 면밀한 주의 및 문제점을 시정하기 위한 조치가 필요함
5 등급 (위험:Critically deficient)	- 전자금융업무와 정보기술부문 전반에 걸쳐 취약점이 매우 심각하여 정상적인 업무처리를 할 수 없는 상황임

<별표 5-2> 보안관리방안 <신설 2015.4.8> <개정 2016.11.10>

단계	세부사항
입찰	○ 입찰 공고 이전에 투입이 예상되는 자료 · 장비 가운데 보안관리가 필요한 사항에 대하여 금융회사또는 전자금융업자의 내부관리기준과 관련 법규를 검토하고 필요한 보안요구 사항을 마련 ○ 입찰 공고시에 금융회사 또는 전자금융업자가 자체 작성한 중요정보, 부정당업자 제재조치, 기밀유지 의무 및 위반시 불이익 등을 정확히 공지 ○ 제안서 평가요소에 자료 · 장비 · 네트워크 보안대책 및 중요정보 관리 방안 등 보안관리 계획의 평가항목 및 배점기준 마련 ○ 업체가 입찰제안서에 제시한 용역사업 전반에 대한 보안관리 계획이 타당한지를 검토하여 사업자 선정시에 이를 반영
계약	○ 계약서 작성 초기 단계부터 정보보안사항 포함여부에 대한 검토 실시 ○ 용역사업에 투입되는 자료 · 장비 등에 대해 대외보안이 필요한 경우 보안의 범위 · 책임을 명확히 하기 위해 사업수행 계약서와 별도로 비밀유지계약서 작성 ○ 비밀유지계약서에는 비밀정보의 범위, 보안준수 사항, 위반시 손해배상 책임, 지적재산권 문제, 자료의 반환 등이 포함되도록 명시 ○ 용역사업 참여인원은 금융회사 또는 전자금융업자의 사전 동의 없이 용역업체가 임의로 교체할 수 없도록 명시 ○ 금융회사 또는 전자금융업자의 요구사항을 사업자에게 명확히 전달키 위하여 작성하는 과업지시서 · 계약서(입찰 공고 포함)에 인원 · 장비 · 자료 등에 대한 보안조치 사항과 정보유출 및 부정당업자에 대한 손해배상 내용 등을 정확히 기술 ○ 용역업체가 사업에 대한 하도급 계약을 체결할 경우 원래 사업계약 수준의 비밀 유지 조항을 포함토록 조치 ○ 규정 제7조 각호에 규정한 사항의 준수를 위하여 외부주문업체 등의 협조가 요구되는 사항
수행	[인력] ○ 용역사업 참여인원에 대해서는 '정보 유출' 방지 조항 및 개인의 자필 서명이 들어간 보안서약서 징구 ○ 용역사업 수행前 참여인원에 대해 법적 또는 금융회사 또는 전자금융업자의 규정에 따른 비밀유지 의무 준수 및 위반시 처벌내용 등에 대한 보안교육 실시 * 유출 금지 대상정보 및 정보 유출시 부정당업자 제재조치 등에 대한 교육 병행 ○ 금융회사 또는 전자금융업자는 사업 수행 중 업체 인력에 대한 보안점검 실시, '유출금지 대상정보' 외부 유출여부 확인 [자료] ○ 계약서 등에 명시한 중요정보를 업체에 제공할 경우 자료관리 대장을 작성, 인계자 · 인수자가 직접 서명한 후 제공하고 사업완료시 관련자료 회수 ○ 용역사업 관련자료 및 사업과정에서 생산된 모든 산출물은 금융회사 또는 전자금융업자의 파일서버에 저장하거나 금융회사 또는 전자금융업자가 지정한 PC에 저장 · 관리 ○ 용역사업 관련 자료는 인터넷 웹하드 · P2P 등 인터넷 자료공유사이트 및 개인메일함에 저장을 금지하고 금융회사 또는 전자금융업자와 용역업체간 전자우편을 이용해 전송이 필요한 경우에는 자체 전자우편을 이용하고, 첨부자료 중 중요정보 포함자료는 암호화 후 수발신

	○ 금융회사 또는 전자금융업자가 제공한 사무실에서 업체가 용역사업을 수행할 경우, 유출금지 대상 정보가 포함된 자료는 매일 퇴근시 시건장치가 된 보관함에 보관 ○ 용역사업 수행으로 생산되는 산출물 및 기록은 금융회사 또는 전자금융업자가 인가하지 않은 비인가자에게 제공·대여·열람을 금지 [사무실·장비] ○ 용역사업 수행장소는 금융회사 또는 전자금융업자 전산실 등 중요시설과 분리하고 CCTV·시건장치 등 비인가자의 출입통제 대책을 마련 ○ 용역업무를 수행하는 공간에 대한 보안점검을 정기적으로 실시 ○ 용역직원이 노트북 등 관련 장비를 외부에서 반입하여 내부망에 접속시 악성코드 감염여부 및 반출시마다 자료 무단반출 여부 확인 ○ 인가받지 않은 USB메모리 등의 휴대용 저장매체 사용을 금지하며 산출물 저장을 위하여 휴대용 저장매체가 필요한 경우 금융회사 또는 전자금융업자의 승인하에 사용 [내·외부망 접근시] ○ 금융회사 또는 전자금융업자는 개발시스템과 운영시스템을 분리하고, 용역업체는 업무상 필요한 서버에만 제한적 접근 허용 ○ 용역사업 수행시 금융회사 또는 전자금융업자 전산망 이용이 필요한 경우 -사업 참여인원에 대한 사용자계정(ID)은 하나의 그룹으로 등록하고 계정별로 정보시스템 접근권한을 차등 부여하되 허용되지 않은 금융회사 또는 전자금융업자의 내부문서 접근 금지 -계정별로 부여된 접속권한은 불필요시 즉시 해지하거나 계정을 폐기 -참여인원에게 부여한 계정은 별도로 기록 관리하고 수시로 해당 계정에 접속하여 저장된 자료와 작업이력 확인 -금융회사 또는 전자금융업자는 내부서버 및 네트워크 장비에 대한 접근기록 이상 여부를 정기 점검 ○ 용역업체에서 사용하는 PC는 인터넷 연결을 금지하되, 사업수행상 연결이 필요한 경우에는 금융회사 또는 전자금융업자의 보안통제하에 제한적 허용 ○ 용역업체 사용 전산망에서 P2P, 웹하드 등 인터넷 자료공유사이트로의 접속을 원천 차단
완료	○ 사업 완료 후 생산되는 최종 산출물 등 대외보안이 요구되는 자료는 대외비 이상으로 작성·관리하고 불필요한 자료는 삭제 및 폐기 ○ 용역업체에 제공한 자료, 장비와 중간·최종 산출물 등 용역과 관련된 제반자료는 전량 회수하고 업체에 복사본 등 별도 보관 금지 ○ 용역사업 완료 후 업체 소유 PC·서버의 하드디스크·휴대용 저장매체 등 전자기록 저장매체는 복원이 불가능한 방법으로 완전 삭제 후 반출 ○ 용역사업 관련자료 회수 및 삭제조치 후 업체에게 복사본 등 용역사업관련 자료를 보유하고 있지 않다는 대표자 명의의 확약서 징구

<별표 5-3> 중요 점검사항 <신설 2015.4.16, 개정 2015.9.17>

	점검 항목
1	이용자 정보의 조회·출력에 대한 통제 및 이용자 정보 조회시 사용자, 사용일시, 변경·조회내역, 접속방법 기록·관리
2	테스트시 이용자 정보 사용금지(부하 테스트 등 사용이 불가피한 경우 이용자 정보를 변환하여 사용하고 테스트 종료 즉시 삭제)
3	운영시스템 접속·사용 통제
4	내부통신망의 비인가 전산장비·무선통신 접속 통제(정보처리시스템을 이용한 통제장치 마련시 통제 장치에 대한 일일점검으로 대체 가능)
5	전산자료 및 전산장비 반출·반입 통제
6	전산실 등 출입자 관리기록부 기록·보관
7	인터넷(무선통신망 포함) 사용 통제(정보처리시스템을 이용한 통제 장치 마련시 통제장치에 대한 일일점검으로 대체 가능)
8	운영체제 및 악성코드 치료프로그램을 최신으로 유지
9	USB 등 보조기억매체 사용 통제
10	단말기에 이용자 정보 등 중요정보 보관 금지

<별표 6> 경영지도비율 산정기준

1. 자본적정성

$$\text{미상환잔액 대비 자기자본비율} = \frac{\text{자기자본}}{\text{미상환잔액}} \times 100$$

2. 자산건전성

$$\text{총자산 대비 투자위험성이 낮은 자산의 비율} = \frac{\text{투자 위험성이 낮은 자산}}{\text{총자산}} \times 100$$

※ 투자 위험성이 낮은 자산 : 규정 〈별표 6〉 참조

3. 유동성

$$\text{유동성비율} = \frac{\text{유동자산}}{\text{유동부채}} \times 100$$

<별표7> 망분리 대체 정보보호통제 <개정 2020. 11. 6., 2022. 12. 29.>

구분	통제 사항		
공통	○ 외부망에서 내부망으로 전송되는 전산자료를 대상으로 악성코드 감염여부 진단·치료 ○ 지능형 해킹(APT)차단 대책 수립·적용 ○ 전산자료 외부전송 시 정보유출 탐지·차단·사후 모니터링		
메일 시스템	○ 본문과 첨부파일 포함하여 메일을 통한 악성코드 감염 예방 대책 수립·적용 ○ 메일을 통한 정보유출 탐지·차단·사후 모니터링 대책 수립·적용		
업무용 단말기	○ 사용자의 관리자 권한 제거 ○ 승인된 프로그램만 설치·실행토록 대책 수립·적용 ○ 전산자료 저장 시 암호화		
연구·개발	○ 유해 사이트 차단 등 외부 인터넷 접근통제 대책 수립·적용 ○ 연구·개발망과 내부망간 독립적인 네트워크 구성 ○ 연구·개발 단말기 및 시스템에 대한 보호대책 수립·적용 및 중요정보(고유식별정보, 개인신용정보 등) 처리여부 모니터링 ○ 연구·개발망의 침해사고 예방 및 사고대응 대책 수립·적용 ○ 중요 소스코드 등에 대한 외부 반출방지 등 보안관리 대책 수립·적용		
원격 접속	외부 단말기	공통	○ 백신 프로그램 설치, 실시간 업데이트 및 검사 수행 ○ 안전한 운영체제 사용 및 최신 보안패치 적용 ○ 로그인 비밀번호 및 화면 보호기 설정 ○ 화면 및 출력물 등으로 인한 정보유출 방지대책 적용
		업무용 단말기를 경유하여 내부망에 접속하는 경우 (간접접속)	○ 외부 단말기와 업무용 단말기의 파일 송·수신 차단
		외부 단말기에서 내부망에 직접 접속하는 경우 (직접접속)	○ 인가되지 않은 S/W 설치 차단 ○ 보안 설정 임의 변경 차단 ○ USB 등 외부 저장장치 읽기/쓰기 차단 ○ 전산자료 (파일, 문서) 암호화 저장 ○ 단말기 분실 시 정보 유출 방지 대책적용 (하드디스크 암호화, CMOS비밀번호 적용 등)
	내부망 접근통제	○ 업무상 필수적인 IP, Port에 한하여 연결 허용 ○ 원격접속 기록 및 저장(예: 접속자 ID, 접속일자, 접속 시스템 등)	
	인증	○ 이중 인증 적용(예: ID/PW + OTP) ○ 일정 횟수(예 : 5회) 이상 인증 실패 시 접속 차단	
	통신 회선	○ 안전한 알고리즘으로 네트워크 구간 암호화 ○ 내부망 접속시 인터넷 연결 차단 (단, 직접 내부망으로 접속하는 외부 단말기는 인터넷 연결 상시 차단) ○ 원격 접속 후 일정 유휴시간 경과 시 네트워크 연결 차단	
	기타	○ 원격접속자에 대한 보안서약서 징구 ○ 공공장소에서 원격 접속 금지	

<별지 제1호 서식>

- 업무보고서 양식 및 기재사항(엑셀파일 참고) -

<별지 제2호 서식> <개정 2015.4.8>

작 성 자 :	(직 위)
전화번호 :	

정보기술부문 및 전자금융 사고보고서

문서번호 20 . . .

수 신

참 조

제 목 정보기술부문 및 전자금융 사고보고

전자금융감독규정 제73조에 따라 붙임과 같이 사고를 보고합니다.

붙 임 사고내용 1부. 끝.

○ ○ 금융회사 사장 (인)

<별첨1>

정보기술부문 및 전자금융 사고내용

보고형태	☐ 최초 ☐ 중간 ☐ 종결		
사고유형	IT보안사고	정보기술장애	전자금융사기사고
	☐ 전산자료/프로그램조작 ☐ 정보유출사고 ☐ 내부망 해킹 ☐ 시스템 위변조 ☐ DDoS 공격 ☐ 원인미정(파악중)	☐ 천재지변에 의한 장애 ☐ 시스템/설비 장애 ☐ 프로그램 오류 ☐ 인적 재해 ☐ 외부요인으로 인한 장애 ☐ 원인미정(파악중)	☐ 피싱/파밍(인터넷) ☐ 피싱/파밍(모바일) ☐ 피싱/파밍(텔레뱅킹) ☐ 전자상거래 위변조 ☐ 매체위변조 ☐ 신종 전자금융사기사고 ☐ 계약체결/거래지시 전송·처리 사고 ☐ 원인미정(파악중)
최초 인지	☐ 금융회사 ☐ 고객(민원인) ☐ 기타: ( )		
사고인지일시			
발생일시 및 지속시간			
발생 장소			
피해자 정보 및 피해금액	피해자 성명	생년월일	피해금액
배상금액		배상인원수	
사고내용			
사고원인			
파급영향			
처리결과			
대 책			

<선택 입력사항> 금융회사 공격자의 정보 제공

공격 유형	☐ DDoS ☐ 파밍악성코드 ☐ C&C서버 ☐ 기타
공격방법	
공격자IP	
공격자 MAC	
Domain정보	
상세내용	

<별첨2>

일괄보고서

보고연월	OO년 OO월			
보고형태	□ 최초			
사고유형	전자금융사기사고			
전체피해금액			전체피해인원수	
피해자별 사고내역	피해자명			
	세부 사고유형	□ 피싱/파밍(인터넷) □ 피싱/파밍(모바일) □ 피싱/파밍(텔레뱅킹) □ 전자상거래 위변조 □ 매체위변조 □ 신종 전자금융사기사고 □ 계약체결/거래지시 전송·처리 사고 □ 원인미정(파악중)		
	최초인지	□ 금융회사 □ 고객(민원인) □ 기타: ( )		
	사고인지일시			
	발생일지			
	종료일시			
	지속시간			
	발생장소			
	피해금액			
	배상금액			
	사고내용			
	사고원인			
	파급영향			
	처리결과			
	대 책			

<별지 제3호 서식> 자체 보안성심의 결과보고서 <신설 2015.9.17> <개정 2016.7.27>

작 성 자 :	(직 위)
전화번호 :	

자체 보안성심의 결과보고서(신규 전자금융서비스)

20 . . .

문서번호

수 신

참 조

제 목 자체 보안성심의 결과보고서

전자금융감독규정 제36조에 따라 붙임과 같이 자체 보안성심의 결과보고서를 제출합니다.

붙 임 자체 보안성심의 개요 1부.
자체 보안성심의 결과 1부. 끝.

OO 금융회사 대표이사 (인)

(붙임1)

자체 보안성심의 개요

1. 업무명 :

2. 업무적용일 : 20 년 월 일 완료

3. 업무개요

※ *서비스 목적, 대상 및 주요 내용을 기재*

4. 업무처리 절차

※ *가입절차, 이용절차 등을 기재*

5. 자체 보안성심의 결과

☐ 20 년 월 일 완료 ('붙임2. 자체 보안성심의 결과' 참조)

※ *자체 보안성심의 결과(자율양식)를 붙임2로 첨부*

6. 담당자

소 속	직 위	이 름	담당업무	연락처	e-mail

(붙임2)

자체 보안성심의 결과

※ *보안성심의 기준별 심의 결과 및 판단근거 등을 상세하게 기재*

<별지 제4호> <신설 2016.7.27>

작 성 자 :	(직위)
전화번호 :	

자체 보안성심의 결과보고서(공동 표준안)

20 . . .

문서번호

수 신

참 조

제 목 자체 보안성심의 결과보고서

전자금융감독규정 제36조에 따라 붙임과 같이 자체 보안성심의 결과보고서를 제출합니다.

붙 임 자체 보안성심의 개요 1부.
자체 보안성심의 결과 1부. 끝.

OO 금융회사 대표이사 (인)

(붙임1)

자체 보안성심의 개요

1. 표준명 :

2. 표준 제정일 : 20 년 월 일 제정

3. 개요

※ *참여 회사, 서비스 목적, 대상 및 주요 내용을 기재*

4. 업무처리 방안

※ *공동 표준안 관리 방안, 각 개별회사에 대한 적용 방안 등을 기재*

5. 자체 보안성심의 결과

□ 20 년 월 일 완료 ('붙임2. 자체 보안성심의 결과' 참조)

※ *자체 보안성심의 결과(자율양식)를 붙임2로 첨부*

6. 표준화 그룹 담당자

회사명[1]	직 위	이 름	담당업무	연락처	e-mail

1) 보안성심의 진행과 관련하여 대표자(또는 회사)가 있다면 회사명 앞에 별도 표기

(붙임2)

자체 보안성심의 결과

※ *보안성심의 기준별 심의 결과 및 판단근거 등을 상세하게 기재*

<별지 제5호 서식> <신설 2016.7.27>

전자금융 거래금액 기준 초과 신고서

문서번호 20 . . .

수 신

참 조

제 목 전자금융 거래금액 기준 초과 관련 신고서 제출

전자금융감독규정 제42조의2 제3항 및 동 시행세칙 제8조의3 제1항에 따라 붙임과 같이 전자금융 거래금액 기준을 초과한 사실을 신고합니다.

붙 임 전자금융 거래금액 기준 초과 내역 및 자본금 증액 계획 1부. 끝.

○ ○ ○ ○ 대표이사 (인)

(붙임)

전자금융 거래금액 기준 초과 내역 및 자본금 증액 계획

1. 거래금액 기준 초과 내역

(단위: 원)

	전전기	전기	당기
연도 및 분기[1]	*(예시) 2016년 4분기*	*(예시) 2017년 1분기*	*(예시) 2017년 2분기*
거래금액[2]	*(예시) 2,000,000,000*	*(예시) 4,000,000,000*	*(예시) 5,000,000,000*

[작성요령]

1) 연도 및 분기
- 당기 : 분기 거래총액이 2분기 연속 30억원을 초과한 경우의 두번째 분기
- 전기 : 분기 거래총액이 2분기 연속 30억원을 초과한 최초 분기
- 전전기 : '전기'의 전분기

2) 거래금액
- 전자지급결제대행 : 결제시(신용카드, 계좌이체, 가상계좌, 기타(상품권 등) 포함) 이용자가 지불한 재화나 용역의 가격을 말하며, 분기중 누적금액으로 작성
- 결제대금예치 : 이용자가 결제대금예치 서비스 제공업자와 거래한 총액으로서, 분기중 누적금액으로 작성
- 전자고지결제 : 이용자가 전자고지결제 서비스 제공업자와 거래한 총액으로서, 분기중 누적금액으로 작성

2. 자본금 증액 계획

(단위: 원)

	등록시 자본금[1]	변경 후 자본금[2]	자본금 변경 신고 예정일[2]
자본금	*(예시) 300,000,000*	*(예시) 1,000,000,000*	*(예시) 2017.12.31.*

[작성요령]

1) 전자지급결제대행에 관한 업무 : 3억원 이상
결제대금예치업 : 3억원 이상
전자고지결제업 : 3억원 이상
2) 전자지급결제대행에 관한 업무 : 10억원 이상
결제대금예치업 : 10억원 이상
전자고지결제업 : 5억원 이상

2) 자본금 변경 신고 예정일 : 거래금액이 2분기 연속 30억원을 초과한 시점부터 6월 이내에 금융감독원에 제출해야 함

<별지 제6호 서식> <개정 2022. 12. 29.>

작 성 자 : (직 위)
전화번호 :

클라우드컴퓨팅서비스 이용업무 지정/변경 보고

문서번호 20 . . .

수 신

참 조

제 목 클라우드컴퓨팅서비스 이용업무 지정/변경 보고

전자금융감독규정 **제14조의2 제4항**에 따라 붙임과 같이 클라우드컴퓨팅서비스 이용업무 지정/변경결과를 제출합니다.

붙 임 클라우드컴퓨팅서비스 이용업무 지정/변경 보고서 1부. 끝.

○ ○ ○ ○ 대표이사 (인)

(붙임)

클라우드컴퓨팅서비스 이용업무 지정/변경 보고서

1. 클라우드컴퓨팅서비스 이용정보

클라우드컴퓨팅서비스 제공자명	중요정보* 처리여부	시스템명 및 용도	계약체결일	서비스 개시일

* 고유식별정보, 개인신용정보

2. 클라우드컴퓨팅서비스 이용 관련 자체평가 결과

1) 「금융회사의 정보처리 업무위탁에 관한 규정」 제7조 제1항 각 호에 관한 서류 구비 적정성		
충족	부분충족	미충족
(O, X)	(O, X)	(O, X)
2) 클라우드컴퓨팅서비스 이용업무 중요도 평가 기준 및 평가결과		
충족	부분충족	미충족
(O, X)	(O, X)	(O, X)
3) 클라우드컴퓨팅서비스 제공자의 건전성 및 안전성 등에 대한 평가결과		
충족	부분충족	미충족
(O, X)	(O, X)	(O, X)
4) 클라우드컴퓨팅서비스 이용 관련 업무 연속성 계획 및 안전성 확보조치에 관한 사항		
충족	부분충족	미충족
(O, X)	(O, X)	(O, X)

5) 클라우드컴퓨팅서비스 이용대상 정보처리 시스템 중요도 평가결과, 클라우드컴퓨팅서비스 제공자의 건전성·안전성 등 평가결과, 업무연속성 계획 및 안전성 확보조치에 대한 정보보호위원회 심의·의결 결과				
일시				
안건				
심의내용				
심의결과				
심의위원	소속	직급	성명	비고

※ 금융회사 등은 상기 자체평가 결과에 대한 근거문서를 보유하여야 하고, 부분충족 및 미충족에 대해서는 보완대책을 마련·이행하여야 함

3. 클라우드컴퓨팅서비스 이용 책임자 정보

소속	직위	이름	담당업무	연락처	e-mail

첨부문서 :

1. 「금융회사의 정보처리 업무위탁에 관한 규정」 제7조 제1항 각 호에 관한 서류
2. 클라우드컴퓨팅서비스 이용업무 중요도 평가 기준 및 평가결과
3. 클라우드컴퓨팅서비스 제공자의 건전성 및 안전성 등에 대한 평가 결과
4. 클라우드컴퓨팅서비스 이용관련 업무 연속성 계획 및 안전성 확보조치에 관한 사항
5. 「전자금융감독규정」 제14조의2 제2항에 따른 정보보호위원회 심의·의결 결과(회의록 포함)
6. 「전자금융감독규정」 <별표 2의5>의 계약서 주요 기재사항을 포함한 클라우드컴퓨팅서비스 이용계약서
7. 「전자금융감독규정」 제14조의2 제4항 제2호 내지 제4호에 따른 보고의 경우 발생 사유, 관련 자료 및 대응계획

<별지 제7호 서식> <신설 2021.2.25.>

작 성 자 : (직 위)
전화번호 :

약관 제정(변경)보고

문서번호

발신일자

수 신 금융감독원장

참 조

「전자금융거래법」 제25조 제1항 및 「전자금융감독규정」 제41조 제2항, 제4항에 의거하여 ○○약관의 제정(변경)을 붙임과 같이 보고합니다.

붙 임 : 1. 약관 제정(변경) 보고서
2. 자체심사표

○ ○ ○ ○ 대표이사 (인)

(붙임1)

약관제정(변경)보고서

1. 약관(상품)명 :

2. 제정(변경)의 필요성 :

3. 주요 제정(변경)내용 :

4. 신구조문 대비표(변경의 경우) :

5. 시행(예정)일자(변경의 경우 서비스 개시일도 병기) :

6. 이용자에 대한 고지방법 및 고지시작시점(변경의 경우) :

7. 사후보고 근거 (「전자금융감독규정」 제41조 제1항 제2호의 경우에는 기보고된 동일·유사 약관명을 구체적으로 명시) :

8. 약관 본문 (전체) :

9. 자체심사표상 특이사항 :

10. 최근 5년간 약관의 변경이력

약관(상품)명	제정 · 변경일	변경내용 요약

11. 변경권고에 따른 약관 변경 여부 :

12. 기타 참고사항 :

(붙임2)

자체심사표(점검일자 : . . .)

약관(상품)명 :
확인자 : (직위) (성명) (서명 또는 인)
작성자 : (직위) (성명) (서명 또는 인) (전화번호)

점검항목	점검결과
1. 형식적 요건 점검	
①약관 제정·변경 보고 **서식**을 **준수**하였는가	
②약관 보고 **제출 기한**을 준수하였는가	
③**첨부서류**는 빠짐이 없는가	
④법규상 **사전보고(사후보고)** 대상에 해당하는가	
2. 실질적 요건 점검	
①**회사의 고의 또는 중과실**로 인한 **법률상 책임**을 **배제**하고 있지 않은가	
②상당한 이유 없이 회사의 **손해배상범위**를 **제한**하거나 회사가 부담하여야 할 **위험**을 고객에게 **전가**시키는 조항은 없는가	
③고객에 대하여 **부당하게 과중한 손해배상의무**를 부담시키는 조항은 없는가	
④**이용자**의 **해제권 및 해지권**을 **배제**하거나 그 행사를 제한하는 조항은 없는가	
⑤**회사에게** 법률에서 규정하고 있지 아니하는 **해제권·해지권**을 **부여**하거나 법률의 규정에 의한 해제권·해지권의 행사요건을 완화하여 이용자에 대하여 부당하게 불이익을 주는 조항은 없는가	
⑥상당한 이유 없이 회사가 이행하여야 할 **급부**나 이용자의 **채무내용** 등을 회사가 **일방적으로 결정·변경**할 수 있도록 권한을 부여하는 조항은 없는가	
⑦이용자의 **항변권, 철회권** 등의 권리를 상당한 이유없이 배제 또는 제한하는 조항은 없는가	
⑧이용자에게 부여된 **기한의 이익**을 상당한 이유 없이 상실케 하는 조항은 없는가	
⑨이용자의 **제3자와의 계약 체결을 부당하게 제한**하는 조항은 없는가	
⑩회사와 이용자의 **의사표시와 관련한 부당한 의제**를 통하여 이용자에게 부당하게 불이익을 주는 조항은 없는가	
⑪그외 「약관의 규제에 관한 법률」에서 정한 사항에 위배되는 조항은 없는가	
⑫**모호한 표현**을 사용하여 약관의 자의적 해석 및 불필요한 **분쟁**을 야기할 **소지**는 없는가	
⑬**계약조건** 등 **설명·표시의**무가 필요한 **중요 기재사항**이 누락되지는 않았는가	
⑭특정금융상품으로 **오인**될 소지가 있는 **문구** 또는 **상품명**을 사용하고 있지 않은가	
⑮이용자와 회사간 소송이 제기될 경우 **관할 법원** 조항이 민사소송법 규정 등과 달리 이용자에게 불리하지는 않는가	
⑯**법규상 약관에 포함되어야 할 사항**이 누락되지는 않았는가	
⑰선불전자지급수단을 발행한 경우 이용자의 **선불전자지급수단**에 기록된 잔액의 **환급받을 권리**를 제한하고 있지 않은가	