

## ◎ 금융위원회 공고 제2016-206호

「전자금융감독규정」을 일부 개정함에 있어 개정 이유와 주요 내용을 국민에게 미리 알려, 이에 대한 의견을 듣고자 행정절차법 제41조에 따라 다음과 같이 「전자금융감독규정 일부개정규정안」을 공고합니다.

2016년 6월 30일

금융위원회

### 「전자금융감독규정 일부개정규정안」 규정변경 예고

#### 1. 개정 이유

클라우드 등 새로운 IT 기술 확산 및 핀테크 산업 발전 등 변화된 현실에 맞게 관련 규제를 합리적으로 개선하고 그 밖의 일부 제도개선 사항 등을 규정에 반영하고자 하는 것임

#### 2. 주요내용

가. 금융권의 클라우드 이용 활성화를 위해 금융회사 등이 고객 정보 처리시스템을 제외한 전산시스템 중 일부를 클라우드를 활용하는 시스템으로 자율적으로 지정할 수 있도록 하고,

지정된 시스템에 대해서는 물리적 망분리 등 클라우드 활용을 불가능하게 하는 규제 적용 제외 (안 제7조의2)

나. 전용회선을 사용한 정보보호시스템의 원격관리 허용 등 기존과 동등한 수준의 새로운 보안 기술 적용을 허용 (안 제15조, 제60조)

다. 전자금융사고 발생 시 피해자에게 적절한 수준의 보상이 이루어 질 수 있도록, 카드정보저장 전자금융업자의 책임보험가입 기준 금액 등을 상향 (안 제5조)

라. 전자금융사고 발생시 피해보상이 신속하게 이루어 질 수 있도록, 금융회사등이 적립하는 준비금의 관리·지급 관련 절차 마련을 의무화 (안 제5조)

마. 대규모 고정자산을 보유한 겸업 전자금융업자 등에게 과도한 규제로 작용해 온 현행 안전자산 보유 기준\*을 “총자산대비 10%의 안전자산 보유” 또는 “미정산 잔액 대비 100%의 안전 자산 보유”로 개선 (안 제63조)

\* “총자산대비 10%의 안전자산 보유”만 기준으로 규정

바. 금융권 통합 보안관제센터 운영 등 금융권 사이버보안 강화를 위한 침해사고 대응기관의 역할 명확화 (안 제37조)

### 3. 의견제출

이 법률 개정안에 대하여 의견이 있는 단체 또는 개인은 2016년 8월 9일까지 다음 사항을 기재한 의견서를 금융위원회(참조 : 전자금융과, 전화 : 02-2100-2975, 팩스 : 02-2100-2946, 이메일 : crisis@korea.kr)로 제출하여 주시기 바랍니다.

가. 입법예고사항에 대한 의견

(찬성 또는 반대 의견과 그 사유 및 기타 참고사항)

나. 성명(단체의 경우 단체명과 대표자명), 주소 및 전화번호

다. 보내실 곳 : 금융위원회 전자금융과

(주소 : 03171 서울특별시 종로구 세종대로 209 정부서울청사)

※ 자세한 사항은 금융위원회 홈페이지([www.fsc.go.kr](http://www.fsc.go.kr)/법령정보/규정변경예고)를 참고하시기 바랍니다.

## 전자금융감독규정 일부개정규정안

전자금융감독규정 일부를 다음과 같이 개정한다.

제5조제1항제6호를 제7호로 하고, 같은 항에 제6호를 다음과 같이 신설한다.

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

제5조제1항제7호(중전의 제6호) 중 “제5호”를 “제5호, 제6호”로 하고, 같은 조 제2항 중 “보유하여야”를 “보유하고 책임이행이 신속히 이루어 질 수 있도록 준비금 관리 및 지급에 관한 내부 절차를 수립하여 운영하여야”로 한다.

제3장제1절에 제7조의2를 다음과 같이 신설한다.

제7조의2(비중요 정보처리시스템 지정) ① 금융회사 또는 전자금융업자는 자체적으로 수립한 정보자산 중요도 평가기준에 따라 전자금융거래의 안전성 및 신뢰성에 미치는 영향이 현저히 낮은 정보처리시스템을 비중요 정보처리시스템으로 지정할 수 있다. 다만, 개인의 고유식별정보 또는 「신용정보의 이용 및 보호에 관한 법률」에 따른 개인신용정보를 처리하는 정보처리시스템은 비중요 정보처리시스템으로 지정할 수 없다.

② 금융회사 또는 전자금융업자는 제1항에 따라 비중요 정보처리시스템 지정시 제8조의2에 따른 정보보호위원회의 심의·의결을 거쳐야 한다.

③ 금융회사 또는 전자금융업자는 제1항에 따라 비중요 정보처리시스템을 지정한 날로부터 7일 이내에 금융감독원장이 정하는 양식에 따라 정보자산 중요도 평가기준, 지정 결과, 관리 방안 등을 포함한 보고서를 금융감독원에 제출하여야 한다.

④ 금융감독원장은 제3항에 따라 제출한 보고서를 검토한 결과, 평가기준, 지정 결과, 관리 방안 등이 적합하지 않다고 판단되는 경우에는 금융회사 또는 전자금융업자에 대하여 개선·보완을 요구할 수 있다.

⑤ 제1항의 비중요 정보처리시스템만 위치한 전산실에 대해서는 제11조제11호 및 제12호, 제15조제1항제5호를 적용하지 아니한다.

제8조제3항에 단서를 다음과 같이 신설한다.

다만, 허가, 등록 또는 인가를 마친 후 1년이 지나지 않은 금융회사 또는 전자금융업자는 공시하지 아니할 수 있다.

제13조제1항제10호 중 “부하 테스트 등”을 “법인인 이용자 정보는 금융감독원장이 정하는 바에 따라 이용자의 동의를 얻은 경우 사용 가능하며, 그 외 부하 테스트 등 이용자 정보의”로 한다.

제15조제2항제4호를 다음과 같이 한다.

4. 정보보호시스템 원격관리 금지. 다만, 원격관리가 불가피한 경우 전용회선(또는 전용회선과 동등한 보안수준을 갖춘 가상의 전용회선) 사용, 접근통제 등을 포함한 원격 접속 보안 대책을 수립·운영할 것

제15조제2항제5호를 제6호로 하고, 같은 항에 제5호를 다음과 같이 신설한다.

5. 정보보호시스템의 작동 상태를 주기적으로 점검할 것

제23조제1항 각 호 외의 부분 중 “수립하여야”를 “수립·준수하여야”로 하고, 같은 조 제4항 중 “수립”을 “수립·준수”로 하며, 같은 조 제5항 중 “수립하여야”를 “수립·운영하여야”로 한다.

제37조의4제2항에 제4호를 다음과 같이 신설한다.

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

제37조의4제4항 중 “제3항”을 “제2항에 따른 침해사고 긴급대응을 위한 침해사고대응기관의 업무 수행 또는 제3항”으로 하고, 같은 조 제5항 각 호 외의 부분 전단 중 “결과”를 “계획 및 결과”로 하며, 같은 조에 제7항을 다음과 같이 신설한다.

⑦ 금융위원장은 침해사고대응기관의 장으로 하여금 시행령 제11조의 6제1항제4호에 따른 보안취약점 통보를 위하여 금융회사 및 전자금융업자가 사용하고 있는 소프트웨어에 대한 조사·분석을 실시하게 할 수 있다.

제60조제1항제5호 중 “전용회선”을 “전용회선(또는 전용회선과 동등한 보안수준을 갖춘 가상의 전용회선)”으로 한다.

제63조제1항제4호 본문 중 “유지”를 “유지하거나 미상환 잔액 대비 투자 위험성이 낮은 자산의 비율을 100분의 100이상으로 유지”로 한다.

## 부 칙

제1조(시행일) 이 규정은 고시한 날부터 시행한다. 다만, 제5조제1항제 6호 및 제5조제2항의 개정규정은 이 규정 고시 후 6개월이 경과한 날부터 시행한다.

제2조(인력, 조직 및 예산 기준 미준수 공시에 관한 적용례) 제8조제3항의 개정규정은 이 규정 시행 전에 허가, 등록 또는 인가를 마친 금융회사 또는 전자금융업자에 대하여도 적용한다.

## 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. 1. ~ 5. (생략) <u>&lt;신설&gt;</u>	제5조(전자금융사고 책임이행을 위한 보험 등의 가입에 관한 기준) ① ----- ----- ----- ----- -----.
6. 제5호 이외의 전자금융업자 : 1억원	1. ~ 5. (현행과 같음)
② 금융회사 또는 전자금융업자가 전자금융사고 책임이행을 위한 준비금을 적립하는 경우에는 제1항 각 호에서 정한 금액 이상의 금액을 <u>보유하여야</u> 한다.	6. 법 제28조제2항제4호의 전자금융업자 중 제1호 또는 제2호에 속하는 금융회사가 발급한 신용카드, 직불카드 등 거래지시에 사용되는 접근매체의 정보를 저장하는 전자금융업자 : 10억원
	7. 제5호, 제6호 ----- -----
	② ----- ----- ----- ----- ----- 보유하고 책임이행이 신속히 이루어 질 수 있도록 준비금 관리 및 지급에 관한



③ · ④ (생략)

<신설>

내부 절차를 수립하여 운영하여야 --.

③ · ④ (현행과 같음)

제7조의2(비중요 정보처리시스템 지정) ① 금융회사 또는 전자금융업자는 자체적으로 수립한 정보자산 중요도 평가기준에 따라 전자금융거래의 안전성 및 신뢰성에 미치는 영향이 현저히 낮은 정보처리시스템을 비중요 정보처리시스템으로 지정할 수 있다. 다만, 개인의 고유식별정보 또는 「신용정보의 이용 및 보호에 관한 법률」에 따른 개인 신용정보를 처리하는 정보처리시스템은 비중요 정보처리시스템으로 지정할 수 없다.

② 금융회사 또는 전자금융업자는 제1항에 따라 비중요 정보처리시스템 지정시 제8조의2에 따른 정보보호위원회의 심의·의결을 거쳐야 한다.

③ 금융회사 또는 전자금융업자는 제1항에 따라 비중요 정보처리시스템을 지정한 날로부터 7일 이내에 금융감독원장이 정하는 양식에 따라 정보자산 중요

제8조(인력, 조직 및 예산) ① · ②  
(생략)

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. <단서 신설>

도 평가기준, 지정 결과, 관리 방안 등을 포함한 보고서를 금융감독원에 제출하여야 한다.

④ 금융감독원장은 제3항에 따라 제출한 보고서를 검토한 결과, 평가 기준, 지정 결과, 관리 방안 등이 적합하지 않다고 판단되는 경우에는 금융회사 또는 전자금융업자에 대하여 개선·보완을 요구할 수 있다.

⑤ 제1항의 비중요 정보처리시스템만 위치한 전산실에 대해서는 제11조제11호 및 제12호, 제15조제1항제5호를 적용하지 아니한다.

제8조(인력, 조직 및 예산) ① · ②  
(현행과 같음)

③ -----  
-----  
-----  
-----  
-----  
-----  
-----  
-----  
-----  
-----  
- 다만, 허가, 등록 또는 인가를 마친 후 1년이 지나지 않은

<p>④ (생 략)</p> <p>제13조(전산자료 보호대책) ① 금융회사 또는 전자금융업자는 전산자료의 유출, 파괴 등을 방지하기 위하여 다음 각 호를 포함한 전산자료 보호대책을 수립·운용하여야 한다.</p> <p>1. ~ 9. (생 략)</p> <p>10. 이용자 정보의 조회·출력에 대한 통제를 하고 테스트 시 이용자 정보 사용 금지(다만, 부하 테스트 등 사용이 불가피한 경우 이용자 정보를 변환하여 사용하고 테스트 종료 즉시 삭제하여야 한다)</p> <p>11. ~ 14. (생 략)</p> <p>② ~ ⑤ (생 략)</p> <p>제15조(해킹 등 방지대책) ① (생 략)</p> <p>② 제1항제1호의 규정에 따른 정보보호시스템을 설치·운영하는 경우에는 다음 각 호의 사항을 준수하여야 한다.</p> <p>1. ~ 3. (생 략)</p>	<p><u>금융회사 또는 전자금융업자는 공시하지 아니할 수 있다.</u></p> <p>④ (현행과 같음)</p> <p>제13조(전산자료 보호대책) ① -- ----- ----- ----- ----- -----.</p> <p>1. ~ 9. (현행과 같음)</p> <p>10. ----- ----- ----- <u>법인인 이용자 정보는 금융감독원장이 정하는 바에 따라 이용자의 동의를 얻은 경우 사용 가능하며, 그 외 부하 테스트 등 이용자 정보의 --</u></p> <p>11. ~ 14. (현행과 같음)</p> <p>② ~ ⑤ (현행과 같음)</p> <p>제15조(해킹 등 방지대책) ① (현행과 같음)</p> <p>② ----- ----- ----- -----.</p> <p>1. ~ 3. (현행과 같음)</p>
---	---

4. 정보보호시스템의 원격관리를 금지하고 주기적으로 작동 상태를 점검할 것

<신 설>

5. (생략)

③ ~ ⑥ (생략)

제23조(비상대책 등의 수립·운영) ① 금융회사 또는 전자금융업자는 장애·재해·파업·테러 등 긴급한 상황이 발생하더라도 업무가 중단되지 않도록 다음 각 호의 내용을 포함한 업무지속성 확보방안을 수립하여야 한다.

1. ~ 7. (생략)

②·③ (생략)

④ 「국가위기관리기본지침」에 따라 금융위원회가 지정한 금융회사는 금융위원회의 「금융전산분야위기대응실무매뉴얼」에 따라 위기대응행동매뉴

4. 정보보호시스템 원격관리 금지. 다만, 원격관리가 불가피한 경우 전용회선(또는 전용회선과 동등한 보안수준을 갖춘 가상의 전용회선) 사용, 접근통제 등을 포함한 원격 접속 보안 대책을 수립·운영할 것

5. 정보보호시스템의 작동 상태를 주기적으로 점검할 것

6. (현행 제5호와 같음)

③ ~ ⑥ (현행과 같음)

제23조(비상대책 등의 수립·운영) ① -----  
-----  
-----  
-----  
----- 수립·준수하여야 --.

1. ~ 7. (현행과 같음)

②·③ (현행과 같음)

④ -----  
-----  
-----  
-----  
-----

얼(이하 "행동매뉴얼"이라 한다)을 수립하고 이를 금융위원회에 알려야 한다.

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 수립하여야 한다.

⑥ ~ ⑩ (생략)

제37조의4(침해사고대응기관 지정 및 업무범위 등) ① (생략)

② 침해사고대응기관은 다음 각 호의 업무를 수행한다.

1. ~ 3. (생략)

<신설>

③ (생략)

④ 금융위원장은 제3항에 따른 침해사고 원인분석 및 긴급조치를 위하여 금융회사 및 전자금

수립·준수

⑤

⑥ ~ ⑩ (현행과 같음)

제37조의4(침해사고대응기관 지정 및 업무범위 등) ① (현행과 같음)

②

1. ~ 3. (현행과 같음)

4. 금융회사 및 전자금융업자와 관련된 해킹 등 전자적 침해 행위 정보를 탐지·분석하여 즉시 대응 조치를 하기 위한 기구(이하 "금융권 통합 보안 관제센터"라 한다)의 운영

③ (현행과 같음)

④ 제2항에 따른 침해사고 긴급대응을 위한 침해사고대응기관의 업무 수행

업자, 전자금융보조업자에 협조를 요청할 수 있다.

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

1. ~ 4. (생략)

⑥ (생략)

<신설>

제60조(외부주문등에 대한 기준)

① 금융회사 또는 전자금융업자는 전자금융거래를 위한 외부주문등의 경우에는 다음 각 호의 사항을 준수하여야 한다.

1. ~ 4. (생략)

또는 제3항-----  
-----.

⑤ -----  
-----  
-----  
-----  
----- 계획  
및 결과-----  
-----.  
-----.

1. ~ 4. (현행과 같음)

⑥ (현행과 같음)

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

제60조(외부주문등에 대한 기준)

① -----  
-----  
-----  
-----.

1. ~ 4. (현행과 같음)

<p>5. 금융회사와 전자금융보조업자 간의 접속은 <u>전용회선</u>을 사용</p> <p>6. ~ 14. (생략)</p> <p>② ~ ④ (생략)</p> <p>제63조(전자금융업자 경영지도기준) ① 법 제42조제2항에 따른 구체적인 경영지도기준은 다음과 같다.</p> <p>1. ~ 3. (생략)</p> <p>4. 총자산 대비 투자위험성이 낮은 자산의 비율은 100분의 10 이상으로 <u>유지</u>할 것. 단, 법 제28조제1항의 규정에 따라 허가를 받은 전자금융업자 및 법 제28조제2항제3호의 규정에 따라 등록을 한 전자금융업자는 제외한다. 이 때 투자위험성이 낮은 자산은 &lt;별표 6&gt;와 같다.</p> <p>5. (생략)</p> <p>② · ③ (생략)</p>	<p>5. ----- ----- <u>전용회선</u>(또는 <u>전용회선과 동등한 보안수준을 갖춘 가상의 전용회선</u>)- -</p> <p>6. ~ 14. (현행과 같음)</p> <p>② ~ ④ (현행과 같음)</p> <p>제63조(전자금융업자 경영지도기준) ① ----- ----- -----.</p> <p>1. ~ 3. (현행과 같음)</p> <p>4. ----- ----- ----- <u>유지하거나 미상환 잔액 대비 투자위험성이 낮은 자산의 비율을 100분의 100이상으로 유지</u>-. ----- ----- -----.</p> <p>5. (현행과 같음)</p> <p>② · ③ (현행과 같음)</p>
--	--