

보도시점 2024. 2. 2.(금) 조간 배포 2024. 2. 1.(목) 9:00

## 「전자금융감독규정」 개정안 규정변경 예고 ('24.2.1. ~ '24.3.12.)

◆ 금융보안 규제를 ①원칙중심으로 개선(수범사항 293개 → 166개)하고 ② 금융전산 복원력을 강화하여 재해·전자적 침해 등으로부터 금융시스템을 안정적으로 보호하는 내용을 담은 「전자금융감독규정」 개정안에 대한 규정변경을 예고

2.1일(목), 금융위원회는 금융보안 규제를 “규칙(Rule) → 원칙(Principle) 중심”으로 개선하여 금융권의 자율보안 토대를 마련하고, 금융전산 복원력을 강화하여 재해·전자적 침해 등으로부터 금융시스템을 안정적으로 보호하는 등의 내용을 담은 「전자금융감독규정」 개정안에 대한 규정변경을 예고 하였다('24.2.1. ~ '24.3.12.)

전자금융감독규정은 '06년 제정된 미시적 행위규칙(Rule) 중심의 금융보안 규제를 현재까지 큰 틀에서 유지하고 있어, 상황별 유연한 보안대응을 곤란<sup>1)</sup>하게 하고 금융회사의 소극적 행태<sup>2)</sup>를 초래한다는 지적이 있어 왔다. 특히, AI, 클라우드 등 기술변화 및 고도화되는 사이버 위협 등에 효과적으로 대응하기 위해 금융보안체계의 유연성 제고와 회복력 강화에 중점을 둔 제도개선의 필요성이 제기되어 왔다. 이에, 금융보안규제를 목표·원칙 중심으로 합리화하여 금융회사의 자율적 판단영역을 확대하고 적극적 보안투자를 이끌어 내기 위해 전자금융감독규정 개정안을 마련하였다.

\* 1) 감독규정상 보안방법 등을 특정함에 따라 자율적으로 동일 목적을 달성하거나 보안을 강화할 수 있는 他 방법에 대한 가능성을 차단

2) 규정상 의무만 준수하면 모든 보안책임을 다한 것이라는 인식 등

우선, 금융회사 스스로 새로운 리스크에 유연하게 대응해 나갈 수 있도록 293개에 달하는 세세한 행위규칙(Rule)을 166개로 획기적으로 줄였다. 규정 형식도 사전통제적·열거적 형식을 지양하고 원칙과 목적을 제시하는 방향으로 개선하였고, 나머지 세세한 부분은 금융회사가 스스로 결정할 수 있도록 하였다. 대표적으로, 사용자 비밀번호 설정 방식\*을 구체적으로 특정하던 규정을 삭제하고 금융회사 스스로 안전하다고 판단되는 비밀번호 및 인증수단 관리방식을 도입할 수 있도록 허용하였다. 또한, 건물·설비·전산실 관리 및 각종 내부통제·사업운영 등과 관련하여서도 금융회사의 자율성을 대폭 확대하였다. (주요 사례 : 참고2)

\* 例 : (현행) '주민등록번호, 동일숫자, 연속숫자 등 제3자가 쉽게 유추할 수 있는 비밀번호의 등록 불가' 등 세부규칙 존재

→ (개선) 제3자가 쉽게 유추할 수 없는 비밀번호 작성규칙 및 등록·변경 절차를 수립·운영할 것

한편, '22년 카카오 데이터센터 화재 이후, 재해·전자적 침해 등으로부터 금융전산 복원력(Cyber Resilience) 강화와 신속한 소비자 피해구제 필요성 등이 증대되었다. 이에, 그간 규제 사각지대에 있던 일부 중소금융사 및 전자금융업자 등에 대한 재해복구센터 설치 및 업무복구 목표시간 설정 등이 의무화된다. 동시에, 최고경영자, 이사회 등의 금융보안 의사결정 참여도를 높여 금융권 전반의 금융보안 거버넌스를 두텁게하고, 소비자 피해 구제에 만전을 기할 수 있도록 전자금융사고시 책임이행보험의 한도 등도 함께 상향한다.

이 외, 상기 설명한 규제완화·규제강화에 포함되지 않은 현행유지 규정도 세부적·지엽적 내용은 가능한 범위내에서 최대한 원칙중심으로 합리화하여 금융회사 등의 규제부담을 경감하고자 한다. 또한, 법률개정이 필요한 사항은 국회와 긴밀히 협의하여 향후 전자금융거래법 개정을 통해 금융회사 등의 자율보안체계로의 전환을 뒷받침하고자 한다.

금번 전자금융감독규정 개정안에 대해서는 '24.2.1일(목)부터 '24.3.12일(화)까지 규정변경을 예고하게 되며, 이후 금융위원회 의결 등의 절차를 거쳐 공고시부터 시행될 예정이다. 다만, 재해복구센터 설치 등 일부 조항에 대해서는 금융회사의 준비기간 등을 감안하여 시행시점을 일정기간 유예하는 등의 경과규정을 마련할 예정이다.

### 〈 규정변경예고 관련 안내사항 〉

- 예고기간 : 2024.2.1일(목) ~ 2024.3.12일(화), (40일)
  - 규정변경예고된 내용에 대해 의견이 있으시면 다음 사항을 기재한 의견서를 아래의 제출처로 제출해 주시기 바랍니다.
    - 예고 사항에 대한 찬성 또는 반대 의견(반대의 경우 이유 명시)
    - 성명(기관·단체의 경우 기관·단체명과 대표자명), 주소·전화번호
- 일반우편 : 서울시 종로구 세종대로 209 정부서울청사 금융위원회 금융안전과
  - 전자우편 : han3320@korea.kr      - 팩스 : 02-2100-2946

※ 개정안 전문(全文)은 “금융위 홈페이지([www.fsc.go.kr](http://www.fsc.go.kr)) > 정책마당 > 법령정보 > 입법예고/규정변경예고”에서 확인 가능합니다.

※ 전자금융 감독규정 규정변경예고 관련 자세한 내용은 별첨 자료를 참고해 주시기 바랍니다.

별첨. 전자금융 감독규정 정비 계획

담당 부서 <총괄>	금융위원회 금융안전과	책임자	과 장	김수호 (02-2100-2970)
		담당자	사무관 사무관	박석훈 (02-2100-2811) 장희진 (02-2100-2979)
<공동>	금융감독원 금융IT안전국	책임자	국 장	백규정 (02-3145-7120)
		담당자	팀 장	이성욱 (02-3145-7125)

## 참고1

## 전자금융 감독규정 정비 개요

- 293개 수범사항 (§8~§37) 중 ① 삭제 134건, ② 강화 5건,  
③ 현행유지 114건, ④ 조정·합리화 45건 : 293개→ 166개로 축소

- ① ‘삭제’는 총 134건으로 29건은 시행세칙에 규정, 그 밖에 규정은 폐지·통합 하거나 해설서로 설명

\* 시행세칙은 위임법령과 결합하여 대외적 구속력을 가지나, 해설서는 시행세칙 등의 이해를 위한 설명자료에 해당(미준수시에도 제재 등 X)

- i)내용이 지나치게 지엽적·미시적이거나, ii)유사 입법례 대비 과도한 규정의 경우, iii)금융회사의 자율성이 존중되어야 하는 경우, iv)과거 제재사례가 드문 경우 등은 원칙적으로 삭제

- ② ‘강화’는 총 5건으로 재해복구센터 확충, 사고시 이용자 보호체계 강화, 보안거버넌스 개선 등에 중점

\* 카카오 데이터센터 화재('22.10월) 등 관련 사이버복원력 및 피해보상 강화 목적

- ③ ‘현행 유지’는 총 114건으로, 정보보안·해킹방지 등 금융보안 핵심내용을 유지하고, 운영복원력·제3자 리스크 관리 강화 등 글로벌 추세 등을 감안하여 꼭 필요한 내용을 존치

\* 현행유지 규정의 경우도 세부적·지엽적 내용은 최대한 원칙중심으로 합리화

- ④ 기타 규정 조정·합리화는 총 45건

### < 전자금융 감독규정 정비 검토 결과 >

구분	삭제	유지	조정· 합리화	강화	소계	
					현행	개선
(2절) 인력·조직·예산	5	14	3(신설2)	1	22	19
(3절) 시설	13	0	2	0	15	2
(4절) 정보기술	54	40	25(신설2)	1	119	67
(5절) 내부통제	56	46	13(신설3)	3	115	62
(6절) 전자금융업무	6	14	2	0	22	16
총 계	134	114	45(신설7)	5	293	166

## [1] 건물(§ 9), 설비(§ 10), 전산실(§ 11) 관련

□ (주요내용) 건물·설비·전산실 등 관리·보호를 위한 규정

\* 예 : 경비원에 의한 통제(건물), 자물쇠 설치(설비), 항온·항습기 구비(전산실)

⇒ (검토결과) ① 자율에 맡겨도 충분한 지엽적·상식적 내용이 많고, ② 규정위반으로 인한 제재사례가 거의 없는 점\* 등을 감안,

\* 건물(§9), 설비(§10)는 제재사례가 없고, 전산실(§11)은 과거 1건에 불과

→ 감독규정에는 원칙만 남기고 세부내용(각 호)은 삭제

※ 필수 조항(재해복구센터 국내 설치의무 등)만 남기고 해설서(전산실 출입기록 등)로 전환

### [건물에 관한 사항(§9)]

▪ (현행) 출입구 경비원 통제, 비상계단 및 정전대비 유도등 설치, 피뢰설비 등  
→(개선) 원칙중심으로 규정화(출입·보안대책 수립·운용), 각 호(1~6호)는 삭제

### [전원·공조 등 설비에 관한 사항(§10)]

▪ (현행) 자물쇠 설치, 자가발전 설비, 무정전 전원장치 등  
→(개선) 원칙중심으로 규정화(안전성 기준을 수립·준수), 각 호(1~7호)는 삭제

### [전산실 등에 관한 사항(§11)]

▪ (현행) CCTV설치, 출입문 이중 안전장치, 이중바닥설치, 항온계·항습계 등  
→(개선) 원칙중심으로 규정화하되, 상세 내용은 해설서로 안내

## [2] 악성코드(§ 16) 및 공개형 웹서버 관리대책(§ 17) 관련

□ (주요내용) 악성코드 감염방지를 위한 진단·치료·복구절차 및 공개형 웹서버(홈페이지 등) 접근·통제 방안 등을 규정

⇒ (검토결과) 다른 규정(제15조 해킹방지 등)과 중복되는 내용은 통합하고, 유사 입법례를 참조하여 지나치게 구체적인 규율은 삭제하고 원칙중심으로 합리화하여 자율보안 시행

### [ 악성코드 (§16) ]

- (현행) 금융회사 또는 전자금융업자는 악성코드 감염을 방지하기 위하여 다음 각 호를 포함한 대책을 수립·운용하여야 한다.

→(개선) 금융회사 또는 전자금융업자는 악성코드 감염 방지, 확산, 피해 최소화 및 복구를 위한 대책을 수립·준수하여야 한다. (각 호 삭제 또는 통합)

❖ (관련 법령) 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시 별표 7 나. 보호대책 요구사항, 2.10.9 악성코드 통제  
바이러스·웜·트로이목마·랜섬웨어 등의 악성코드로부터 개인정보 및 중요정보, 정보시스템 및 업무용 단말기 등을 보호하기 위하여 악성코드 예방·탐지·대응 등의 보호대책을 수립·이행하여야 한다.

### [ 공개형 웹서버 (§17) ]

- (현행) 금융회사 또는 전자금융업자는 공개용 웹서버에 게재된 내용에 대하여 다음 각 호의 사항을 준수하여야 한다.

→(개선) 금융회사 또는 전자금융업자는 공개용 웹서버에 자료 게시 절차·내용에 관한 내부통제 방안과 개인정보 유출 및 위·변조를 방지하기 위한 보안조치 방안을 수립·운용하여야 한다. (각 호 삭제 또는 통합)

❖ (관련 법령) 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시 별표 7 나. 보호대책 요구사항, 2.10. 시스템 및 서비스 보안관리, 2.10.3 공개서버 보안  
외부 네트워크에 공개되는 서버의 경우 내부 네트워크와 분리하고 취약점 점검, 접근 통제, 인증, 정보 수집·저장·공개 절차 등 강화된 보호대책을 수립·이행하여야 한다.

## [3] 직무분리 세부규정(§ 26) 관련

- (주요내용) 권한·책임을 명확화하여 권한 오·남용을 방지하고 잠재적인 피해를 예방하기 위해 직무간 분리를 규정

### [ 직무분리 각 호 규정(예시) ]

- 프로그래머와 오퍼레이터 간 직무 분리
- 응용프로그래머 ⇔ 시스템프로그래머 간 직무분리
- 시스템보안관리자 ⇔ 시스템프로그래머 간 직무분리
- 전산자료관리자 ⇔ 그 밖의 업무담당자 간 직무분리
- 업무운영자 ⇔ 내부감사자 간 직무분리

⇒ (검토결과) ① 타 입법례\* 대비 규정이 지나치게 세분화되어 있고,  
② 직무용어에 대한 해석상 혼선이 가능하다는 점 등을 감안하여

→ 내부통제 직무분리 원칙만 남기고 각 호는 삭제

\* (정보보호고시 별표 7) 권한 오남용 등으로 인한 잠재적인 피해 예방을 위하여 직무분리기준을 수립하고 적용하여야 한다.

#### **[4] 사업추진(§ 20), 계약(§ 21), 감리(§ 22) 관련**

- (주요내용) IT시스템 사업추진, 계약 및 감리 관련 사업 타당성, 계약의 공정성 등을 확보하기 위한 규정

\* 예 : 사업 타당성 및 비용-효과분석, IT계약시 업체선정 기준·절차 및 공정가격 기준 마련, 감리 기준 등

- ⇒ (검토결과) ① 자율적 판단이 특히 요구되는 경영·운영 사항으로, ② 정보보안, 해킹방지 등과 달리 금융보안과 직결되지 않으며, ③ 추상적 수준의 내용\*인 점 등을 감안하여,

\* “충분한 타당성 검토”, “공정하고 합리적인 가격 산출”, “계약시 귀속관계를 명확히 하여 사후분쟁 방지” 등 내용으로 사실상 제재사례 없음

→ 감독규정상 세부내용(각 호) 삭제(필요시 해설서에 예시로 제공)

#### **[5] 비밀번호 설정방식(§ 32, § 33) 관련**

- (주요내용) 내부 사용자, 이용자 등의 비밀번호 관리에 있어 안전성·보안성 유지를 위한 규정

\* 예 : 비밀번호는 아이디, 생년월일, 주민등록번호, 전화번호를 포함하지 않은 숫자와 영문자 및 특수문자 등을 혼합하여 8자리 이상으로 설정

- ⇒ (검토결과) ① 비밀번호 설정 방식을 구체적으로 특정하는 것은 오히려 보안에 뛰어난 다른 비밀번호 정책 채택을 제한할 수 있고, ② 타 입법례\*와 비교하여도 과도하며, ③ 생체정보 등 신기술을 활용한 인증수단\*\* 도입에도 장애로 작용

\* 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시, 신용정보업감독규정 등

\*\* 문자·숫자로 표시될 수 없는 지문인증 등 수단에 대한 관리기준이 부재

→ 규정상 원칙만을 존치하고 각 호는 삭제하되, 비밀번호 이외 수단(지문인증 등) 등이 사용될 수 있는 점을 고려하여 생체인증 수단 등 비밀번호에 준하는 수단을 포함

▪ (현행) ‘주민등록번호, 동일숫자, 연속숫자 등 제3자가 쉽게 유추할 수 있는 비밀번호의 등록 불가’ 등 세부규칙 존재

→(개선) 제3자가 쉽게 유추할 수 없는 비밀번호 작성규칙 및 등록·변경 절차를 수립·운영할 것



## 금융보안 선진화 추진계획



규칙(Rule) → 원칙(Principle) 중심으로 감독규정 합리화

### 1단계 감독규정 정비

#### Before

293개 수범사항

인력·조직·예산(22개)  
건물·설비·전산실(15개)  
정보기술(119개)  
내부통제(115개)  
전자금융업무 등(22개)

#### After

166개 수범사항

지나치게 미시적·세부적  
사항은 원칙적 삭제(134건)  
이용자 보호 등은 강화(5건)  
금융보안 핵심은 유지(114건)  
기타 조정·합리화(45건)

급변하는 금융IT 환경·보안 리스크에 유연한 대응 및  
금융권의 자율보안 체계 확립 토대 마련

### 2단계 법률 개정



자율보안 책임성 강화 등을 위한 법률 개정



금융보안 거버넌스 강화



금융회사 사후책임성 강화 등

### 3단계 자율보안 체계 전환



자율보안으로 금융보안 패러다임 전환

규정위반 여부 감독 중심

자율보안 수립·이행 검증 중심



금융회사 등



금융당국