전자금융감독규정 제 3 장 (현행 감독규정 제 7 조-제 41 조)의 개정 방향 [예시]

[금융위원회 고시]

제 3 장 전자금융거래의 안전성 확보 및 이용자 보호

제 1 절 규제자의 임무

제 7 조(금융소비자 보호) 금융위원회와 금융감독원은 전자금융 서비스가 기술 발전을 반영한 합리적 방법으로 안전하게 제공되고, 전자금융거래와 관련된 분쟁이 신속하고 정당하게 해결되도록 하여 금융소비자가 적절히 보호되는데 필요한 감독을 수행한다.

제 8 조(금융회사 등의 책임성 확보) 금융위원회와 금융감독원은 금융회사 등이 우월적 지위를 남용하거나 법령이 정한 책임을 부당하게 소비자 또는 다른 사업자에게 전가하거나 회피하지 않도록 하는데 필요한 감독을 수행한다.

제 9 조(기술 및 서비스의 자유로운 경쟁과 발전) 금융위원회와 금융감독원은 전자금융거래 서비스 제공에 사용되는 거래기술, 보안기술 및 보안감사 서비스가 활발하고 공정하게 경쟁하고 발전할 수 있는 시장 환경이 손상되지 않도록 감독을 수행한다.

제 10 조(규제의 투명성 및 형평성) 금융위원회와 금융감독원은 전자금융거래 서비스와 관련된 정보가 적절한 수준에서 투명하게 공개되고 규제의 형평성이 유지되도록 한다.

제 2 절 금융회사 최고 경영진의 책임

제 11 조(관리 감독 체계의 확립) 금융회사 등의 이사진과 최고 경영진은 전자금융 사업에 관한 위험을 관리하고 책임소재를 분명히 하는데 필요한 관리 감독 체계를 자체적으로 확립하여야 한다.

제 12 조(일괄 위임의 금지) 금융회사 등의 이사진과 최고 경영진은 자신의 전자금융 사업에 적용되는 보안 통제 절차의 핵심적 사항을 직접 검토하고 승인한다.

제 13 조(외주 계약 관계 등의 점검과 관리) 금융회사 등의 이사진과 최고 경영진은 자신의 전자금융 사업이 외주 계약 관계 등 제 3 자에게 의존하는 부분에 대하여 적절히 점검하고 관리하는데 필요한 상시적 체계를 수립한다.

제 14 조(직원의 훈련 및 교육) 금융회사 등의 이사진과 최고 경영진은 전자금융 사업에 수반되는 위험을 관리하는데 필요한 인력을 충분히 확보하고 그들에 대한 상시적이고 정기적인 훈련 및 교육 프로그램을 마련한다.

제 3 절 보안 통제 조치

제 15 조(적절한 인증기술의 채택) 금융회사 등은 거래의 성격과 해당 거래에 수반하는 위험의 수준을 고려하여 업계의 기술 수준을 반영한 합리적인 당사자 인증 기술을 채택하여야 한다.

제 16 조(분쟁 예방 및 대처) 금융회사 등은 거래 내용을 고객이 분명히 이해할 수 있도록 유저 인터페이스를 설계하고, 거래의 주체와 거래의 내역을 신뢰성 있는 방법으로 확인하고, 거래 데이터가 변조되지 않도록 하며, 변조 여부를 판별하는데 필요한 합리적 조치를 채택함으로써 전자금융거래와 관련된 분쟁을 예방하고, 분쟁에 대처하여야 한다.

제 17 조(업무 권한의 분할) 금융회사 등은 전자금융거래 시스템, 데이타베이스, 프로그램의 운용에 있어서 각 직원의 임무가 적절히 분리, 분할되도록 하는데 필요한 조치를 취함으로써 자신의 전자금융 업무가 직원들 간에 상호 검증될 수 있도록 해야 한다.

제 18 조(접근, 출입 권한의 통제) 금융회사 등은 전자금융거래 시스템, 데이타베이스, 프로그램에 대한 접근 권한 및 출입 권한 통제가 적절히 이루어지도록 함으로써 각 직원이 자기 권한을 스스로 변경할 수 없도록 하며, 업무권한의 분리, 분할을 통한 상호 검증 체계가 우회되지 않도록 해야 한다.

제 19 조(거래 기록 등의 보호) 금융회사 등은 전자금융거래 내역, 거래 기록 등의 정보가 변경되지 않고 보존될 수 있도록 하는데 필요한 조치를 마련하여야 한다.

제 20 조(검사 이력 및 증거 확보) 금융회사 등은 고객의 모든 전자금융거래에 대하여 감사/검사 이력(audit trails)이 남도록 하고, 법원에 제출될 수 있는 증거자료를 평소에 확보하고, 증거자료가 사후에 변조되지 않도록 하는데 필요한 적절한 조치들을 상시로 취해야 한다.

제 21 조(고객의 비밀 보호) 금융회사 등은 전자금융거래 내역의 비밀성을 유지하는데 필요한 적절한 조치를 마련하여야 한다.

제 4 절 법적 책임 및 평판에 관한 사항

제 22 조(고객에게 제공되어야 할 정보) 금융회사 등은 고객이 거래할지 여부를 제대로 판단하는데 필요한 정보(명칭, 규제상황 등)를 적절히 제공하여야 한다.

제 23 조(개인정보보호) 금융회사 등은 고객의 개인정보를 법령에 따라 준수하여야 한다.

제 24 조(사업지속에 필요한 대비책) 금융회사 등은 전자금융 서비스가 상시 제공될 수 있도록 사업규모, 사업지속 및 비상 대책에 관한 사전 기획 절차를 마련하여야 한다.

제 25 조(재난 회복 및 사고 대응책) 금융회사 등은 전자금융 서비스에 대한 내부자의 공격이나 외부자의 공격 등 불의의 사태를 관리하고 피해를 최소화 하는데 필요한 사고 대응책을 적절히 개발하여 시행한다.

제 26 조(사고 보고 및 분쟁절차 모니터링) 금융감독원은 전자금융 사고거래의 내용과 규모를 정확히 파악하고, 공평하고 신속한 분쟁해결을 위하여 다음 조치를 취한다:

1. 전자금융 서비스와 관련된 소비자의 불만, 이의, 환불신청 등을 통합적으로 접수할 수 있는 페이지(금융소비자 보호페이지)를 금융감독원이 관리하고, 각 금융회사는 이 페이지의 링크를 자신의 홈페이지에 게시한다.
2. 금융감독원은 금융소비자 보호페이지를 통하여 접수된 소비자의 불만, 이의, 환불신청을 해당 금융회사 등에 이첩하고, 분쟁해결 과정을 모니터링 한다.
3. 금융감독원은 각 금융회사 별 사고거래의 내용과 규모를 신뢰성 있는 방법으로 파악하여 보안기술의 연구 개발 및 서비스 품질 향상에 필요한 한도에서 적절한 수준과 방법으로 공표한다.

제 5 절 보안감사 서비스

제 27 조(정기적, 전문적, 독립적 보안감사) ① 금융회사 등은 다음 중 하나의 보안점검 기준에 따른 보안감사를 수행할 전문성과 독립성이 있는 보안감사 업체와 계약을 체결하고 보안감사를 년 1 회 이상 받아야 한다.

1. PCI DSS 등 국제적으로 인정받는 금융거래 보안 기준
2. 금융감독원이 공표하는 별지의 보안 기준(금융감독원 데이터 보안 기준; Korea Financial Supervisory Service Data Security Standards)(이하, FSS DSS 라 함)

② 금융감독원은 FSS DSS 의 지속적인 업데이트 및 국제화 작업, FSS DSS 기준에 따른 보안감사 서비스 제공자의 자격 요건 및 품질 관리에 필요한 업무를 지원한다.

제 28 조(신규 솔루션에 대한 제 3 자 검증) ① 금융회사 등이 전자금융 거래 솔루션을 신규로 채용할 경우에는 독립적이고 전문적인 보안감사 업체의 검증을 받고, 그 검증 보고서를 해당 서비스 개시 후 6 개월 이내에 금융감독원에 제출하여야 한다.
② 전항의 검증 보고서는 해당 금융회사의 웹사이트에도 공지하여야 한다.