12. pielikums  
Finanšu un kapitāla tirgus komisijas  
25.08.2020. normatīvajiem noteikumiem Nr. 138

**Informācijas sistēmu drošības politikas aprakstā iekļaujamā informācija**

Iesnieguma iesniedzējs iesniedz informācijas sistēmu drošības pārvaldības aprakstu, kurš izstrādāts, ņemot vērā Finanšu un kapitāla tirgus komisijas informācijas sistēmu drošības jomas normatīvo noteikumu prasības, un kurā iekļauj vismaz tālāk minēto informāciju.

|  |  |  |
| --- | --- | --- |
| Nr. | Iekļaujamā informācija | Informācijas atrašanās vieta aprakstā |
| 1. | Detalizēts riska novērtējums par maksājumu pakalpojumiem un elektroniskās naudas pakalpojumiem, ko iesnieguma iesniedzējs plāno sniegt, iekļaujot arī krāpšanas risku un drošības kontroles un riska mazināšanas pasākumus, ko veic, lai pienācīgi aizsargātu maksājumu pakalpojumu izmantotājus un elektroniskās naudas turētājus no identificētajiem riskiem. |  |
| 2. | IT sistēmu apraksts, kurā jāiekļauj šāda informācija:  a) sistēmu un to tīkla elementu arhitektūra (datortīkla un pieslēgumu shēma);  b) informācijas sistēmas, kas atbalsta īstenoto komercdarbību, piemēram, iesnieguma iesniedzēja tīmekļa vietne, elektroniskie maki, maksājumu sistēma, risku un krāpšanas pārvaldības sistēmas un klientu uzskaites sistēma;  c) IT atbalsta sistēmas, ko izmanto iesnieguma iesniedzēja darbības organizācijai un pārvaldībai, piemēram, grāmatvedības, personālvadības, attiecību ar klientiem pārvaldības informācijas sistēmas, e-pasta sistēma un iekšējā failu sistēma;  d) informācija, vai iesnieguma iesniedzējs vai tā grupa jau izmanto minētās informācijas sistēmas; paredzamais to ieviešanas datums, ja piemērojams. |  |
| 3. | Atļautie ārējo pieslēgumu veidi, piemēram, partneriem, pakalpojumu sniedzējiem, grupas vienībām un darbiniekiem, kuri strādā attālināti, tostarp šādu pieslēgumu loģiskais pamatojums, norādot ieviestos loģiskās drošības pasākumus un kontroles mehānismus. |  |
| 4. | Loģiskās drošības pasākumi un mehānismi, kas regulē iekšējo piekļuvi IT sistēmām. |  |
| 5. | Iesnieguma iesniedzēja darba vietu un datu centra fiziskās drošības pasākumi un mehānismi, piemēram, fiziskās piekļuves kontroles pasākumi un vides drošības pārvaldība. |  |
| 6. | Maksājumu procesu un elektroniskās naudas pakalpojumu procesu drošība, iekļaujot šādu informāciju:  a) klientu autentifikācijas procedūra, ko izmanto gan informatīvai piekļuvei, gan piekļuvei maksājuma vai maksājuma ierosināšanas nolūkā;  b) autentifikācijas elementu droša nodošana likumīgajam maksājumu pakalpojumu izmantotājam vai elektroniskās naudas turētājam, nodrošinot integritāti gan to sākotnējās ieviešanas, gan atjaunošanas gadījumā;  c) sistēmu un procedūru, ko iesnieguma iesniedzējs ieviesis maksājumu analīzei un aizdomīgu vai neparastu maksājumu identificēšanai, apraksts. |  |
| 7. | To galveno procedūru saraksts, kuras attiecas uz iesnieguma iesniedzēja informācijas sistēmām, vai attiecībā uz procedūrām, kas vēl nav formalizētas, – paredzamais to spēkā stāšanās datums. |  |