LATVIJAS BANKA
EIROSISTĒMA

K. VALDEMĀRA IELA 2A, RĪGA, LV-1050, LATVIJA. TĀLRUNIS +371 67022300, E-PASTS INFO@BANK.LV, WWW.BANK.LV

Projekts (2.versija)

[Datums] Noteikumi Nr. XX
Rīgā

Prasības digitālās darbības nepārtrauktības un noturības jomā finanšu tirgus dalībniekiem, kuriem nepiemēro Eiropas Parlamenta un Padomes 2022. gada 14. decembra regulu (ES) 2022/2554 par finanšu nozares digitālās darbības noturību un ar ko groza regulas (EK) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 un (ES) 2016/1011

Izdoti saskaņā ar
Finanšu tirgus digitālās darbības noturības un
mākslīgā intelekta izmantošanas likuma
6. panta trešo daļu

I. Vispārīgie jautājumi

1. Noteikumi nosaka:
1.1. pasākumus, lai nodrošinātu dokumentētu un visaptverošu informācijas un komunikācijas tehnoloģiju (turpmāk – IKT) riska pārvaldības un kontroles sistēmu;
1.2. prasības IKT sistēmu drošības un darbības uzraudzībai;
1.3. prasības IKT sistēmām, fiziskajai videi, procedūrām un IKT operāciju pārvaldībai;
1.4. prasības kritiski svarīgo funkciju nepārtrauktības nodrošināšanai, rezerves kopiju veidošanai, atjaunošanas pasākumiem un to testēšanai.

2. Noteikumi attiecas uz:
2.1. alternatīvo ieguldījumu fondu pārvaldniekiem, ja tie atbilst Finanšu tirgus digitālās darbības noturības un mākslīgā intelekta izmantošanas likuma 6. panta pirmās daļas 1. punktā noteiktajam;
2.2. apdrošināšanas sabiedrībām un pārapdrošināšanas sabiedrībām, kuras ievēro Finanšu tirgus digitālās darbības noturības un mākslīgā intelekta izmantošanas likuma 6. panta pirmās daļas 2. punktā noteikto;
2.3. apdrošināšanas starpniekiem, pārapdrošināšanas starpniekiem un apdrošināšanas papildpakalpojuma starpniekiem, kuri ir mikrouzņēmumi, mazie uzņēmumi vai vidējie uzņēmumi;
2.4. fiziskajām un juridiskajām personām Finanšu instrumentu tirgus likuma 101. panta septītās daļas 2., 3., 4., 6., 7., 9., 12., 13., 15. un 16. punkta izpratnē;
2.5. krājaizdevu sabiedrībām;
2.6. nelieliem privātajiem pensiju fondiem, kuru reģistrētajos pensiju plānos kopā nav vairāk par 15 pensiju plāna dalībniekiem;
2.7. žiro norēķinu iestādēm.

3. Finanšu tirgus dalībnieks (turpmāk – tirgus dalībnieks), īstenojot šo noteikumu prasības, ievēro proporcionalitātes principu un uz risku pārvaldību balstītu pieeju, ņemot

vērā darbības jomu, darbinieku skaitu, sniegto pakalpojumu veidu, kā arī to sarežģītību un kopējo IKT izmantošanas līmeni.

4. Šo noteikumu 2.3., 2.4. un 2.6. apakšpunktā minētajiem tirgus dalībniekiem piemēro tikai šo noteikumu 12.1. apakšpunktu, 13. punktu, 18.3., 18.4., 26.7. un 26.8. apakšpunktu un 28. punktu.

II. Vadība un organizācija

5. Tirgus dalībnieks ievieš un dokumentē IKT riska pārvaldības un kontroles sistēmu, kas nodrošina IKT riska efektīvu pārvaldību, lai sasniegtu augstu digitālās darbības noturības līmeni.

6. Tirgus dalībnieks savas IKT riska pārvaldības un kontroles sistēmas ietvaros nodrošina, ka tā vadība:
6.1. uzņemas vispārējo atbildību par to, lai nodrošinātu, ka IKT riska pārvaldības un kontroles sistēma ļauj sasniegt tirgus dalībnieka uzņēmējdarbības stratēģijā noteiktos mērķus saskaņā ar tā vēlmi uzņemties risku, un nodrošina, ka šajā kontekstā tiek ņemts vērā arī IKT risks;
6.2. nosaka visus ar IKT izmantošanu saistītos pienākumus un atbildību;
6.3. nosaka informācijas drošības mērķus un IKT prasības;
6.4. apstiprina, pārrauga un periodiski pārskata:
6.4.1. tirgus dalībnieka informācijas aktīvu un IKT aktīvu klasifikāciju;
6.4.2. tirgus dalībnieka darbības nepārtrauktības plānus, tai skaitā uzņēmējdarbības ietekmes analīzi;
6.5. piešķir un vismaz reizi gadā pārskata budžetu, kas nepieciešams, lai apmierinātu tirgus dalībnieka digitālās darbības noturības vajadzības attiecībā uz visu veidu resursiem, tai skaitā IKT drošības izpratnes veidošanas programmām un IKT izmantošanas prasmju apmācību visiem darbiniekiem;
6.6. nosaka un īsteno pasākumus, lai identificētu, novērtētu un pārvaldītu IKT risku, kam tirgus dalībnieks ir pakļauts, tai skaitā ar trešajām personām saistīto IKT risku;
6.7. nosaka un īsteno procedūras un kontroles, kas nepieciešamas, lai aizsargātu visus informācijas aktīvus un IKT aktīvus;
6.8. nodrošina, ka tirgus dalībnieka darbinieki pastāvīgi atjaunina zināšanas un prasmes, kas ļauj pietiekami izprast un novērtēt IKT risku un tā ietekmi uz tirgus dalībnieka darbību;
6.9. nosaka kārtību, kādā notiek ziņošana vadībai par incidentiem, kas saistīti ar IKT, un par digitālās darbības noturību, tai skaitā nosaka ziņojumu regularitāti, formu un saturu.

7. Tirgus dalībnieks var IKT pakalpojumu sniegšanu uzticēt trešajām personām. Šādā gadījumā tirgus dalībnieks joprojām ir pilnībā atbildīgs par IKT riska pārvaldības prasību izpildi un pakalpojumu uzraudzību.

III. Informācijas drošības politika un pasākumi

8. Tirgus dalībnieks izstrādā, dokumentē un īsteno informācijas drošības politiku, kurā noteikti augsta līmeņa principi un noteikumi, lai aizsargātu datu un sniegto pakalpojumu konfidencialitāti, integritāti un pieejamību.

9. Pamatojoties uz šo noteikumu 8. punktā minēto informācijas drošības politiku, tirgus dalībnieks nosaka un īsteno IKT drošības pasākumus, lai mazinātu savu pakļautību IKT riskam, tai skaitā nosaka riska mazināšanas pasākumus, kurus īsteno trešās personas, kas sniedz IKT pakalpojumus.

IV. Informācijas aktīvu un IKT aktīvu klasifikācija

10. Tirgus dalībnieks kā daļu no IKT riska pārvaldības un kontroles sistēmas identificē, klasificē, dokumentē un pēc vajadzības pārskata un aktualizē visas kritiski svarīgās un svarīgās funkcijas, tās atbalstošos informācijas aktīvus un IKT aktīvus un to savstarpējo atkarību.

11. Tirgus dalībnieks identificē arī visas kritiski svarīgās funkcijas, kuras nodrošina trešās personas, kas sniedz IKT pakalpojumus.

V. IKT riska pārvaldība

12. Tirgus dalībnieks izstrādā, dokumentē un uztur IKT riska pārvaldības un kontroles sistēmu, kurā iekļauj vismaz šādus elementus:
12.1. IKT riska identifikāciju, novērtējumu un tā mazināšanas pasākumus, tai skaitā par trešo personu sniegtajiem IKT pakalpojumiem;
12.2. riska mazināšanas stratēģijas noteikšanu un tās efektivitātes uzraudzību;
12.3. tādu IKT un informācijas drošības risku identifikāciju un novērtējumu, kuri izriet no nozīmīgām IKT sistēmu vai IKT pakalpojumu vai procesu izmaiņām vai IKT drošības testēšanas rezultātiem vai būtiska IKT incidenta.

13. Tirgus dalībnieks ne retāk kā reizi gadā veic un dokumentē IKT riska novērtējumu.

14. Tirgus dalībnieks pastāvīgi uzrauga draudus un ievainojamības, kas ir būtiskas attiecībā uz tā kritiski svarīgajām funkcijām, informācijas aktīviem un IKT aktīviem, un regulāri pārskata riska scenārijus, kas ietekmē minētās kritiski svarīgās funkcijas.

15. Tirgus dalībnieks nosaka IKT incidentu identificēšanas, reģistrēšanas un klasificēšanas kārtību, kā arī ziņošanas tā vadībai kārtību.

VI. Fiziskā drošība

16. Tirgus dalībnieks identificē un īsteno fiziskās drošības pasākumus, lai rūpīgi un pienācīgi aizsargātu visus informācijas aktīvus un IKT aktīvus, tai skaitā darbstacijas, datoru programmatūru un aparatūru, kā arī lai aizsargātu visus attiecīgos fiziskos komponentus un infrastruktūru, piemēram, telpas un datu centru.

VII. Piekļuves kontrole

17. Tirgus dalībnieks izstrādā, īsteno, uzrauga un regulāri pārskata procedūras loģiskās un fiziskās piekļuves kontrolei. Minētās procedūras ietver šādus loģiskās un fiziskās piekļuves kontroles elementus:
17.1. tiesības attiecībā uz piekļuvi informācijas aktīviem, IKT aktīviem un to atbalstītajām funkcijām, kas tiek pārvaldītas saskaņā ar principiem "vajadzība zināt" un "vajadzība izmantot" un mazāko tiesību principu, arī attiecībā uz attālinātu un ārkārtas piekļuvi;
17.2. lietotāju un sistēmu darbību reģistrēšana, kas nodrošina, ka lietotājus attiecībā uz IKT sistēmās veiktajām darbībām var identificēt. Tirgus dalībnieks nosaka atbilstošu sistēmas žurnālu glabāšanas termiņu, lai tas spētu identificēt, reģistrēt un ziņot par incidentiem, kas saistīti ar IKT, kā arī uzturēt nepieciešamos pierakstus izmeklēšanas un uzraudzības vajadzībām;
17.3. lietotāju kontu pārvaldības procedūras, lai piešķirtu, mainītu vai atsauktu piekļuves tiesības lietotāju un vispārējiem kontiem, tai skaitā vispārējiem administratoru kontiem;

17.4. autentifikācijas metodes, kas ir samērīgas ar šo noteikumu 10. punktā minēto klasifikāciju un IKT aktīvu vispārējo riska profilu un atbilst labākajai praksei;
17.5. piekļuves tiesības tiek periodiski, bet ne retāk kā reizi gadā pārskatītas un atsauktas nekavējoties, kad tās vairs nav vajadzīgas. Tirgus dalībnieks piekļuves tiesības attiecībā uz IKT resursiem un to izmaiņas dokumentē un uztur atbilstošā reģistrā;
17.6. šo noteikumu 17.4. apakšpunkta nolūkos tirgus dalībnieks izmanto stingrās divu vai vairāku faktoru uz labāko praksi balstītas autentifikācijas metodes attiecībā uz attālinātu piekļuvi tirgus dalībnieka datortīklam, privileģētu piekļuvi un piekļuvi IKT aktīviem, kas atbalsta kritiski svarīgas funkcijas, kuras ir publiski pieejamas.

VIII. IKT darbības drošība

18. Tirgus dalībnieks savas IKT riska pārvaldības un kontroles sistēmas ietvaros un attiecībā uz IKT aktīviem:
18.1. uzrauga un pārvalda IKT aktīvu dzīves ciklu;
18.2. attiecīgā gadījumā uzrauga, vai IKT aktīvus atbalsta trešās personas, kas sniedz IKT pakalpojumus;
18.3. veic automatizētu ievainojamību izvērtēšanu un izmanto drošības ielāpus, lai novērstu identificētās ievainojamības;
18.4. pārvalda riskus, kas saistīti ar novecojušiem, neatbalstītiem vai mantotiem IKT aktīviem;
18.5. reģistrē notikumus, kas saistīti ar pieejas tiesību un IKT izmaiņu pārvaldību;
18.6. identificē un īsteno pasākumus, lai uzraudzītu un analizētu informāciju par IKT sistēmu anomālām darbībām un uzvedību;
18.7. īsteno pasākumus, lai uzraudzītu būtisko un aktuālo informāciju par kiberdraudiem.

IX. Datu, sistēmu un tīkla drošība

19. Tirgus dalībnieks kā daļu no IKT riska pārvaldības un kontroles sistēmas izstrādā un īsteno aizsardzības pasākumus, kas nodrošina tīklu aizsardzību pret ielaušanos un datu ļaunprātīgu izmantošanu. Tirgus dalībnieks nosaka:
19.1. drošības pasākumus un nodrošina to īstenošanu, lai aizsargātu datus, kad tie tiek izmantoti, nosūtīti vai glabāti;
19.2. drošības pasākumus un nodrošina to īstenošanu, lai novērstu un atklātu neatļautu pieslēgšanos tirgus dalībnieka tīklam un aizsargātu tīkla datplūsmas starp tā iekšējiem tīkliem un internetu vai citiem ārējiem pieslēgumiem;
19.3. procesu to datu drošai dzēšanai, kuri tirgus dalībniekam vairs nav nepieciešami;
19.4. procesu, lai droši utilizētu vai izņemtu no ekspluatācijas datu glabāšanas ierīces, kas satur konfidenciālu informāciju;
19.5. drošības pasākumus, lai nodrošinātu, ka attālināts darbs un privātu galapunkta ierīču izmantošana nelabvēlīgi neietekmē tirgus dalībnieka spēju veikt tā kritiski svarīgās funkcijas.

X. IKT drošības testēšana

20. Tirgus dalībnieks izstrādā un īsteno IKT drošības testēšanas plānu, lai novērtētu to savu IKT drošības pasākumu efektivitāti, kuri izstrādāti saskaņā ar šo noteikumu prasībām. Tirgus dalībnieks nodrošina, ka minētajā testēšanas plānā ir ņemti vērā draudi un ievainojamības, kas identificētas IKT riska pārvaldības sistēmas ietvaros.

21. Tirgus dalībnieks uzrauga un izvērtē IKT drošības testēšanas rezultātus un savlaicīgi pārskata un atjaunina drošības pasākumus tādu IKT sistēmu gadījumā, kas atbalsta kritiski svarīgas funkcijas.

XI. IKT sistēmu iegāde, izstrāde un uzturēšana

22. Tirgus dalībnieks IKT sistēmu iegādē, izstrādē un uzturēšanā ievēro uz risku balstītu pieeju, tai skaitā:
22.1. nodrošina, ka pirms IKT sistēmu iegādes vai izstrādes attiecīgā uzņēmējdarbības struktūrvienība nosaka un apstiprina funkcionālās un nefunkcionālās prasības, tostarp informācijas drošības prasības;
22.2. nodrošina IKT sistēmu testēšanu un apstiprināšanu pirms to pirmreizējās izmantošanas un pirms izmaiņu ieviešanas ražošanas vidē;
22.3. nosaka pasākumus, lai mazinātu IKT sistēmu nejaušas pārveides vai tīšas manipulācijas risku sistēmas izstrādē un ieviešot tās ražošanas vidē.

XII. IKT projektu un izmaiņu pārvaldība

23. Tirgus dalībnieks ievēro IKT projektu pārvaldības labo praksi, kas aptver visus IKT projektu posmus no to uzsākšanas līdz slēgšanai.

24. Tirgus dalībnieks izstrādā un īsteno IKT izmaiņu pārvaldības procedūru, lai nodrošinātu, ka IKT sistēmu izmaiņas tiek reģistrētas, testētas un ieviestas kontrolētā veidā un ievērojot pienācīgus aizsardzības pasākumus.

XIII. IKT darbības nepārtrauktības pārvaldība

25. Tirgus dalībnieks izstrādā un dokumentē darbības nepārtrauktības plānu, ņemot vērā uzņēmējdarbības ietekmes rezultātus un scenārijus, kam varētu būt pakļauti IKT aktīvi, kuri atbalsta kritiski svarīgas funkcijas, tai skaitā kiberuzbrukuma scenāriju.

26. IKT darbības nepārtrauktības plāni:
26.1. tiek apstiprināti tirgus dalībnieka vadības struktūrā;
26.2. tiek dokumentēti un ir ātri pieejami krīzes gadījumā;
26.3. paredz pietiekamus resursus plāna izpildei;
26.4. nosaka plānotos seku novēršanas līmeņus un termiņus funkciju, tai skaitā trešo personu atbalstīto funkciju, atgūšanai un atjaunošanai;
26.5. paredz nosacījumus IKT darbības nepārtrauktības plānu aktivizēšanai;
26.6. nosaka atjaunošanas pasākumus kritiski svarīgām uzņēmējdarbības funkcijām, atbalsta procesiem un informācijas aktīviem, lai izvairītos no nelabvēlīgas ietekmes uz tirgus dalībnieka darbību;
26.7. paredz rezerves kopiju veidošanas procedūras un pasākumus, kas nosaka to datu tvērumu, kuriem jāveido rezerves kopijas, un rezerves kopiju veidošanas biežumu, pamatojoties uz šos datus izmantojošās funkcijas svarīgumu;
26.8. ņem vērā alternatīvas iespējas, ja atgūšana īstermiņā nav iespējama izmaksu vai neparedzētu apstākļu dēļ;
26.9. nosaka iekšējās un ārējās saziņas kārtību, tai skaitā eskalācijas plānus;
26.10. tiek atjaunināti saskaņā ar pieredzi, kura gūta no incidentiem, testiem un jauniem riskiem, kā arī būtiskām izmaiņām tirgus dalībnieka organizācijā un IKT aktīvos, kas atbalsta kritiski svarīgas uzņēmējdarbības funkcijas.

XIV. Darbības nepārtrauktības plānu testēšana

27. Tirgus dalībnieks darbības nepārtrauktības plānu testē vismaz reizi gadā vai ikreiz, kad notiek būtiskas izmaiņas, ņemot vērā iespējamos scenārijus, tai skaitā kiberuzbrukumus.

28. Tirgus dalībnieks rezerves kopiju veidošanas un atjaunošanas procedūras testē vismaz reizi gadā vai ikreiz, kad notiek būtiskas izmaiņas tirgus dalībnieka darbības nepārtrauktības plānā.

29. Tirgus dalībnieks dokumentē darbības nepārtrauktības plāna testēšanas rezultātus un analizē un novērš minētajā testēšanā konstatētās nepilnības.

XV. Noslēguma jautājums

30. Noteikumi stājas spēkā 2026. gada 15. janvārī.

ŠIS DOKUMENTS IR ELEKTRONISKI PARAKSTĪTS AR DROŠU ELEKTRONISKO PARAKSTU UN SATUR LAIKA ZĪMOGU

Latvijas Bankas prezidents M. Kazāks