



Laidiens: 13.10.2010., Nr. 162

Finanšu un kapitāla tirgus komisijas normatīvie noteikumi Nr.278

Rīgā 2010.gada 8.oktobrī

(Finanšu un kapitāla tirgus komisijas padomes sēdes protokols Nr.39 2.p.)

**Finanšu un kapitāla tirgus dalībnieku informācijas sistēmu drošības
normatīvie noteikumi**

*Izdoti saskaņā ar Kredītiestāžu likuma 50.⁸ panta sesto daļu
un 50.⁹ panta astoto daļu, Finanšu instrumentu tirgus likuma
123.³ panta sesto daļu un 123.⁴ panta astoto daļu, Apdrošināšanas sabiedrību
un to uzraudzības likuma 50. panta otro daļu, likuma
"Par privātajiem pensiju fondiem" 28. panta sesto daļu un
Finanšu un kapitāla tirgus komisijas likuma 7. panta pirmās daļas 1. punktu*

I. Vispārīgie jautājumi

1. "Finanšu un kapitāla tirgus dalībnieku informācijas sistēmu drošības normatīvie noteikumi" (tālāk tekstā – noteikumi) ir saistoši Latvijā reģistrētiem finanšu un kapitāla tirgus dalībniekiem (tālāk tekstā – tirgus dalībnieks): kredītiestādēm, krājaizdevu sabiedrībām, maksājumu iestādēm, apdrošināšanas sabiedrībām, apdrošināšanas starpniekiem, privātajiem pensiju fondiem, regulētā tirgus organizētājiem, Latvijas Centrālajam depozitārijam, ieguldījumu brokeru sabiedrībām un ieguldījumu pārvaldes sabiedrībām.
2. Noteikumu mērķis ir ierobežot tirgus dalībnieku darbībai un klientiem sniegto pakalpojumu nodrošināšanai izmantojamo informācijas sistēmu (tālāk tekstā arī – IS) riskus, kā arī noteikt vienoti strukturētas prasības tirgus dalībnieku IS drošības risku pārvaldībai.
3. Noteikumi nosaka prasību minimumu. Tirgus dalībnieks var ieviest papildu aizsardzības pasākumus atkarībā no informācijas resursu klasifikācijas līmeņa un veiktās risku analīzes, ņemot vērā uzņēmuma sniegtos pakalpojumus, darbinieku skaitu un informācijas tehnoloģiju (tālāk tekstā – IT) izmantošanas līmeni.

II. Termins

4. Auditācijas pieraksti – analīzei pieejami pieraksti, kuros reģistrēti dati par noteiktiem notikumiem IS (piekļuve, datu ievade, maiņa, dzēšana, izvade u.c.).
5. Ārpakalpojuma sniedzējs – trešā persona, kas pēc tirgus dalībnieka pieprasījuma nodrošina tirgus dalībnieka IT un IS pārvaldību, attīstību, drošību, auditu vai sniedz citu tirgus dalībniekam nepieciešamu pakalpojumu, kas saistīts ar IS.

6. Drošības pasākumi – tehniski vai organizatoriski pasākumi, kas tiek noteikti risku pārvaldības ietvaros un samazina IS risku līdz pieļaujamajam līmenim.
7. Ievainojamība – IS nepilnība, kas ļauj kādam noteiktam apdraudējumam īstenoties un ietekmēt IS drošību.
8. Informācijas devējs – persona, kas iesniegusi informāciju tirgus dalībniekam, vai persona, ar kuru saistītā informācija ir ietverta IS (piemēram, tirgus dalībnieka klienti).
9. Informācijas sistēma – datu ievades, uzglabāšanas un apstrādes sistēma, kas nodrošina noteikto funkciju izpildi un paredz lietotājpieeju tajā glabātajiem datiem vai informācijai.
10. Informācijas konfidencialitāte – piekļuves nodrošināšana informācijai tikai pilnvarotām personām.
11. Informācijas integritāte – informācijas un tās apstrādes metožu precizitāte, pareizība un pilnīgums.
12. Informācijas pieejamība – iespēja pilnvarotām personām lietot informāciju noteiktā laikā un vietā.
13. Informācijas resursi – informācijas vienības, kurās ietilpst datu faili, kas satur IS glabājamo, apstrādājamo un IS lietotājiem pieejamo informāciju, kā arī visi IS ievades un izvades dokumenti neatkarīgi no datu nesēja veida.
14. Informācijas resursu turētājs – persona, kas ir atbildīga par informācijas resursiem un rīkojas ar tiem tirgus dalībnieka uzdevumā.
15. IS drošība – IS konfidencialitātes, integritātes un pieejamības prasību nodrošināšana.
16. IS drošības incidents – kaitīgs notikums vai nodarījums, kura rezultātā tiek apdraudēta vai var tikt apdraudēta IS drošība (t.sk. uzbrukumi IS vai datortīkla iekārtai, darbības, kas izraisa vai var izraisīt neautorizētu piekļuvi IS, pakalpojuma atteikumi).
17. IS lietotājs – persona, kura piešķirto pilnvaru robežās lieto IS.
18. IS resursi – šo noteikumu 13. un 21. punktā minētie resursi.
19. IS resursu turētājs – informācijas resursu vai tehnoloģisko resursu turētājs.
20. Risks – ar IS funkcionēšanu saistīta organizācijas varbūtēja nespēja pilnvērtīgi un kvalitatīvi veikt kādu savu saistību vai funkciju izpildi, ko nosaka kā nevēlamā notikuma iespējamības un tā seku kombināciju.
21. Tehnoloģiskie resursi – IS sastāvdaļa, kurā ietilpst sistēmprogrammas, lietojumprogrammas, palīgprogrammas, sistēmfaili, datori, datortīkli, aparatūra un citas iekārtas, kas nodrošina IS darbību.
22. Tehnoloģisko resursu turētājs – persona, kas ir atbildīga par tehnoloģiskajiem resursiem un rīkojas ar tiem tirgus dalībnieka uzdevumā.

III. Informācijas sistēmu drošības organizēšana

23. Vadības atbildība un atbalsts

23.1. Tirgus dalībnieka vadība ir atbildīga par IS drošības politikas un IT stratēģijas noteikšanu un īstenošanu, darbinieku pienākumu un atbildības noteikšanu, kontroles organizēšanu, kā arī adekvātu resursu piešķiršanu IS drošības un IS audita funkciju pilnvērtīgai nodrošināšanai.

23.2. IS drošības politikas mērķis ir definēt tirgus dalībnieka vadības nostāju un atbalstu IS drošības nodrošināšanai atbilstoši tirgus dalībnieka un tā klientu vajadzībām.

24. Normatīvi

24.1. Tirgus dalībnieks apstiprina hierarhiski strukturētu dokumentu kopumu, kas nosaka IS pārvaldību, t.sk. IS drošības pārvaldību un IS drošības pasākumu piemērošanas kārtību.

24.2. Tirgus dalībnieks dokumentē vismaz tos IS pārvaldības procesus, kuru neizpilde var radīt IS drošības riskus.

24.3. Tirgus dalībnieks nodrošina normatīvu aktualizāciju un pieejamību darbiniekiem.

24.4. Tirgus dalībnieks nosaka darbinieku atbildību par normatīvu neievērošanu.

25. IS drošības funkcija

25.1. Tirgus dalībnieks nodrošina IS drošības funkciju, lai realizētu risku kontroli un IS drošības pasākumu īstenošanu.

25.2. IS drošības funkcijas ietvaros tirgus dalībnieks nodrošina vismaz:

25.2.1. IS drošības normatīvu izstrādi un aktualizēšanu;

25.2.2. IS klasifikācijas un risku vadības procesa koordināciju;

25.2.3. vadības informēšanu par drošības līmeņa atbilstību prasībām un būtiskiem IS drošības incidentiem;

25.2.4. noteikto drošības pasākumu uzraudzību;

25.2.5. darbinieku apmācību un informēšanu IS drošības jomā;

25.2.6. IS drošības incidentu risināšanu un izmeklēšanu;

25.2.7. dalību IS darbības atjaunošanas un nepārtrauktības plānošanā.

25.3. Tirgus dalībnieks nodrošina IS drošības funkcijas neatkarību no IS izstrādes un uzturēšanas funkcijām. Ja par IS drošību atbildīgais darbinieks savus pienākumus veic darbu apvienošanas kārtībā, tad ievēro pienākumu nodalīšanas principu – darbu izpildītājs nedrīkst pats sevi kontrolēt.

26. IS audita funkcija

26.1. Tirgus dalībnieks nodrošina IS audita funkciju, lai nodrošinātu IS drošības pasākumu īstenošanas neatkarīgu pārbaudi.

26.2. Audita funkciju var nodrošināt arī ārpakalpojuma sniedzējs.

26.3. Tirgus dalībnieks līdz katra gada 1. martam iesniedz Finanšu un kapitāla tirgus komisijai iepriekšējā gadā veikto ar IS drošību saistīto auditu sarakstu, norādot auditu tēmas, mērķus un auditu veicēju.

27. Ārpakalpojumu vadība

27.1. Tirgus dalībnieka IT un IS pārvaldību, attīstību vai drošību var nodrošināt trešā persona – ārpakalpojuma sniedzējs.

27.2. Pirms lēmuma pieņemšanas par ārpakalpojumu iegādi tirgus dalībnieks veic risku izvērtēšanu.

27.3. IS drošības līmenis nedrīkst būt zemāks par šajos noteikumos un tirgus dalībnieka noteikto, ja IS attīsta vai uztur ārpakalpojuma sniedzējs.

27.4. Tirgus dalībnieks veic ārpakalpojumu uzraudzību. Ārpakalpojuma saņemšana neatbrīvo tirgus dalībnieku no normatīvajos aktos vai līgumā ar tā klientiem noteiktās atbildības – tas ir atbildīgs par ārpakalpojuma sniedzēja veikumu tādā pašā mērā kā par savu.

IV. Informācijas sistēmu resursu pārvaldība

28. Resursu piederība

28.1. Tirgus dalībnieks rakstveidā norīko IS resursu turētājus visiem informācijas un tehnoloģiskajiem resursiem.

28.2. Informācijas resursu turētāja pienākumi ir šādi:

28.2.1. klasificēt viņa turējumā esošos informācijas resursus;

28.2.2. piedalīties viņa turējumā esošo informācijas resursu un saistīto IS risku analizē;

28.2.3. apstiprināt pieejas tiesības IS;

28.2.4. apstiprināt IS izmaiņu veikšanu un ieviešanu;

28.2.5. noteikt prasības auditācijas pierakstu veidošanai;

28.2.6. sadarboties ar IS tehnoloģisko resursu turētāju IS funkcionalitātes un drošības jautājumos.

28.3. Tirgus dalībnieks nodrošina informācijas resursu turētāju apmācību to pienākumu izpildē.

28.4. Tehnoloģisko resursu turētāja pienākumi ir šādi:

28.4.1. nodrošināt tehnoloģisko resursu fizisko un loģisko aizsardzību;

28.4.2. sadarboties ar informācijas resursu turētāju, lai īstenotu viņa prasības par informācijas resursu aizsardzību un piekļuvi tiem;

28.4.3. piedalīties risku analizē, noteikt ar tehnoloģiskajiem resursiem saistītos IS apdraudējumus un novērtēt šo apdraudējumu īstenošanās varbūtību;

28.4.4. nodrošināt IS atjaunošanas procedūras, ja tehnoloģiskie resursi ir bojāti un IS funkcionēšana traucēta vai neiespējama;

28.4.5. sadarboties ar IS informācijas resursu turētāju IS funkcionalitātes un drošības jautājumos.

28.5. Resursu turētājs minētos pienākumus var uzdot pildīt resursu aizbildņiem – personām, kuras norīkojis resursu turētājs un kuras ikdienā ir atbildīgas par attiecīgajiem IS resursiem vai to daļu.

29. IS klasifikācija

29.1. Klasifikācijas mērķis ir novērtēt IS nozīmību un nodrošināt tās aizsardzību atbilstoši klasifikācijas līmenim. Tirgus dalībnieks veic visu IS klasificēšanu, nosakot IS konfidencialitātes, vērtības un pieejamības līmeni, un to dokumentē.

29.2. Konfidencialitātes līmeni IS tirgus dalībnieks piešķir atkarībā no kaitējuma, kas varētu tikt nodarīts informācijas devējam vai tirgus dalībniekam, ja tiktu pieļauts, ka šai IS piekļūst nepilnvarotas personas.

29.3. Vērtības līmeni IS tirgus dalībnieks piešķir atkarībā no kaitējuma, kas varētu tikt nodarīts informācijas devējam vai tirgus dalībniekam, ja netiktu nodrošināta IS integritāte.

29.4. Resursu pieejamības līmeni IS tirgus dalībnieks nosaka atkarībā no tirgus dalībnieka pamatdarbības vajadzībām (*business requirements*), ņemot vērā kaitējumu, kas varētu tikt nodarīts informācijas devējam vai tirgus dalībniekam, ja netiktu nodrošināta IS resursu pieejamība, un nosaka pieļaujamo laiku, kādu IS var nebūt pieejama (*Recovery Time Objective*), un pieļaujamo laika periodu, par kuru datus var zaudēt (*Recovery Point Objective*).

29.5. Tirgus dalībnieks pielieto IS klasifikācijas shēmu, kura atbilst šiem noteikumiem un kurā ir vismaz divi katras klasifikācijas kategorijas līmeņi.

29.6. Tirgus dalībnieks atbilstoši informācijas klasifikācijas līmenim nosaka klasificētas informācijas lietošanas un aizsardzības prasības.

V. Risku analīze un pārvaldība

30. Risku analīzes un pārvaldības mērķi ir:

30.1. noteikt pieļaujamo jeb akceptējamo risku lielumu (risku limitu);

30.2. novērtēt IS apdraudējuma īstenošanās varbūtību, kurā IS apdraudējums ir ar nodomu (tīši) vai aiz neuzmanības izdarīta darbība vai bezdarbība, vai iespējams notikums, kas var izraisīt IS drošības incidentu;

30.3. novērtēt iespējamo kaitējumu informācijas devējam, tirgus dalībniekam vai citai personai, ja nav nodrošināta IS drošība;

30.4. noteikt atbilstošos un nepieciešamos drošības pasākumus, ja risks ir nepieņemams;

30.5. akceptēt pēc drošības pasākumu īstenošanas atlikušo risku (atbilstību noteiktajam risku limitam).

31. Risku analīze ir regulārs process. Tirgus dalībnieks to veic visā IS dzīves ciklā, t.sk. sākot IS projektu, veicot nozīmīgas IS izmaiņas, parādoties jauniem būtiskiem apdraudējumiem, īstenojoties nozīmīgiem incidentiem vai pieaugot to kopējam skaitam.

32. Tirgus dalībnieks risku analīzi veic, lietojot tā apstiprināto metodiku. Tirgus dalībnieks lieto tādu risku analīzes metodiku, kas ļauj efektīvi realizēt šo noteikumu 30. punktā noteiktos mērķus.

33. Tirgus dalībnieks plāno un īsteno drošības pasākumus, ja risku analīzē novērtētais risks ir nepieņemams, un plānotajiem drošības pasākumiem nosaka realizācijas prioritātes, termiņus un atbildīgos.

34. Drošības pasākumu mērķis ir samazināt atlikušo risku līdz pieņemamam līmenim. Tirgus dalībnieks drošības pasākumus nosaka, pamatojoties uz to izmaksu un iespējamo zaudējumu samērojamību.

VI. Personāla loma informācijas sistēmu drošībā

35. Tirgus dalībnieks risku pārvaldīšanas ietvaros veic pasākumus, kas ierobežo no darbinieku darbības vai bezdarbības izrietošos IS drošības riskus, kā arī nosaka darbinieku lomu IS drošības pasākumos un veicina personāla izpratni par IS lietošanas kārtību un aizsardzības nepieciešamību.

36. Tirgus dalībnieks nodrošina, ka IS lietotāju zināšanu līmenis ir atbilstošs IS lietošanas vajadzībām.

37. Tirgus dalībnieks pirms darba pienākumu izpildes iepazīstina darbiniekus ar IS darbību reglamentējošajiem dokumentiem.

38. Tirgus dalībnieks nosaka IS lietotāja:

38.1. atbildību par IS darbību reglamentējošo dokumentu neievērošanu;

38.2. atbildību par visām darbībām, kuras IS ir veiktas ar viņa lietotāja vārdu;

38.3. pienākumu ievērot konfidencialitātes saistības attiecībā uz datiem, kuri nonāk šīs personas rīcībā, veicot darba pienākumus;