**Izdevējs: Finanšu un kapitāla tirgus komisija**
**Veids: noteikumi**
**Numurs: 158**
**Pieņemts: 26.09.2018.**
**Stājas spēkā: 05.10.2018.**

**Publicēts:**
**Latvijas Vēstnesis, 196 (6282), 04.10.2018.**
**OP numurs: 2018/196.34**

**Finanšu un kapitāla tirgus komisijas normatīvie noteikumi Nr. 158**

Rīgā 2018. gada 26. septembrī

(Finanšu un kapitāla tirgus komisijas padomes sēdes protokols Nr. 44 5. p.)

# Informācijas sistēmu drošības normatīvie noteikumi

*Izdoti saskaņā ar Finanšu un kapitāla tirgus komisijas likuma 7. panta pirmās daļas 1. punktu, Kredītiestāžu likuma 34.[1] panta otro daļu un 50. panta trešo daļu, Maksājumu pakalpojumu un elektroniskās naudas likuma 45. panta pirmo daļu un 104.[1] panta piekto daļu, Finanšu instrumentu tirgus likuma 123.[5] panta otro daļu, 124. panta 1.[1] daļu un likuma "Par privātajiem pensiju fondiem" 28. panta sesto daļu*

## I. Vispārīgie jautājumi

1. "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, elektroniskās naudas iestādēm, apdrošināšanas sabiedrībām, apdrošināšanas starpniekiem, privātajiem pensiju fondiem, regulētā tirgus organizētājiem, vērtspapīru centrālajam depozitārijam, ieguldījumu brokeru sabiedrībām, ieguldījumu pārvaldes sabiedrībām un alternatīvo ieguldījumu fondu pārvaldniekiem.

2. Noteikumu mērķis ir ierobežot tirgus dalībnieku darbībai un klientiem sniegto pakalpojumu nodrošināšanai izmantojamo informācijas sistēmu (tālāk tekstā arī – IS) riskus, kopumā tiecoties uz piesardzīgu informācijas sistēmu risku pārvaldības līmeni (risku apetīti), kā arī noteikt vienoti strukturētas prasības tirgus dalībnieku IS drošības risku pārvaldībai.

3. Tirgus dalībnieks, ieviešot drošības pasākumus, ievēro proporcionalitātes principu un risku pārvaldībā balstītu pieeju, ņemot vērā darbības jomu, darbinieku skaitu, sniegto pakalpojumu veidu, kā arī to sarežģītību un kopējo informācijas tehnoloģiju (tālāk tekstā – IT) izmantošanas līmeni.

## II. Termini

4. Auditācijas pieraksti – analīzei pieejami pieraksti, kuros reģistrēti dati par noteiktiem notikumiem IS (piekļuve, datu ievade, maiņa, dzēšana, izvade u.c.).

5. Drošības pasākumi – tehniski vai organizatoriski pasākumi, kas tiek noteikti risku pārvaldības ietvaros un samazina IS risku līdz pieļaujamajam līmenim.

6. Ievainojamība – IS nepilnība, kas ļauj kādam noteiktam apdraudējumam īstenoties un ietekmēt IS drošību.

7. Informācijas sistēma – datu ievades, uzglabāšanas un apstrādes sistēma, kas nodrošina noteikto funkciju izpildi un paredz lietotājpieeju tajā glabātajiem datiem vai informācijai.

8. Informācijas konfidencialitāte – piekļuves nodrošināšana informācijai tikai pilnvarotām personām vai procesiem.

9. Informācijas integritāte – informācijas un tās apstrādes metožu precizitāte, pareizība un pilnīgums.

10. Informācijas pieejamība – iespēja pilnvarotām personām lietot IS noteiktā laikā un vietā.

11. 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.

12. Informācijas resursu turētājs – persona, kas ir atbildīga par informācijas resursiem un rīkojas ar tiem tirgus dalībnieka uzdevumā.

13. Stingrā autentifikācija – autentifikācija, kas sastāv no diviem vai vairākiem elementiem, ko klasificē kā zināšanas (to, ko zina tikai maksājumu pakalpojumu izmantotājs, piemēram, parole, PIN), valdījumu (to, kas ir tikai maksājumu pakalpojumu izmantotāja valdījumā, piemēram, kodu kalkulators, mobilā ierīce) un neatņemamas īpašības (maksājumu pakalpojumu izmantotājam raksturīgas īpašības, piemēram, pirkstu nospiedums), un kas ir savstarpēji neatkarīgi, proti, viena elementa uzticamības zaudēšanas gadījumā cita elementa uzticamība netiek apdraudēta, un kas ir izstrādāti tā, lai nodrošinātu autentifikācijas datu konfidencialitātes aizsardzību.

14. IS drošība – IS konfidencialitātes, integritātes un pieejamības prasību nodrošināšana.

15. IS drošības incidents – notikums vai vairāki saistīti notikumi, kurus tirgus dalībnieks nav plānojis un kuri negatīvi ietekmē vai, iespējams, ietekmēs IS drošību.

16. IS lietotājs – persona, kura piešķirto pilnvaru robežās lieto IS.

17. 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.

18. Tehnoloģiskie resursi – IS sastāvdaļa, kurā ietilpst sistēmprogrammas, lietojumprogrammas, palīgprogrammas, sistēmfaili, datori, datortīkli, aparatūra un citas iekārtas, kas nodrošina IS darbību.

19. Tehnoloģisko resursu turētājs – persona, kas ir atbildīga par tehnoloģiskajiem resursiem un rīkojas ar tiem tirgus dalībnieka uzdevumā.

## III. Informācijas sistēmu drošības organizēšana

20. Vadības atbildība un atbalsts

20.1. 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.

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

21. Normatīvi

21.1. Tirgus dalībnieks apstiprina hierarhiski strukturētu dokumentu kopumu, kas nosaka IS pārvaldību, t.sk. IS drošības pārvaldību. Definējot IS drošības pārvaldību, nosaka IS drošības mērķus, lomas, atbildību un IS drošības pasākumu piemērošanas kārtību.

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

21.3. Tirgus dalībnieks nodrošina normatīvu aktualizāciju un pieejamību darbiniekiem.

21.4. Tirgus dalībnieks nosaka darbinieku atbildību par normatīvu neievērošanu.

21.5. Tirgus dalībnieks izveido un uztur aktuālu informācijas plūsmas shēmu.

22. IS drošības jeb IS risku pārvaldības funkcija (tālāk tekstā – IS drošības funkcija)

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

22.2. IS drošības funkcijas ietvaros tirgus dalībnieks nodrošina vismaz:

22.2.1. IS drošības normatīvu izstrādi un aktualizēšanu;

22.2.2. IS klasifikācijas un risku vadības procesa koordināciju un apdraudējumu identifikāciju;

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

22.2.4. noteikto drošības pasākumu uzraudzību;

22.2.5. darbinieku apmācību un informēšanu IS drošības jomā;

22.2.6. IS drošības incidentu pārvaldību;

22.2.7. dalību IS darbības atjaunošanas un nepārtrauktības plānošanā.

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

23. IS audita funkcija

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

23.2. Audita funkciju var nodrošināt arī ārpakalpojuma sniedzējs.

24. Ārpakalpojumu vadība

24.1. Tirgus dalībnieks var izmantot trešās personas – ārpakalpojuma sniedzēja – pakalpojumus. Tirgus dalībnieks veic visu izmantoto ārpakalpojumu uzskaiti.

24.2. 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. IS drošības līmenis, ja IS attīsta vai uztur ārpakalpojuma sniedzējs, nav zemāks par tirgus dalībnieka noteikto.

24.3. Pirms lēmuma pieņemšanas par ārpakalpojumu iegādi tirgus dalībnieks izvērtē piegādātājus un, ņemot vērā prasības pakalpojuma kvalitātei un drošībai, tostarp pieejamībai, izvērtē riskus, kā arī nosaka pakalpojuma izbeigšanas stratēģiju.

24.4. Tirgus dalībnieks izveido un regulāri atjaunina visu izmantoto ārpakalpojumu sarakstu un veic ārpakalpojumu uzraudzību, kontrolējot to atbilstību drošības un darbības mērķiem. Tirgus dalībnieks līgumā ar ārpakalpojumu sniedzēju ietver prasības ārpakalpojuma kontrolei, piemēram, skaidru pakalpojuma aprakstu, drošības prasības, konfidencialitātes saistības, tiesības saņemt pakalpojuma uzraudzībai nepieciešamo informāciju, prasību ārpakalpojumu sniedzējam nekavējoties ziņot par incidentiem, tiesības pārtraukt līgumu.

24.5. Izmantojot ārpakalpojumus, t.sk. mākoņskaitļošanu, tirgus dalībniekam ir pienākums saglabāt nepieciešamo kontroli pār informācijas resursiem, kas satur informāciju par tirgus dalībnieka klientiem. Tirgus dalībnieka klasificētas IS drošā veidā ir fiziski vai loģiski jānošķir no ārpakalpojuma sniedzēja citu klientu IS. Jāsagatavo un regulāri jāaktualizē pakalpojuma pārtraukšanas plāns, paredzot datu, programmatūras un tehnisko resursu atpakaļnodošanu un klientu informācijas dzēšanu pie pakalpojuma sniedzēja.

24.6. Tirgus dalībnieks veic ārpakalpojumu kvalitātes uzraudzību un drošības kontroli, t.sk. saņem pārskatus par pakalpojuma kvalitāti un incidentiem.

24.7. Tirgus dalībniekam, ja tas sniedz ārpakalpojumu trešajai pusei, izmantojot savas IS, tostarp autentifikācijas ārpakalpojumu, ir pienākums kontrolēt risinājuma ieviešanu trešās puses uzņēmumā. Tirgus dalībnieks informē sadarbības partnerus par riskiem, kas saistīti ar šādu pakalpojumu izmantošanu. Drošības prasību neizpildes gadījumā tirgus dalībniekam ir pienākums pārtraukt sadarbību.

## IV. Informācijas sistēmu resursu pārvaldība

25. Resursu piederība

25.1. Tirgus dalībnieks rakstveidā norīko IS resursu (informācijas un tehnoloģisko resursu) turētājus visiem informācijas un tehnoloģiskajiem resursiem.

25.2. Informācijas resursu turētāja pienākumi ir šādi:

25.2.1. klasificēt viņa turējumā esošos informācijas resursus;

25.2.2. piedalīties viņa turējumā esošo informācijas resursu un saistīto IS risku analīzē un to apstiprināt;

25.2.3. apstiprināt pieejas tiesības IS;

25.2.4. apstiprināt IS izmaiņu veikšanu un ieviešanu;

25.2.5. noteikt prasības auditācijas pierakstu veidošanai;

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

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

25.4. Tehnoloģisko resursu turētāja pienākumi ir šādi:

25.4.1. nodrošināt tehnoloģisko resursu fizisko un loģisko aizsardzību;

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

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

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

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

25.5. 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.

26. IS un IT klasifikācija

26.1. Tirgus dalībnieks izveido un regulāri atjaunina IS vai IT pakalpojumu sarakstu un veic to klasifikāciju.

26.2. Klasifikācijas mērķis ir novērtēt IS un/vai IT pakalpojumu nozīmību un nodrošināt to aizsardzību atbilstoši pakalpojuma nozīmībai un piemērojamajiem operacionālajiem un drošības riskiem. Tirgus dalībnieks veic klasificēšanu, nosakot konfidencialitātes, vērtības un pieejamības līmeni.

26.3. Tirgus dalībnieks regulāri pārvērtē IS un/vai IT pakalpojumu klasifikāciju.

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

## V. Risku analīze un pārvaldība

27. Tirgus dalībnieks pastāvīgi uzrauga apdraudējumus un ievainojamības un regulāri pārskata tos riska scenārijus, kas ietekmē IS un/vai IT pakalpojumus. IS risku pārvaldība ir integrēta uzņēmuma kopējā risku pārvaldības ietvarā.

28. Risku analīzes un pārvaldības mērķi ir:

28.1. noteikt pieļaujamo jeb akceptējamo risku lielumu (risku limitu jeb apetīti);

28.2. novērtēt IS apdraudējuma un ievainojamības īstenošanās varbūtību atbilstoši dažādiem riska scenārijiem;

28.3. novērtēt iespējamo kaitējumu vai ietekmi uz tirgus dalībnieku, klientu vai citu personu, ja nav nodrošināta IS drošība;

28.4. noteikt papildu drošības pasākumus, ja risks ir nepieņemams;

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

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

30. Tirgus dalībnieks risku analīzi veic, lietojot tā apstiprināto metodiku, kas nosaka arī risku analīzes regularitāti. Tirgus dalībnieks lieto tādu risku analīzes metodiku, kas ļauj efektīvi realizēt šo noteikumu 28. punktā noteiktos mērķus.

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

32. 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

33. 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.

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

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

36. Tirgus dalībnieks nosaka IS lietotāja:

36.1. atbildību par IS darbību reglamentējošo dokumentu neievērošanu;

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

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

36.4. pienākumu informēt atbilstošo personu (piemēram, IS drošības vadītāju) par IT drošības incidentiem un apdraudējumiem.

37. Drošības apzināšanās veicināšana

37.1. Tirgus dalībnieks regulāri veic plānveida pasākumus, kas sekmē katra darbinieka izpratni par IS aizsardzību un veicina darbinieku kopējo IS drošības apzināšanos (*security awareness*).

37.2. Tirgus dalībnieks nosaka, kā un cik bieži darbinieki tiek informēti un apmācīti par IS drošības jautājumiem.

37.3. Tirgus dalībnieks veic darbinieku apmācību klasificētas informācijas aizsardzībā.

## VII. Fiziskās un vides drošības pārvaldība

38. Tirgus dalībnieks risku pārvaldīšanas ietvaros veic IS fiziskās aizsardzības pasākumus, kas aizsargā no nevēlamiem apkārtējās vides (ugunsgrēks, plūdi, temperatūras svārstības u.c.), tehniskajiem (neatbilstoša elektroenerģijas padeve, elektromagnētiskā lauka iedarbība u.c.) un cilvēkfaktoriem (tīši vai netīši bojājumi, zādzība u.c.).

39. IS infrastruktūras (tehnoloģisko resursu, t.sk. serveru, disku masīvu, datortīkla iekārtu un kabeļu u.c., izņemot gala lietotāju tehnoloģiskos resursus) fiziskā aizsardzība

39.1. Tirgus dalībnieks IS infrastruktūru ekspluatē ierobežotas pieejas telpās, kuru fiziskā aizsardzība nodrošina tikai pilnvarotu personu piekļuvi. Ja to nosaka tehnoloģiska nepieciešamība, tad, ekspluatējot ārpus ierobežotas pieejas telpām, IS tehnoloģiskos resursus fiziski norobežo. IS infrastruktūras telpas izvieto ēkas vietās, kurās ir mazāka apdraudējumu īstenošanās iespējamība.

39.2. Tirgus dalībnieks nosaka, kuras personas drīkst iekļūt šo noteikumu 39.1. punktā minētajās telpās, un to piekļuvi reģistrē. Šo personu sarakstā iekļauj tikai tās personas, kurām darba pienākumu izpildei nepieciešama fiziska piekļuve IS infrastruktūrai.

39.3. Trešās personas IS infrastruktūras telpās drīkst uzturēties tikai to personu klātbūtnē, kurām ir tiesības piekļūt IS infrastruktūras telpām.

39.4. Tirgus dalībnieks nodrošina IS infrastruktūras telpu mikroklimatu (mitrumu, temperatūru u.tml.) atbilstoši IS infrastruktūras darbināšanai izmantotās aparatūras ražotāju noteiktajām prasībām.

39.5. Tirgus dalībnieks aprīko IS infrastruktūras telpas ar apsardzes signalizāciju un vides detektoriem.

39.6. Tirgus dalībnieks tehnoloģiskos resursus administrējošā personāla darba vietas nodala ierobežotas pieejas telpās.

40. Datu nesēju fiziskā aizsardzība

40.1. Tirgus dalībnieks veic nepieciešamos drošības pasākumus datu nesēju fiziskai aizsardzībai atkarībā no IS klasifikācijas, bet neatkarīgi no to veida (t.sk. demontētas disku iekārtas, papīra izdrukas, zibatmiņas kartes u.tml.).

40.2. Tirgus dalībnieks nosaka kārtību, kādā lieto, glabā un drošā veidā iznīcina datu nesējus.

40.3. Tirgus dalībnieks datu nesēju aizsardzības ietvaros veic datu izvades iekārtu fizisko aizsardzību, novēršot nesankcionētu informācijas resursu iegūšanu (piemēram, printeru iekārtu aizsardzība, saskarņu lietošanas ierobežošana).

40.4. Ja datu nesēju, kas satur nepubliskojamus IS resursus, ir paredzēts iznīcināt, tad tirgus dalībnieks to dara tādā veidā, lai nebūtu iespējams veikt datu atjaunošanu.

41. Tirgus dalībnieks veic papildu fiziskās aizsardzības pasākumus atkarībā no IS klasifikācijas līmeņa. Nepieciešamības gadījumā fiziskās aizsardzības pasākumus drīkst kompensēt ar loģiskās aizsardzības (programmatūras un procesu) līdzekļiem.

## VIII. Informācijas sistēmu pieejas tiesību pārvaldība

42. Jauna IS lietotāja reģistrāciju, tiesību piešķiršanu, anulēšanu un bloķēšanu tirgus dalībnieks veic saskaņā ar dokumentētu pieprasījumu, kuru apstiprina informācijas resursu turētājs. Dokumentēšanas metodei jānodrošina iespēja veikt efektīvu aktuālo pieejas tiesību kontroli.

43. Katram tirgus dalībnieka IS lietotājam un administratoram tiek piešķirts unikāls lietotāja kods.

44. Lietotāja autentiskuma noteikšana

44.1. Lietotāja autentiskuma noteikšanas mērķis ir pārliecināties, ka klasificētu IS lieto pilnvarotais lietotāja koda īpašnieks.

44.2. Tirgus dalībnieks nosaka autentifikācijas līdzekļu (piemēram, paroļu, kodu kalkulatoru, privāto atslēgu, biometrisko līdzekļu u.c.) lietošanas kārtību, t.sk. paroļu politiku (paroles garumu, sarežģītību, derīguma termiņu, atkārtojamības ierobežojumu).

44.3. IS paroles glabā šifrētā veidā. Ievadot paroli, tā nedrīkst būt salasāma uz ekrāna. Paroli nekavējoties nomaina, ja tā varētu būt vai ir nesankcionēti kļuvusi zināma citai personai.

44.4. Izveidojot, piegādājot un aktivizējot autentifikācijas līdzekli, tirgus dalībnieks nodrošina, ka tas lietošanai ir pieejams vienīgi attiecīgā lietotāja koda īpašniekam (t.sk. drošs personalizācijas un lietotāja paroles izveides process).

44.5. Ja tirgus dalībnieka lietotās tehnoloģijas to pieļauj, papildus iebūvētam administratora kontam tirgus dalībnieks izveido individuālu kontu katram administratoram, kurš tiek izmantots ikdienas IS uzturēšanas darbu veikšanai. IS administratoru kodu un paroļu kopijas glabā drošā ierobežotas pieejas vietā ārpus datortīklam pievienotajiem tehnoloģiskajiem resursiem.

45. Pieejas tiesības IS tirgus dalībnieks nosaka saskaņā ar dokumentēti apstiprinātām lomām vai lietotāju profiliem. IS lietotājam piešķir pieeju tikai tai informācijai un funkcijām, kas ir nepieciešamas viņa pienākumu izpildei.

46. Veidojot IS administratoru kontus, papildus mazāko privilēģiju *(least priviledge)* principam izmanto metodes, lai nodalītu augstu privilēģiju kontus un ierobežotu to lietošanu ikdienas darbību veikšanai.

47. Veidojot kontus dažādu tehnoloģisku procesu veikšanai, piemēram, rezerves kopēšanai, kontam piešķirtās privilēģijas tiek ierobežotas tikai līdz procesa veikšanai nepieciešamajām.

48. IS administratoriem, izmantojot paaugstinātu privilēģiju lietotāju kontus, droši nodala pieeju kritisko sistēmu administrēšanas videi no publiskā tīkla, piemēram, interneta pārlūkošanas vides.

49. IS lietotāja vai administratora darba pienākumu maiņas vai darba attiecību izbeigšanas gadījumā tirgus dalībnieks nekavējoties maina vai bloķē IS lietotāja un administratora tiesības.

50. Tirgus dalībnieks regulāri veic aktuālo pieejas tiesību pārbaudi, lai kontrolētu šo noteikumu 45.–49. punktā noteikto prasību ievērošanu.

## IX. Komunikāciju un operāciju pārvaldība

51. Darbiniekiem, kas veic IS uzturēšanu, tirgus dalībnieks nosaka pienākumus un atbildību un nodrošina aizstājamību un kvalifikācijas uzturēšanu. Procesu kontroles nodrošināšanai veic pienākumu nodalīšanu.

52. Konfigurācijas pārvaldība un kontrole

52.1. Tirgus dalībnieks veic tehnoloģisko resursu un to aktuālo konfigurāciju uzskaiti.

52.2. Tirgus dalībnieks nosaka kārtību, kādā pieprasa, autorizē, testē, maina un dokumentē tehnoloģiskos resursus.

52.3. Tirgus dalībnieks risku kontroles ietvaros uztur un kontrolē IS konfigurāciju, ņemot vērā drošības prakses ieteikumus (*hardening standards*) un zināmās sistēmu ievainojamības, kā arī veic konfigurāciju integritātes pārbaudes.

52.4. Tirgus dalībnieks risku kontroles ietvaros veic nepieciešamās un tehnoloģiski iespējamās izmaiņas tehnoloģisko resursu standarta konfigurācijā un samazina funkcionalitāti līdz nepieciešamajam apjomam.

52.5. Tirgus dalībnieks savlaicīgi veic nepieciešamos IS standarta programmatūras atjaunināšanas darbus (t.sk. drošības labojumu uzstādīšanu).

53. Datortīklu aizsardzība

53.1. Tirgus dalībnieks iekšējo datortīklu nodala no ārējā datortīkla. Datu plūsmā starp iekšējo un ārējo datortīklu atļauj tikai tos pakalpojumus, kas ir nepieciešami tirgus dalībnieka funkciju izpildei.

53.2. Tirgus dalībnieks izveido un uztur aktuālu datortīkla un pieslēgumu shēmu.

53.3. Tirgus dalībnieks regulāri pārbauda visu ārējo savienojumu eksistenci un pārliecinās, ka pastāv tikai tie savienojumi, kuri atbilst tirgus dalībnieka darbības vajadzībām.

53.4. Tirgus dalībnieks risku kontroles ietvaros realizē nepieciešamos un iespējamos papildu datu plūsmas ierobežojumus (t.sk. lietojumprogrammu, vietņu ierobežošanu) starp iekšējo un ārējo datortīklu.

53.5. Tirgus dalībnieks veic datortīkla monitoringu un ievainojamības (t.sk. kaitīgo programmu) kontroli.

53.6. Ja IS administrēšana tiek veikta no attālinātas vietas, tirgus dalībnieks lieto kriptogrāfijas līdzekļus (piemēram, virtuālo privāto tīklu (*VPN*)) un stingro autentifikāciju.

53.7. Ja tiek lietotas bezvadu datu pārraides tehnoloģijas, tirgus dalībnieks risku pārvaldības ietvaros veic to papildu aizsardzību, lai nodrošinātu vienīgi autorizētu IS lietošanu.

54. Personālo datoru un ierīču aizsardzība

54.1. Tirgus dalībnieks nosaka, kādus informācijas resursus drīkst glabāt un kā tos aizsargāt individuālās lietošanas datu apstrādes iekārtās, t.sk. galda un portatīvajā datorā (tālāk tekstā – personālais dators), viedtālrunī, planšetdatorā u.tml.

54.2. Personālajā datorā tiek uzstādīta un lietota tikai tā programmatūra un tādā konfigurācijā, kādu noteicis tirgus dalībnieks, kurš arī nosaka kārtību un veic pasākumus aizsardzībai pret kaitīgām programmām, izmantojot, piemēram, antivīrusu programmatūru, *software restriction policy*.

54.3. Personālā datora funkcionalitāti tirgus dalībnieks ierobežo līdz darba vajadzībām nepieciešamajam funkciju līmenim, t.sk. kontrolē datora portu izmantošanu un iekārtu pieslēgšanu, kontrolē pieeju publiskā tīkla informācijai (*blacklisting*, *whitelisting*) un loģiski nodala pieeju publiskā tīkla (interneta) informācijai no organizācijas iekšējām IS, izmantojot, piemēram, virtualizāciju.

54.4. Personālais dators tiek pieslēgts tikai tirgus dalībnieka noteiktiem datortīkliem.

54.5. Tirgus dalībnieks nodrošina, ka, lietotājam atstājot personālo datoru bez uzraudzības, atsākt IS lietošanu vai pieslēgties tirgus dalībnieka datortīklam iespējams tikai tad, ja ir veikta lietotāja autentifikācija.

54.6. Izmantojot personālos datorus, kuriem ir pastiprināti fiziskās drošības apdraudējumi, t.sk. portatīvās ierīces, kuras lieto ārpus tirgus dalībnieka telpām, klasificētā informācija tiek pārraidīta un glabāta šifrētā veidā.

54.7. Tirgus dalībnieks veic visu tā rīcībā esošo personālo datoru, kurus paredzēts lietot ārpus tirgus dalībnieka telpām, uzskaiti, lai noteiktu, kura persona lieto attiecīgo iekārtu.

54.8. Ja tirgus dalībnieks ļauj darbiniekiem darba vajadzībām lietot viņiem piederošus personālos datorus, tas nosaka lietošanas kārtību. Šī kārtība nedrīkst samazināt noteikto IS aizsardzības līmeni.

54.9. Ja tiek sniegta attālināta pieeja tirgus dalībnieka IS, izmantojot viedtālruni vai planšetdatoru, šo ierīču drošību aizsargā, lai incidenta gadījumā tiktu novērsta klientu vai tirgus dalībnieka sensitīvu datu nokļūšana trešo pušu rīcībā (piemēram, aizsargāta pieeja ierīcei, dati ierīcē netiek glabāti vai pēc sesijas tiek automātiski dzēsti).

55. Datu rezerves kopēšana

55.1. Lai ierobežotu integritātes un pieejamības riskus, tirgus dalībnieks veic datu rezerves kopēšanu.

55.2. Tirgus dalībnieks izstrādā dokumentētu datu rezerves kopiju veidošanas kārtību, nosakot, kāda tehnoloģija un darbības ir noteiktas datu rezerves kopiju izgatavošanai un informācijas atjaunošanai, kā arī nosaka, cik bieži un kādā apjomā tiek veidotas datu rezerves kopijas, ņemot vērā pieļaujamo laiku, kādu IS var nebūt pieejama (*Recovery Time Objective*), un laika periodu, par kuru datus var zaudēt (*Recovery Point Objective*), kā arī cik bieži tiek veikta kopiju un atjaunošanas procedūru pārbaude.

55.3. Tirgus dalībnieks nodrošina, ka vismaz tām IS, kuras nodrošina tirgus dalībniekam vai tā klientiem būtiskus pakalpojumus, datu rezerves kopēšanu veic ar metodi, kas minimizē riskus (no IS fiziski vai loģiski nodalīti datu nesēji). Datu rezerves kopijas glabā no IS ģeogrāfiski nošķirtā vietā.

55.4. Tirgus dalībnieks aizsargā datu rezerves kopijas pret nesankcionētu lietošanu un bojāšanu.

56. IS pārraudzība

56.1. Tirgus dalībnieks IS pārraudzībai nosaka vismaz šādus mērķus – veikt preventīvās darbības IS drošības uzturēšanai un savlaicīgu incidentu identificēšanu. Pārraudzības pasākumi tiek piemēroti atbilstoši IS klasifikācijai.

56.2. Tirgus dalībnieks pastāvīgi veic IS pārraudzību:

56.2.1. savlaicīgi identificējot gan iekšējo, gan ārējo apdraudējumu;

56.2.2. identificējot sistēmu ievainojamību un veicot to novēršanu;

56.2.3. uzraugot neautorizētu iekārtu un programmatūras lietošanu un veicot tās novēršanu;

56.2.4. uzraugot IS administratoru piekļuvi sistēmām un reģistrējot veiktās darbības;

56.2.5. kontrolējot ārpakalpojumu sniedzēju piekļuvi IS;

56.2.6. pārraugot IS, iekārtu un procesu pieejamību.

57. Auditācijas pierakstu pārvaldība

57.1. Lai identificētu lietotāju veiktās darbības un IS kļūdas, tirgus dalībnieks veido, uzglabā un analizē auditācijas pierakstus.

57.2. Auditācijas pierakstos tirgus dalībnieks iekļauj vismaz visu veiksmīgas un neveiksmīgas pieslēgšanās gadījumu laiku un lietotāju kodus. Papildu auditācijas pierakstus veic par IS parametru maiņu, t.sk. par darbībām ar lietotāju kontiem, ciktāl to var nodrošināt ar lietoto tehnoloģisko risinājumu.

57.3. Tirgus dalībnieks lieto metodes un rīkus, kas ļauj efektīvi analizēt auditācijas pierakstus. Šie rīki ir pieejami tikai autorizētam personālam.

57.4. Tirgus dalībnieks nodrošina auditācijas pierakstu integritāti.

57.5. Tirgus dalībnieks sinhronizē visu to IS laika uzskaiti, kuras ir savstarpēji saistītas datu apmaiņā vai transakciju apstrādē.

58. Kriptogrāfijas līdzekļu lietošana

58.1. Tirgus dalībnieks atkarībā no informācijas resursu konfidencialitātes līmeņa lieto kriptogrāfijas līdzekļus.

58.2. Tirgus dalībnieks nosaka kriptogrāfijas līdzekļu lietošanas kārtību, kā arī veic to aizsardzību.

## X. Attālināto pakalpojumu drošības pārvaldība

59. Tirgus dalībnieks, klientiem piedāvājot attālinātos pakalpojumus, nodrošina pakalpojumu drošības pārvaldību, lai minimizētu klientu riskus.

60. Klienta autentifikācijas līdzekļi (rīki, programmatūra) tiek pieprasīti, piegādāti un aktivizēti drošā veidā. Tirgus dalībnieks veic klienta identifikāciju un citus nepieciešamos pasākumus, lai attālināto pakalpojumu autentifikācijas līdzekli saņemtu tikai tā īpašnieks.

61. Maksājumu pakalpojumu sniedzējam ir pienākums piemērot stingro autentifikāciju, kad klients tiešsaistē piekļūst maksājumu kontam, ierosina maksājumu, piekļūst vai izmaina sensitīvus maksājuma datus, tostarp uzticamu maksājumu saņēmēju sarakstu, izmantojot attālināto pakalpojumu.

62. Maksājumu pakalpojumu sniedzēji var izmantot alternatīvus klienta autentifikācijas pasākumus:

62.1. maksājumiem, kas tiek veikti uzticamam saņēmējam, kurš iekļauts apstiprināto maksājumu sarakstā (*white list*);

62.2. darījumiem starp viena klienta diviem kontiem, kurus uztur viens un tas pats maksājumu pakalpojumu sniedzējs;

62.3. pārvedumiem viena un tā paša maksājumu pakalpojumu sniedzēja ietvaros, ja šādu iespēju pieļauj maksājumu pakalpojumu sniedzēja veiktais risku novērtējums;

62.4. maza apmēra maksājumiem ne vairāk kā 30 *euro* apmērā, ja iepriekšējo attālināti veikto elektronisko maksājumu darījumu, kurus maksātājs iniciējis kopš pēdējās stingrās autentifikācijas izmantošanas, kopējā summa nepārsniedz 100 *euro*.

63. Maksājumu pakalpojumu sniedzēja izsniegtajām maksājumu kartēm jāatbalsta kartes turētāja stingrā autentifikācija darījumiem internetā.

64. Maksājumu pakalpojumu sniedzēji izmanto darījumu uzraudzības un pārraudzības risinājumus, kas paredzēti, lai novērstu, atklātu un bloķētu krāpnieciskus maksājumus, pirms maksājumu pakalpojumu sniedzējs tos ir autorizējis. Aizdomīgiem vai augsta riska darījumiem piemēro īpašu uzraudzības un izvērtēšanas procesu.

65. Maksājumu pakalpojumu sniedzējs nosaka maksājumu limitus. Maksājumu pakalpojumu sniedzējs var vienoties ar klientu par klientu riska profilam atbilstošu maksājumu limitu katram maksājuma instrumentam. Maksātājam tiek nodrošināta iespēja koriģēt šos ierobežojumus līdz maksimālajai robežai, par kuru ir notikusi vienošanās.

66. Maksājumu pakalpojumu sniedzēji nodrošina klientiem iespēju saņemt brīdinājumus par ierosinātiem maksājumiem un neveiksmīgiem mēģinājumiem ierosināt maksājumu, kas ļauj klientiem konstatēt krāpniecisku vai ļaunprātīgu sava konta izmantošanu.

67. Pārsūtot klienta datus, tos aizsargā ar kriptogrāfijas līdzekļiem. Pārsūtot klienta datus, tos var nešifrēt, ja informācija nesatur cita klienta datus un klients akceptē iespējamos riskus.

68. Tirgus dalībnieks lieto vismaz viena faktora klienta autentifikāciju, ja:

68.1. pakalpojums ļauj skatīt tikai to informāciju par klienta kontu, kas neietver trešo personu datus, t.sk. konta atlikumu, darījumu vēsturi, konta numuru;

68.2. pakalpojums ietver finanšu instrumentu izmantošanu (pirkšana/pārdošana).

69. Klienta lietotāja piekļuve tiek bloķēta ne vairāk kā pēc pieciem neveiksmīgiem autentifikācijas mēģinājumiem. Lietotāja piekļuve atkārtoti tiek aktivizēta drošā veidā.

70. Klienta neaktīva sesija tiek bloķēta ne vēlāk kā pēc piecpadsmit minūtēm.

71. Tirgus dalībnieks klientu drošības apzināšanās programmas ietvaros nodrošina klientiem pilnvērtīgu informāciju par attālināto pakalpojumu lietošanas riskiem un informāciju par to, kā droši un efektīvi lietot IS. Tirgus dalībnieks, pirms klientam sniedz pieeju attālinātiem pakalpojumiem un arī turpmāk, regulāri sadarbības laikā informē klientu par tirgus dalībnieka un klienta tiesībām un atbildību, pakalpojuma izmantošanu, nepieciešamajiem drošības pasākumiem klienta pusē (t.sk. klienta darbstacijā, mobilajā iekārtā), autentifikācijas līdzekļu drošu izmantošanu un darbībām to nozaudēšanas gadījumā, kā arī pasākumiem, lai identificētu iespējamas krāpnieciskās darbības, tostarp t.s. "naudas mūļu" *(money mule)* riskus.

72. Tirgus dalībnieks, sazinoties ar klientu, izvērtē informācijas saturu un nepieciešamības gadījumā izmanto drošu

komunikācijas veidu.

73. Pirms attālināto pakalpojumu ieviešanas, parādoties jauniem apdraudējumiem vai veicot būtiskas izmaiņas IS, tirgus dalībnieks veic drošības pārbaudes vai testus un bez liekas kavēšanās uzlabo drošības pasākumus.

74. Tirgus dalībnieks vismaz 18 mēnešus glabā auditācijas pierakstus par veiktajiem un atteiktajiem attālināto pakalpojumu izmantošanas pieslēgumiem (t.sk. avota IP adresi, laiku) un lietotāja veikto transakciju un citu darbību identificēšanai nepieciešamo informāciju.

## XI. Informācijas sistēmu izstrāde un izmaiņu pārvaldība

75. Tirgus dalībnieks vada IS izstrādes un izmaiņu pārvaldības procesus, lai minimizētu IS drošības riskus gan izstrādājamajai IS, gan citām saistītajām IS.

76. Tirgus dalībnieks nosaka IS izstrādes, iegādes, testēšanas, ieviešanas un izmaiņu pārvaldīšanas procesus.

77. IS izstrādes sākšana

77.1. Tirgus dalībnieks nosaka par IS projektu atbildīgās personas, t.sk. saskaņā ar šiem noteikumiem nosaka arī izstrādājamās IS resursu turētājus.

77.2. Atbildīgās personas veic IS projekta un to IS, kuru darbību var ietekmēt jaunā IS, risku analīzi, kā arī nosaka IS drošības prasības un risku ierobežošanas pasākumus.

77.3. Nosakot IS prasības, tiek izmantota metode, ar kuru sistēmas arhitektūrā un uzturēšanas procesos iestrādā preventīvās, detektīvās un reaktīvās kontroles (*security by design*). Drošības arhitektūrai ir jāparedz vairāklīmeņu drošības sistēma, kas nodrošinātu kopējo IS aizsargspēju saglabāšanu arī kāda drošības līmeņa kompromitēšanas gadījumā.

78. IS izstrāde

78.1. Tirgus dalībnieks IS izstrādes vidi nodala no lietošanas vides.

78.2. Tirgus dalībnieks dokumentē katru IS. Dokumentācijā iekļauj nepieciešamo informācijas apjomu, lai varētu kvalitatīvi veikt IS lietošanu, uzturēšanu un izmaiņu pārvaldīšanu (piemēram, IS apraksts, IS administratora un lietotāju instrukcijas u.c.).

78.3. Tirgus dalībnieks dokumentāciju glabā un lieto atbilstoši šīs dokumentācijas klasifikācijas līmenim.

79. IS testēšana

79.1. Pirms IS ieviešanas tirgus dalībnieks saskaņā ar plānu veic IS testus. Testa plānā iekļauj arī IS drošības testu, kura laikā, pamatojoties uz novērotajiem drošības apdraudējumiem un veiktajām izmaiņām, veic testēšanu, ietverot iespējamo uzbrukumu scenārijus.

79.2. Tirgus dalībnieks nodala IS testa vidi no lietošanas vides.

79.3. Testa un izstrādes vidē neizmanto lietošanas vides datus, tomēr, ja IS drošības risku mazināšanas nolūkā testa vai izstrādes vidē nepieciešams izmantot lietošanas vides datus, tad tos lieto un tiem piemēro tādus pašus drošības pasākumus kā lietošanas vidē (t.sk. tiesību piešķiršanas, autentifikācijas, auditācijas kārtību).

80. IS ieviešana

80.1. IS ievieš pēc IS resursu turētāju atļaujas saņemšanas, kas apliecina, ka testēšana ir pabeigta un IS ir gatava ieviešanai.

80.2. Pirms IS nodošanas lietošanai tirgus dalībnieks veic darbinieku apmācību.

80.3. Tirgus dalībnieks nodrošina, ka tiek veikta IS versiju kontrole.

81. Izmaiņu pārvaldība

81.1. IS izmaiņas veic tikai ar saistīto IS resursu turētāju atļauju.

81.2. Tirgus dalībnieks analizē, kā izmaiņas ietekmēs esošos IS drošības pasākumus un piešķirtajās pieejas tiesībās pieejamo informāciju un vai izmaiņu rezultātā nesamazināsies IS drošības līmenis.

81.3. Tirgus dalībnieks veic IS dokumentācijas papildināšanu.

81.4. Tirgus dalībnieks izstrādā kārtību par darbībām ārkārtas (neplānotu) izmaiņu apstākļos un nosaka, kas ir tiesīgs pieņemt lēmumu par ārkārtas izmaiņām. Tirgus dalībnieks nosaka, kā tiek plānoti pasākumi, lai preventīvi samazinātu nepieciešamību veikt ārkārtas izmaiņas, un veic pasākumus, lai nepieļautu neautorizētu izmaiņu veikšanu.

82. Pārtraucot IS lietošanu, likvidējot vai nododot to citai personai, t.sk. gadījumos, ja tirgus dalībnieks pārtrauc kādu darbības veidu, kuru nodrošina šī IS, tirgus dalībnieks veic nepieciešamos drošības pasākumus, t.sk. risku analīzi.

## XII. Incidentu pārvaldība

83. Incidentu pārvaldības mērķis ir minimizēt IS drošības incidentu ietekmi uz tirgus dalībnieka klientiem un tirgus dalībnieka darbību un mazināt to atkārtošanās risku.

84. Tirgus dalībnieks nosaka un īsteno praksē IS drošības incidentu pārvaldības procesu, kas ietver vismaz:

84.1. IS drošības incidentu identificēšanu;

84.2. incidenta ietekmes mazināšanu un seku likvidēšanu;

84.3. incidentu reģistrēšanu incidentu reģistrā;

84.4. notikušā IS drošības incidenta analīzi (t.sk. cēloņu un risku mazināšanas pasākumu noteikšanu) un vadības informēšanu;

84.5. nepieciešamo pierādījumu saglabāšanu.

85. Maksājumu pakalpojumu sniedzēji, kas ir Latvijā reģistrētas kredītiestādes, licencētas maksājumu iestādes vai licencētas elektroniskās naudas iestādes, iesniedz ziņojumus par notikušajiem būtiskajiem incidentiem atbilstoši Finanšu un kapitāla tirgus komisijas 2018. gada 26. septembra normatīvajiem noteikumiem Nr. 157 "Normatīvie noteikumi par ziņošanu par būtiskiem maksājumu pakalpojumu incidentiem".

86. IS darbības atjaunošana

86.1. Tirgus dalībnieks nodrošina savlaicīgu IS darbības un datu atjaunošanu, ja noticis IS darbības pārtraukums.

86.2. Tirgus dalībnieks izstrādā IS darbības atjaunošanas plānu saskaņā ar tirgus dalībnieka darbības nepārtrauktības plānu. Tirgus dalībnieks ņem vērā iespējamos nelabvēlīgos scenārijus, ar kuriem tas varētu

saskarties.

86.3. IS darbības atjaunošanas plānā tirgus dalībnieks iekļauj atjaunojamos IS pakalpojumus prioritārā secībā, izmantojamos resursus, veicamo darbu sarakstu un atbildīgos darbiniekus.

86.4. Tirgus dalībnieks saskaņā ar iepriekš noteiktu kārtību veic regulāru IS darbības atjaunošanas procesos iesaistīto personu apmācību un dokumentētu plāna testēšanu saskaņā ar atbilstošajiem scenārijiem un izmaiņu gadījumā plānu atjauno, lai nodrošinātu tā aktualitāti.

87. Tirgus dalībnieks ārkārtas situācijas gadījumā, kā arī darbības nepārtrauktības plāna īstenošanas laikā veic efektīvus krīzes komunikācijas pasākumus, lai visas attiecīgās iekšējās un ārējās atbildīgās personas, tostarp ārpakalpojumu sniedzēji, tiktu savlaicīgi un pietiekami informēti.

## XIII. Noslēguma jautājums

88. Atzīt par spēku zaudējušiem Finanšu un kapitāla tirgus komisijas 2015. gada 7. jūlija noteikumus Nr. 112 "Finanšu un kapitāla tirgus dalībnieku informācijas sistēmu drošības normatīvie noteikumi".

Finanšu un kapitāla tirgus komisijas
priekšsēdētāja vietniece *G. Razāne*