LIKUMI

Izdevējs: Ministru kabinets
Veids: noteikumi
Numurs: 397
Pieņemts: 25.06.2025.
Stājas spēkā: 02.07.2025.

Publicēts:
Latvijas Vēstnesis, 123, 01.07.2025.
OP numurs: 2025/123.1

Ministru kabineta noteikumi Nr. 397

Rīgā 2025. gada 25. jūnijā (prot. Nr. 25 37. §)

Minimālās kiberdrošības prasības

Izdoti saskaņā ar Nacionālās kiberdrošības likuma 9. panta ceturto daļu, 12. panta trešo daļu, 24. panta otro daļu, 25. panta pirmo daļu, 26. pantu, 28. panta otro daļu, 33. pantu, 34. panta pirmo, septīto un desmito daļu, 36. panta pirmo daļu, 42. panta trešo daļu, 43. panta otro daļu un 44. panta otro daļu, Nacionālās drošības likuma 22.^{2} panta sesto daļu, Elektronisko sakaru likuma 8. panta pirmo un otro daļu un Valsts informācijas sistēmu likuma 16. pantu

1. Vispārīgie jautājumi

1. Noteikumi nosaka:

1.1. minimālās kiberdrošības prasības būtisko pakalpojumu sniedzējiem, svarīgo pakalpojumu sniedzējiem un informācijas un komunikācijas tehnoloģiju (turpmāk – IKT) kritiskās infrastruktūras īpašniekiem vai tiesiskajiem valdītājiem (turpmāk kopā – subjekti, katrs atsevišķi – subjekts);

1.2. kārtību, kādā subjekti nodrošina savu tīklu un informācijas sistēmu atbilstību minimālajām kiberdrošības prasībām;

1.3. prasības un veicamos pasākumus subjektu tīklu un informācijas sistēmu konfidencialitātes, integritātes un pieejamības nodrošināšanai un datu atjaunošanai;

1.4. IKT kritiskās infrastruktūras drošības prasības, pasākumus un to plānošanas un īstenošanas kārtību;

1.5. IKT kritiskās infrastruktūras, tai skaitā Eiropas IKT kritiskās infrastruktūras, apzināšanas, drošības pasākumu un darbības nepārtrauktības plānošanas un īstenošanas kārtību;

1.6. publisko elektronisko sakaru tīklu un tajos izmantoto iekārtu, programmatūru un ārpakalpojumu drošības prasības;

1.7. valsts informācijas sistēmu savietotāju, valsts platformu un integrētā valsts informācijas sistēmā ietilpstošo valsts informācijas sistēmu aizsardzības prasības;

1.8. prasības subjekta kiberdrošības pārvaldniekam;

1.9. veidu, kādā subjekts sniedz Nacionālajam kiberdrošības centram un Satversmes aizsardzības birojam Nacionālās kiberdrošības likuma 22. panta pirmajā, otrajā un piektajā daļā, 23. panta pirmajā, otrajā un piektajā daļā un 25. panta otrajā un ceturtajā daļā minēto informāciju;

1.10. subjekta kiberrisku pārvaldības un IKT darbības nepārtrauktības plānā iekļaujamās informācijas veidu un apjomu, kā arī plāna izpildes uzraudzības un kontroles kārtību;

1.11. kiberincidentu nozīmīguma kritērijus;

1.12. kārtību informēšanai par kiberincidentu, un to kiberincidentu kritērijus, par kuriem ir sniedzama informācija kompetentajai kiberincidentu novēršanas institūcijai;

1.13. agrīnā brīdinājuma, sākotnējā ziņojuma, starpposma ziņojuma, progresa ziņojuma un galaziņojuma par nozīmīgu kiberincidentu saturu un iesniegšanas kārtību;

1.14. kritērijus un kārtību subjekta elektronisko sakaru tīklu un informācijas sistēmu drošības skenēšanai;

1.15. nosacījumus un kārtību, kādā lietotājam tiek slēgta piekļuve elektronisko sakaru tīklam;

1.16. subjekta atbilstības pašvērtējuma ziņojuma veidlapu un tajā iekļaujamās informācijas saturu un apjomu, kā arī pašvērtējuma ziņojuma iesniegšanas termiņu un regularitāti;

1.17. subjektiem kiberhigiēnas pasākumu pamatelementus un prasības attiecībā uz kiberhigiēnas pasākumu īstenošanu;

1.18. kiberdrošības auditoram izvirzāmās prasības un kiberdrošības auditoru reģistrācijas kārtību;

1.19. kompetentās iestādes, kas uzrauga publisko elektronisko sakaru tīklu drošības prasību piemērošanu, un to funkcijas uzraudzības jomā;

1.20. kārtību ziņošanai par tiešās vai pastarpinātās pārvaldes iestādēm, citām valsts institūcijām un atvasinātajām publiskajām personām, kuras nepilda Nacionālās kiberdrošības likumā minētos lēmumus, pieprasījumus vai tām uzliktos tiesiskos pienākumus;

1.21. prasības kiberincidentu novēršanas institūcijām.

2. Noteikumos lietotie termini:

2.1. **autentifikācija** – process, kurā elektroniskajā vidē tiek pārbaudīta lietotāja identitāte;

2.2. **autorizācija** – process, kurā lietotājam pēc veiksmīgas autentifikācijas tiek piešķirtas tiesības veikt konkrētas darbības informācijas sistēmā vai tehniskajā resursā;

2.3. **ārpakalpojums** – jebkura veida vienošanās starp subjektu un pakalpojuma sniedzēju IKT jomā, saskaņā ar kuru šis pakalpojuma sniedzējs nodrošina procesu, sniedz pakalpojumu, veic tehnisko resursu piegādi vai veic citu darbību subjekta uzdevumā IKT infrastruktūrā;

2.4. **datu nesējs** – fiziskā vai virtuālā tehnoloģiskā ierīce vai uzglabāšanas vieta, kas paredzēta datu elektroniskajai uzglabāšanai un nolasīšanai, piemēram, cietais disks, zibatmiņa, CD, DVD, magnētiskā kasete;

2.5. **drošības pasākumi** – tehniski vai organizatoriski pasākumi, kas tiek noteikti risku pārvaldības ietvaros un samazina risku līdz pieņemamam līmenim;

2.6. **IKT resursi** – tehnisko resursu un informācijas resursu kopums;

2.7. **informācijas resurss** – strukturēta digitālo datu vienība;

2.8. **informācijas sistēma** – organizēta sistēma, kas paredzēta informācijas resursu pārvaldībai un elektroniskajai apstrādei, izmantojot tehniskos resursus;

2.9. **integritāte** – informācijas resursa un tā elektroniskās apstrādes metožu precizitāte, pareizība un pilnīgums;

2.10. **konfidencialitāte** – piekļuve informācijas resursam tikai pilnvarotiem IKT procesiem un lietotājiem;

2.11. **konts** – mehānisms, ar kuru lietotājam tiek piešķirta piekļuve IKT resursam vai informācijas sistēmai. Kontam ir unikāls identifikators, kas nodrošina darbības autora identificēšanu un pieejamo darbību un funkciju apjoma noteikšanu IKT resursā. Konts var būt piesaistīts konkrētai fiziskajai personai (piemēram, standarta lietotāja konts, administratora lietotāja konts) vai nebūt piesaistāms nevienai fiziskajai personai (piemēram, sistēmkonts);

2.12. **lietotāja konts** – konts, kas ir piesaistīts konkrētam lietotājam;

2.13. **lietotājs** – persona, kurai ir piešķirtas tiesības lietot IKT resursu vai informācijas sistēmu;

2.14. **mašīnlasāms formāts** – informācijas formāts, kas ir strukturēts tā, lai lietojumprogrammas var automatizēti nolasīt informāciju, kā arī viegli identificēt, atpazīt un iegūt no tās specifiskus datus, tostarp atsevišķas vienības un to iekšējo struktūru. Mašīnlasāma informācija var tikt elektroniski apstrādāta bez manuālas apstrādes no lietotāja puses;

2.15. **pamattīkls** – publiskā elektronisko sakaru tīkla daļa, kurā ir savienotas pamattīkla iekārtas (pārraides, komutēšanas, maršrutēšanas, multipleksēšanas vai ekvivalentas iekārtas) un kurai ir pievienots piekļuves tīkls, un kas nodrošina savienojumu ar citu elektronisko sakaru tīklu;

2.16. **pieejamība** – iespēja lietotājam lietot informācijas sistēmu vai informācijas resursu noteiktā laikā un vietā;

2.17. **sistēmkonts** – konts, kas nodrošina IKT funkciju vai procesu un nav piesaistāms nevienam lietotājam;

2.18. **šifrēšana** – process, kurā dati tiek pārveidoti, izmantojot speciālu algoritmu un atslēgu, lai padarītu tos neizprotamus vai neizlasāmus bez atbilstošas atslēgas. Šifrētos datus iespējams atšifrēt atpakaļ oriģinālajā formā, izmantojot pareizu atslēgu un atbilstošo atšifrēšanas algoritmu. Šifrēšanu var izmantot gan datu uzglabāšanā, gan pārraidē;

2.19. **tehniskais resurss:**

2.19.1. aparatūra, iekārta, kas ir tīkla vai informācijas sistēmas sastāvdaļa vai IKT infrastruktūrā izmantota iekārta, kas veic datu apmaiņu ar informācijas sistēmu;

2.19.2. programmatūra, tostarp operētājsistēmas, sistēmfaili, sistēmprogrammas, lietojumprogrammas un palīgprogrammas;

2.20. **tīkls** – komutācijas aparatūras un ar to saistīto tehnisko resursu kopums, kas savstarpēji savienots ar sakaru kanāliem;

2.21. **žurnālfaili** – analīzei pieejami pieraksti, kuri tiek automatizēti reģistrēti un satur datus par konkrētiem IKT notikumiem (piemēram, piekļuve, datu ievade, maiņa, dzēšana, izvade);

2.22. **4G tīkls** – ceturtās paaudzes mobilo elektronisko sakaru tīkls;

2.23. **5G tīkls** – piektās paaudzes mobilo elektronisko sakaru tīkls.

3. Noteikumi attiecas uz subjektiem un to īpašumā un valdījumā esošajiem tīkliem un informācijas sistēmām, izņemot tās, kurās tiek veikta valsts noslēpuma, Ziemeļatlantijas līguma organizācijas (turpmāk – NATO), Eiropas Savienības un ārvalstu institūciju klasificētās informācijas elektroniskā apstrāde.

4. Uz domēnu vārdu reģistrācijas pakalpojumu sniedzējiem attiecas tikai šo noteikumu 9. punkts.

5. Noteikumi neattiecas uz:

5.1. kabeļtelevīzijas tīkliem;

5.2. publiskajos elektronisko sakaru tīklos izmantotajām iekārtām, kuras neapstrādā signālus vai kuru darbībai nav nepieciešama enerģija;

5.3. publisko elektronisko sakaru tīklu galiekārtām pie klienta un citām tā galalietotāja iekārtām;

5.4. tālākpārdošanai paredzētajiem tehniskajiem resursiem.

6. Noteikumos ietvertās kiberrisku pārvaldības pasākumu tehniskās un metodiskās prasības Nacionālās kiberdrošības likuma 20. panta 1. punktā, 2. punktā, 4. punktā, 8. punkta "s", "t", "u" un "v" apakšpunktā, 21. panta pirmās daļas 2. punkta "l", "m", "n" apakšpunktā un 6. punktā minētajiem subjektiem piemēro, ciktāl tās nav pretrunā ar Eiropas Komisijas 2024. gada 17. oktobra Īstenošanas regulu (ES) 2024/2690, kas attiecībā uz DNS pakalpojumu sniedzējiem, TLD nosaukumu reģistriem, mākoņdatošanas pakalpojumu sniedzējiem, datu centru pakalpojumu sniedzējiem, satura piegādes tīkla nodrošinātājiem, pārvaldītu pakalpojumu sniedzējiem, pārvaldītu drošības pakalpojumu sniedzējiem, tiešsaistes tirdzniecības vietu, tiešsaistes meklētājprogrammu un sociālās tīklošanās pakalpojumu platformu nodrošinātājiem un uzticamības pakalpojumu sniedzējiem nosaka Direktīvas (ES) 2022/2555 piemērošanas noteikumus, kuri attiecas uz kiberdrošības risku pārvaldības pasākumu tehniskajām un metodiskajām prasībām un precizē, kādos gadījumos incidentu uzskata par būtisku (turpmāk – regula 2024/2690).

2. Statusa paziņošanas kārtība

7. Būtisko vai svarīgo pakalpojumu sniedzējs paziņo Nacionālajam kiberdrošības centram, nosūtot uz Aizsardzības ministrijas oficiālo elektronisko adresi elektroniski aizpildītu un ar drošu elektronisko parakstu parakstītu būtisko vai svarīgo pakalpojumu sniedzēja statusa paziņojuma veidlapu (1. pielikums):

7.1. Nacionālās kiberdrošības likuma 22. panta pirmajā daļā noteiktajā termiņā – par savu atbilstību būtisko pakalpojumu sniedzēja vai svarīgo pakalpojumu sniedzēja statusam;

7.2. Nacionālās kiberdrošības likuma 22. panta otrajā daļā noteiktajā termiņā – par izmaiņām statusa reģistrācijas veidlapā norādītajās ziņās;

7.3. par būtisko pakalpojumu sniedzēja vai svarīgo pakalpojumu sniedzēja statusa zaudēšanu.

8. Ja būtisko vai svarīgo pakalpojumu sniedzējs vienlaikus ir arī IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs, tas šo noteikumu 7. punktā minēto statusa paziņojumu iesniedz arī Satversmes aizsardzības birojam.

9. Domēnu vārdu reģistrācijas pakalpojumu sniedzējs paziņo Nacionālajam kiberdrošības centram, nosūtot uz Aizsardzības ministrijas oficiālo elektronisko adresi elektroniski aizpildītu un ar drošu elektronisko parakstu parakstītu domēnu nosaukumu reģistrācijas pakalpojumu sniedzēja statusa paziņojuma veidlapu (2. pielikums):

9.1. Nacionālās kiberdrošības likuma 23. panta pirmajā daļā noteiktajā termiņā – par savu atbilstību domēnu vārdu reģistrācijas pakalpojumu sniedzēja statusam;

9.2. Nacionālās kiberdrošības likuma 23. panta otrajā daļā noteiktajā termiņā – par izmaiņām domēnu vārdu reģistrācijas pakalpojumu sniedzēja paziņojuma veidlapā norādītajās ziņās;

9.3. par domēnu vārdu reģistrācijas pakalpojumu sniedzēja statusa zaudēšanu.

3. Pamatprasības subjektiem

3.1. Kiberdrošības pārvaldnieks

10. Subjekts paziņo Nacionālajam kiberdrošības centram, nosūtot uz Aizsardzības ministrijas oficiālo elektronisko adresi, un Satversmes aizsardzības birojam, nosūtot uz tā oficiālo elektronisko adresi, elektroniski aizpildītu un ar drošu elektronisko parakstu parakstītu paziņojuma par kiberdrošības pārvaldnieku veidlapu (3. pielikumu):

10.1. Nacionālās kiberdrošības likuma 25. panta otrajā daļā noteiktajā termiņā – par kiberdrošības pārvaldnieka noteikšanu;

10.2. Nacionālās kiberdrošības likuma 25. panta ceturtajā daļā noteiktajā termiņā – par izmaiņām šo noteikumu 10.1. apakšpunktā minētā paziņojuma veidlapā norādītajās ziņās.

11. IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs par kiberdrošības pārvaldnieku nosaka fizisku personu:

11.1. kurai ir Latvijas pilsonība;

11.2. kura ir pilngadīga;

11.3. pār kuru nav nodibināta aizgādnība;

11.4. kura nav sodīta par tīšu noziedzīgu nodarījumu, izņemot gadījumu, ja persona ir reabilitēta, vai sodāmība ir noņemta vai dzēsta;

11.5. kurai ir augstākā vai vidējā profesionālā izglītība informācijas tehnoloģiju, kiberdrošības pārvaldības vai citā saistītā jomā un vismaz divu gadu darba pieredze kiberdrošības pārvaldībā, kas iegūta pēdējo piecu gadu laikā, vai kurai ir spēkā esošs starptautiski atzīts sertifikāts, kas apliecina personas kvalifikāciju kiberdrošības jomā (piemēram, CISM, CISSP);

11.6. kura nav un nav bijusi PSRS, Latvijas PSR vai kādas ārvalsts drošības dienesta, izlūkdienesta vai pretizlūkošanas dienesta štata vai ārštata darbinieks, aģents, rezidents vai konspiratīvā dzīvokļa turētājs;

11.7. kura nav un nav bijusi ar Latvijas Republikas likumiem, Augstākās padomes lēmumiem vai tiesas nolēmumiem aizliegto organizāciju dalībnieks (biedrs) pēc šo organizāciju aizliegšanas;

11.8. kura nepieder pie organizētās noziedzības grupējuma, nelikumīga militarizēta vai bruņota formējuma;

11.9. kurai nav diagnosticēti psihiski traucējumi vai alkohola, narkotisko, psihotropo vai toksisko vielu atkarība, kas dod pamatu apšaubīt fiziskās personas uzticamību;

11.10. par kuru Satversmes aizsardzības birojs nav konstatējis drošības riskus.

12. Būtisko pakalpojumu sniedzējs, kurš nav IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs, par kiberdrošības pārvaldnieku nosaka fizisku personu:

12.1. kurai ir NATO, Eiropas Savienības vai Eiropas Brīvās tirdzniecības asociācijas (turpmāk – EBTA) dalībvalsts pilsonība;

12.2. kura atbilst šo noteikumu 11.2., 11.3. un 11.4. apakšpunktā noteiktajām prasībām;

12.3. kurai ir augstākā vai vidējā profesionālā izglītība informācijas tehnoloģiju, kiberdrošības pārvaldības vai citā saistītā jomā vai kurai ir spēkā esošs starptautiski atzīts sertifikāts, kas apliecina personas kvalifikāciju kiberdrošības jomā (piemēram, CISM, CISSP), vai kurai ir vismaz divu gadu darba pieredze kiberdrošības pārvaldībā, kas iegūta pēdējo piecu gadu laikā.

13. Svarīgo pakalpojumu sniedzējs, kurš nav IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs, par kiberdrošības pārvaldnieku nosaka fizisku personu:

13.1. kurai ir NATO, Eiropas Savienības vai EBTA dalībvalsts pilsonība;

13.2. kura atbilst šo noteikumu 11.2. un 11.3. apakšpunktā noteiktajām prasībām;

13.3. kurai ir augstākā vai vidējā profesionālā izglītība informācijas tehnoloģiju, kiberdrošības pārvaldības vai citā saistītā jomā vai kurai ir spēkā esošs starptautiski atzīts sertifikāts, kas apliecina personas kvalifikāciju kiberdrošības jomā (piemēram, CISM, CISSP), vai kurai ir vismaz divu gadu darba pieredze kiberdrošības pārvaldībā.

14. IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs kiberdrošības pārvaldnieku nosaka uz termiņu līdz

trim gadiem. IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs kiberdrošības pārvaldnieka pretendenta saskaņošanai iesniedz Satversmes aizsardzības birojam elektroniski aizpildītu un ar drošu elektronisko parakstu parakstītu kiberdrošības pārvaldnieka pretendenta saskaņošanas veidlapu (4. pielikums).

15. Satversmes aizsardzības birojs pārbauda IKT kritiskās infrastruktūras īpašnieka vai tiesiskā valdītāja kiberdrošības pārvaldnieka pretendenta atbilstību šo noteikumu 11. punktā minētajām prasībām triju mēnešu laikā no šo noteikumu 14. punktā minētās veidlapas saņemšanas brīža un par pārbaudes rezultātiem informē attiecīgā subjekta vadītāju. Satversmes aizsardzības birojs var neveikt kiberdrošības pārvaldnieka pretendenta pārbaudi, ja kiberdrošības pārvaldnieka pretendentam ir izsniegta speciālā atļauja pieejai valsts noslēpumam.

16. Ne vēlāk kā trīs mēnešus pirms noteiktā kiberdrošības pārvaldnieka darbības termiņa beigām IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs paziņo par kiberdrošības pārvaldnieka pretendentu, iesniedzot Satversmes aizsardzības birojam šo noteikumu 14. punktā minēto veidlapu.

17. Fiziska persona, kura noteikta par:

17.1. A kategorijas IKT kritiskās infrastruktūras īpašnieka vai tiesiskā valdītāja kiberdrošības pārvaldnieku, nedrīkst būt noteikta par kiberdrošības pārvaldnieku citā subjektā;

17.2. B vai C kategorijas IKT kritiskās infrastruktūras īpašnieka vai tiesiskā valdītāja kiberdrošības pārvaldnieku, nedrīkst būt noteikta par kiberdrošības pārvaldnieku citā IKT kritiskās infrastruktūras īpašniekā vai tiesiskajā valdītājā.

18. Fiziskā persona vienlaikus drīkst būt noteikta par kiberdrošības pārvaldnieku ne vairāk kā piecos būtisko pakalpojumu sniedzējos, kas nav IKT kritiskās infrastruktūras īpašnieki vai tiesiskie valdītāji.

19. Šo noteikumu 18. punktā minētais ierobežojums neattiecas uz būtisko pakalpojumu sniedzēja, kurā fiziskā persona ir noteikta par kiberdrošības pārvaldnieku, pakļautībā esošiem būtisko pakalpojumu sniedzējiem un būtisko pakalpojumu sniedzējiem, kuru kapitāldaļu īpašnieks vai turētājs ir attiecīgais būtisko pakalpojumu sniedzējs, vai privāto tiesību juridisko personu, kuru attiecīgais būtisko pakalpojumu sniedzējs ir deleģējis pildīt valsts pārvaldes uzdevumu.

20. IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs nodrošina, ka kiberdrošības pārvaldnieks subjektā vienlaikus nav atbildīgā persona par žurnālfailu pārvaldību vai nav atbildīgā persona par rezerves kopiju veidošanu, glabāšanu, pārbaudi un dzēšanu.

3.2. Kiberdrošības pārvaldības dokumentācija

21. Subjekta kiberdrošības pārvaldības dokumentu kopumu veido:

21.1. kiberdrošības politika;

21.2. IKT resursu un informācijas sistēmu katalogs;

21.3. kiberrisku pārvaldības un IKT darbības nepārtrauktības plāns;

21.4. kiberincidentu žurnāls.

22. Subjekts katru kiberdrošības pārvaldības dokumentu kopuma daļu var veidot kā vienotu dokumentu vai vairāku tematiski saistītu dokumentu kopu.

23. Subjekts nodrošina, ka kiberdrošības pārvaldības dokumentu kopuma daļas ir pieejamas tikai personām, kurām tās nepieciešamas darba pienākumu vai ārpakalpojuma izpildei.

24. Subjekts kiberdrošības pārvaldības dokumentu kopumu veido un uztur arī elektroniskā formātā.

25. Subjekts nodrošina, ka kiberdrošības pārvaldības dokumentu kopumā ietilpstošo dokumentu kopijas tiek uzglabātas atsevišķi no oriģināliem un ir pieejamas gadījumā, ja dokumentu oriģināli nav pieejami (piemēram, datu nesēja bojājuma gadījumā).

26. IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs:

26.1. pēc šo noteikumu 21.1. un 21.3. apakšpunktā noteikto kiberdrošības pārvaldības dokumentu kopuma daļu apstiprināšanas vai aktualizēšanas nekavējoties, bet ne vēlāk kā viena mēneša laikā tās iesniedz Satversmes aizsardzības birojam;

26.2. šo noteikumu 21.2. un 21.4. apakšpunktā minētā kiberdrošības pārvaldības dokumentu kopuma daļas iesniedz Satversmes aizsardzības birojam kopā ar pašvērtējuma ziņojumu atbilstoši šo noteikumu 8.3. apakšnodaļai;

26.3. pēc citu šo noteikumu 21. punktā nenorādītu kiberdrošības dokumentu apstiprināšanas vai aktualizēšanas nekavējoties, bet ne vēlāk kā viena mēneša laikā tos iesniedz Satversmes aizsardzības birojam.

27. Satversmes aizsardzības birojs var veikt IKT kritiskās infrastruktūras īpašnieka vai tiesiskā valdītāja kiberdrošības pārvaldības dokumentos un citos kiberdrošības dokumentos iekļautās informācijas pārbaudi un tajos noteikto prasību izpildes kontroles pasākumus un sniegt norādījumus pārbaudēs un izpildes kontroles pasākumos konstatēto trūkumu novēršanai.

3.3. Kiberdrošības politika

28. Subjekts izstrādā, uztur un regulāri, bet ne retāk kā reizi trijos gados pārskata un nepieciešamības gadījumā aktualizē kiberdrošības politiku.

29. Kiberdrošības politikā iekļauj:

29.1. vispārīgu informāciju par subjektu, tā darbības jomu, sniegtajiem pakalpojumiem un procesiem, kurus var ietekmēt kiberapdraudējums;

29.2. subjekta kiberdrošības pārvaldības mērķus, principus un vispārīgas pamatnostādnes;

29.3. informāciju par subjekta kiberdrošības pārvaldības struktūru, atbildīgo personu un struktūrvienību

funkcijām un pienākumiem kiberdrošības jomā, sadarbību ar citiem subjektiem un institūcijām;

29.4. informāciju par nozīmīgākajiem kiberapdraudējumu veidiem, kuriem ir pakļauti subjekta īpašumā un valdījumā esošie IKT resursi un informācijas sistēmas;

29.5. informāciju par Nacionālās kiberdrošības likuma, šo noteikumu un citu subjektam saistošo normatīvo aktu, standartu un sertifikācijas shēmu prasībām kiberdrošības jomā, kuras attiecas uz subjekta īpašumā un valdījumā esošajiem IKT resursiem un informācijas sistēmām.

3.4. IKT resursu un informācijas sistēmu katalogs

30. Subjekts apzina un uzskaita visus tā īpašumā un valdījumā esošos IKT resursus un informācijas sistēmas, kas pakļauti kiberriskiem.

31. Subjekts izveido, uztur, pārskata un izmaiņu gadījumā nekavējoties, bet ne vēlāk kā viena mēneša laikā aktualizē IKT resursu un informācijas sistēmu katalogu.

32. Subjekts nosaka konfidencialitātes, integritātes un pieejamības drošības klasi (A, B vai C) atbilstoši šo noteikumu 5. pielikumā ietvertajai metodikai katrai subjekta īpašumā un valdījumā esošajai informācijas sistēmai un informācijas resursu kategorijai.

33. Šo noteikumu izpratnē informācijas sistēma uzskatāma par:

33.1. A klases (paaugstinātas drošības) informācijas sistēmu, ja tai ir noteikta vismaz viena A konfidencialitātes, integritātes vai pieejamības drošības klase;

33.2. B klases (pamata drošības) informācijas sistēmu, ja tai ir noteikta vismaz viena B konfidencialitātes, integritātes vai pieejamības drošības klase, bet nav noteikta neviena A konfidencialitātes, integritātes vai pieejamības drošības klase;

33.3. C klases (minimālās drošības) informācijas sistēmu, ja tai ir noteiktas tikai C konfidencialitātes, integritātes un pieejamības drošības klases.

34. Kritiskās infrastruktūras kopumā iekļautu informācijas sistēmu uzskata par A klases informācijas sistēmu, nepiemērojot šo noteikumu 32. un 33. punktā minēto kārtību.

35. Ja kritiskās infrastruktūras kopumā ir iekļauta visa subjekta IKT infrastruktūra, subjekts informācijas sistēmām nosakāmās drošības klases saskaņo ar Satversmes aizsardzības biroju.

36. IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs pirms jaunas A vai B klases informācijas sistēmas izveides iesniedz Satversmes aizsardzības birojam jaunveidojamās informācijas sistēmas funkcionālo aprakstu.

37. Subjekts, kurš ir publiskā elektronisko sakaru tīkla īpašnieks vai tiesiskais valdītājs, identificē publiskā elektronisko sakaru tīkla kritiskās daļas saskaņā ar šo noteikumu 6. pielikumu. Subjekts var identificēt kā kritiskas arī citas publiskā elektronisko sakaru tīkla daļas.

38. Nacionālais kiberdrošības centrs sadarbībā ar Satversmes aizsardzības biroju izstrādā, vismaz reizi gadā pārskata un nepieciešamības gadījumā aktualizē informācijas sistēmas drošības klases noteikšanas vadlīnijas un par tām informē subjektu.

3.5. Kiberrisku pārvaldības un IKT darbības nepārtrauktības plāns

39. Subjekts uztur kiberrisku pārvaldības un IKT darbības nepārtrauktības plānu. Subjekts var izstrādāt vairākus kiberrisku pārvaldības un IKT darbības nepārtrauktības plānus atbilstoši subjekta darbības specifikai (piemēram, valsts informācijas sistēmai, subjekta datu centram). Šādā gadījumā par kiberrisku pārvaldības un IKT darbības nepārtrauktības plānu uzskatāms šo plānu kopums.

40. Kiberrisku pārvaldības un IKT darbības nepārtrauktības plānu pārskata un aktualizē:

40.1. IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs un būtisko pakalpojumu sniedzējs, kura īpašumā vai valdījumā ir vismaz viena A klases informācijas sistēma, – vismaz reizi gadā;

40.2. būtisko pakalpojumu sniedzējs, kura īpašumā vai valdījumā nav A klases informācijas sistēmas, – vismaz reizi divos gados;

40.3. svarīgo pakalpojumu sniedzējs – vismaz reizi trijos gados.

41. Kiberrisku pārvaldības un IKT darbības nepārtrauktības plānā iekļauj:

41.1. kiberrisku novērtēšanas metodiku, kas ietver analizējamo kiberrisku uzskaitījumu un metodoloģijas aprakstu šo risku nozīmīguma novērtēšanai (piemēram, kiberriska pieņemamās vērtības, novērtēšanas matrica, pārskatīšanas periodiskums);

41.2. kiberrisku novērtējumu, kas ietver identificēto kiberrisku uzskaitījumu un analīzi, tostarp ar piegādes ķēdēm saistīto risku analīzi, katra kiberriska nozīmīguma novērtējumu attiecībā uz subjekta īpašumā vai valdījumā esošajiem tīkliem, informācijas sistēmām un ar tiem saistītajiem IKT resursiem, kā arī salīdzinājumu ar iepriekšējā perioda kiberrisku pārvaldības un darbības nepārtrauktības plānā ietverto kiberrisku novērtējumu, ja tāds ir bijis;

41.3. kiberrisku pārvaldības pasākumu plānu, kas ietver identificēto kiberrisku uzskaitījumu, konkrētus pasākumus šo kiberrisku pārvaldībai, atbildīgos par pasākumu īstenošanu un kontroli, kā arī šo pasākumu īstenošanas termiņus vai to periodiskumu;

41.4. rīcības plānu darbības nepārtrauktības nodrošināšanai, kas ietver tīklu, informācijas sistēmu vai to veidojošo elementu darbības nepārtrauktības raksturlielumus (piemēram, atjaunošanas punkta mērķis (RPO), atjaunošanas laika mērķis (RTO), maksimāli pieļaujamais dīkstāves laiks (MTD)), šo raksturlielumu uzraudzības metodiku un rīcības plānu šo raksturlielumu pārsniegšanas gadījumā, tostarp rīcības plānu darbības atjaunošanai nozīmīga kiberincidenta vai krīzes gadījumā.

42. Plānojot kiberrisku pārvaldības pasākumus, subjekts:

42.1. apzina savā īpašumā vai valdījumā esošo informācijas sistēmu un IKT resursu nozīmīgumu un vērtību, tai skaitā potenciālo zaudējumu un ietekmes apjomu kiberincidenta gadījumā;

42.2. A un B klases informācijas sistēmām paredz rezerves IKT resursus darbības nepārtrauktības

nodrošināšanai nozīmīgā kiberincidenta vai krīzes gadījumā (piemēram, lai nodrošinātu šo noteikumu 41.4. apakšpunktā minētajā rīcības plānā minēto pasākumu izpildi);

42.3. A klases informācijas sistēmām iespēju robežās nodrošina no interneta piekļuves pakalpojuma sniedzēja neatkarīgas (autonomas) interneta protokola (turpmāk – IP) adreses vai adrešu apgabalus.

43. Subjekta kiberdrošības pārvaldnieks nodrošina kiberrisku pārvaldības un IKT darbības nepārtrauktības plāna izpildes uzraudzību un kontroli. Ja IKT kritiskās infrastruktūras īpašnieka vai tiesiskā valdītāja kiberdrošības pārvaldnieks ir vienlaikus atbildīgs arī par kiberrisku pārvaldības un IKT darbības nepārtrauktības plāna izstrādi, pārskatīšanu un aktualizēšanu, tad konkrētā IKT kritiskās infrastruktūras īpašnieka vai tiesiskā valdītāja vadītājs nodrošina kiberrisku pārvaldības un IKT darbības nepārtrauktības plāna izpildes uzraudzību un kontroli.

44. Subjekta vadītājs nodrošina, ka kiberdrošības pārvaldniekam un, ja attiecināms, citām par darbības nepārtrauktības pasākumu īstenošanu atbildīgajām personām ir nepieciešamās zināšanas un pilnvaras, lai nekavējoties veiktu tūlītējās nepieciešamās darbības kiberapdraudējuma novēršanai, kiberincidentu risināšanai vai kiberuzbrukuma seku novēršanai.

45. IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs:

45.1. nosaka atbildīgo personu par kiberrisku pārvaldības un IKT darbības nepārtrauktības plāna izstrādi, pārskatīšanu un aktualizēšanu, kā arī par plānā ietverto pasākumu īstenošanu;

45.2. nekavējoties, bet ne vēlāk kā piecu darbdienu laikā pēc šo noteikumu 45.1. apakšpunktā minētās personas noteikšanas par to informē Satversmes aizsardzības biroju.

3.6. Kiberincidentu pārvaldība un kiberincidentu žurnāls

46. Subjekts ievieš pārvaldības procesus, lai identificētu kiberincidentus, gandrīz notikušus kiberincidentus un ievainojamības, kā arī lai risinātu un novērstu kiberincidentus un ievainojamības, nosakot vismaz:

46.1. subjekta nodarbināto un ārpakalpojumu sniedzēju (ja attiecināms) lomas un atbildību kiberincidenta pazīmju konstatēšanas gadījumā vai informācijas saņemšanas gadījumā par iespējamo vai gandrīz notikušu kiberincidentu;

46.2. procedūras kiberincidentu identificēšanai, reģistrēšanai, ietekmes novērtēšanai un mazināšanai, risināšanai un seku likvidēšanai, pirmcēloņu atklāšanai, analīzei un novēršanai, pierādījumu saglabāšanai un drošības pasākumu uzlabošanai;

46.3. iekšējās un ārējās komunikācijas plānus, procedūras saziņai ar kompetento kiberincidentu novēršanas institūciju, citām kompetentajām institūcijām, citiem subjektiem un pakalpojumu saņēmējiem.

47. Subjekts uztur kiberincidentu žurnālu, kurā reģistrē ziņas par subjekta īpašumā un valdījumā esošajos tīklos un informācijas sistēmās konstatētajiem kiberincidentiem. Subjekts nodrošina ziņu reģistrēšanu žurnālā ne vēlāk kā 24 stundu laikā no kiberincidenta konstatēšanas brīža vai pēc jebkādām izmaiņām iepriekš žurnālā norādītajās ziņās.

48. Kiberincidentu žurnālā iekļauj vismaz šādu informāciju par kiberincidentiem:

48.1. kiberincidenta konstatēšanas datumu un laiku, kā arī kiberincidenta datumu un laiku, ja tāds ir zināms;

48.2. kiberincidenta veida kodu vai kodus atbilstoši šo noteikumu 7. pielikumā ietvertajai tipoloģijai;

48.3. kiberincidenta vispārīgo aprakstu;

48.4. kiberincidenta cēloņus un kompromitēšanas indikatorus, ja tādi ir zināmi;

48.5. kiberincidenta ietekmes novērtējumu;

48.6. atzīmi par to, vai kiberincidents uzskatāms par nozīmīgu kiberincidentu;

48.7. atzīmi par kiberincidenta paziņošanu kiberincidentu novēršanas institūcijai (nozīmīga kiberincidenta gadījumā – arī par agrīnā brīdinājuma, sākotnējā ziņojuma, galaziņojuma, progresa ziņojuma, starpposma ziņojuma iesniegšanu);

48.8. aktuālo kiberincidenta risināšanas statusu (piemēram, "neiesākts", "procesā", "atrisināts").

3.7. Lietotāju un piekļuves tiesību pārvaldība

49. Subjekts nodrošina lietotāju piekļuves tiesību pārvaldību, kā arī informācijas resursu kontrolētu un izsekojamu elektronisko apstrādi.

50. Subjekts katrai tā īpašumā vai valdījumā esošajai informācijas sistēmai, loģiski nodalītai informācijas sistēmas daļai (modulim) un informācijas sistēmā elektroniski apstrādājamo informācijas resursu veidam:

50.1. identificē lietotāju grupas, izvērtējot lietotāju nepieciešamību piekļūt informācijas resursam;

50.2. nosaka identificēto lietotāju piekļuves tiesību līmeni un autentifikācijas metodes, ņemot vērā informācijas resursa veidu un informācijas sistēmas klasi;

50.3. piešķir lietotāju kontiem piekļuves tiesības, ievērojot principu "nepieciešamība zināt" un mazāko privilēģiju principu, nodrošinot tikai minimāli nepieciešamo piekļuves tiesību līmeni lietotāja kontam, lai lietotājs spētu veikt subjekta noteiktās darbības informācijas sistēmā, ja vien tas ir tehniski iespējams.

51. Subjekts nodrošina, ka:

51.1. lietotājs var veikt darbības ar informācijas resursiem informācijas sistēmā tikai pēc veiksmīgas autentifikācijas ar viņam piešķirto lietotāja kontu. Ja informācijas sistēmas darbības nepārtrauktības dēļ aktīvā lietotāja konta nomaiņa tās lietošanas laikā nav iespējama, pieļaujams pēc veiksmīgas autentifikācijas informācijas sistēmā izmantot kopīgu kontu vairākiem lietotājiem, ja tiek nodrošināta iespēja identificēt lietotāju citā veidā (piemēram, maiņu grafiks, videonovērošana, elektronisks vai papīra lietotāju žurnāls);

51.2. sistēmkontiem ir tikai tādas tiesības tehniskajos resursos, kādas nepieciešamas, lai nodrošinātu tīkla vai informācijas sistēmas darbību, tehniskā resursa funkciju vai pakalpojumu;

51.3. ja vien tas tehniski ir iespējams, informācijas sistēmas tehniskajos resursos ir iestrādāti kontroles mehānismi, lai novērstu iespēju lietotājiem lietot sistēmkontus;

51.4. standarta lietotāja kontu neizmanto tīklu, informācijas sistēmu vai tehnisko resursu administrēšanai. Ja informācijas sistēmas tehniskais risinājums ļauj droši veikt administrēšanu, piešķirot (eskalējot) standarta lietotāja kontam administratora tiesības, tad uzskatāms, ka standarta lietotāja konts ar administratora tiesībām ir administratora lietotāja konts;

51.5. administratora lietotāja kontu neizmanto ikdienas darbam ar informācijas sistēmu vai IKT resursu;

51.6. pastāv tehniskas iespējas apturēt jebkura konta darbību, ja tas ir nepieciešams drošības apsvērumu dēļ.

52. Subjekts nodrošina obligātu daudzfaktoru autentifikācijas izmantošanu, lai piekļūtu:

52.1. A klases informācijas sistēmas administratora lietotāja kontam un standarta lietotāja kontam;

52.2. B klases informācijas sistēmas administratora lietotāja kontam;

52.3. B klases informācijas sistēmas standarta lietotāja kontam, ja tiek izmantota attālināta piekļuve informācijas sistēmai no ārējā tīkla un šai piekļuvei netiek izmantots šifrēta virtuālā privātā tīkla (VPN) risinājums ar daudzfaktoru autentifikāciju.

53. Subjekts nodrošina, ka visi informācijas sistēmas reģistrētie lietotāji ir iepazinušies ar informācijas sistēmas lietošanas noteikumiem. Subjekta pienākums ir nodrošināt, ka:

53.1. visi informācijas sistēmas reģistrētie lietotāji ir informēti par informācijas sistēmas lietošanas noteikumiem pirms informācijas sistēmas lietošanas uzsākšanas;

53.2. informācijas sistēmas lietošanas noteikumi ir pieejami informācijas sistēmas reģistrētajiem lietotājiem visā informācijas sistēmas lietošanas laikā.

54. Subjekta kiberdrošības pārvaldniekam ir tiesības:

54.1. pārbaudīt lietotāju kontu sarakstu, tiem piešķirtās piekļuves tiesības un to veiktās darbības informācijas sistēmā, tostarp lietotāju veiktās informācijas resursu izmaiņas un tehnisko resursu konfigurāciju izmaiņas;

54.2. nodrošināt žurnālfailu ierakstu analīzi par lietotāju veiktajām darbībām;

54.3. ja noticis kiberincidents vai ja ir pamatotas aizdomas par to, bloķēt vai uzdot administratoram bloķēt ar kiberincidentu saistītos lietotāju kontus;

54.4. pārbaudīt reģistrēto lietotāju zināšanas par informācijas sistēmas lietošanas noteikumiem un nepieciešamības gadījumā organizēt papildu apmācības, lai šīs zināšanas pilnveidotu;

54.5. pieprasīt no informācijas sistēmas uzturētāja informācijas sistēmas žurnālfailu ierakstus, ja informācijas sistēmu vai tās daļu uzturēšana notiek ārpus subjekta īpašumā vai valdījumā esošās IKT infrastruktūras.

3.8. Tīklu pārvaldība

55. IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs un būtisko pakalpojumu sniedzējs ievieš procesus savā īpašumā vai valdījumā esošo tīklu pārvaldībai, nodrošinot, ka:

55.1. tīkls ir sadalīts loģiskos segmentos atbilstoši to lietojumam, subjekta darbības specifikai un elektroniski apstrādājamo informācijas resursu drošības klasēm;

55.2. ja attiecināms, subjekta viesu (apmeklētāju) piekļuve internetam tiek nodrošināta, izmantojot no iekšējā tīkla fiziski vai loģiski atdalītu tīklu ar atsevišķu reālo publisko IP adresi;

55.3. tīkla iekārtas un cita aparatūra, kas nav paredzēta tiešai lietotāju izmantošanai, ir loģiski atdalīta, izmantojot atsevišķus virtuālus vai fiziskus tīklus, nodrošinot tai piekļuvi tikai pilnvarotam personālam;

55.4. ja attiecināms, iekšējā bezvadu tīklā izmanto vismaz WPA2, WPA3 vai jaunāku bezvadu drošības protokolu ar līdzvērtīgu vai augstāku aizsardzības līmeni;

55.5. iekšējais tīkls ir fiziski vai loģiski nodalīts no ārējā tīkla;

55.6. informācijas sistēmu darbībai paredzētās datu plūsmas ir fiziski vai loģiski nodalītas no lietotāju ikdienas darbam ar informācijas sistēmām paredzētajām datu plūsmām;

55.7. datu pārraide starp iekšējo un ārējo tīklu, kā arī starp iekšējā tīkla segmentiem ir kontrolējama, nosakot atļauto datu plūsmu (piemēram, ugunsmūriem, starpniekserveriem);

55.8. piekļuve iekšējā tīklā esošajiem informācijas resursiem ārpus iekšējā tīkla ir iespējama, tikai izmantojot šifrētu virtuālā privātā tīkla (VPN) risinājumu ar daudzfaktoru autentifikāciju.

56. Svarīgo pakalpojumu sniedzējs ievieš procesus savā īpašumā un valdījumā esošo tīklu pārvaldībai, nodrošinot šo noteikumu 55.1., 55.2., 55.3. un 55.4. apakšpunktā minēto prasību ievērošanu.

3.9. Žurnālfailu pārvaldība

57. Subjekts nodrošina informācijas sistēmu žurnālfailu un tīkla plūsmas žurnālfailu veidošanu un uzglabāšanu. Žurnālfailus uzglabā:

57.1. A klases informācijas sistēmām un to darbību nodrošinošām operētājsistēmām, pakalpēm (servisiem), tīklu un serveru iekārtām – vismaz 18 mēnešus pēc ieraksta izdarīšanas;

57.2. B klases informācijas sistēmām un to darbību nodrošinošām operētājsistēmām, pakalpēm (servisiem), tīklu un serveru iekārtām – vismaz 12 mēnešus pēc ieraksta izdarīšanas;

57.3. C klases informācijas sistēmām un to darbību nodrošinošām operētājsistēmām, pakalpēm (servisiem), tīklu un serveru iekārtām – vismaz 6 mēnešus pēc ieraksta izdarīšanas.

58. Informācijas sistēmas žurnālfailos ietver informāciju par konkrētiem informācijas sistēmas notikumiem, tostarp:

58.1. informācijas sistēmas ieslēgšanu un izslēgšanu;

58.2. kontu izveidi, grozīšanu vai dzēšanu, kontu piekļuves tiesību izmaiņām;

58.3. kontu piekļuvi informācijas resursiem, tostarp neveiksmīgiem piekļuves mēģinājumiem;

58.4. datu pievienošanu, izmaiņām, dzēšanu un datu atlasi;

58.5. tehnisko resursu konfigurāciju izmaiņām;

58.6. informācijas sistēmas paziņojumiem, brīdinājumiem un citiem IKT notikumiem, kas varētu liecināt par kiberincidentu vai citu apdraudējumu informācijas sistēmas vai informācijas resursa drošībai.

59. Informācijas sistēmas žurnālfailos fiksē informācijas sistēmas notikuma laiku, kas sinhronizēts ar augstas precizitātes tīkla laika protokola (NTP) serveri (vismaz STRATUM 2 līmeņa), IP adresi, no kuras veikta darbība, vai citu iekārtas unikālu identifikatoru, kas kombinēts ar lietotāja identifikatoru un ļauj nepārprotami identificēt iekārtu un lietotāja kontu, no kura veikta darbība, darbības aprakstu, kā arī informāciju par darbības iniciatoru (piemēram, lietotāja identifikators, pieslēguma metadati).

60. Tīkla plūsmas žurnālfailos ietver informāciju par datu nosūtīšanas un saņemšanas notikumiem. Tīkla plūsmas žurnālfailos fiksē vismaz šādu informāciju:

60.1. notikuma laiku, kas sinhronizēts ar augstas precizitātes tīkla laika protokola (NTP) serveri;

60.2. datu nosūtītāja (avota) un saņēmēja (galamērķa) IP adreses;

60.3. avota un galamērķa izmantotos tīkla aplikācijas līmeņa protokolus (piemēram, HTTP, HTTPS, FTP);

60.4. ja attiecināms, avota unikālo identifikatoru (MAC adrese);

60.5. izmantoto tīkla transporta protokolu (piemēram, TCP, UDP);

60.6. pārsūtīto datu apjomu.

61. Ja informācijas sistēmas vai tīkla uzbūves dēļ tehniski nav iespējams nodrošināt laika fiksēšanas risinājuma sinhronizēšanu ar kiberincidentu novēršanas institūcijas tīmekļvietnē norādīto augstas precizitātes tīkla laika protokola (NTP) serveri, subjektam ir pienākums nodrošināt citu laika fiksēšanas metodi, to saskaņojot attiecīgi ar Nacionālo kiberdrošības centru vai Satversmes aizsardzības biroju.

62. Žurnālfailu ierakstus veido mašīnlasāmā formātā. Pārvaldot žurnālfailus, subjekts īsteno drošības pasākumus, lai nodrošinātu IKT notikumu ticamu reģistrēšanu un efektīvu kiberincidentu analīzi.

63. Subjekts nodrošina žurnālfailu aizsardzību pret neautorizētu piekļuvi, ierakstu izmainīšanu un dzēšanu.

64. Subjekts iekšējos normatīvajos aktos nosaka žurnālfailu pārvaldības prasības un kārtību, tostarp žurnālfailu ierakstu analīzes, pārbaužu kārtību un regularitāti, atbildīgos par žurnālfailu pārvaldību, kā arī žurnālfailu aizsardzības prasības.

65. Subjekta kiberdrošības pārvaldnieks nodrošina žurnālfailu pārvaldības un aizsardzības prasību ievērošanas kontroli.

66. IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs:

66.1. nosaka par žurnālfailu pārvaldību atbildīgo personu;

66.2. nekavējoties, bet ne vēlāk kā piecu darbdienu laikā pēc šo noteikumu 66.1. apakšpunktā minētās personas noteikšanas par to informē Satversmes aizsardzības biroju.

3.10. Rezerves kopiju pārvaldība

67. Subjekts nodrošina, ka katrai tā īpašumā vai valdījumā esošajai informācijas sistēmai tiek veidotas rezerves kopijas.

68. Veidojot rezerves kopijas, subjekts nodrošina, ka rezerves kopija satur visus nepieciešamos datus, lai varētu atjaunot informācijas sistēmas darbību pilnā apjomā uz to brīdi, kad tika izveidota rezerves kopija, tai skaitā informācijas sistēmā glabātos datus, izpildāmo kodu, atbalsta programmatūru, automatizēto darbību skriptus, tehniskajos resursos regulāri veicamās darbības, operētājsistēmas uzdevumu pārvaldnieka komandas un izpildāmās datnes.

69. Subjekts nodrošina, ka ir pieejamas vismaz:

69.1. informācijas sistēmas tehniskās dokumentācijas rezerves kopijas;

69.2. informācijas sistēmas versijas un saistīto bibliotēku versiju pirmkoda rezerves kopijas, ja tiek izmantotas atvērtā koda bibliotēkas;

69.3. informācijas sistēmas darbību nodrošinošo tehnisko resursu konfigurāciju rezerves kopijas, ja vien tas ir tehniski iespējams.

70. Subjekts nodrošina, ka rezerves kopiju veidošanas periodiskums un uzglabāšanas laiks ļauj atjaunot informācijas sistēmu vismaz tādā stāvoklī, kāds bija:

70.1. A klases informācijas sistēmai – iepriekšējā dienā, pirms nedēļas (7–31 diena), pirms mēneša (30–365 dienas), iepriekšējā gadā (vecāku par 365 dienām);

70.2. B klases informācijas sistēmai – pēdējās nedēļas laikā (1–7 dienas), pirms nedēļas (7–31 diena), pirms mēneša (30–365 dienas), iepriekšējā gadā (vecāku par 365 dienām);

70.3. C klases informācijas sistēmai – pirms pēdējām nozīmīgajām izmaiņām informācijas sistēmā (piemēram, pirms migrācijas uz citu tehnoloģisku platformu), bet ne senāk kā pirms sešiem mēnešiem.

71. Subjekts nodrošina, ka:

71.1. par katru rezerves kopijas izveides gadījumu tiek veikts atbilstošs ieraksts žurnālfailos;

71.2. par rezerves kopijām atbildīgā persona un kiberdrošības pārvaldnieks tiek nekavējoties brīdināti, ja kārtējā rezerves kopijas izveide nav izdevusies;

71.3. A klases informācijas sistēmai pēc rezerves kopijas izveides, ja netiek izmantotas citas tehniskās metodes kopijas integritātes pārbaudei, tiek izveidota rezerves kopijas satura kontrolsumma.

72. Uzglabājot A un B klases informācijas sistēmu rezerves kopijas, subjekts nodrošina, ka:

72.1. rezerves kopijām gan fiziski, gan elektroniskajā vidē var piekļūt subjekta pilnvarotās personas, kā arī par rezerves kopiju atbildīgā persona un kiberdrošības pārvaldnieks;

72.2. A klases informācijas sistēmai vismaz viena pilna rezerves kopija tiek uzglabāta no informācijas sistēmas atdalītos tehniskajos resursos (piemēram, datu nesējos), ģeogrāfiski attālinātā vietā, telpās, kas aizsargātas pret nesankcionētu piekļuvi un aprīkotas ar automātisko ugunsgrēka atklāšanas un trauksmes signalizācijas sistēmu;

72.3. A un B klases informācijas sistēmai pēc rezerves kopijas pārvietošanas citā datu nesējā tiek pārbaudīta rezerves kopijas integritāte (piemēram, pārbaudot tās satura kontrolsummu).

73. Subjekts iekšējos dokumentos nosaka rezerves kopiju pārvaldības prasības un kārtību, tostarp rezerves kopiju veidošanas, glabāšanas un dzēšanas kārtību un kārtību, kādā pārbauda, vai, izmantojot rezerves kopijas, iespējams atjaunot informācijas resursus un informācijas sistēmas darbību, atbildīgos par rezerves kopiju pārvaldību, kā arī rezerves kopiju aizsardzības prasības.

74. Subjekta kiberdrošības pārvaldnieks nodrošina rezerves kopiju pārvaldības un aizsardzības prasību ievērošanas kontroli, tostarp veic:

74.1. ikdienas rezerves kopiju sagatavošanas uzraudzību;

74.2. rezerves kopiju nolasīšanas pārbaudi izlases kārtā izvēlētai informācijas sistēmai, informācijas resursam vai tehniskā resursa konfigurācijai. Pārbaudi veic ne retāk kā reizi sešos mēnešos A klases informācijas sistēmai un ne retāk kā reizi gadā B klases informācijas sistēmai vai pēc būtiskām kopējamās informācijas sistēmas vai rezerves kopiju veidošanas procedūras izmaiņām.

75. IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs:

75.1. nosaka par rezerves kopiju veidošanu, glabāšanu, pārbaudi un dzēšanu atbildīgo personu;

75.2. nekavējoties, bet ne vēlāk kā piecu darbdienu laikā pēc šo noteikumu 75.1. apakšpunktā minētās personas noteikšanas par to informē Satversmes aizsardzības biroju.

3.11. Kiberhigiēnas pasākumi

76. Subjekts organizē tā nodarbinātajiem un amatpersonām, kuri ir subjekta IKT resursu un informācijas sistēmu reģistrētie lietotāji, apmācību kiberdrošības jautājumos, izvēloties tādu apmācības veidu un saturu, kas atbilst nodarbināto un amatpersonu profesionālajai sagatavotībai, ņemot vērā viņu izglītību, iepriekšējo apmācību, darba pieredzi un spējas, kā arī subjekta darbības specifiku. Apmācību kopums ietver:

76.1. subjekta nodarbināto un amatpersonu, kuri lieto IKT resursus un informācijas sistēmas, kiberdrošības instruktāžas, tai skaitā:

76.1.1. sākotnējās kiberdrošības instruktāžas – ne vēlāk kā viena mēneša laikā no fiziskās personas lietotāja konta reģistrācijas brīža;

76.1.2. kārtējās kiberdrošības instruktāžas – vismaz reizi kalendāra gadā;

76.1.3. ārkārtas kiberdrošības instruktāžas – pēc kiberdrošības pārvaldnieka ieskatiem (piemēram,

identificējot jaunu risku, ievainojamību vai kiberapdraudējumu, paredzot normatīvo aktu prasību izmaiņas, plānojot vai veicot nozīmīgas izmaiņas IKT infrastruktūrā, programmatūrā vai biznesa procesos);

76.2. subjekta nodarbināto un amatpersonu IKT personāla apmācības kiberrisku pārvaldības un IKT darbības nepārtrauktības pasākumu efektīvai īstenošanai – vismaz reizi kalendāra gadā. Kiberdrošības pārvaldnieks ir tiesīgs organizēt papildu apmācības, piemēram, identificējot jaunu risku, ievainojamību vai kiberapdraudējumu.

77. IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs:

77.1. piešķir fiziskajai personai lietotāja kontu pēc šo noteikumu 76.1.1. apakšpunktā noteiktās sākotnējās kiberdrošības instruktāžas;

77.2. liedz fiziskajai personai piekļuvi tās lietotāja kontam, ja tai nav veikta šo noteikumu 76.1.2. apakšpunktā noteiktā ikgadējā kiberdrošības instruktāža;

77.3. organizē ārpakalpojuma sniedzēja darbiniekiem, kas ir iesaistīti līguma izpildē, kiberdrošības instruktāžas pirms līguma izpildes uzsākšanas.

78. Subjekts nodrošina, ka apmācību saturs tiek pārskatīts un nepieciešamības gadījumā aktualizēts vismaz reizi gadā vai mainoties apstākļiem (piemēram, izceļoties jauniem kiberapdraudējumiem, mainoties kiberriska līmenim, notiekot kiberincidentam).

79. Subjekts nodrošina, ka visiem tā nodarbinātajiem un amatpersonām, kas lieto subjekta IKT resursus un informācijas sistēmas, ir pieejami aktuālie kiberdrošības instruktāžu materiāli.

80. Subjekts uzskaita organizētās kiberdrošības instruktāžas un novērtē nodarbināto un amatpersonu, kuri lieto subjekta IKT resursus un informācijas sistēmas, zināšanas kiberdrošības jautājumos un īstenoto kiberdrošības instruktāžu efektivitāti.

3.12. Šifrēšanas prasības

81. Subjekts lieto šifrēšanas risinājumus, ja tas ir tehniski iespējams, vismaz:

81.1. A un B konfidencialitātes klases informācijas resursu pārsūtīšanai un pārraidei publiskajos datu pārraides tīklos, kā arī ārējos un iekšējos IKT infrastruktūras bezvadu tīklos;

81.2. A konfidencialitātes klases informācijas resursu glabāšanai.

82. Subjekts var lietot šifrēšanas risinājumus B konfidencialitātes klases informācijas resursu glabāšanai, kā arī C konfidencialitātes klases informācijas resursu pārsūtīšanai, pārraidei vai glabāšanai.

83. Subjekts var nelietot šo noteikumu 81. punktā minētos šifrēšanas risinājumus, ja subjekts risku novērtējuma ietvaros ir noteicis risku novēršanas pasākumus gadījumā, ja šifrēšanas risinājumu izmantošana nav tehniski iespējama.

84. Nacionālais kiberdrošības centrs sadarbībā ar Satversmes aizsardzības biroju izstrādā, vismaz reizi gadā pārskata un nepieciešamības gadījumā aktualizē vadlīnijas subjektiem šifrēšanas risinājumu izmantošanai. Vadlīnijas publicē Nacionālā kiberdrošības centra un Satversmes aizsardzības biroja tīmekļvietnē.

85. Subjekts iekšējos normatīvajos aktos nosaka:

85.1. minimālo pieļaujamo šifrēšanas aizsardzības (noturības) līmeni, ņemot vērā informācijas resursu konfidencialitātes līmeni;

85.2. šifrēšanas atslēgu pārvaldības politiku, lai nodrošinātu, ka tikai autorizētas personas var atšifrēt datus;

85.3. prasības drošai šifrēšanas atslēgu izveidošanai, uzstādīšanai, glabāšanai, nomaiņai un likvidēšanai, tai skaitā fiziskās un digitālās drošības prasības.

4. Ārpakalpojumu prasības

4.1. Vispārīgās ārpakalpojumu prasības

86. Subjekts ārpakalpojuma līgumu par IKT resursa vai pakalpojuma iegādi nedrīkst slēgt:

86.1. ja ārpakalpojuma sniedzējs ir juridiska persona, kas reģistrēta Krievijas Federācijā, Baltkrievijas Republikā vai valstī, kuru Eiropas Parlaments vai Latvijas Republikas Saeima ir atzinusi par terorismu atbalstošu valsti;

86.2. ja ārpakalpojuma sniedzējs, tā dalībnieks, kapitāla daļu īpašnieks vai patiesais labuma guvējs (ja saskaņā ar Noziedzīgi iegūtu līdzekļu legalizācijas un terorisma un proliferācijas finansēšanas novēršanas likumu patieso labuma guvēju ir iespējams noskaidrot) ir šo noteikumu 86.1. apakšpunktā minētās valsts pilsonis;

86.3. ja ārpakalpojuma sniedzēja juridiskās personas valde un padome sastāv no fiziskām personām, kuras ir šo noteikumu 86.1. apakšpunktā minētās valsts pilsoņi;

86.4. ja ārpakalpojuma sniegšanā ir iesaistīts šo noteikumu 86.1. apakšpunktā minētās valsts pilsonis;

86.5. ja iegādājamā IKT resursa ražotājs ir šo noteikumu 86.1. apakšpunktā minētajā valstī reģistrēta juridiska persona vai šīs valsts pilsonis.

87. Iegādājoties ārpakalpojumu, subjekts:

87.1. sniedz ārpakalpojuma aprakstu un nosaka precīzas prasības attiecībā uz ārpakalpojuma apjomu un kvalitāti;

87.2. sniedz norādes uz Nacionālās kiberdrošības likumā un šajos noteikumos noteiktajām prasībām;

87.3. paredz subjekta un ārpakalpojuma sniedzēja tiesības un pienākumus, tai skaitā:

87.3.1. subjekta tiesības pastāvīgi uzraudzīt ārpakalpojuma sniegšanas kvalitāti un tiesības saņemt pakalpojuma uzraudzībai nepieciešamo informāciju, tai skaitā žurnālfailus;

87.3.2. ārpakalpojuma sniedzēja pienākumu nekavējoties ziņot subjektam par konstatēto kiberincidentu, ja tas ietekmē vai var ietekmēt subjekta darbību vai ārpakalpojuma sniedzēja sniegto pakalpojumu, kā arī veikt visas kiberincidenta novēršanai nepieciešamās darbības;

87.3.3. ārpakalpojuma sniedzēja pienākumu informēt subjektu par ārpakalpojuma sniedzēja ārpakalpojuma izpildei piesaistītu citu pakalpojuma sniedzēju (turpmāk – apakšuzņēmējs) un viņa atbilstību šajos noteikumos un ārpakalpojuma līgumā noteiktajām prasībām;

87.3.4. konfidencialitātes saistības;

87.4. nosaka tīklam vai informācijas sistēmai veicamās pārbaudes, tostarp Nacionālajā kiberdrošības likumā un šajos noteikumos noteiktās obligātās pārbaudes, kā arī pārbaudes, kuras subjekts ir noteicis atbilstoši kiberdrošības politikai un kiberrisku pārvaldības un IKT darbības nepārtrauktības plānam;

87.5. nosaka piekļuves prasības datiem un to uzglabāšanai, kā arī pienākumu ārpakalpojuma sniedzējam pēc līguma termiņa beigām pēc subjekta izvēles dzēst ārpakalpojuma sniedzēja rīcībā nonākušos datus vai tos atdot subjektam, dzēšot visas esošās kopijas, izņemot gadījumu, ja līgums tiek pagarināts.

88. Slēdzot ārpakalpojuma līgumu par jaunas informācijas sistēmas izstrādi vai esošās informācijas sistēmas izmaiņām, subjekts:

88.1. nosaka informācijas sistēmas uzturēšanas un atbalsta nodrošināšanas (tai skaitā informācijas sistēmas drošības nepilnību novēršanas) laikposmu;

88.2. paredz iespēju šo noteikumu 88.1. apakšpunktā noteiktajā laikposmā turpināt informācijas sistēmas ekspluatēšanu ar informācijas sistēmas funkcionēšanai obligāti nepieciešamā programmnodrošinājuma jaunākām versijām;

88.3. paredz, ka A un B konfidencialitātes klases informācijas sistēmu:

88.3.1. testa vidē tiek izmantoti tikai sintētiski dati (no sākotnējiem datiem izveidoti mākslīgi dati, kas attēlo sākotnējo datu īpašības un struktūru un, veicot vienu un to pašu datu analīzi, sniedz līdzvērtīgus rezultātus);

88.3.2. ārpakalpojuma līguma izpilde netiek veikta attiecīgās informācijas sistēmas produkcijas vidē.

89. Pirms ārpakalpojuma iegādes subjekts apzina un novērtē ar ārpakalpojuma iegādi saistītos riskus, tostarp piegādes ķēdes drošības riskus, un nosaka ārpakalpojuma kvalitātes, drošības un pieejamības prasības minēto risku mazināšanai, kā arī ārpakalpojuma izbeigšanas stratēģiju.

90. Ārpakalpojuma sniedzējs nodrošina, ka apakšuzņēmējs atbilst visām prasībām, kas noteiktas ārpakalpojuma sniedzējam, un ka ievēro tās. Subjekts un ārpakalpojuma sniedzējs ir atbildīgs par apakšuzņēmējiem deleģēto pakalpojumu uzraudzību un atbilstību šajā nodaļā noteiktajām prasībām.

91. Ārpakalpojuma sniedzējs ne vēlāk kā līdz līguma noslēgšanai par informācijas sistēmas izstrādi, esošās informācijas sistēmas izmaiņām, informācijas sistēmas uzturēšanu vai IKT resursu apkopi iesniedz subjektam ārpakalpojuma izpildē iesaistīto fizisko personu sarakstu ar skaidrojumu attiecīgās fiziskās personas iesaistei ārpakalpojuma līguma izpildē. Ārpakalpojuma sniedzējs informē subjektu par ārpakalpojuma izpildē iesaistīto fizisko personu izmaiņām līguma izpildes laikā.

92. Subjekts nodrošina, ka pirms ārpakalpojuma līguma slēgšanas tas tiek saskaņots ar subjekta kiberdrošības

pārvaldnieku. Subjekts nosaka atbildīgo personu par līguma izpildes uzraudzību kiberdrošības jomā.

4.2. Īpašās ārpakalpojumu prasības IKT kritiskajai infrastruktūrai

93. IKT kritiskās infrastruktūras īpašniekam vai tiesiskajam valdītājam ārpakalpojuma līgumu par pakalpojuma sniegšanu A klases informācijas sistēmai atļauts slēgt tikai pēc Satversmes aizsardzības biroja atzinuma saņemšanas, izņemot gadījumu, ja ārpakalpojuma sniedzēja kapitāla daļu turētājs vai netiešās ietekmes guvējs ir Valsts pārvaldes iekārtas likumā noteiktā publiskā persona. Satversmes aizsardzības birojs atzinumu sniedz triju mēnešu laikā, nepieciešamības gadījumā atzinuma sniegšanu var pagarināt uz vēl vienu mēnesi.

94. IKT kritiskās infrastruktūras īpašniekam vai tiesiskajam valdītājam ārpakalpojuma līgumu par A klases informācijas sistēmas tehnisko resursu iegādi atļauts slēgt, ja ārpakalpojuma sniedzējs un tehniskā resursa ražotājs ir:

94.1. juridiska persona, kura atbilst šādām prasībām:

94.1.1. tā ir reģistrēta NATO, Eiropas Savienības vai EBTA dalībvalstī vai NATO Indijas un Klusā okeāna reģiona sadarbības valstī (turpmāk – IP4 valsts);

94.1.2. tās valde un padome sastāv no fiziskām personām, kuras ir NATO, Eiropas Savienības vai EBTA dalībvalstu vai IP4 valstu pilsoņi;

94.1.3. tās patiesais labuma guvējs ir NATO, Eiropas Savienības vai EBTA dalībvalsts vai IP4 valsts pilsonis (ja saskaņā ar Noziedzīgi iegūtu līdzekļu legalizācijas un terorisma un proliferācijas finansēšanas novēršanas likumu patieso labuma guvēju ir iespējams noskaidrot);

94.1.4. tās dalībnieki un kapitāla daļu īpašnieki (turētāji) ir juridiskas personas, kuras ir reģistrētas NATO, Eiropas Savienības, EBTA dalībvalstī vai IP4 valstī, vai fiziskas personas, kuras ir NATO, Eiropas Savienības vai EBTA dalībvalsts vai IP4 valsts pilsoņi;

94.2. fiziska persona, kura ir NATO, Eiropas Savienības vai EBTA dalībvalsts vai IP4 valsts pilsonis.

95. Šo noteikumu 94. punktā minētās prasības nepiemēro:

95.1. ja ārpakalpojumu sniedzēja kapitāla daļu turētājs vai netiešās ietekmes guvējs ir Valsts pārvaldes iekārtas likumā noteiktā publiskā persona;

95.2. ja ir saņemts Satversmes aizsardzības biroja atzinums, ka līgumu var slēgt izņēmuma kārtā.

96. Lai saņemtu šo noteikumu 93. punktā vai 95.2. apakšpunktā minēto atzinumu, IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs Satversmes aizsardzības birojam iesniedz:

96.1. elektroniski aizpildītu un ar drošu elektronisko parakstu parakstītu atzinuma pieprasījuma veidlapu (8. pielikums);

96.2. juridiskās personas un ārpakalpojumu izpildē iesaistīto apakšuzņēmēju (ja attiecināms) piekrišanu pārbaudes veikšanai, kā arī to ārpakalpojuma izpildē iesaistīto fizisko personu piekrišanu pārbaudes veikšanai vai fiziskas personas kā ārpakalpojuma sniedzēja piekrišanu pārbaudes veikšanai.

97. Satversmes aizsardzības birojs, sagatavojot atzinumu, var ņemt vērā šādu informāciju par ārpakalpojuma sniedzēju, apakšuzņēmēju un ar tiem saistītajām personām:

97.1. par juridisku personu:

97.1.1. juridiskās personas reģistrācijas valsti;

97.1.2. juridiskās personas valdes locekļu, dalībnieku, padomes locekļu, kapitāla daļu īpašnieku (turētāju), patieso labuma guvēju un netiešās ietekmes guvēju izcelsmes valsti;

97.1.3. informāciju par juridiskās personas darbības laikā konstatētajiem un ar to saistītajiem kiberincidentiem;

97.1.4. informāciju par juridiskās personas, tās valdes locekļu, dalībnieku, kapitāla daļu īpašnieku (turētāju), patieso labuma guvēju un netiešās ietekmes guvēju komercdarbības veikšanu Krievijas Federācijā vai Baltkrievijas Republikā vai dalību biedrībās, nodibinājumos vai citās juridiskās personās, kuru darbība ir saistīta ar Krievijas Federāciju vai Baltkrievijas Republiku;

97.1.5. informāciju, kas liecina, ka juridiskā persona varētu būt pakļauta tādai ārvalstu, organizāciju vai citu personu ietekmei, kas var radīt apdraudējumu nacionālās drošības interesēm;

97.1.6. citus Satversmes aizsardzības biroja konstatētus drošības riskus;

97.2. par fizisku personu:

97.2.1. pilsonību;

97.2.2. sodāmību;

97.2.3. piederību pie aizliegtām organizācijām vai atbalsta sniegšanu tām;

97.2.4. informāciju, kas liecina, ka fiziskā persona varētu būt pakļauta tādai ārvalstu, organizāciju vai citu personu ietekmei, kas var radīt apdraudējumu nacionālās drošības interesēm;

97.2.5. informāciju par fiziskās personas veikto saimniecisko darbību Krievijas Federācijā vai Baltkrievijas Republikā vai dalību biedrībās, nodibinājumos vai citās juridiskās personās, kuru darbība ir saistīta ar Krievijas Federāciju vai Baltkrievijas Republiku;

97.2.6. diagnosticētus psihiskus traucējumus vai alkohola, narkotisko, psihotropo vai toksisko vielu atkarību, kas dod pamatu apšaubīt personas uzticamību;

97.2.7. citus Satversmes aizsardzības biroja konstatētus drošības riskus.

98. Šo noteikumu 93. punktā un 95.2. apakšpunktā minētā atzinuma saņemšana ir attiecināma arī uz ārpakalpojuma sniedzēja ārpakalpojuma līguma izpildē piesaistītajiem apakšuzņēmējiem.

99. IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs, slēdzot vispārīgo vienošanos, ietver atsauci attiecīgi uz šo noteikumu 93. vai 94. punktā minētajiem ierobežojumiem, kas piemērojami, vispārīgās vienošanās ietvaros slēdzot ārpakalpojuma līgumus.

100. IKT kritiskās infrastruktūras īpašniekam vai tiesiskajam valdītājam ir pienākums informēt Satversmes

aizsardzības biroju:

100.1. par izmaiņām šo noteikumu 93. punktā minētā ārpakalpojuma līguma ārpakalpojuma sniedzēja vai apakšuzņēmēja valdes un padomes, dalībnieku un kapitāla daļu īpašnieku (turētāju) sastāvā un patiesā labuma guvēja un netiešās ietekmes guvēja izmaiņām. Minētā informācija iesniedzama ne vēlāk kā 10 darbdienu laikā no tās iegūšanas brīža;

100.2. par ārpakalpojuma izpildē iesaistīto fizisko personu izmaiņām šo noteikumu 93. punktā noteiktā ārpakalpojuma līguma izpildes laikā, pirms attiecīgo fizisko personu iesaistes ārpakalpojuma līguma izpildē iesniedzot šo noteikumu 96. punktā minēto informāciju.

4.3. Īpašās ārpakalpojumu prasības būtisko pakalpojumu sniedzējiem

101. Būtisko pakalpojumu sniedzējam, kas nav IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs, ārpakalpojuma līgumu A klases informācijas sistēmai atļauts slēgt:

101.1. ja ārpakalpojuma sniedzējs tehniskā resursa iegādei un tehniskā resursa ražotājs atbilst šo noteikumu 94. punktā noteiktajām prasībām;

101.2. ja ārpakalpojuma sniedzējs pakalpojuma sniegšanai atbilst šo noteikumu 94. punktā minētajām prasībām un ārpakalpojuma līguma izpildē iesaistītā fiziskā persona ir NATO, Eiropas Savienības, EBTA dalībvalsts vai IP4 valsts pilsonis.

102. Būtisko pakalpojumu sniedzējs, kurš ir publiskā elektronisko sakaru tīkla īpašnieks vai tiesiskais valdītājs, slēdzot ārpakalpojuma līgumu par publiskā elektronisko sakaru tīkla kritiskajās daļās izmantojamo tehnisko resursu vai pakalpojumu iegādi, piemēro šo noteikumu 101. punktā noteiktās prasības.

103. Šo noteikumu 101. punktu nepiemēro:

103.1. ja ārpakalpojuma sniedzēja kapitāla daļu turētājs vai netiešās ietekmes guvējs ir Valsts pārvaldes iekārtas likumā noteiktā publiskā persona;

103.2. ja ir saņemts Satversmes aizsardzības biroja atzinums, ka tā rīcībā nav negatīvas informācijas par ārpakalpojuma sniedzēju vai tehniskā resursa ražotāju.

104. Lai pieprasītu šo noteikumu 103.2. apakšpunktā minēto atzinumu, būtisko pakalpojumu sniedzējs nosūta uz Satversmes aizsardzības biroja oficiālo elektronisko adresi:

104.1. elektroniski aizpildītu un ar drošu elektronisko parakstu parakstītu atzinuma pieprasījuma veidlapu (8. pielikums);

104.2. juridiskās personas un ārpakalpojumu izpildē iesaistīto apakšuzņēmēju (ja attiecināms) piekrišanu pārbaudes veikšanai, kā arī to ārpakalpojuma izpildē iesaistīto fizisko personu pārbaudes veikšanai vai fiziskās personas kā ārpakalpojuma sniedzēja piekrišanu pārbaudes veikšanai.

105. Šo noteikumu 103.2. apakšpunktā minētā atzinuma saņemšana ir attiecināma arī uz ārpakalpojuma līguma izpildē iesaistītajiem apakšuzņēmējiem.

106. Būtisko pakalpojumu sniedzējs, slēdzot vispārīgo vienošanos, ietver atsauci uz šo noteikumu 101. punktā minētajiem ierobežojumiem, kas piemērojami, vienošanās ietvaros slēdzot ārpakalpojuma līgumus.

107. Būtisko pakalpojumu sniedzējam ir pienākums informēt Satversmes aizsardzības biroju:

107.1. par izmaiņām šo noteikumu 101.2. apakšpunktā noteiktajā ārpakalpojuma sniedzējā vai apakšuzņēmējā, ja tās neatbilst šo noteikumu 101.2. apakšpunktā minētajām prasībām;

107.2. par ārpakalpojuma izpildē iesaistīto fizisko personu izmaiņām šo noteikumu 101.2. apakšpunktā noteiktā pakalpojuma sniegšanas laikā, pirms attiecīgo fizisko personu iesaistes ārpakalpojuma līguma izpildē iesniedzot šo noteikumu 104. punktā minēto informāciju.

5. Papildu prasības IKT kritiskajai infrastruktūrai

108. IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs savā darbībā izmanto IKT, kas atbilst šajos noteikumos noteiktajām prasībām, kā arī ņem vērā Satversmes aizsardzības biroja norādījumus kiberdrošības jomā, tai skaitā par izmantojamām IKT un veicamajiem kiberdrošības pasākumiem.

109. Satversmes aizsardzības birojs:

109.1. apzina iespējamo A, B un C kategorijas IKT kritisko infrastruktūru un iespējamo Eiropas mērogā īpaši nozīmīgu kritisko infrastruktūru;

109.2. sniedz priekšlikumus par A, B un C kategorijas IKT kritiskās infrastruktūras iekļaušanu un izslēgšanu no kritiskās infrastruktūras kopuma;

109.3. informē A, B vai C kategorijas IKT kritiskās infrastruktūras īpašnieku vai tiesisko valdītāju:

109.3.1. par IKT kritiskās infrastruktūras iekļaušanu kritiskās infrastruktūras kopumā;

109.3.2. par IKT kritiskās infrastruktūras noteikšanu par Eiropas mērogā īpaši nozīmīgu kritisko infrastruktūru;

109.3.3. par IKT kritiskās infrastruktūras izslēgšanu no kritiskās infrastruktūras kopuma.

110. IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs, izbeidzot darba tiesiskās attiecības ar personu, kurai ir izveidots administratora lietotāja konts, bloķē konkrēto administratora lietotāja kontu brīdī, kad personai tiek paziņots par darba tiesisko attiecību izbeigšanu.

111. IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs:

111.1. izstrādā vienu visaptverošu darbības nepārtrauktības plānu valsts apdraudējuma gadījumam atbilstoši šo noteikumu 9. pielikumam. Darbības nepārtrauktības plāns valsts apdraudējuma gadījumam pirms tā pirmreizējas apstiprināšanas, kā arī pirms izmaiņu apstiprināšanas tiek saskaņots ar Satversmes aizsardzības

biroju;

111.2. nosaka par darbības nepārtrauktības plānošanu valsts apdraudējuma gadījumam atbildīgo personu un nosaka tās uzdevumus:

111.2.1. sadarbībā ar nozares ministriju un Aizsardzības ministriju sagatavo darbības nepārtrauktības plānu valsts apdraudējuma gadījumam;

111.2.2. sadarbībā ar nozares ministriju un Aizsardzības ministriju nodrošina darbības nepārtrauktības plāna valsts apdraudējuma gadījumam regulāru aktualizēšanu;

111.3. nekavējoties, bet ne vēlāk kā piecu darbdienu laikā pēc šo noteikumu 111.2. apakšpunktā minētās personas noteikšanas par to informē Satversmes aizsardzības biroju.

112. IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs darbības nepārtrauktības plānu valsts apdraudējuma gadījumam pēc tā apstiprināšanas vai aktualizēšanas nekavējoties, bet ne vēlāk kā viena mēneša laikā nosūta Satversmes aizsardzības birojam.

113. Ja kritiskās infrastruktūras kopumā iekļauj IKT kritisko infrastruktūru, kuras īpašniekam vai tiesiskajam valdītājam civilās aizsardzības plānos, valsts apdraudējuma pārvarēšanas plānos vai katastrofu medicīnas plānos ir noteikta darbības nepārtrauktība vai kurai ir ārējā audita sertificēta darbības nepārtrauktības nodrošināšanas sistēma, jauns darbības nepārtrauktības plāns valsts apdraudējuma gadījumam netiek izstrādāts, bet IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs norīko par darbības nepārtrauktības plānošanu valsts apdraudējuma gadījumam atbildīgo personu sadarbībā ar nozares ministriju un Aizsardzības ministriju, ja nepieciešams, papildināt esošos darbības nepārtrauktības plānus.

114. IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs ne retāk kā reizi četros gados vai, ja ir būtiskas izmaiņas, ne vēlāk kā gada laikā iesniedz Aizsardzības ministrijā, nozares ministrijā un Satversmes aizsardzības birojā pašvērtējumu par darbības nepārtrauktības plāna valsts apdraudējuma gadījumam aktualizēšanu. Nozares ministrija sadarbībā ar Aizsardzības ministriju var jebkurā laikā izlases veidā izvērtēt darbības nepārtrauktības plānu valsts apdraudējuma gadījumam un, ja nepieciešams, ieteikt tajā veicamās izmaiņas.

6. Papildu prasības kiberincidentu novēršanas institūcijām

115. Kiberincidentu novēršanas institūcija:

115.1. nodrošina savu saziņas kanālu (oficiālā elektroniskā adrese, e-pasts, telefons un citi atbilstoši saziņas kanāli) augstu pieejamības līmeni;

115.2. nodrošina piekļuvei savām telpām atbilstošu apmeklētāju kontroli un to, ka ēka, kurā tā atrodas, tiek apsargāta;

115.3. nodrošina, ka tās informācijas sistēmu darbības nodrošināšanai paredzētā aparatūra ir izvietota telpās ar dublētiem elektroenerģijas un interneta pieslēgumiem;

115.4. nodrošina, ka tā ir aprīkota ar piemērotu sistēmu atbalsta pieprasījumu pārvaldībai un novirzīšanai, lai atvieglotu efektīvu un lietpratīgu pieprasījumu apstrādi;

115.5. nodrošina savu darbību konfidencialitāti un uzticamību;

115.6. nodrošina, ka tai ir pietiekams atbilstoši apmācītu darbinieku skaits, lai nodrošinātu savu uzdevumu izpildi un darbības nepārtrauktību;

115.7. nodrošina rezerves informācijas sistēmas un rezerves darba telpas vai iespējas pāriet uz attālinātu darbu, lai nodrošinātu kiberincidentu novēršanas institūcijas darbības nepārtrauktību;

115.8. nodrošina, ka tās rīcībā ir piemērota, droša un noturīga saziņas un IKT infrastruktūra, lai nodrošinātu informācijas apmaiņu ar subjektiem un citām personām, tai skaitā lai nodrošinātu dalību starptautiskos sadarbības tīklos, veicinot drošu kopīgošanas rīku ieviešanu;

115.9. sadarbojoties ar citām privāto un publisko tiesību juridiskajām personām, tiešās un pastarpinātās pārvaldes iestādēm, atvasinātām publiskajām personām un citām valsts institūcijām, veicina vienotas vai standartizētas prakses, klasifikācijas shēmas un taksonomiju pieņemšanu un izmantošanu attiecībā uz incidentu risināšanas procedūrām, krīžu pārvaldību un koordinētu ievainojamību atklāšanu.

116. Kiberincidentu novēršanas institūcijas vadītājs izvērtē tās atbilstību šo noteikumu 115. punktā minētajām prasībām vismaz reizi piecos gados un par to informē Nacionālo kiberdrošības centru.

7. Kiberincidentu vadība

117. Konstatējot kiberincidentu, subjekts nekavējoties novērtē kiberincidenta nozīmīgumu.

118. Kiberincidents ir uzskatāms par nozīmīgu, ja:

118.1. tas atbilst būtiska kiberincidenta definīcijai regulas 2024/2690 3. panta 1. punkta izpratnē;

118.2. tas atbilst vismaz vienai no šādām pazīmēm:

118.2.1. kiberincidents apdraud sabiedrības veselību vai drošību, valsts drošību, ekonomisko drošību, valsts reputāciju, ārējās attiecības, pilsonisko brīvību vai pamattiesības;

118.2.2. kiberincidents rada mantiskus zaudējumus subjektam, citiem subjektiem, Latvijas Republikai, pakalpojumu saņēmējiem vai citām personām vismaz 500 000 *euro* vai 5 % apmērā no subjekta pēdējā finanšu gada apgrozījuma (atkarībā no tā, kura summa ir mazāka);

118.2.3. kiberincidents rada vai var radīt kaitējumu fiziskās personas dzīvībai vai veselībai;

118.2.4. kiberincidents rada vai var radīt ietekmi uz ierobežotas pieejamības vai klasificētās informācijas konfidencialitāti, integritāti vai pieejamību;

118.2.5. kiberincidents ir izraisījis vai var izraisīt būtiskā vai svarīgā pakalpojuma saņemšanas vai IKT kritiskās infrastruktūras funkcionēšanas traucējumus;

118.2.6. kiberincidents ir pārrobežu kiberincidents Nacionālā kiberdrošības likuma 1. panta 21. punkta izpratnē.

119. Par nozīmīgu kiberincidentu subjekts Nacionālās kiberdrošības likuma 34. panta otrajā, trešajā, piektajā un sestajā daļā noteiktajos termiņos ziņo kompetentajai kiberincidentu novēršanas institūcijai, nosūtot uz tās elektroniskā

pasta adresi elektroniski aizpildītu un ar drošu elektronisko parakstu parakstītu:

119.1. agrīnā brīdinājuma veidlapu (10. pielikums);

119.2. sākotnējā ziņojuma veidlapu (11. pielikums);

119.3. progresa ziņojuma veidlapu (12. pielikums), ja attiecināms;

119.4. starpposma ziņojuma veidlapu (13. pielikums), ja attiecināms;

119.5. galaziņojuma veidlapu (14. pielikums).

120. Par kiberincidentu, kurš nav uzskatāms par nozīmīgu kiberincidentu, subjekts ziņo kompetentajai kiberincidentu novēršanas institūcijai, nosūtot uz tās elektroniskā pasta adresi kiberincidenta aprakstu brīvā formā.

121. IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs un būtiskā pakalpojuma sniedzējs šo noteikumu 119. un 120. punktā minētos ziņojumus nosūta arī Satversmes aizsardzības birojam.

8. Subjektu kiberdrošības uzraudzība

8.1. Atbilstības audits

122. Lai subjekts varētu veikt atbilstības auditu, kas noteikts Nacionālās kiberdrošības likumā, Digitālās drošības uzraudzības komiteja kiberdrošības auditoru sarakstā (turpmāk – auditoru saraksts) reģistrē auditoru, kurš atbilst šādām prasībām:

122.1. auditors ir juridiska vai fiziska persona, kura atbilst šo noteikumu 94. punktā minētajām prasībām;

122.2. auditoram vai tā nodarbinātajam personālam ir nepieciešamās zināšanas kiberdrošības audita jomā, ko apliecina starptautiski atzīti sertifikāti (piemēram, CISA, ISO/IEC 27001 *Lead Auditor*, CISSP);

122.3. auditoram ir tehniskas iespējas noteikt subjekta tīklu, informācijas sistēmu, IKT resursu un procedūru drošības atbilstību normatīvo aktu prasībām kiberdrošības jomā.

123. Papildus šo noteikumu 122. punktā noteiktajām prasībām auditoram, kurš ir tiesīgs veikt mākoņdatošanas pakalpojumu vai datu centru pakalpojumu sniedzēja atbilstības auditu, piemēro šādas prasības:

123.1. auditoram vai tā nodarbinātajam personālam ir nepieciešamās zināšanas datu centru kiberdrošības audita jomā, ko apliecina starptautiski atzīti sertifikāti (piemēram, CDCAP) un vismaz divu gadu darba pieredze kiberdrošības auditu jomā;

123.2. auditoram ir tehniskas iespējas veikt datu centra auditu pēc starptautisko standartu prasībām datu centru kiberdrošības jomā.

124. Lai auditors tiktu reģistrēts auditoru sarakstā, tas iesniedz Digitālās drošības uzraudzības komitejai:

124.1. aizpildītu un parakstītu kiberdrošības auditora reģistrācijas pieteikuma veidlapu (15. pielikums);

124.2. šo noteikumu 122.2. apakšpunktā minēto sertifikātu kopijas;

124.3. ja attiecināms, šo noteikumu 123.1. apakšpunktā minēto sertifikātu kopijas.

125. Ievērojot šo noteikumu 123. punktu, Digitālās drošības uzraudzības komiteja auditoru sarakstā izdara atzīmi par to, vai konkrētais auditoru sarakstā reģistrētais auditors ir tiesīgs veikt mākoņdatošanas pakalpojumu un datu centru pakalpojumu sniedzēju atbilstības auditu.

126. Auditoru sarakstā reģistrētajam auditoram ir pienākums nekavējoties, bet ne vēlāk kā mēneša laikā ziņot Digitālās drošības uzraudzības komitejai par jebkādām izmaiņām auditora reģistrācijas pieteikuma anketā norādītajos datos. Ja nepieciešams, Digitālās drošības uzraudzības komiteja var precizēt auditoru sarakstā iekļautās ziņas par auditoru, ja minētās izmaiņas pēc būtības neietekmē auditora atbilstību šo noteikumu 122. punktā minētajām prasībām.

127. Digitālās drošības uzraudzības komiteja izslēdz auditoru no auditoru saraksta, ja:

127.1. saņemts auditora iesniegums par izslēgšanu no saraksta;

127.2. konstatēts, ka auditors neatbilst Nacionālajā kiberdrošības likumā vai šajos noteikumos noteiktajām prasībām;

127.3. auditors Digitālās drošības uzraudzības komitejai sniedzis nepatiesas ziņas;

127.4. pastāv objektīvas šaubas par auditora zināšanām kiberdrošības audita jomā vai spēju nodrošināt atbilstības audita veikšanu (piemēram, ja pēcpārbaudes ietvaros tiek atklāts, ka auditors ir nekvalitatīvi veicis savus pienākumus);

127.5. publiskos reģistros konstatēts, ka auditors – juridiskā persona – ir likvidēts;

127.6. publiskos reģistros konstatēts, ka auditors – fiziskā persona – ir miris.

128. Digitālās drošības uzraudzības komiteja auditoru sarakstu pārskata ne retāk kā reizi kalendāra gadā. Auditoru sarakstu publicē Nacionālā kiberdrošības centra tīmekļvietnē.

129. Slēdzot ārpakalpojuma līgumu par atbilstības auditu, subjekts paredz, ka:

129.1. auditoram ir nepieciešamās zināšanas, prasmes un pieredze, lai sniegtu neatkarīgu, objektīvu un vispusīgu vērtējumu;

129.2. auditors apstrādā audita ietvaros iegūto informāciju vienīgi NATO, Eiropas Savienības un EBTA dalībvalstu teritorijā.

129.3. auditors pēdējo triju gadu laikā nav piedalījies auditējamās informācijas sistēmas vai tās daļas izstrādē, uzturēšanā vai testēšanā;

129.4. auditors atbilst Nacionālās kiberdrošības likuma 44. panta otrās daļas prasībām, šo noteikumu 122. punkta prasībām un nepastāv citi apstākļi, kuru dēļ nav nodrošināma audita objektivitāte un neatkarība.

130. IKT kritiskās infrastruktūras īpašniekam vai tiesiskajam valdītājam šo noteikumu 129. punktā noteikto ārpakalpojuma līgumu atļauts slēgt tikai pēc Satversmes aizsardzības biroja atzinuma saņemšanas atbilstoši šo noteikumu 93. punktam.

8.2. Ielaušanās testi un drošības skenēšana

131. Ielaušanās testus veic šādos gadījumos:

131.1. A klases informācijas sistēmai:

131.1.1. pirms informācijas sistēmas nodošanas ekspluatācijā;

131.1.2. vismaz reizi trijos gados informācijas sistēmas ekspluatācijas laikā;

131.2. jebkurai informācijas sistēmai – pēc subjekta iniciatīvas;

131.3. jebkurai informācijas sistēmai – pēc Nacionālā kiberdrošības centra vai Satversmes aizsardzības biroja pieprasījuma.

132. Šo noteikumu 131.1. un 131.2. apakšpunktā minētos ielaušanās testus var veikt:

132.1. subjekta nodarbinātais personāls, kurš pēdējo triju gadu laikā nav bijis iesaistīts testējamās informācijas sistēmas izstrādē vai uzturēšanā;

132.2. svarīgo pakalpojumu sniedzēja vai būtisko pakalpojumu sniedzēja, kas nav IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs, informācijas sistēmai cita persona, kura:

132.2.1. ir saņēmusi starptautiski atzītu sertifikātu, kas apliecina personas kvalifikāciju ielaušanās testu jomā (piemēram, CEH, OSCP), vai kurai ir vismaz divu gadu darba pieredze ielaušanās testu veikšanā, kas iegūta pēdējo piecu gadu laikā;

132.2.2. pēdējo triju gadu laikā nav bijusi iesaistīta testējamās informācijas sistēmas izstrādē vai uzturēšanā;

132.3. IKT kritiskās infrastruktūras īpašnieka vai tiesiskā valdītāja informācijas sistēmai cita persona, par kuru ir

saņemts Satversmes aizsardzības biroja atzinums šo noteikumu 98. punktā noteiktajā kārtībā un kura atbilst šo noteikumu 132.2.1. un 132.2.2. apakšpunktā noteiktajām prasībām.

133. Šo noteikumu 131.3. apakšpunktā minētos ielaušanās testus var veikt:

133.1. svarīgo pakalpojumu sniedzēja vai būtisko pakalpojumu sniedzēja, kas nav IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs, informācijas sistēmai Nacionālā kiberdrošības centra vai kompetentās kiberincidentu novēršanas institūcijas amatpersonas, darbinieki vai persona, kas atbilst šo noteikumu 132.2. apakšpunktā noteiktajām prasībām;

133.2. IKT kritiskās infrastruktūras īpašnieka vai tiesiskā valdītāja informācijas sistēmai:

133.2.1. kompetentās kiberincidentu novēršanas institūcijas darbinieki pēc Satversmes aizsardzības biroja pieprasījuma;

133.2.2. cita persona, par kuru ir saņemts Satversmes aizsardzības biroja atzinums atbilstoši šo noteikumu 93. punktam un kura atbilst šo noteikumu 132.2. apakšpunktā noteiktajām prasībām.

134. IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs nekavējoties, bet ne vēlāk kā 10 darbdienu laikā informē Satversmes aizsardzības biroju par ielaušanās testa rezultātiem.

135. Subjekta IKT infrastruktūras drošības skenēšanu (turpmāk – drošības skenēšana) veic:

135.1. pēc Nacionālā kiberdrošības centra pieprasījuma attiecībā uz svarīgo vai būtisko pakalpojumu sniedzēju, kas nav IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs;

135.2. pēc Satversmes aizsardzības biroja pieprasījuma attiecībā uz IKT kritiskās infrastruktūras īpašnieku vai tiesisko valdītāju;

135.3. pēc subjekta pieprasījuma.

136. Drošības skenēšanu IKT kritiskās infrastruktūras īpašnieka vai tiesiskā valdītāja IKT infrastruktūrā var veikt:

136.1. Satversmes aizsardzības biroja amatpersonas;

136.2. kompetentā kiberincidentu novēršanas institūcija pēc Satversmes aizsardzības biroja pieprasījuma;

136.3. cita persona, par kuru ir saņemts Satversmes aizsardzības biroja atzinums atbilstoši šo noteikumu 93. punktam.

137. Drošības skenēšanu veic visā IKT kritiskās infrastruktūras īpašnieka vai tiesiskā valdītāja IKT infrastruktūrā, ja Satversmes aizsardzības biroja pieprasījumā nav noteikts citādi.

138. Ja drošības skenēšanu IKT kritiskās infrastruktūras īpašnieka vai tiesiskā valdītāja IKT infrastruktūrā veic saskaņā ar šo noteikumu 136.2. un 136.3. apakšpunktu:

138.1. drošības skenēšanu veic no vides, kura nav kritiskās infrastruktūras īpašnieka vai tiesiskā valdītāja īpašumā vai valdījumā, lietojot informāciju, kura ir šīs kritiskās infrastruktūras īpašnieka vai tiesiskā valdītāja

rīcībā;

138.2. drošības skenēšanas laikā iegūst tikai to informāciju un tādā apjomā, kas ir nepieciešama pārvaldāmo risku identificēšanai;

138.3. drošības skenēšanas veicējs ne vēlāk kā 48 stundas pirms skenēšanas uzsākšanas rakstiski informē par skenēšanas laiku un ilgumu kritiskās infrastruktūras īpašnieku vai tiesisko valdītāju, kā arī Satversmes aizsardzības biroju;

138.4. drošības skenēšana tiek veikta tā, lai tā neradītu kaitējumu IKT kritiskās infrastruktūras īpašnieka vai tiesiskā valdītāja IKT infrastruktūrai;

138.5. detalizētus drošības skenēšanas rezultātus drošības skenēšanas veicējs nekavējoties nosūta attiecīgajam kritiskās infrastruktūras īpašniekam vai tiesiskajam valdītājam un Satversmes aizsardzības birojam, sniedzot arī attiecīgus ieteikumus;

138.6. drošības skenēšanas veicējs apkopo informāciju par katru veikto drošības skenēšanu, norādot tās veicējus, skenēšanas laiku, rezultātu kopsavilkumu un sniegtos ieteikumus. Drošības skenēšanas veicējs nodrošina, ka visa ar drošības skenēšanu saistītā informācija ir pieejama tikai drošības skenēšanas veicējam, konkrētajam IKT kritiskās infrastruktūras īpašniekam vai tiesiskajam valdītājam un Satversmes aizsardzības birojam.

139. Vērtējot šo noteikumu 131.3. apakšpunktā minētā ielaušanās testa vai šo noteikumu 135.1. vai 135.2. apakšpunktā minētās drošības skenēšanas nepieciešamību, Nacionālais kiberdrošības centrs vai Satversmes aizsardzības birojs ņem vērā vismaz vienu no šādiem apsvērumiem:

139.1. subjekta veidu un darbības jomu;

139.2. subjekta IKT infrastruktūras kritiskumu un tajā uzturēto informācijas sistēmu klasi;

139.3. subjekta sniegtā būtiskā vai svarīgā pakalpojuma nozīmīgumu, tostarp ietekmi uz nacionālo drošību, IKT kritiskās infrastruktūras darbības nepārtrauktību, citiem būtiskajiem un svarīgajiem pakalpojumiem;

139.4. pēdējo triju gadu laikā subjekta IKT infrastruktūrā konstatēto kiberincidentu nozīmīgumu un apjomu;

139.5. uzraudzības procesa ietvaros iegūto informāciju par subjekta kiberdrošību, atklātajām ievainojamībām un nepieciešamajiem uzlabojumiem;

139.6. no citām kompetentajām iestādēm (tostarp ārvalstu partnerdienestiem) saņemto informāciju par iespējamo kiberapdraudējumu.

140. Drošības skenēšanu svarīgo vai būtisko pakalpojumu sniedzēja, kas nav IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs, IKT infrastruktūrā var veikt Nacionālā kiberdrošības centra, kompetentās kiberincidenta novēršanas institūcijas darbinieks vai cita persona, kura atbilst šo noteikumu 94. punkta prasībām.

8.3. Pašvērtējuma ziņojums

141. Subjekts veic pašvērtējumu par savu atbilstību Nacionālās kiberdrošības likumā un šajos noteikumos ietvertajām prasībām:

141.1. reizi gadā – subjekts, kurš ir IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs vai kura īpašumā vai valdījumā ir vismaz viena A klases informācijas sistēma;

141.2. reizi trijos gados – subjekts, kura īpašumā un valdījumā nav nevienas A klases informācijas sistēmas, ja vien Nacionālais kiberdrošības centrs nav noteicis citādāk.

142. Veicot šo noteikumu 141. punktā minēto pašvērtējumu, līdz attiecīgā kalendāra gada 1. oktobrim pašvērtējuma ziņojuma veidlapu (16. pielikums) iesniedz:

142.1. būtisko vai svarīgo pakalpojumu sniedzējs, kas nav IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs, – Nacionālajam kiberdrošības centram;

142.2. IKT kritiskās infrastruktūras īpašnieki un tiesiskie valdītāji – Satversmes aizsardzības birojam.

143. Ja atbilstība subjekta statusam ir iestājusies pēc 1. jūlija, subjekts pirmreizējo pašvērtējuma ziņojumu iesniedz ne vēlāk kā triju mēnešu laikā no atbilstības brīža.

8.4. Neatbilstību novēršana valsts un pašvaldību institūcijās

144. Ja subjekts, kurš ir tiešās pārvaldes iestāde, neveic visus nepieciešamos, piemērotos un samērīgos pasākumus konstatētās neatbilstības novēršanai, Nacionālais kiberdrošības centrs vai Satversmes aizsardzības birojs atbilstoši Nacionālās kiberdrošības likuma 41. pantā noteiktajam uzraudzības dalījumam par šo neatbilstību ziņo attiecīgajam Ministru kabineta loceklim. Atbildīgais Ministru kabineta loceklis par neatbilstības novēršanas gaitu ziņo Ministru kabinetam.

145. Ja subjekts, kurš ir pašvaldība vai pašvaldības dibināta pastarpinātās pārvaldes iestāde, neveic visus nepieciešamos, piemērotos un samērīgos pasākumus konstatētās neatbilstības novēršanai, Nacionālais kiberdrošības centrs vai Satversmes aizsardzības birojs atbilstoši Nacionālās kiberdrošības likuma 41. pantā noteiktajam uzraudzības dalījumam par šo neatbilstību ziņo attiecīgās pašvaldības domes priekšsēdētājam, kā arī informē viedās administrācijas un reģionālās attīstības ministru.

146. Ja subjekts, kurš ir šo noteikumu 144. un 145. punktā neminēta atvasināta publiska persona, pastarpinātās pārvaldes iestāde vai cita valsts institūcija, neveic visus nepieciešamos, piemērotos un samērīgos pasākumus konstatētās neatbilstības novēršanai, Nacionālais kiberdrošības centrs vai Satversmes aizsardzības birojs atbilstoši Nacionālās kiberdrošības likuma 41. pantā noteiktajam uzraudzības dalījumam par konstatēto neatbilstību ziņo Ministru kabinetam.

8.5. Piekļuves slēgšana elektronisko sakaru tīklam

147. Nacionālās kiberdrošības likuma 34. panta desmitajā daļā minēto pieprasījumu slēgt lietotājam piekļuvi elektronisko sakaru tīklam (turpmāk – piekļuves slēgšanas pieprasījums) Nacionālais kiberdrošības centrs vai Satversmes aizsardzības birojs paziņo elektronisko sakaru komersantam, kura pakalpojumus lietotājs izmanto, un lietotājam, kā arī par piekļuves slēgšanas pieprasījuma nosūtīšanas faktu informē Valsts policiju.

148. Pēc piekļuves slēgšanas pieprasījuma saņemšanas elektronisko sakaru komersants nekavējoties atslēdz

lietotāju no elektronisko sakaru tīkla un veic darbības, ko noteicis Nacionālais kiberdrošības centrs vai Satversmes aizsardzības birojs (piemēram, novirza lietotāja IP adreses vai domēna vārda pieprasījumus uz piekļuves slēgšanas pieprasījumā norādīto vietni).

149. Lietotāju atslēdz no elektronisko sakaru tīkla tā, lai šī darbība skartu pēc iespējas mazāku skaitu citu lietotāju.

150. Pēc piekļuves slēgšanas pieprasījumā norādītā laikposma beigām elektronisko sakaru komersants atjauno lietotājam piekļuvi elektronisko sakaru tīklam, ja vien nepastāv objektīvi iemesli piekļuves neatjaunošanai (piemēram, līgumisko attiecību izbeigšanās starp elektronisko sakaru komersantu un lietotāju).

9. Noslēguma jautājumi

151. Subjekts, kas iegūst A, B vai C kategorijas IKT kritiskās infrastruktūras īpašnieka vai tiesiskā valdītāja statusu pēc šo noteikumu spēkā stāšanās, nodrošina atbilstību šajos noteikumos noteiktajām prasībām 12 mēnešu laikā no šo noteikumu 109.3. apakšpunktā minētās informācijas saņemšanas brīža.

152. Sešu mēnešu laikā no šo noteikumu spēkā stāšanās brīža par noslēgtiem ārpakalpojumu līgumiem un iegādātiem IKT infrastruktūrā izmantotajiem tehniskajiem resursiem, kas neatbilst šo noteikumu prasībām:

152.1. IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs informē Satversmes aizsardzības biroju, sniedzot konstatētās neatbilstības aprakstu;

152.2. būtisko pakalpojumu sniedzējs, kas nav IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs, informē Satversmes aizsardzības biroju un Nacionālo kiberdrošības centru, sniedzot konstatētās neatbilstības aprakstu;

152.3. svarīgo pakalpojumu sniedzējs, kas nav IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs, informē Nacionālo kiberdrošības centru, sniedzot konstatētās neatbilstības aprakstu.

153. Ārpakalpojumu līgumi, kas noslēgti pirms šo noteikumu stāšanās spēkā un neatbilst šajos noteikumos noteiktajām ārpakalpojumu prasībām, var palikt spēkā līdz pilnīgai saistību izpildei, bet ne ilgāk kā piecus gadus no konkrētā ārpakalpojuma līguma noslēgšanas dienas.

154. Šajos noteikumos noteiktās ārpakalpojumu prasības var nepiemērot publiskajiem iepirkumiem, kuri ir uzsākti pirms šo noteikumu spēkā stāšanās.

155. Publiskajiem elektronisko sakaru tīkliem, kuri līdz šo noteikumu spēkā stāšanās dienai ir nodoti ekspluatācijā vai šo noteikumu spēkā stāšanās dienā atrodas projektēšanas, būvniecības, ierīkošanas vai pārbūves stadijā, šo noteikumu 102. punktā minētās prasības piemēro no 2030. gada 1. janvāra.

156. Kiberincidentu novēršanas institūcijas vadītājs pirmreizēji par kiberincidentu novēršanas institūcijas atbilstību šo noteikumu 115. punktā noteiktajām prasībām informē Nacionālo kiberdrošības centru līdz 2025. gada 31. decembrim.

157. Nacionālais kiberdrošības centrs sadarbībā ar Satversmes aizsardzības biroju līdz 2025. gada 1. septembrim

izstrādā šo noteikumu 38. un 88. punktā minētās vadlīnijas.

158. Atzīt par spēku zaudējušiem Ministru kabineta 2023. gada 28. februāra noteikumus Nr. 94 "Publisko elektronisko sakaru tīklu drošības prasības" (Latvijas Vēstnesis, 2023, 46. nr.).

Informatīva atsauce uz Eiropas Savienības direktīvu

Noteikumos iekļautas tiesību normas, kas izriet no Eiropas Parlamenta un Padomes 2022. gada 14. decembra Direktīvas (ES) 2022/2555, ar ko paredz pasākumus nolūkā panākt vienādi augstu kiberdrošības līmeni visā Savienībā un ar ko groza Regulu (ES) Nr. 910/2014 un Direktīvu (ES) 2018/1972 un atceļ Direktīvu (ES) 2016/1148 (TID 2 direktīva).

Ministru prezidente *E. Siliņa*

Aizsardzības ministra pienākumu izpildītāja – kultūras ministre *A. Lāce*

Aizsardzības ministrijas iesniegtajā redakcijā

1. pielikums
Ministru kabineta
2025. gada 25. jūnija
noteikumiem Nr. 397

Būtisko vai svarīgo pakalpojumu sniedzēja statusa paziņojuma veidlapa

BŪTISKO VAI SVARĪGO PAKALPOJUMU SNIEDZĒJA STATUSA PAZIŅOJUMS

Lūgums atzīmēt atbilstošo paziņojuma veidu:

☐ par atbilstību būtisko vai svarīgo pakalpojumu sniedzēja statusam

☐ par izmaiņām iepriekš norādītajos datos

☐ par būtisko vai svarīgo pakalpojumu sniedzēja statusa zaudēšanu

1. Pamatinformācija

Nosaukums (fiz. personai – vārds, uzvārds):

Reģistrācijas Nr. (fiz. personai – pers. kods):

Juridiskais statuss:

☐ tiešās pārvaldes iestāde;
☐ atvasināta publiska persona
☐ pastarpinātās pārvaldes iestāde
☐ cita valsts institūcija
☐ privāto tiesību juridiskā persona – lūgums norādīt darbības formu:
☐ fiziskā persona
☐ cits statuss – lūgums norādīt, kāds:

2. Kontaktinformācija

Juridiskā adrese:

E-pasta adrese:

Tālruņa numurs:

Tīmekļvietnes adrese (ja ir):

3. Pakalpojumu sniedzēja statuss

Pakalpojumu sniedzēja statuss:

☐ **būtisko pakalpojumu sniedzējs** (NKDL 20. pants)
☐ **svarīgo pakalpojumu sniedzējs** (NKDL 21. pants)
☐ **nav būtisko vai svarīgo pakalpojumu sniedzējs**
(atzīmēt tikai subjekta statusa zaudēšanas gadījumā)

4. Darbības joma

Drošībai nozīmīgs subjekts

Vai subjekts ir sabiedrības drošībai, sabiedrībai vai veselībai nozīmīga organizācija (1) (piemēram, nacionālajai drošībai nozīmīga komercsabiedrība)

☐ Jā ☐ Nē

Būtisko pakalpojumu jomas

Lūgums atzīmēt visas atbilstošās būtisko pakalpojumu jomas, kurās darbojas subjekts (ja attiecināms):

Nozare	Kods	Būtisko pakalpojumu joma	
Valsts pārvalde	01	tiešās pārvaldes iestāde vai cita valsts institūcija	☐
	02	atvasināta publiskā persona	☐
	03	pastarpinātās pārvaldes iestāde	☐
	04	privāto tiesību juridiskā persona, kura pilda valsts pārvaldes deleģētu uzdevumu	☐
Mediji, elektroniskie sakari un uzticamības pakalpojumi	05	sabiedriskais elektroniskais plašsaziņas līdzeklis	☐
	06	elektronisko sakaru komersants	☐
	07	kvalificēts uzticamības pakalpojumu sniedzējs	☐
Digitālā infrastruktūra	08	augstākā līmeņa domēnu nosaukumu reģistra uzturētājs	☐
	09	domēnu nosaukumu sistēmas pakalpojumu sniedzējs	☐
	10	interneta plūsmu apmaiņas punkta pakalpojumu sniedzējs	☐
	11	mākoņdatošanas pakalpojumu sniedzējs	☐
	12	datu centru pakalpojumu sniedzējs	☐
	13	satura piegādes tīkla pakalpojumu sniedzējs	☐
	14	IKT pārvaldības vai kiberdrošības pakalpojumu sniedzējs	☐
Enerģētika	15	energoapgādes komersants	☐
	16	naftas apgādes komersants	☐
	17	ūdeņraža apgādes komersants	☐

Transports	18	aeronavigācijas pakalpojumu sniedzējs, gaisa kuģa ekspluatants vai lidlauka vai citu civilās aviācijas objektu un iekārtu ekspluatants	☐
	19	dzelzceļa pārvadātājs vai dzelzceļa infrastruktūras pārvaldītājs	☐
	20	kuģošanas kompānija, neietverot šīs kompānijas pārvaldītos individuālus kuģus	☐
	21	ostas pārvalde	☐
	22	komersants, kurš veic komercdarbību ostas teritorijā	☐
	23	komersants, kurš pārvalda valsts autoceļus vai veic valsts autoceļu infrastruktūras uzturēšanas darbus	☐
	24	intelektisko transporta sistēmu operators	☐

(1) Iestāde vai saimnieciskās darbības veicējs, kura darbības traucējums var būtiski ietekmēt sabiedrības drošību, valsts aizsardzību, sabiedrības veselību vai var radīt būtisku sistēmisku risku, jo īpaši nozarēs, kurās šādam traucējumam var būt pārrobežu ietekme.

(2) Pakalpojumu sniedzējs, kas sniedz publiski pieejamus rekursīvus domēnu nosaukumu atrises pakalpojumus interneta galalietotājiem vai autoritatīvus domēnu nosaukumu atrises pakalpojumus trešo personu lietošanai, izņemot saknes nosaukumu serverus;

Banku un finanšu pakalpojumi	25	kredītiestāde, centrālais darījumu partneris vai tirdzniecības vieta Finanšu instrumentu tirgus likuma izpratnē	☐
Veselības aprūpe un laboratorijas	26	ārstniecības iestāde	☐
	27	Eiropas Savienības references laboratorija	☐
	28	komersants, kas veic izpētes un izstrādes darbības attiecībā uz zālēm, ražo zāles un aktīvās vielas	☐
	29	kritiski svarīgu medicīnisko ierīču ražotājs (3)	☐
Dzeramais ūdens	30	dzeramā ūdens piegādātājs vai izplatītājs, izņemot gadījumu, kad komersanta pamatdarbība nav saistīta ar dzeramā ūdens izplatīšanu	☐
	31	ūdenssaimniecības pakalpojumu sniedzējs	☐
Kosmoss	32	kosmosā izvietotu pakalpojumu sniedzējs vai šo pakalpojumu sniegšanai izmantojamās infrastruktūras operators	☐

Cits	99	cits būtiskais pakalpojums (piemēram, pakalpojums, kura traucējums var būtiski ietekmēt sabiedrības drošību, valsts aizsardzību, sabiedrības veselību vai var radīt būtisku sistēmisku risku)	☐

Ja attiecināms, lūdzu, aprakstīt subjekta sniegtos būtiskos pakalpojumus (līdz 100 vārdiem par katru pakalpojumu):

Svarīgo pakalpojumu jomas

Lūgums atzīmēt visas atbilstošās svarīgo pakalpojumu jomas, kurās darbojas subjekts:

Nozare	Kods	Būtisko pakalpojumu joma	
Uzticamības pakalpojumi	33	cits uzticamības pakalpojumu sniedzējs	☐
Pasts un kurjeri	34	pasta komersants	☐
Atkritumi	35	atkritumu apsaimniekotājs	☐
Ķimikālijas	36	ķīmisko vielu vai to maisījumu ražotājs vai izplatītājs vairumtirdzniecībā, ja ķīmisko vielu vai to maisījumu izplatīšana ir komersanta pamatdarbība	☐
	37	komersants, kurš ražo izstrādājumus no ķīmiskajām vielām vai to maisījumiem	☐
Pārtika	38	komersants, kura pamatdarbība ir pārtikas rūpnieciska ražošana, pārstrāde vai pārtikas izplatīšana vairumtirdzniecībā	☐
Industriālā ražošana	39	medicīnisko ierīču ražotājs	☐
	40	datoru, elektronisko un optisko iekārtu ražotājs	☐
	41	elektrisko iekārtu ražotājs	☐
	42	citur neklasificētu iekārtu, mehānismu un darba mašīnu ražotājs	☐
	43	automobiļu, piekabju un puspiekabju ražotājs	☐
	44	citu transportlīdzekļu ražotājs	☐

(3) Atbilstoši Eiropas Parlamenta un Padomes 2022. gada 25. janvāra regulas (ES) 2022/123 par pastiprinātu Eiropas Zāļu aģentūras lomu attiecībā uz zālēm un medicīniskajām ierīcēm krīžgatavības un krīžu pārvarēšanas kontekstā 22. pantam.

Digitālie pakalpojumi	45	tiešsaistes tirdzniecības vietas pakalpojumu sniedzējs	☐
	46	tiešsaistes meklētājprogrammas pakalpojumu sniedzējs	☐
	47	sociālo mediju platformas pakalpojumu sniedzējs	☐
Izglītība un zinātne	48	zinātniskā institūcija	☐
	49	izglītības informācijas sistēmas uzturētājs (4)	☐
Apsardze	50	apsardzes pakalpojumu sniedzējs	☐

Ja attiecināms, lūdzu, aprakstīt subjekta sniegtos svarīgos pakalpojumus (līdz 100 vārdiem par katru pakalpojumu):

Vienīgais būtiskā vai svarīgā pakalpojuma sniedzējs

Vai subjekts ir vienīgais iepriekš norādītā pakalpojuma veida sniedzējs Latvijas Republikā?

☐ Jā ☐ Nē

Ja jā, lūgums norādīt pakalpojuma veidu:

5. Valstis, kurās subjekts sniedz pakalpojumus

Lūdzu, norādiet visas valstis, kurās subjekts sniedz pakalpojumus:

6. IP adrešu diapazoni un domēnu nosaukumi

Lūdzu, norādiet subjekta pastāvīgi izmantojamo interneta protokola (IP) adrešu diapazonus:

Lūdzu, norādiet subjekta izmantojamos domēnu nosaukumus (nav obligāti):

7. Kontaktpersona

Kontaktpersonas vārds, uzvārds:	
Kontaktpersonas amats:	
Kontaktpersonas e-pasts:	
Kontaktpersonas tālruņa Nr.:	

(4) Izglītības informācijas sistēma ir tāda informācijas sistēma, kurā tiek veikta Latvijas Republikā akreditētas izglītības iestādes izglītojamo personas datu elektroniskā apstrāde

8. Kiberdrošības pārvaldnieks (ja ir jau nozīmēts)

Vārds, uzvārds:	
Personas kods:	
Amats:	
E-pasta adrese:	
Tālruņa Nr.:	

Aizsardzības ministrijas iesniegtajā redakcijā

2. pielikums
Ministru kabineta
2025. gada 25. jūnija
noteikumiem Nr. 397

Domēnu nosaukumu reģistrācijas pakalpojumu sniedzēja statusa paziņojuma veidlapa

DOMĒNU NOSAUKUMU REĢISTRĀCIJAS PAKALPOJUMU SNIEDZĒJA STATUSA PAZIŅOJUMS

Lūgums atzīmēt atbilstošo paziņojuma veidu:

☐ par atbilstību domēnu nosaukumu reģistrācijas pakalpojumu sniedzēja statusam

☐ par izmaiņām iepriekš norādītajos datos

☐ par domēnu nosaukumu reģistrācijas pakalpojumu sniedzēja statusa zaudēšanu

1. Pamatinformācija

Nosaukums (fiz. personai – vārds, uzvārds)**:**

Reģistrācijas Nr. (fiz. personai – pers. kods):

Juridiskais statuss:

☐ tiešās pārvaldes iestāde;
☐ atvasināta publiska persona
☐ pastarpinātās pārvaldes iestāde
☐ cita valsts institūcija
☐ privāto tiesību juridiskā persona – lūgums norādīt darbības formu:
☐ fiziskā persona
☐ cits statuss – lūgums norādīt, kāds:

2. Kontaktinformācija

Juridiskā adrese:

E-pasta adrese:

Tālruņa numurs:

Tīmekļvietnes adrese (ja ir):

3. Domēnu nosaukumu reģistrācijas pakalpojumu sniedzēja statuss

Pašreizējais statuss: ☐ **domēnu nosaukumu reģistrācijas pakalpojumu sniedzējs**

☐ **nav domēnu nosaukumu reģistrācijas pakalpojumu sniedzējs**
(atzīmēt statusa zaudēšanas gadījumā)

Papildu statuss:
(atzīmēt, ja attiecināms):

☐ **būtisko pakalpojumu sniedzējs** (NKDL 20. pants)
☐ **svarīgo pakalpojumu sniedzējs** (NKDL 21. pants)

4. Valstis, kurās subjekts sniedz pakalpojumus

Lūdzu, norādiet visas valstis, kurās domēnu nosaukumu reģistrācijas pakalpojumu sniedzējs sniedz pakalpojumus:

5. Būtiskie un svarīgie pakalpojumi
(aizpilda, ja domēnu nosaukumu reģistrācijas pakalpojumu sniedzējs ir arī būtisko pakalpojumu sniedzējs vai svarīgo pakalpojumu sniedzējs)

Drošībai nozīmīga organizācija
Vai domēnu nosaukumu reģistrācijas pakalpojumu sniedzējs ir sabiedrības drošībai, sabiedrībai vai veselībai nozīmīga organizācija[1] (piemēram, nacionālajai drošībai nozīmīga komercsabiedrība)

☐ Jā ☐ Nē

Būtisko pakalpojumu jomas
Lūgums atzīmēt visas atbilstošās būtisko pakalpojumu jomas, kurās darbojas domēnu nosaukumu reģistrācijas pakalpojumu sniedzējs:

Nozare	**Kods**	**Būtisko pakalpojumu joma**	
Valsts pārvalde	01	tiešās pārvaldes iestāde vai cita valsts institūcija	☐
	02	atvasināta publiskā persona	☐
	03	pastarpinātās pārvaldes iestāde	☐
	04	privāto tiesību juridiskā persona, kura pilda valsts pārvaldes deleģētu uzdevumu	☐
Mediji, elektroniskie sakari un uzticamības pakalpojumi	05	sabiedriskais elektroniskais plašsaziņas līdzeklis	☐
	06	elektronisko sakaru komersants	☐
	07	kvalificēts uzticamības pakalpojumu sniedzējs	☐
	08	cits uzticamības pakalpojumu sniedzējs	☐
Digitālā infrastruktūra	09	augstākā līmeņa domēnu nosaukumu reģistra uzturētājs	☐
	10	domēnu nosaukumu sistēmas pakalpojumu sniedzējs[2]	☐
	11	interneta plūsmu apmaiņas punkta pakalpojumu sniedzējs	☐
	12	mākoņdatošanas pakalpojumu sniedzējs	☐
	13	datu centru pakalpojumu sniedzējs	☐
	14	satura piegādes tīkla pakalpojumu sniedzējs	☐
	15	IKT pārvaldības vai kiberdrošības pakalpojumu sniedzējs	☐
Enerģētika	16	energoapgādes komersants	☐

	17	naftas apgādes komersants	☐
	18	ūdeņraža apgādes komersants	☐
Transports	19	aeronavigācijas pakalpojumu sniedzējs, gaisa kuģa ekspluatants vai lidlauka vai citu civilās aviācijas objektu un iekārtu ekspluatants	☐
	20	dzelzceļa pārvadātājs vai dzelzceļa infrastruktūras pārvaldītājs	☐
	21	kuģošanas kompānija, neietverot šīs kompānijas pārvaldītos individuālus kuģus	☐
	22	ostas pārvalde	☐
	23	komersants, kurš veic komercdarbību ostas teritorijā	☐
	24	komersants, kurš pārvalda valsts autoceļus vai veic valsts autoceļu infrastruktūras uzturēšanas darbus	☐
	25	intelektisko transporta sistēmu operators	☐
Banku un finanšu pakalpojumi	26	kredītiestāde, centrālais darījumu partneris vai tirdzniecības vieta Finanšu instrumentu tirgus likuma izpratnē	☐
Veselības aprūpe un laboratorijas	27	ārstniecības iestāde	☐
	28	Eiropas Savienības references laboratorija	☐
	29	komersants, kas veic izpētes un izstrādes darbības attiecībā uz zālēm, ražo zāles un aktīvās vielas	☐
	30	kritiski svarīgu medicīnisko ierīču ražotājs[3]	☐
Dzeramais ūdens	31	dzeramā ūdens piegādātājs vai izplatītājs, izņemot gadījumu, kad komersanta pamatdarbība nav saistīta ar dzeramā ūdens izplatīšanu	☐
	32	ūdenssaimniecības pakalpojumu sniedzējs	☐
Kosmoss	33	kosmosā izvietotu pakalpojumu sniedzējs vai šo pakalpojumu sniegšanai izmantojamās infrastruktūras operators	☐

Cits	99	cits būtiskais pakalpojums (piemēram, pakalpojums, kura traucējums var būtiski ietekmēt sabiedrības drošību, valsts aizsardzību, sabiedrības veselību vai var radīt būtisku sistēmisku risku)	☐

Ja attiecināms, lūdzu, aprakstīt domēnu nosaukumu reģistrācijas pakalpojumu sniedzēja sniegtos būtiskos pakalpojumus (līdz 100 vārdiem par katru pakalpojumu):

Svarīgo pakalpojumu jomas

Lūgums atzīmēt visas atbilstošās svarīgo pakalpojumu jomas, kurās darbojas domēnu nosaukumu reģistrācijas pakalpojumu sniedzējs:

Nozare	**Kods**	**Svarīgo pakalpojumu joma**	
Pasts un kurjerpakalpojumi	34	pasta komersants	☐
Atkritumi	35	atkritumu apsaimniekotājs	☐
Ķimikālijas	36	ķīmisko vielu vai to maisījumu ražotājs vai izplatītājs vairumtirdzniecībā, ja ķīmisko vielu vai to maisījumu izplatīšana ir komersanta pamatdarbība	☐

	37	komersants, kurš ražo izstrādājumus no ķīmiskajām vielām vai to maisījumiem	☐
Pārtika	38	komersants, kura pamatdarbība ir pārtikas rūpnieciska ražošana, pārstrāde vai pārtikas izplatīšana vairumtirdzniecībā	☐
Industriālā ražošana	39	medicīnisko ierīču ražotājs	☐
	40	datoru, elektronisko un optisko iekārtu ražotājs	☐
	41	elektrisko iekārtu ražotājs	☐
	42	citur neklasificētu iekārtu, mehānismu un darba mašīnu ražotājs	☐
	43	automobiļu, piekabju un puspiekabju ražotājs	☐
	44	citu transportlīdzekļu ražotājs	☐
Digitālie pakalpojumi	45	tiešsaistes tirdzniecības vietas pakalpojumu sniedzējs	☐
	46	tiešsaistes meklētājprogrammas pakalpojumu sniedzējs	☐
	47	sociālo mediju platformas pakalpojumu sniedzējs	☐
Izglītība un zinātne	48	zinātniskā institūcija	☐
	49	izglītības informācijas sistēmas uzturētājs[4]	☐
Apsardze	50	apsardzes pakalpojumu sniedzējs	☐

Ja attiecināms, lūdzu, aprakstīt domēnu nosaukumu reģistrācijas pakalpojumu sniedzēja sniegtos svarīgos pakalpojumus (līdz 100 vārdiem par katru pakalpojumu):

Vienīgais būtiskā vai svarīgā pakalpojuma sniedzējs

Vai domēnu nosaukumu reģistrācijas pakalpojumu sniedzējs ir vienīgais iepriekš norādītā būtiskā vai svarīgā pakalpojumu veida sniedzējs Latvijas Republikā?

☐ Jā ☐ Nē

Ja jā, lūgums norādīt pakalpojuma veidu:

5. IP adrešu diapazoni un domēnu nosaukumi

Lūdzu, norādiet domēnu nosaukumu reģistrācijas pakalpojumu sniedzēja pastāvīgi izmantojamo interneta protokola (IP) adrešu diapazonus:

Lūdzu, norādiet domēnu nosaukumu reģistrācijas pakalpojumu sniedzēja pastāvīgi izmantojamos domēnu nosaukumus (ja ir attiecināms):

6. Kontaktpersona

Kontaktpersonas vārds, uzvārds:

Kontaktpersonas amats:	
Kontaktpersonas e-pasts:	
Kontaktpersonas tālruņa Nr.:	

---

[1] Iestāde vai saimnieciskās darbības veicējs, kura darbības traucējums var būtiski ietekmēt sabiedrības drošību, valsts aizsardzību, sabiedrības veselību vai var radīt būtisku sistēmisku risku, jo īpaši nozarēs, kurās šādam traucējumam var būt pārrobežu ietekme.

[2] Pakalpojumu sniedzējs, kas sniedz publiski pieejamus rekursīvus domēnu nosaukumu atrises pakalpojumus interneta galalietotājiem vai autoritatīvus domēnu nosaukumu atrises pakalpojumus trešo personu lietošanai, izņemot saknes nosaukumu serverus;

[3] Atbilstoši Eiropas Parlamenta un Padomes 2022. gada 25. janvāra regulas (ES) 2022/123 par pastiprinātu Eiropas Zāļu aģentūras lomu attiecībā uz zālēm un medicīniskajām ierīcēm krīžgatavības un krīžu pārvarēšanas kontekstā 22. pantam.

[4] Izglītības informācijas sistēma ir tāda informācijas sistēma, kurā tiek veikta Latvijas Republikā akreditētas izglītības iestādes izglītojamo personas datu elektroniskā apstrāde

Aizsardzības ministrijas iesniegtajā redakcijā

3. pielikums
Ministru kabineta
2025. gada 25. jūnija
noteikumiem Nr. 397

Paziņojuma par kiberdrošības pārvaldnieku veidlapa

PAZIŅOJUMS PAR KIBERDROŠĪBAS PĀRVALDNIEKU

Lūgums atzīmēt atbilstošo paziņojuma veidu:

☐ par jauna kiberdrošības pārvaldnieka nozīmēšanu

☐ par izmaiņām iepriekš norādītajos datos

1. Subjekta pamatinformācija

Nosaukums (fiz. personai – vārds, uzvārds)**:**

Reģistrācijas Nr. (fiz. personai – pers. kods):

2. Kiberdrošības pārvaldnieks

Vārds, uzvārds:

Personas kods:

Amats:

E-pasta adrese:

Tālruņa numurs:

3. Kiberdrošības pārvaldnieka apliecinājums

☐ Apliecinu, ka kiberdrošības pārvaldnieks atbilst normatīvajos aktos par minimālajām kiberdrošības prasībām noteiktajām prasībām (tostarp attiecībā uz kiberdrošības pārvaldnieka kvalifikāciju un atbilstību drošības prasībām).

☐ Apliecinu, ka kiberdrošības pārvaldniekam ir nepieciešamās zināšanas, prasmes un pieredze, lai efektīvi pildītu kiberdrošības pārvaldnieka pienākumus.

☐ Apliecinu, ka piekrītu būt par kiberdrošības pārvaldnieku.

Aizsardzības ministrijas iesniegtajā redakcijā

4. pielikums
Ministru kabineta
2025. gada 25. jūnija
noteikumiem Nr. 397

Kiberdrošības pārvaldnieka pretendenta saskaņošanas veidlapa

PAR KIBERDROŠĪBAS PĀRVALDNIEKA PRETENDENTA SASKAŅOŠANU

1. Subjekta pamatinformācija

Nosaukums (fiz. personai – vārds, uzvārds):	
Reģistrācijas Nr. (fiz. personai – pers. kods):	

2. Kiberdrošības pārvaldnieka pretendents

Vārds, uzvārds:	
Personas kods:	

3. Prasības

IKT kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs par kiberdrošības pārvaldnieku nosaka fizisku personu:
– kurai ir Latvijas pilsonība;
– kura ir pilngadīga;
– pār kuru nav nodibināta aizgādnība;
– kura nav sodīta par tīšu noziedzīgu nodarījumu, izņemot, ja persona ir reabilitēta, vai sodāmība ir noņemta vai dzēsta;
– kurai ir augstākā vai vidējā profesionālā izglītība informācijas tehnoloģiju, kiberdrošības pārvaldības vai citā saistītā jomā un vismaz divu gadu darba pieredze kiberdrošības pārvaldībā, kas iegūta pēdējo piecu gadu laikā, vai kurai ir spēkā esošs starptautiski atzīts sertifikāts, kas apliecina personas kvalifikāciju kiberdrošības jomā (piemēram, CISM, CISSP);
– kura nav un nav bijusi PSRS, Latvijas PSR vai kādas ārvalsts drošības dienesta, izlūkdienesta vai pretizlūkošanas dienesta štata vai ārštata darbinieks, aģents, rezidents vai konspiratīvā dzīvokļa turētājs;
– kura nav un nav bijusi ar Latvijas Republikas likumiem, Augstākās padomes lēmumiem vai tiesas nolēmumiem aizliegto organizāciju dalībnieks (biedrs) pēc šo organizāciju aizliegšanas;
– kura nepieder pie organizētās noziedzības grupējuma, nelikumīga militarizēta vai bruņota formējuma;
– kurai nav diagnosticēti psihiski traucējumi vai alkohola, narkotisko, psihotropo vai toksisko vielu atkarība, kas dod pamatu apšaubīt fiziskās personas uzticamību;
– par kuru Satversmes aizsardzības birojs nav konstatējis drošības riskus.

4. Apliecinājums

Es, _____, ar savu elektronisko parakstu apliecinu, ka:
(pretendenta vārds, uzvārds)

☐ esmu informēts un piekrītu pildīt kiberdrošības pārvaldnieka pienākumus;

☐ atbilstu kiberdrošības pārvaldniekam izvirzītajām prasībām un manā rīcībā nav informācija par iespējamiem drošības riskiem, kas varētu liegt man pildīt kiberdrošības pārvaldnieka pienākumus;

☐ esmu informēts un piekrītu, ka Satversmes aizsardzības birojs veic manu personas datu apstrādi un manis kā kiberdrošības pārvaldnieka pretendenta pārbaudi.

Svarīgi! Veidlapu elektroniski paraksta gan konkrētā subjekta vadītājs, gan kiberdrošības pārvaldnieka pretendents

5. pielikums
Ministru kabineta
2025. gada 25. jūnija
noteikumiem Nr. 397

Metodika informācijas sistēmas konfidencialitātes, integritātes un pieejamības drošības klases noteikšanai pēc tajā elektroniski apstrādājamajiem informācijas resursiem

Drošības klase	**Pazīmes**		
	Konfidencialitātes klase	Integritātes klase	Pieejamības klase
A klase (augstākais riska līmenis)	informācijas resurss satur vismaz 1 000 000 datu subjektu personas datus	informācijas resurss ļauj informācijas sistēmā veikt darbības ar personai piederošo nekustamo īpašumu vai transportlīdzekļu īpašumtiesību reģistrāciju	informācijas resursa pieejamības neplānots pārtraukums informācijas sistēmas paredzētajā darbības laikā summāri nedrīkst pārsniegt 0,1 % mēnesī
	informācijas resurss satur vismaz 500 000 datu subjektu īpašu kategoriju personas datus	informācijas resursa integritātes pārkāpums var pārtraukt vai būtiski apgrūtināt valsts vai pašvaldības pamatfunkciju īstenošanu vai kritiskās infrastruktūras darbību	informācijas resursa nepieejamība var pārtraukt vai būtiski apgrūtināt valsts vai pašvaldības pamatfunkciju īstenošanu vai kritiskās infrastruktūras darbību
	informācijas resurss satur informāciju, kuras neatļauta izpaušana vai noplūde kaitētu nacionālās drošības interesēm	informācijas resursa integritātes pārkāpums var izraisīt katastrofu	no informācijas resursa pieejamības ir atkarīga citas informācijas sistēmas darbība, kurai noteikta A pieejamības klase
B klase (vidējais riska līmenis)	informācijas resurss satur ierobežotas pieejamības informāciju vai vismaz 5000 datu subjektu īpašu kategoriju personas datus	informācijas resursa integritātes pārkāpums var pārtraukt vai būtiski apgrūtināt subjekta darbību vai tā būtiskā vai svarīgā pakalpojuma sniegšanu	informācijas resursa pieejamības neplānots pārtraukums informācijas sistēmas paredzētajā darbības laikā summāri nedrīkst pārsniegt 1 % mēnesī
	informācijas resurss satur informāciju, kuras neatļauta izpaušana vai noplūde kaitētu Latvijas Republikas reputācijai	informācijas resursa integritātes pārkāpums var pārtraukt vai būtiski apgrūtināt citu subjektu darbību vai to sniegto būtisko un svarīgo pakalpojumu sniegšanu	no informācijas resursa pieejamības ir atkarīga citas informācijas sistēmas darbība, kurai noteikta B pieejamības klase
C klase (zemākais riska līmenis)	informācijas resurss satur informāciju, kuras neatļauta izpaušana vai noplūde neradītu kaitējumu Latvijas Republikas reputācijai	informācijas resursa integritātes pārkāpums būtiski neietekmē subjekta vai citu subjektu pamatfunkciju īstenošanu, būtisko vai svarīgo	informācijas resursa pieejamības neplānots pārtraukums informācijas sistēmas paredzētajā darbības laikā summāri drīkst pārsniegt 1 %

		pakalpojumu sniegšanu	mēnesī

6. pielikums
Ministru kabineta
2025. gada 25. jūnija
noteikumiem Nr. 397

Publisko elektronisko sakaru tīklu kritiskās daļas

1. Par publiskā elektronisko sakaru tīkla (turpmāk – sakaru tīkls) kritisko daļu tiek atzīta tāda daļa, ar kuru pilnībā vai daļēji īsteno vismaz vienu no šādām funkcijām:

1.1. galvenās maršrutēšanas funkcijas un cita veida galalietotāju datplūsmas kontrole vai vadīšana sakaru tīklā, kas var būtiski ietekmēt datplūsmu sakaru tīklā (piemēram, sakaru tīkla vai pakalpojuma sastāvdaļas, ja tās kontrolē vai vada būtisku datplūsmas daļu visā tīklā);

1.2. galalietotāju piekļuves pārvaldība, verifikācija un apstiprināšana, tīkla IKT resursu piešķiršana galalietotājiem un galalietotāju savienojumu un sesiju pārvaldība;

1.3. sakaru tīkla un pakalpojumu funkciju reģistrācija, verifikācija un apstiprināšana;

1.4. infrastruktūras pakalpojumi, kas vajadzīgi sakaru tīkla un pakalpojumu darbībai un tā darbības atbalstam;

1.5. funkcijas, ko izmanto, lai īstenotu saskarnes starp sakaru tīkliem vai pakalpojumiem, tostarp viesabonēšanu;

1.6. funkcijas, kas savstarpēji savieno sakaru tīklus vai pakalpojumus, ja šāda funkcija var būtiski ietekmēt piekļuvi sakaru tīklam vai datplūsmu caur tīklu;

1.7. galvenās drošības funkcijas (piemēram, centralizēta sakaru tīkla, tā funkciju un galalietotāju šifrēšanas un atslēgu pārvaldība);

1.8. tīkla pārvaldības un tīkla uzraudzības sistēmas, ja tās attiecas uz sakaru tīkla kritisko daļu pārvaldību vai uzraudzību vai ja tās citādi var būtiski ietekmēt piekļuvi tīklam vai datplūsmu tīklā, kā arī citas rēķinu sagatavošanas, atbalsta un aizmugursistēmas, kas var būtiski ietekmēt piekļuvi sakaru tīklam vai datplūsmu tīklā;

1.9. funkcijas, kas veic telekomunikāciju pārtveršanu vai uzraudzību tiesībaizsardzības iestāžu vajadzībām;

1.10. virtualizācija, ja to izmanto tādas funkcijas vai pasākuma īstenošanai, ko uzskata par kritisku sakaru tīkla daļu;

1.11. jebkura cita funkcija vai pasākums, ja to īsteno, izmantojot virtualizāciju, ko uzskata par kritisku sakaru tīkla daļu, kas minēta šā pielikuma 1.10. apakšpunktā;

1.12. galvenās funkcijas un pasākumi, kas ļauj piekļūt datiem par sakaru tīklā apstrādātās saskarnes vai galiekārtas ģeogrāfisko atrašanās vietu vai ļauj noteikt atrašanās vietu, izmantojot sakaru tīklu.

2. Papildus šā pielikuma 1. punktā minētajām sakaru tīkla kritiskās daļas 4G tīkla pamatfunkcijām ir pakotņu komutācijas funkcijas tādā apmērā, kādā tās būtiski kontrolē vai vada piekļuvi tīklam un datplūsmu tīklā. Sakaru tīkla kritiskās daļas ietver vismaz tās funkcijas un pasākumus, kas pilnīgi vai daļēji īsteno vienu no šā pielikuma 1. tabulā norādītajām 4G tīkla funkcijām.

1. tabula

4G tīkla kritiskās daļas

Nr. p. k.	Funkcijas	Apraksts
2.1.	Mājas abonentu serveris (HSS)	Abonentu reģistrs, kurā glabā datus, lai apstrādātu lietotāja sesijas un savienojumus
2.2.	Iekārtu identifikatoru reģistrs (EIF)	Iekārtu identifikatoru reģistrs, kurā ir informācija par atļauju izmantot mobilās ierīces
2.3.	Abonementa atrašanās vietas noteikšanas funkcija (SLF)	Funkcija, kas uz citām tīkla funkcijām pārraida centrālās datubāzes nosaukumu, kurā ir lietotāja dati (HSS)
2.4.	Mobilo sakaru pārvaldības struktūra (MME)	Struktūrvienība, kas atbild par galiekārtas savienojumu un mobilitātes pārvaldību
2.5.	Apkalpojošā vārteja (SGW)	Apkalpojošā vārteja, kas atbild par datplūsmas maršrutēšanu lietotāja līmenī
2.6.	Pakešdatu tīkla vārteja (PDN GW)	Komutējama pakešu tīkla vārteja starp operatora iekšējo IP tīklu un ārējo IP tīklu
2.7.	Paplašināta pakešdatu vārteja (EPDG)	Vārteja lietotāju savienošanai ārpus mobilā tīkla
2.8.	3GPP AAA serveris un 3GPP AAA starpniekserveris	Serveris un starpniekserveris, kas atbild par lietotāju verifikāciju un apstiprināšanu ārpus mobilā tīkla
2.9.	Piekļuves tīkla noteikšana un atlases funkcija (ANDSF)	Funkcija, kas kontrolē lietotāja datplūsmu starp mobilo sakaru tīklu un fiksēto sakaru tīklu
2.10.	Politikas un maksas noteikumu funkcija (PCRF)	Lietotāja saskarnes politika un rēķinu izrakstīšanas funkcija

3. Papildus šā pielikuma 1. punktā minētajām sakaru tīkla kritiskās daļas 5G pamattīkla funkcijām ir arī citas funkcijas tādā mērā, kādā tās būtiski kontrolē vai vada piekļuvi tīklam un datplūsmu tīklā.

4. Sakaru tīkla kritiskās daļas ietver vismaz tās funkcijas un pasākumus, kas pilnīgi vai daļēji īsteno vienu no šā pielikuma 2. tabulā norādītajām 5G tīkla funkcijām.

2. tabula

5G tīkla kritiskās daļas

Nr. p. k.	Funkcijas	Apraksts
4.1.	Piekļuves un mobilo sakaru pārvaldības funkcija (AMF)	Atbild par lietotāju kontroles datplūsmas terminoloģiju, galiekārtu reģistrāciju un mobilo sakaru pārvaldību
4.2.	Lietotāja plaknes funkcija (UPF)	Atbild par lietotāja datplūsmas maršrutēšanu, vadīšanu un pārvaldību
4.3.	Politikas kontroles funkcija (PCF)	Atbild par datplūsmas kontroli un piekļuves pārvaldības politikas īstenošanu
4.4.	Autentifikācijas servera funkcija (AUSF)	Atbild par lietotāju galiekārtu verificēšanu
4.5.	Vienota datu pārvaldība (UDM)	Atbild par lietotāju piekļuves pārvaldību un šifrēšanas atslēgu izveidi un pārvaldību
4.6.	Lietojumprogrammas funkcija (AF)	Tiešsaistē atbalsta maršrutēšanas lēmumus

4.7.	Tīkla ekspozīcijas funkcija (NEF) un vidējā NEF (I-NEF)	Ļauj nodrošināt 5G pamattīkla funkcijas trešajām personām un ārējām lietojumprogrammām
4.8.	Tīkla repozitorija funkcija (NRF)	Atbild par tīkla pakalpojumu pieejamību, reģistrēšanu un apstiprināšanu
4.9.	Tīkla sadaļu atlases funkcija (NSSF)	Atbild par tīkla sadalīšanas pakalpojumiem un specifikācijām
4.10.	Tīkla sadaļu īpašās autentifikācijas un apstiprināšanas funkcija (NSAAF)	Atbild par tīkla sadaļu verifikāciju un apstiprināšanu
4.11.	Sesiju pārvaldības funkcija (SMF)	Atbild par lietotāja sesiju pārvaldību
4.12.	Drošmalu aizsardzības starpniekserveris (SEPP)	Starpniekserveris, kas ļauj nodrošināt savienojumu ar citiem tīkliem
4.13.	Nestrukturētu datu glabāšanas funkcija (UDSF)	Funkcija, ko izmanto, lai glabātu un izgūtu nestrukturētus datus
4.14.	Vienotais datu repozitorijs (UDR)	Repozitorijs, kas spēj glabāt un izgūt cita starpā abonenta informāciju
4.15.	UE radio iespēju pārvaldības funkcija (UCMF)	Funkcija, kas glabā un saglabā galiekārtu ID radio iespējas datus
4.16.	Funkcija mijiedarbībai ārpus 3GPP tīkla (N3IWF)	Funkcija, kas lietotājiem ārpus mobilā tīkla ļauj piekļūt tīkla funkcijām
4.17.	5G iekārtu identifikatoru reģistrs (5G-EIR)	Iekārtu identifikatoru reģistrs, kurā ir informācija par atļauju izmantot mobilās ierīces
4.18.	Pakalpojuma sakaru starpniekserviss (SCP)	Maršrutē ziņojumus uz citām tīkla funkcijām
4.19.	Tīkla datu analīzes funkcija (NWDAF), izņemot dalīto funkciju, tādā mērā, kādā tā būtiski nekontrolē vai nevada piekļuvi tīklam un datplūsmu tīklā	Vāc un analizē datus tīkla kontrolei

7. pielikums
Ministru kabineta
2025. gada 25. jūnija
noteikumiem Nr. 397

Kiberincidentu un gandrīz notikušu kiberincidentu tipoloģija

Kods	Kiberincidenta vai gandrīz notikuša kiberincidenta veids
01	Neatbilstošs saturs (piemēram, mēstule, nelegāls saturs)
02	Ļaundabīgs kods
03	Informācijas vākšana
04	Ielaušanās mēģinājums
05	Ielaušanās
06	Pieejamības traucējums
07	Datu drošības pārkāpums (piemēram, nesankcionēta piekļuve vai modificēšana)
08	Krāpniecība
09	Ievainojamība
10	Cits kiberincidenta veids
99	Pārbaude (mācības)

8. pielikums
Ministru kabineta
2025. gada 25. jūnija
noteikumiem Nr. 397

Satversmes aizsardzības biroja atzinuma pieprasījuma veidlapa

PAR ATZINUMA SAŅEMŠANU

1. Subjekta informācija

Nosaukums:

Reģistrācijas Nr.:

2. Iemesls atzinuma saņemšanai

☐ 2.1. IKT resursa iegāde

☐ 2.2. Ārpakalpojuma līguma slēgšana (izņemot 2.1.)

2.1. IKT resursa iegāde

IKT resursa nosaukums

Informācijas sistēmas nosaukums, kurā IKT resurss tiks izmantots

Iepirkuma datums, Nr. (ja attiecināms)

Konstatētās neatbilstības minimālajām kiberdrošības prasībām vai citu to nepiemērošanas iemeslu apraksts

2.2. Ārpakalpojuma līguma slēgšana

Ārpakalpojuma priekšmets

Informācijas sistēmas nosaukums, kurā ārpakalpojums tiks izmantots

Iepirkuma datums, Nr.

Ārpakalpojuma darbu apraksts

Informācija par pretendentu (juridiskās personas nosaukums un reģistrācijas Nr./fiziskās personas vārds, uzvārds un personas kods)

Informācija par pretendenta piesaistītajiem apakšuzņēmējiem (juridiskās personas nosaukums un reģistrācijas Nr./fiziskās personas vārds, uzvārds un personas kods)

Ārpakalpojuma līguma izpildē iesaistītie speciālisti:

Nr.	Vārds	Uzvārds	Personas kods	Specialitāte

9. pielikums
Ministru kabineta
2025. gada 25. jūnija
noteikumiem Nr. 397

Minimālās prasības darbības nepārtrauktības plāna izstrādei valsts apdraudējuma gadījumam

1. IKT kritiskās infrastruktūras, tai skaitā Eiropas mērogā īpaši nozīmīgas kritiskās infrastruktūras (turpmāk – kritiskā infrastruktūra), īpašnieks vai tiesiskais valdītājs sadarbībā ar attiecīgo nozares ministriju un Aizsardzības ministriju izstrādā kritiskās infrastruktūras darbības nepārtrauktības plānu valsts apdraudējuma gadījumam (turpmāk – plāns).

2. Plānā nosaka:

2.1. kritiskos pakalpojumus un to minimālo apmēru, kas valsts apdraudējuma laikā jānodrošina vismaz noteiktajā līmenī;

2.2. kritisko personālu un tā pienākumus, kā arī personāla sagatavošanas pasākumus;

2.3. darbībai nepieciešamo nodrošinājumu (infrastruktūra, tehnoloģiskās iekārtas un nepieciešamie materiāltehniskie līdzekļi, resursi un izejvielas, cits nodrošinājums);

2.4. rīcības algoritmus krīzes laikā.

3. Minimālās prasības attiecībā uz kritisko pakalpojumu sniegšanas nepārtrauktību, kas jānodrošina valsts apdraudējuma laikā, tiek noteiktas individuāli sadarbībā ar nozares ministriju un Aizsardzības ministriju un tiek iekļautas plānā. Plānā:

3.1. apraksta kritiskās funkcijas un procesus;

3.2. definē kritisko pakalpojumu apjomu, kas jānodrošina noteiktajā līmenī;

3.3. definē maksimālo pieļaujamo pārtraukuma ilgumu kritisko pakalpojumu sniegšanā, pēc kura nav iespējams turpināt attiecīgā kritiskā pakalpojuma sniegšanu;

3.4. nosaka nepieciešamo atjaunošanas laiku un prioritātes kritisko funkciju atjaunošanai un turpināšanai.

4. Attiecībā uz cilvēkresursiem kritisko funkciju nodrošināšanai kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs:

4.1. izvērtē un nosaka nepieciešamo kritisko personālu, tostarp arī atbalsta personālu, lai nodrošinātu kritisko pakalpojumu sniegšanas nepārtrauktību un procesu norisi. Valsts apdraudējuma gadījumā izsludināta izņēmuma stāvokļa laikā kritiskais personāls nav pakļauts mobilizācijai, bet tā pienākums ir turpināt strādāt. Kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs nosaka kritiskajam personālam aizliegumu uzteikt darba līgumu;

4.2. informē kritisko personālu par tā statusu un pienākumiem, nosakot to darba līgumā un amata aprakstā, vai ar atsevišķu iestādes izdotu rīkojumu (piemēram, par kritisko personālu) vai citādi, kā arī nodrošina kritiskā personāla apmācību vai sagatavošanu;

4.3. izstrādā kritiskā personāla aizvietošanas vai pastiprināšanas kārtību, tostarp procedūru gadījumā, ja daļa kritiskā personāla nav pieejama;

4.4. atbilstoši iespējām laikus pielāgo infrastruktūru un piešķir resursus, lai nodrošinātu darbu maiņās, personāla nakšņošanu vai ilgstošu uzturēšanos darba telpās;

4.5. nosaka saziņas un iekšējās komunikācijas veidu (tai skaitā izmantojamos sakaru līdzekļus) kritiskā personāla apziņošanai un informēšanai.

5. Infrastruktūras nodrošinājumā paredz pāreju uz alternatīvām darba telpām (alternatīvo lokāciju), ja ikdienas darba telpas nav pieejamas. Šajā nolūkā kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs, ja iespējams, izvērtē konkrētā kritiskās infrastruktūras objekta specifiku un:

5.1. laikus apzina piemērotu infrastruktūru (alternatīvu lokāciju), kas atrodas ne mazāk kā 50 kilometru attālumā no esošās infrastruktūras un ir piemērota kritisko funkciju nodrošināšanai (nepieciešamais minimums – sakaru nodrošinājums, atbilstoši iespējām – alternatīvie energoapgādes risinājumi, ūdens pieejamība);

5.2. izstrādā kārtību, kādā uz alternatīvajām darba telpām tiek pārvietots (īslaicīgi vai ilglaicīgi) personāls un tehnoloģiskās iekārtas, laikus identificējot nepieciešamo transporta vienību skaitu un citu nodrošinājuma atbalstu (tostarp personāla izmitināšanai, izvietošanai);

5.3. identificē iespējas piesaistīt alternatīvajā lokācijā pieejamo personālu, iekārtas un materiāltehniskos līdzekļus, laikus definējot prasības.

6. Attiecībā uz kritisko pakalpojumu sniegšanai nepieciešamo tehnoloģisko iekārtu (turpmāk – iekārtas) un materiāltehnisko līdzekļu risinājumu plānā paredz:

6.1. kritiski svarīgu iekārtu un materiāltehnisko līdzekļu uzskaitījumu;

6.2. kritiski svarīgu iekārtu un materiāltehnisko līdzekļu alternatīvu apzināšanu, aizvietošanas iespējas;

6.3. nepārtrauktības nodrošināšanu iekārtu un materiāltehnisko līdzekļu zaudējuma vai nedarbošanās gadījumā;

6.4. rīcību attiecībā uz iekārtu remontu, atjaunošanu, uzlabošanu vai alternatīvu izveidi (tai skaitā ārpakalpojumu nodrošinātāju aizvietošanu);

6.5. digitālo sistēmu un iekārtu savlaicīgu dublēšanu, lai nodrošinātu pieeju datiem, sistēmām un procesiem arī no alternatīvās lokācijas;

6.6. piegāžu drošības ietekmi uz iekārtu darbības nepārtrauktību (atbalsta personāla pieejamība, rezerves daļu pieejamība, remonts);

6.7. informācijas sistēmu elektroapgādes pieslēguma dublēšanu un aprīkojumu ar autonomu elektroapgādes sistēmu;

6.8. kritiskā pakalpojuma sniegšanas nepārtrauktības nodrošināšanu alternatīvā veidā ar alternatīviem līdzekļiem, ja Latvijas teritorijā neatrodas informācijas sistēmas, kas nodrošina kritiskā pakalpojuma sniegšanu.

7. Nav ieteicams izmantot tādu uzņēmumu ražotās tehnoloģijas, kuru reputācija Eiropas Savienības un NATO dalībvalstīs tiek apšaubīta saistībā ar aizdomām par privātuma pārkāpumiem, publiski nepieejamas informācijas nesankcionētu iegūšanu vai valsts drošības apdraudējumu.

8. Attiecībā uz kritisko pakalpojumu sniegšanai nepieciešamo transportu (ja attiecināms) plānā identificē un apzina:

8.1. kritisko pakalpojumu sniegšanai nepieciešamo transportu;

8.2. alternatīvas;

8.3. autovadītāju un speciālistu pieejamību, aizvietošanas iespējas;

8.4. nodrošinājumu ar degvielu.

9. Plānā atspoguļo:

9.1. elektronisko sakaru un balss telefonijas iekārtas un to datubāzes (tai skaitā pieeju no alternatīvajām darba telpām, alternatīvās vai dublējošās sakaru un datu pārraides sistēmas);

9.2. elektroenerģijas apgādes iekārtas, alternatīvas un ārpakalpojumu ietekmi;

9.3. dabasgāzes un naftas produktu pieejamību (alternatīvas);

9.4. siltumapgādi (apkuri), ūdensapgādi, kanalizācijas pieejamību (alternatīvas);

9.5. loģistikas risinājumus un to alternatīvas (transporta nepieejamība).

10. Resursu (piegāžu) sistēma paredz kritiskās infrastruktūras darbības specifikai nepieciešamo resursu (piemēram, kritisko izejvielu identificēšana) pieejamību un piegādi valsts apdraudējuma gadījumā, tostarp izvērtējot piegāžu drošības un nepārtrauktības aspektus un laikus apzinot alternatīvās piegāžu ķēdes vai alternatīvu kritiskajām izejvielām, tostarp to iespējamās atrašanās vietas.

11. Informāciju par identificētajiem kritisko izejvielu un materiālu trūkumiem, materiāltehnisko resursu nepieejamību un citām konstatētajām ievainojamībām kopā ar kritiskās infrastruktūras pašvērtējumu iesniedz attiecīgajai nozares ministrijai.

12. Plānā nosaka piegāžu drošības un noturības jautājumus:

12.1. vismaz pirmā līmeņa piegādātāju identificēšana un to ģeogrāfiskā izvietošana, lai apzinātu ievainojamības starptautisko piegāžu ķēžu pārrāvuma situācijās un laikus identificētu iespējamās alternatīvas;

12.2. piegāžu risku sadale (*multi-vendor suppliers*), izvairoties no atkarības tikai no viena ārvalstu piegādātāja;

12.3. nav atbalstāma tādu augsta riska piegādātāju iesaiste piegāžu ķēdēs, kuru reputācija Eiropas Savienības un NATO dalībvalstīs tiek apšaubīta saistībā ar aizdomām par privātuma pārkāpumiem, cilvēktiesību neievērošanu, publiski nepieejamas informācijas nesankcionētu iegūšanu vai valsts drošības apdraudējumu;

12.4. no piegāžu drošības un noturības viedokļa priekšroka sniedzama vietējām piegāžu ķēdēm un vietējiem ražotājiem, apstrādātājiem un pakalpojumu sniedzējiem.

13. Plānā atspoguļo rīcības algoritmus krīzes laikā:

13.1. paredz kritisko pakalpojumu sniegšanu noteiktajā apjomā valsts apdraudējuma gadījumā;

13.2. paredz kārtību, kādā valsts apdraudējuma gadījumā sazināties ar personālu (nosaka saziņu un iekšējo komunikāciju, apziņošanu un informēšanu);

13.3. nosaka krīzes vadības komandas aktivizēšanas kārtību un darbību krīzes laikā, kā arī koordinācijas

mehānismu ar nozares ministriju;

13.4. nosaka krīzes komunikācijas protokolu (iekšējo, ārējo);

13.5. nosaka procedūras elastīgai un operatīvai reaģēšanai uz incidentiem, īstenojot krīzes vadības procedūras un protokolus.

14. Uzņēmuma darbības prioritāte ir kritisko pakalpojumu sniegšana noteiktā apmērā, un tam jānovirza visi pieejamie iekšējie uzņēmuma resursi. Kritisko pakalpojumu sniegšanas pārtraukuma gadījumā visi resursi jāvelta noteikto funkciju un darbības procesu atjaunošanai, pēc iespējas mazinot radītos zaudējumus, operatīvi īstenojot atjaunošanas scenārijus vai pārceļoties un turpinot darbību no alternatīvās lokācijas.

15. Darbības pārtraukšana ir pieļaujama tikai:

15.1. saņemot atļauju vai citus uzdevumus no institūcijas, kas atbildīga par apdraudējuma pārvarēšanu;

15.2. situācijās, kad tiek apdraudēta personāla dzīvība un šo apdraudējumu nav iespējams novērst, pat pārceļoties uz alternatīvo lokāciju.

16. Plānā var identificēt arī nepieciešamo atbalstu no valsts institūcijām, lai nodrošinātu kritisko funkciju īstenošanu valsts apdraudējuma gadījumā:

16.1. prioritāru nodrošinājumu ar energoresursiem, gāzi un naftas produktiem;

16.2. sakaru nodrošinājumu;

16.3. fizisko apsardzi;

16.4. loģistikas atbalstu;

16.5. citu atbalstu atbilstoši nozares ministrijas un Aizsardzības ministrijas sniegtajam izvērtējumam.

17. Plānā paredz darbības nepārtrauktības sistēmas testēšanu un pašvērtēšanu, tostarp ne retāk kā reizi četros gados organizējot mācības sadarbībā ar attiecīgo nozares ministriju un Aizsardzības ministriju.

18. Plānu un grozījumus plānā apstiprina kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs.

Aizsardzības ministrijas iesniegtajā redakcijā

10. pielikums
Ministru kabineta
2025. gada 25. jūnija
noteikumiem Nr. 397

Agrīnā brīdinājuma veidlapa

AGRĪNAIS BRĪDINĀJUMS
par nozīmīgu kiberincidentu

—— IESNIEDZAMS 24 STUNDU LAIKĀ ——

1. Informācija par subjektu

Nosaukums (fiz. personai – vārds, uzvārds)**:**

Reģistrācijas Nr. (fiz. personai – pers. kods):

2. Informācija par kiberincidentu

Kiberincidenta datums un laiks (ja zināms):

Kiberincidenta veids (ja zināms, lūgums atzīmēt visas atbilstošās kategorijas):

- ☐ 01 Neatbilstošs saturs (piemēram, mēstule, nelegāls saturs)
- ☐ 02 Ļaundabīgs kods
- ☐ 03 Informācijas vākšana
- ☐ 04 Ielaušanās mēģinājums
- ☐ 05 Ielaušanās
- ☐ 06 Pieejamības traucējums
- ☐ 07 Datu drošības pārkāpums (piemēram, nesankcionēta piekļuve vai modificēšana)
- ☐ 08 Krāpniecība
- ☐ 09 Ievainojamība
- ☐ 10 Cits kiberincidenta veids
- ☐ 99 Pārbaude (mācības)

Kiberincidenta vispārīgs apraksts (brīvā formātā):

3. Informācija par brīdinājuma iesniedzēju

Brīdinājuma iesniedzēja vārds, uzvārds:	
Brīdinājuma iesniedzēja amats:	
Brīdinājuma iesniedzēja e-pasts:	
Brīdinājuma iesniedzēja tālruņa Nr.:	

Aizsardzības ministrijas iesniegtajā redakcijā

11. pielikums
Ministru kabineta
2025. gada 25. jūnija
noteikumiem Nr. 397

Sākotnējā ziņojuma veidlapa

SĀKOTNĒJAIS ZIŅOJUMS
par nozīmīgu kiberincidentu

—— IESNIEDZAMS 72 STUNDU LAIKĀ ——

1. Informācija par subjektu

Nosaukums (fiz. personai – vārds, uzvārds)**:**

Reģistrācijas Nr. (fiz. personai – pers. kods):

2. Informācija par kiberincidentu

Kiberincidenta datums un laiks (ja zināms):

Kiberincidenta veids (lūgums atzīmēt visas atbilstošās kategorijas):

- ☐ 01 Neatbilstošs saturs (piemēram, mēstule, nelegāls saturs)
- ☐ 02 Ļaundabīgs kods
- ☐ 03 Informācijas vākšana
- ☐ 04 Ielaušanās mēģinājums
- ☐ 05 Ielaušanās
- ☐ 06 Pieejamības traucējums
- ☐ 07 Datu drošības pārkāpums (piemēram, nesankcionēta piekļuve vai modificēšana)
- ☐ 08 Krāpniecība
- ☐ 09 Ievainojamība
- ☐ 10 Cits kiberincidenta veids
- ☐ 99 Pārbaude (mācības)

3. Kiberincidenta cēloņi

Lūdzu, norādiet kiberincidenta cēloņus un kompromitēšanas indikatorus, ja tie ir zināmi:

4. Sākotnējais ietekmes novērtējums

4.1. Kiberincidenta ietekmes raksturojums

Lūdzu, novērtējiet kiberincidenta ietekmi:

Ietekme uz pieejamību	**Ietekme uz konfidencialitāti**	**Ietekme uz integritāti**
☐ Augsta ietekme	☐ Augsta ietekme	☐ Augsta ietekme
☐ Vidēja ietekme	☐ Vidēja ietekme	☐ Vidēja ietekme
☐ Zema ietekme	☐ Zema ietekme	☐ Zema ietekme
☐ Nav ietekmes	☐ Nav ietekmes	☐ Nav ietekmes

Ietekmētās datu kopas, resursi, sistēmas, procesi, pakalpojumi:

Ietekmēto lietotāju skaits (ja zināms, indikatīvi): _____ lietotāji

Apzināto zaudējumu apmērs (ja zināms, indikatīvi): _____ EUR

Ja ietekmēta pieejamība:

Dīkstāves ilgums: _____
☐ minūtes
☐ stundas
☐ diennaktis

Vai uz ziņojuma iesniegšanas brīdi pieejamība ir atjaunota?
☐ Jā
☐ Nē

Ja ietekmēta konfidencialitāte:

Vai ir kompromitēti kādi no norādītajiem datiem? (ja zināms, lūgums atzīmēt visas atbilstošās kategorijas)
☐ Autentifikācijas dati (piemēram, lietotāju paroles)
☐ Personas dati
☐ Īpašo kategoriju personas dati
☐ Ierobežotas pieejamības informācija
☐ Citi sensitīvi dati

Ja ietekmēta integritāte:

Vai kiberincidents ir ietekmējis datu pirmavota integritāti vai citādi kompromitējis datu autentiskumu?
☐ Jā (ja zināms, lūgums paskaidrot, kādu datu autentiskums kompromitēts, kā tieši)
☐ Nē
☐ Nav zināms

4.2. Ietekme uz darbības un pakalpojumu nepārtrauktību

Lūdzu, novērtējiet kiberincidenta vispārīgo ietekmi:

uz organizācijas darbības nepārtrauktību

- ☐ Augsta ietekme
- ☐ Vidēja ietekme
- ☐ Zema ietekme
- ☐ Nav ietekmes

uz būtiskajiem un svarīgajiem pakalpojumiem

- ☐ Augsta ietekme
- ☐ Vidēja ietekme
- ☐ Zema ietekme
- ☐ Nav ietekmes

Ja kiberincidents ir ietekmējis organizācijas darbības nepārtrauktību, būtiskos vai svarīgos pakalpojumus, lūgums raksturot šo ietekmi:

4.3. Pārrobežu ietekme

Vai kiberincidents ir ietekmējis citās ES dalībvalstīs sniegtos būtiskos vai svarīgos pakalpojumus vai ar tiem saistītās piegāžu ķēdes?

- ☐ Jā (lūgums paskaidrot, kuras dalībvalstis, kāda ietekme)
- ☐ Nē
- ☐ Nav zināms

4.4. Cita informācija

Cita relevanta informācija par kiberincidenta ietekmi:

5. Novēršanas darbības

Vai par kiberincidentu ir nekavējoties ziņots kiberincidentu novēršanas institūcijai?

- ☐ Jā
- ☐ Nē (lūgums norādīt iemeslu)

Lūdzu, norādiet kiberincidenta novēršanas procesa pašreizējo statusu

- ☐ Neiesākts
- ☐ Procesā
- ☐ Pabeigts

Lūdzu, norādiet veiktās darbības kiberincidenta novēršanai

6. Informācija par ziņojuma iesniedzēju

Ziņojuma iesniedzēja vārds, uzvārds:

Ziņojuma iesniedzēja amats:

Ziņojuma iesniedzēja e-pasts:	
Ziņojuma iesniedzēja tālruņa Nr.:	

Aizsardzības ministrijas iesniegtajā redakcijā

12. pielikums
Ministru kabineta
2025. gada 25. jūnija
noteikumiem Nr. 397

Progresa ziņojuma veidlapa

PROGRESA ZIŅOJUMS
par nozīmīga kiberincidenta risināšanu

—— IESNIEDZAMS 1 MĒNEŠA LAIKĀ, JA KIBERINCIDENTS NAV ATRISINĀTS ——

1. Informācija par subjektu

Nosaukums (fiz. personai – vārds, uzvārds)**:**

Reģistrācijas Nr. (fiz. personai – pers. kods):

2. Informācija par kiberincidentu

Kiberincidenta datums un laiks:

Kiberincidenta veids (lūgums atzīmēt visas atbilstošās kategorijas):

- ☐ 01 Neatbilstošs saturs (piemēram, mēstule, nelegāls saturs)
- ☐ 02 Ļaundabīgs kods
- ☐ 03 Informācijas vākšana
- ☐ 04 Ielaušanās mēģinājums
- ☐ 05 Ielaušanās
- ☐ 06 Pieejamības traucējums
- ☐ 07 Datu drošības pārkāpums (piemēram, nesankcionēta piekļuve vai modificēšana)
- ☐ 08 Krāpniecība
- ☐ 09 Ievainojamība
- ☐ 10 Cits kiberincidenta veids
- ☐ 99 Pārbaude (mācības)

3. Kiberincidenta cēloņi

Lūdzu, norādiet kiberincidenta cēloņus un kompromitēšanas indikatorus, ja tie ir zināmi:

4. Kiberincidenta ietekmes novērtējums

4.1. Kiberincidenta ietekmes raksturojums

Lūdzu, novērtējiet kiberincidenta ietekmi:

Ietekme uz pieejamību	**Ietekme uz konfidencialitāti**	**Ietekme uz integritāti**
☐ Augsta ietekme	☐ Augsta ietekme	☐ Augsta ietekme
☐ Vidēja ietekme	☐ Vidēja ietekme	☐ Vidēja ietekme
☐ Zema ietekme	☐ Zema ietekme	☐ Zema ietekme
☐ Nav ietekmes	☐ Nav ietekmes	☐ Nav ietekmes

Ietekmētās datu kopas, resursi, sistēmas, procesi, pakalpojumi:

Ietekmēto lietotāju skaits (ja zināms, indikatīvi): _____ lietotāji

Apzināto zaudējumu apmērs (ja zināms, indikatīvi): _____ EUR

Ja ietekmēta pieejamība:

Dīkstāves ilgums: _____

☐ minūtes
☐ stundas
☐ diennaktis

Vai uz ziņojuma iesniegšanas brīdi pieejamība ir atjaunota?

☐ Jā
☐ Nē

Ja ietekmēta konfidencialitāte:

Vai ir kompromitēti kādi no norādītajiem datiem? (lūgums atzīmēt visas atbilstošās kategorijas)

☐ Autentifikācijas dati (piemēram, lietotāju paroles)
☐ Personas dati
☐ Īpašo kategoriju personas dati
☐ Ierobežotas pieejamības informācija
☐ Citi sensitīvi dati

Ja ietekmēta integritāte:

Vai kiberincidents ir ietekmējis datu pirmavota integritāti vai citādi kompromitējis datu autentiskumu?

☐ Jā (lūgums paskaidrot, kādu datu autentiskums kompromitēts, kā tieši)

☐ Nē
☐ Nav zināms

4.2. Ietekme uz darbības un pakalpojumu nepārtrauktību

Lūdzu, novērtējiet kiberincidenta vispārīgo ietekmi:

uz organizācijas darbības nepārtrauktību	**uz būtiskajiem un svarīgajiem pakalpojumiem**

☐ Augsta ietekme
☐ Vidēja ietekme
☐ Zema ietekme
☐ Nav ietekmes

☐ Augsta ietekme
☐ Vidēja ietekme
☐ Zema ietekme
☐ Nav ietekmes

Ja kiberincidents ir ietekmējis organizācijas darbības nepārtrauktību, būtiskos vai svarīgos pakalpojumus, lūgums raksturot šo ietekmi:

4.3. Pārrobežu ietekme

Vai kiberincidents ir ietekmējis citās ES dalībvalstīs sniegtos būtiskos vai svarīgos pakalpojumus vai ar tiem saistītās piegāžu ķēdes?

☐ Jā (lūgums paskaidrot, kāda ietekme)

☐ Nē
☐ Nav zināms

4.4. Cita informācija

Cita relevanta informācija par kiberincidenta ietekmi:

5. Novēršanas darbības

Lūdzu, norādiet kiberincidenta novēršanas procesa pašreizējo statusu

☐ Neiesākts
☐ Procesā

Lūdzu, norādiet veiktās darbības kiberincidenta novēršanai

Lūdzu, norādiet iemeslus, kāpēc kiberincidentu nav izdevies novērst 1 mēneša laikā

6. Informācija par ziņojuma iesniedzēju

Ziņojuma iesniedzēja vārds, uzvārds:

Ziņojuma iesniedzēja amats:

Ziņojuma iesniedzēja e-pasts:

Ziņojuma iesniedzēja tālruņa Nr.:

Aizsardzības ministrijas iesniegtajā redakcijā

13. pielikums
Ministru kabineta
2025. gada 25. jūnija
noteikumiem Nr. 397

Starpposma ziņojuma veidlapa

STARPPOSMA ZIŅOJUMS
par nozīmīga kiberincidenta risināšanu

—— IESNIEDZAMS PĒC KOMPETENTĀS IESTĀDES PIEPRASĪJUMA ——

1. Informācija par subjektu

Nosaukums (fiz. personai – vārds, uzvārds)**:**

Reģistrācijas Nr. (fiz. personai – pers. kods):

2. Informācija par kiberincidentu

Kiberincidenta datums un laiks:

Kiberincidenta veids (lūgums atzīmēt visas atbilstošās kategorijas):

- ☐ 01 Neatbilstošs saturs (piemēram, mēstule, nelegāls saturs)
- ☐ 02 Ļaundabīgs kods
- ☐ 03 Informācijas vākšana
- ☐ 04 Ielaušanās mēģinājums
- ☐ 05 Ielaušanās
- ☐ 06 Pieejamības traucējums
- ☐ 07 Datu drošības pārkāpums (piemēram, nesankcionēta piekļuve vai modificēšana)
- ☐ 08 Krāpniecība
- ☐ 09 Ievainojamība
- ☐ 10 Cits kiberincidenta veids
- ☐ 99 Pārbaude (mācības)

3. Kiberincidenta cēloņi

Lūdzu, norādiet kiberincidenta cēloņus un kompromitēšanas indikatorus, ja tie ir zināmi:

4. Kiberincidenta ietekmes novērtējums

4.1. Kiberincidenta ietekmes raksturojums

Lūdzu, novērtējiet kiberincidenta ietekmi:

Ietekme uz pieejamību

- ☐ Augsta ietekme
- ☐ Vidēja ietekme
- ☐ Zema ietekme
- ☐ Nav ietekmes

Ietekme uz konfidencialitāti

- ☐ Augsta ietekme
- ☐ Vidēja ietekme
- ☐ Zema ietekme
- ☐ Nav ietekmes

Ietekme uz integritāti

- ☐ Augsta ietekme
- ☐ Vidēja ietekme
- ☐ Zema ietekme
- ☐ Nav ietekmes

Ietekmētās datu kopas, resursi, sistēmas, procesi, pakalpojumi:

Ietekmēto lietotāju skaits (ja zināms, indikatīvi): _____ lietotāji

Apzināto zaudējumu apmērs (ja zināms, indikatīvi): _____ EUR

Ja ietekmēta pieejamība:

Dīkstāves ilgums: _____

- ☐ minūtes
- ☐ stundas
- ☐ diennaktis

Vai uz ziņojuma iesniegšanas brīdi pieejamība ir atjaunota?

- ☐ Jā
- ☐ Nē

Ja ietekmēta konfidencialitāte:

Vai ir kompromitēti kādi no norādītajiem datiem? (lūgums atzīmēt visas atbilstošās kategorijas)

- ☐ Autentifikācijas dati (piemēram, lietotāju paroles)
- ☐ Personas dati
- ☐ Īpašo kategoriju personas dati
- ☐ Ierobežotas pieejamības informācija
- ☐ Citi sensitīvi dati

Ja ietekmēta integritāte:

Vai kiberincidents ir ietekmējis datu pirmavota integritāti vai citādi kompromitējis datu autentiskumu?

- ☐ Jā (lūgums paskaidrot, kādu datu autentiskums kompromitēts, kā tieši)
- ☐ Nē
- ☐ Nav zināms

4.2. Ietekme uz darbības un pakalpojumu nepārtrauktību

Lūdzu, novērtējiet kiberincidenta vispārīgo ietekmi:

uz organizācijas darbības nepārtrauktību

- ☐ Augsta ietekme

uz būtiskajiem un svarīgajiem pakalpojumiem

- ☐ Augsta ietekme

☐ Vidēja ietekme
☐ Zema ietekme
☐ Nav ietekmes

☐ Vidēja ietekme
☐ Zema ietekme
☐ Nav ietekmes

Ja kiberincidents ir ietekmējis organizācijas darbības nepārtrauktību, būtiskos vai svarīgos pakalpojumus, lūgums raksturot šo ietekmi:

4.3. Pārrobežu ietekme

Vai kiberincidents ir ietekmējis citās ES dalībvalstīs sniegtos būtiskos vai svarīgos pakalpojumus vai ar tiem saistītās piegāžu ķēdes?

☐ Jā (lūgums paskaidrot, kāda ietekme)

☐ Nē
☐ Nav zināms

4.4. Cita informācija

Cita relevanta informācija par kiberincidenta ietekmi:

5. Novēršanas darbības

Lūdzu, norādiet kiberincidenta novēršanas procesa pašreizējo statusu

☐ Neiesākts
☐ Procesā

Lūdzu, norādiet veiktās darbības kiberincidenta novēršanai

Lūdzu, norādiet iemeslus, kāpēc kiberincidenta novēršanas darbi vēl nav pabeigti

6. Informācija par ziņojuma iesniedzēju

Ziņojuma iesniedzēja vārds, uzvārds:

Ziņojuma iesniedzēja amats:

Ziņojuma iesniedzēja e-pasts:

Ziņojuma iesniedzēja tālruņa Nr.:

Aizsardzības ministrijas iesniegtajā redakcijā

14. pielikums
Ministru kabineta
2025. gada 25. jūnija
noteikumiem Nr. 397

Galaziņojuma veidlapa

GALAZIŅOJUMS
par nozīmīga kiberincidenta atrisināšanu

—— IESNIEDZAMS 1 MĒNEŠA LAIKĀ ——

1. Informācija par subjektu

Nosaukums (fiz. personai – vārds, uzvārds)**:**

Reģistrācijas Nr. (fiz. personai – pers. kods):

2. Informācija par kiberincidentu

Kiberincidenta datums un laiks:

Kiberincidenta veids (lūgums atzīmēt visas atbilstošās kategorijas):

- ☐ 01 Neatbilstošs saturs (piemēram, mēstule, nelegāls saturs)
- ☐ 02 Ļaundabīgs kods
- ☐ 03 Informācijas vākšana
- ☐ 04 Ielaušanās mēģinājums
- ☐ 05 Ielaušanās
- ☐ 06 Pieejamības traucējums
- ☐ 07 Datu drošības pārkāpums (piemēram, nesankcionēta piekļuve vai modificēšana)
- ☐ 08 Krāpniecība
- ☐ 09 Ievainojamība
- ☐ 10 Cits kiberincidenta veids
- ☐ 99 Pārbaude (mācības)

3. Kiberincidenta cēloņi

Lūdzu, norādiet kiberincidenta cēloņus un kompromitēšanas indikatorus, ja tie ir zināmi:

4. Kiberincidenta ietekmes novērtējums

4.1. Kiberincidenta ietekmes raksturojums

Lūdzu, novērtējiet kiberincidenta ietekmi:

Ietekme uz pieejamību	**Ietekme uz konfidencialitāti**	**Ietekme uz integritāti**
☐ Augsta ietekme	☐ Augsta ietekme	☐ Augsta ietekme
☐ Vidēja ietekme	☐ Vidēja ietekme	☐ Vidēja ietekme
☐ Zema ietekme	☐ Zema ietekme	☐ Zema ietekme
☐ Nav ietekmes	☐ Nav ietekmes	☐ Nav ietekmes

Ietekmētās datu kopas, resursi, sistēmas, procesi, pakalpojumi:

Ietekmēto lietotāju skaits: ☐ lietotāji

Aprēķināto zaudējumu apmērs: ☐ EUR

Ja ietekmēta pieejamība:

Kopējais dīkstāves ilgums: ☐

☐ minūtes
☐ stundas
☐ diennaktis

Ja ietekmēta konfidencialitāte:

Vai ir kompromitēti kādi no norādītajiem datiem? (lūgums atzīmēt visas atbilstošās kategorijas)

☐ Autentifikācijas dati (piemēram, lietotāju paroles)
☐ Personas dati
☐ Īpašo kategoriju personas dati
☐ Ierobežotas pieejamības informācija
☐ Citi sensitīvi dati

Ja ietekmēta integritāte:

Vai kiberincidents ir ietekmējis datu pirmavota integritāti vai citādi kompromitējis datu autentiskumu?

☐ Jā (lūgums paskaidrot, kādu datu autentiskums kompromitēts, kā tieši)

☐ Nē
☐ Nav zināms

4.2. Ietekme uz darbības un pakalpojumu nepārtrauktību

Lūdzu, novērtējiet kiberincidenta vispārīgo ietekmi:

uz organizācijas darbības nepārtrauktību	**uz būtiskajiem un svarīgajiem pakalpojumiem**
☐ Augsta ietekme	☐ Augsta ietekme

☐ Vidēja ietekme
☐ Zema ietekme
☐ Nav ietekmes

☐ Vidēja ietekme
☐ Zema ietekme
☐ Nav ietekmes

Ja kiberincidents ir ietekmējis organizācijas darbības nepārtrauktību, būtiskos vai svarīgos pakalpojumus, lūgums raksturot šo ietekmi:

4.3. Pārrobežu ietekme

Vai kiberincidents ir ietekmējis citās ES dalībvalstīs sniegtos būtiskos vai svarīgos pakalpojumus vai ar tiem saistītās piegāžu ķēdes?

☐ Jā (lūgums paskaidrot, kāda ietekme)

☐ Nē
☐ Nav zināms

4.4. Cita informācija

Cita relevanta informācija par kiberincidenta ietekmi:

5. Kiberincidenta novēršanas darbības

Lūdzu, norādiet veiktās darbības kiberincidenta novēršanai

6. Informācija par ziņojuma iesniedzēju

Ziņojuma iesniedzēja vārds, uzvārds:

Ziņojuma iesniedzēja amats:

Ziņojuma iesniedzēja e-pasts:

Ziņojuma iesniedzēja tālruņa Nr.:

Aizsardzības ministrijas iesniegtajā redakcijā

15. pielikums
Ministru kabineta
2025. gada 25. jūnija
noteikumiem Nr. 397

Kiberdrošības auditora reģistrācijas pieteikuma veidlapa

KIBERDROŠĪBAS AUDITORA REĢISTRĀCIJAS PIETEIKUMS

1. Pamatinformācija par auditoru (organizāciju)

Nosaukums (fiz. personai – vārds, uzvārds):

Reģistrācijas Nr. (fiz. personai – pers. kods):

Juridiskā adrese:

E-pasta adrese:

Tālruņa numurs:

Tīmekļvietnes adrese (ja ir):

2. Auditora nodarbinātais personāls (fiziskā persona)

Vārds, uzvārds:

Personas kods:

Ziņas par iegūtajiem sertifikātiem: (piemēram, CISA, ISO/IEC 27001 Lead Auditor, CISSP)

PIETEIKUMAM PIEVIENO NORĀDĪTO SERTIFIKĀTU KOPIJAS!

E-pasta adrese:

Tālruņa numurs:

3. Auditora apliecinājums

- [x] Apliecinu, ka auditors atbilst normatīvajos aktos par minimālajām kiberdrošības prasībām noteiktajām prasībām (tostarp attiecībā uz auditora reģistrācijas valsti, dalībnieku reģistrācijas vai pilsonības valsti, patiesā labuma guvēju pilsonību, audita veikšanai izmantoto programmatūru un iekārtu ražotāja reģistrācijas valsti).
- [ ] Apliecinu, ka auditoram ir nepieciešamās zināšanas, prasmes un pieredze, lai sniegtu neatkarīgu, objektīvu un vispusīgu vērtējumu par subjektu kiberdrošību.
- [ ] Apliecinu, ka auditoram ir tehniskas iespējas noteikt subjektu tīklu, informācijas sistēmu, resursu un procedūru drošību atbilstību normatīvo aktu prasībām.

Aizsardzības ministrijas iesniegtajā redakcijā

16. pielikums
Ministru kabineta
2025. gada 25. jūnija
noteikumiem Nr. 397

Pašvērtējuma ziņojuma veidlapa

PAŠVĒRTĒJUMA ZIŅOJUMS
par subjekta atbilstību minimālajām kiberdrošības prasībām

—— SASKAŅĀ AR NACIONĀLĀS KIBERDROŠĪBAS LIKUMA 43. PANTU ——

1. Vispārīga informācija

Ziņojuma sagatavošanas gads: ☐

Subjekta nosaukums (fiz. personai – vārds, uzvārds): ☐

Subjekta reģistrācijas numurs (fiz. personai – pers. kods): ☐

Subjekta veids:
☐ būtisko pakalpojumu sniedzējs
☐ svarīgo pakalpojumu sniedzējs

2. Kiberdrošības pārvaldnieks

Lūdzu, atzīmējiet atbilstošos atbilžu variantus un sniedziet papildu informāciju, ja nepieciešams

■ **0201** Subjekta vadītājs ir noteicis kiberdrošības pārvaldnieku

☐ Jā – Norādīt kiberdrošības pārvaldnieka datus:

Vārds:	Uzvārds:	Pilsonība:
Vecums:	Personas kods:	

☐ Nē – Norādīt iemeslu:

■ **0202** Pār personu, kas noteikta par kiberdrošības pārvaldnieku, nav nodibināta aizgādnība

☐ Jā (Nav nodibināta aizgādnība)

☐ Nē (Ir nodibināta aizgādnība)

☐ N/A (Subjekts nav noteicis kiberdrošības pārvaldnieku)

■ **0203** Kiberdrošības pārvaldnieks, nav bijis sodīts par tīšu noziedzīgu nodarījumu

☐ Jā (Nav sodīts)

☐ Nē (Ir bijis sodīts)

☐ N/A (Subjekts nav noteicis kiberdrošības pārvaldnieku)

■ **0204** Kiberdrošības pārvaldnieks ir ieguvis vismaz augstāko vai profesionālo vidējo izglītību informācijas tehnoloģiju, kiberdrošības pārvaldības jomā vai citā saistītā jomā
Lūdzu, veidlapas pielikumā pievienojiet izglītību apliecinoša dokumenta kopiju

☐ Jā – Norādīt informāciju par iegūto izglītību:

Diploma iegūšanas gads:	Izglītības iestādes nosaukums:	Kvalifikācijas vai grāda nosaukums:

Nepieciešamības gadījumā pievienot tabulai jaunas rindiņas

☐ Nē

☐ N/A (Subjekts nav noteicis kiberdrošības pārvaldnieku)

■ **0205** Kiberdrošības pārvaldnieks ir ieguvis starptautiski atzītus sertifikātus kiberdrošības pārvaldības jomā (piemēram, CISM, CISSP)
Lūdzu, veidlapas pielikumā pievienojiet sertifikāta kopiju

☐ Jā – Norādīt informāciju par iegūtajiem sertifikātiem:

Sertifikāta iegūšanas gads:	Sertifikāta nosaukums:

Nepieciešamības gadījumā pievienot tabulai jaunas rindiņas

☐ Nē

☐ N/A (Subjekts nav noteicis kiberdrošības pārvaldnieku)

■ **0206** Kiberdrošības pārvaldniekam ir vismaz divu gadu darba pieredze kiberdrošības pasākumu plānošanā vai īstenošanā, kas iegūta pēdējo 5 gadu laikā

☐ Jā – Norādīt informāciju par atbilstošo darba pieredzi:

Periods:	Iestāde vai organizācija:	Ieņemamais amats vai veicamais darbs:

Nepieciešamības gadījumā pievienot tabulai jaunas rindiņas

☐ Nē

☐ N/A (Subjekts nav noteicis kiberdrošības pārvaldnieku)

■ **0207** Pārskata periodā kiberdrošības pārvaldnieks vismaz reizi gadā ir apmeklējis kiberincidentu novēršanas institūcijas organizēto apmācību kiberdrošības jautājumos

☐ Jā – Norādīt apmeklētās apmācības:

Apmācības datums:	Apmācības nosaukums/tēma:

Nepieciešamības gadījumā pievienot tabulai jaunas rindiņas

☐ Nē – Norādīt iemeslu:

☐ N/A (Subjekts nav noteicis kiberdrošības pārvaldnieku)

■ **0208** Pārskata periodā kiberdrošības pārvaldnieks vismaz reizi gadā ir organizējis subjekta IKT drošības pārbaudi

☐ Jā – Norādīt pēdējā gada laikā veiktās IKT drošības pārbaudes:

Pārbaudes datums:	Pārbaudes tvērums:

Nepieciešamības gadījumā pievienot tabulai jaunas rindiņas

☐ Nē – Norādīt iemeslu:

☐ N/A (Subjekts nav noteicis kiberdrošības pārvaldnieku)

■ **0299** Cita relevanta informācija par kiberdrošības pārvaldnieku, ko pats subjekts vēlas sniegt uzraudzības iestādei

3. Kiberdrošības politika
(Pievienot dokumenta kopiju šīs veidlapas pielikumā)

Lūdzu, atzīmējiet atbilstošos atbilžu variantus un sniedziet papildu informāciju, ja nepieciešams

■ **0301** Subjekts ir izstrādājis un apstiprinājis subjekta kiberdrošības politiku

☐ Jā – Norādīt dokumenta nosaukumu, datumu un numuru, ja attiecināms

☐ Nē – Norādīt iemeslu:

■ **0302** Pārskata periodā subjekts ir pārskatījis un nepieciešamības gadījumā aktualizējis kiberdrošības politiku:

☐ Biežāk nekā reizi gadā

☐ Reizi gadā

☐ Retāk nekā reizi gadā

☐ Nekad

>> Norādīt iemeslu, ja kiberdrošības politika tikusi pārskatīta retāk nekā reizi gadā vai nekad:

■ **0303** Subjekts kiberdrošības politikā ir iekļāvis šādu informāciju (atzīmēt visus atbilstošos atbilžu variantus):

☐ Vispārīga informācija par subjektu, tā darbības jomu, sniegtajiem pakalpojumiem un procesiem, kurus var ietekmēt kiberapdraudējums

☐ Subjekta kiberdrošības pārvaldības mērķi, principi un vispārīgas pamatnostādnes

☐ Informācija par subjekta kiberdrošības pārvaldības struktūru, atbildīgo personu un struktūrvienību funkcijām un pienākumiem kiberdrošības jomā, sadarbību ar citiem subjektiem un institūcijām

☐ Informācija par nozīmīgākajiem kiberapdraudējumu veidiem, kuriem ir pakļauti subjekta īpašumā un valdījumā esošie IKT resursi un informācijas sistēmas

☐ Informācija par normatīvo aktu, standartu un sertifikācijas shēmu prasībām kiberdrošības jomā, kuras attiecas uz subjekta īpašumā un valdījumā esošajiem IKT resursiem un informācijas sistēmām

>> Norādīt iemeslu, ja subjekta kiberdrošības politikā nav iekļauta kādā no minētajiem punktiem norādītā informācija:

■ **0399** Cita relevanta informācija par kiberdrošības politiku, ko pats subjekts vēlas sniegt uzraudzības iestādei

4. Resursu un informācijas sistēmu katalogs

Lūdzu, atzīmējiet atbilstošos atbilžu variantus un sniedziet papildu informāciju, ja nepieciešams

■ **0401** Subjekts ir apzinājis un uzskaitījis visus tā īpašumā un valdījumā esošos IKT resursus

☐ Jā

☐ Nē – Norādīt iemeslu:

■ **0402** Subjekts ir izveidojis un uztur resursu un informācijas sistēmu katalogu:

☐ Jā – Norādīt, kādā formātā veidots katalogs:

☐ IKT resursu vadības sistēma
☐ Vispārīga materiāltehnisko resursu uzskaites / vadības sistēma
☐ Manuāli veidots katalogs (piem., *.docx*, *.xlsx* vai tml. formātā)
☐ Citā formātā – norādīt, kādā: _____

☐ Nē – Norādīt iemeslu:

0403 Subjekts ir ieviesis procedūras, lai izmaiņu gadījumā nekavējoties aktualizētu resursu un informācijas sistēmu katalogā ietvertās ziņas:

☐ Jā – Norādīt kataloga pārskatīšanas un aktualizēšanas periodiskumu:

☐ Reizi mēnesī vai biežāk
☐ Retāk nekā reizi mēnesī

– Ja attiecināms, norādīt dokumenta nosaukumu, datumu un numuru, kurā noteiktas minētās procedūras:

☐ Nē – Norādīt iemeslu:

0404 Subjekts ir noteicis konfidencialitātes, integritātes un pieejamības drošības klasi (A, B vai C) katrai subjekta īpašumā un valdījumā esošajai informācijas sistēmai

☐ Jā – Norādīt informācijas sistēmām noteiktās klases:

Informācijas sistēmas nosaukums:	Drošības klase (A, B vai C)		
	Konfidencialitāte	Integritāte	Pieejamība

Nepieciešamības gadījumā pievienot tabulai jaunas rindiņas

☐ Nē – Norādīt iemeslu:

0405 Subjekta resursu un informācijas sistēmu katalogā ir iekļauta šāda informācija *(atzīmēt visus atbilstošos atbilžu variantus):*

☐ Informācijas resursu saraksts

☐ Informācijas sistēmu saraksts

☐ Tīkla shēma

☐ Aparatūras saraksts

☐ Datu nesēju saraksts

☐ Programmatūras saraksts

☐ Ziņas par fizisko infrastruktūru

☐ Ziņas par personām, kuras tiesīgas piekļūt IKT resursiem

■ **0499** Cita relevanta informācija par IKT resursu un informācijas sistēmu katalogu, ko pats subjekts vēlas sniegt uzraudzības iestādei:

5. Kiberrisku pārvaldības un IKT darbības nepārtrauktības plāns
(Pievienot dokumenta kopiju šīs veidlapas pielikumā)

Lūdzu, atzīmējiet atbilstošos atbilžu variantus un sniedziet papildu informāciju, ja nepieciešams

■ **0501** Subjekts ir izstrādājis un apstiprinājis subjekta **kiberrisku pārvaldības un IKT darbības nepārtrauktības plānu**:

☐ Jā – Norādīt dokumentu vai dokumentus (ja plāns sastāv no vairākiem dokumentiem):

☐ Nē – Norādīt iemeslu:

■ **0502** Subjekts kiberrisku pārvaldības un IKT darbības nepārtrauktības plānā ir iekļāvis **kiberrisku novērtēšanas metodiku**, kas ietver analizējamo kiberrisku uzskaitījumu un metodoloģijas aprakstu šo risku nozīmīguma novērtēšanai (piemēram, katra analizējamā kiberriska pieļaujamās vērtības, novērtēšanas matrica, pārskatīšanas periodiskums):

☐ Jā

☐ Nē – Norādīt, kāda informācija nav iekļauta, un neiekļaušanas iemeslu:

☐ N/A (Subjekts nav apstiprinājis kiberrisku pārvaldības un IKT darbības nepārtrauktības plānu)

■ **0503** Subjekts kiberrisku pārvaldības un IKT darbības nepārtrauktības plānā ir iekļāvis **kiberrisku novērtējumu**, kas ietver identificēto kiberrisku uzskaitījumu un analīzi, katra kiberriska nozīmīguma novērtējumu attiecībā uz subjekta īpašumā un valdījumā esošajiem tīkliem, informācijas sistēmām un ar tiem saistītajiem resursiem, kā arī, ja attiecināms, salīdzinājumu ar iepriekšējā perioda kiberrisku pārvaldības un IKT darbības nepārtrauktības plānā ietverto kiberrisku novērtējumu

☐ Jā

☐ Nē – Norādīt, kāda informācija nav iekļauta, un neiekļaušanas iemeslu:

☐ N/A (Subjekts nav apstiprinājis kiberrisku pārvaldības un IKT darbības nepārtrauktības plānu)

■ **0504** Subjekts kiberrisku pārvaldības un IKT darbības nepārtrauktības plānā ir iekļāvis **kiberrisku mazināšanas pasākumu plānu**, kas ietver identificēto kiberrisku uzskaitījumu, konkrētus pasākumus šo kiberrisku mazināšanai, atbildīgos par pasākumu īstenošanu un kontroli, kā arī šo pasākumu īstenošanas termiņus vai to periodiskumu

☐ Jā

☐ Nē – Norādīt, kāda informācija nav iekļauta, un neiekļaušanas iemeslu:

☐ N/A (Subjekts nav apstiprinājis kiberrisku pārvaldības un IKT darbības nepārtrauktības plānu)

■ **0505** Subjekts kiberrisku pārvaldības un IKT darbības nepārtrauktības plānā ir iekļāvis **rīcības plānu darbības nepārtrauktības nodrošināšanai**, kas ietver tīklu, informācijas sistēmu vai to veidojošo elementu darbības nepārtrauktības raksturlielumus (piemēram, RPO, RTO, MTD), šo raksturlielumu uzraudzības metodiku un rīcības plānu šo raksturlielumu pārsniegšanas gadījumā, tostarp rīcības plānu darbības atjaunošanai nozīmīga kiberincidenta vai krīzes gadījumā

☐ Jā

☐ Nē – Norādīt, kāda informācija nav iekļauta, un neiekļaušanas iemeslu:

☐ N/A (Subjekts nav apstiprinājis kiberrisku pārvaldības un IKT darbības nepārtrauktības plānu)

■ **0506** Subjekts ir apzinājis savā īpašumā un valdījumā esošo informācijas sistēmu un IKT resursu **nozīmīgumu un vērtību**, tai skaitā potenciālo zaudējumu un ietekmes apjomu kiberincidenta gadījumā:

☐ Jā

☐ Nē – Norādīt iemeslu:

0507 Subjekts ir paredzējis **rezerves IKT resursus** darbības nepārtrauktības nodrošināšanai nozīmīgā kiberincidenta vai krīzes gadījumā (piemēram, galvenā ugunsmūra rezerves risinājums, rezerves interneta pieslēgums):

☐ Jā – Norādīt, kā tika nodrošināta minētās prasības izpilde:

☐ Nē – Norādīt iemeslu:

0508 Subjekts A klases informācijas sistēmām iespēju robežās ir nodrošinājis no interneta piekļuves pakalpojuma sniedzēja **neatkarīgas (autonomas) IP adreses** vai adrešu apgabalus:

☐ Jā – Norādīt, kā tika nodrošināta minētās prasības izpilde:

☐ Nē – Norādīt iemeslu:

☐ N/A (Prasība neattiecas uz subjektu, jo tā īpašumā un valdījumā nav nevienas A klases informācijas sistēmas)

0509 Subjekta kiberdrošības pārvaldnieks pārskata periodā ir nodrošinājis kiberrisku pārvaldības un IKT darbības nepārtrauktības plāna **izpildes kontroli**:

☐ Jā – Norādīt, kā tika nodrošināta kontrole:

☐ Nē – Norādīt iemeslu:

■ **0510** Subjekta vadītājs ir nodrošinājis, ka kiberdrošības pārvaldniekam un, ja attiecināms, citām par darbības nepārtrauktības pasākumu īstenošanu atbildīgajām personām, ir **nepieciešamās zināšanas un pilnvaras**, lai nekavējoties veiktu tūlītējās nepieciešamās darbības kiberapdraudējuma novēršanai (piemēram, tiesības piekļūt informācijas sistēmas tehniskajiem resursiem):

☐ Jā – Norādīt dokumentu, kurā noteiktas attiecīgās pilnvaras:

☐ Nē – Norādīt iemeslu:

■ **0599** Cita relevanta informācija par kiberrisku pārvaldības un IKT darbības nepārtrauktības plānu, ko pats subjekts vēlas sniegt uzraudzības iestādei:

6. Kiberincidentu pārvaldība un kiberincidentu žurnāls (Pievienot dokumenta kopiju šīs veidlapas pielikumā)

Lūdzu, atzīmējiet atbilstošos atbilžu variantus un sniedziet papildu informāciju, ja nepieciešams

■ **0601** Subjekts ir noteicis nodarbināto un ārpakalpojumu sniedzēju (ja attiecināms) **lomas un atbildības** kiberincidenta pazīmju konstatēšanas gadījumā vai informācijas saņemšanas gadījumā par iespējamo kiberincidentu:

☐ Jā – Ja attiecināms, norādīt dokumentu, kurā noteiktas minētās lomas un atbildība:

☐ Nē – Norādīt iemeslu:

■ **0602** Subjekts ir ieviesis procedūras kiberincidentu **identificēšanai un reģistrēšanai**:

☐ Jā

☐ Nē – Norādīt iemeslu:

■ **0603** Subjekts ir ieviesis procedūras kiberincidentu **ietekmes novērtēšanai**:

☐ Jā

☐ Nē – Norādīt iemeslu:

0604 Subjekts ir ieviesis procedūras kiberincidentu **risināšanai, ietekmes mazināšanai, un seku likvidēšanai**:

☐ Jā

☐ Nē – Norādīt iemeslu:

0605 Subjekts ir ieviesis procedūras kiberincidentu **pirmcēloņu atklāšanai, analīzei un novēršanai, pierādījumu saglabāšanai**:

☐ Jā

☐ Nē – Norādīt iemeslu:

0606 Subjekts ir ieviesis procedūras **drošības pasākumu uzlabošanai** pēc kiberincidenta:

☐ Jā

☐ Nē – Norādīt iemeslu:

0607 Subjektam ir **iekšējās un ārējās komunikācijas plāni** kiberincidenta gadījumā:

☐ Jā

☐ Nē – Norādīt iemeslu:

0608 Subjekts ir ieviesis procedūras, lai nekavējoties ziņotu par konstatētajiem kiberincidentiem kompetentajai **kiberincidentu novēršanas institūcijai**:

☐ Jā

☐ Nē – Norādīt iemeslu:

■ **0609** Subjekts ir izveidojis un uztur **kiberincidentu žurnālu**:

☐ Jā – Norādīt, kādā formātā veidots kiberincidentu žurnāls:

- ☐ Kiberincidentu vadības sistēma (piem., SIEM risinājums)
- ☐ Manuāli veidots žurnāls (piem., *.docx*, *.xlsx* vai tml. formātā)
- ☐ Citā formātā – norādīt, kādā:

☐ Nē – Norādīt iemeslu:

■ **0610** Subjekts ir ieviesis procedūras, lai izmaiņu gadījumā nekavējoties, bet ne vēlāk kā 24 stundu laikā **aktualizētu informāciju** kiberincidentu žurnālā:

☐ Jā

☐ Nē – Norādīt iemeslu:

■ **0611** **Kiberincidentu žurnālā** ir iekļauta šāda informācija par subjekta īpašumā un valdījumā esošajos tīklos un informācijas sistēmās konstatētajiem kiberincidentiem *(atzīmēt visus atbilstošos atbilžu variantus):*

☐ Kiberincidenta konstatēšanas datums un laiks, kā arī kiberincidenta datums un laiks, ja tāds ir zināms

☐ Kiberincidenta veids atbilstoši Ministru kabineta noteikumu par minimālajām kiberdrošības prasībām pielikumā ietvertajai tipoloģijai

☐ Kiberincidenta vispārīgs apraksts

☐ Kiberincidenta cēloņi un kompromitēšanas indikatori, ja tādi ir zināmi

☐ Kiberincidenta ietekmes novērtējums

☐ Atzīme par to, vai kiberincidents uzskatāms par nozīmīgu kiberincidentu

☐ Atzīme par kiberincidenta paziņošanu kiberincidentu novēršanas institūcijai

☐ Aktuālais kiberincidenta risināšanas statuss

>> Norādīt iemeslu, ja kiberincidentu žurnālā nav iekļauta kādā no minētajiem punktiem norādītā informācija:

☐ N/A (Subjekta nav izveidojis kiberincidentu žurnālu)

■ **0612** Kiberincidentu pārvaldības **procedūras ir dokumentētas** subjekta kiberdrošības pārvaldības dokumentu kopumā:

☐ Jā – Norādīt dokumentus, kuros noteiktas minētās procedūras:

☐ Nē – Norādīt iemeslu:

■ **0699** Cita relevanta informācija par kiberincidentu žurnālu un kiberincidentu pārvaldību, ko pats subjekts vēlas sniegt uzraudzības iestādei

7. Lietotāju un piekļuves tiesību pārvaldība

Lūdzu, atzīmējiet atbilstošos atbilžu variantus un sniedziet papildu informāciju, ja nepieciešams

■ **0701** Subjekts katrai tā īpašumā un valdījumā esošajai informācijas sistēmai, loģiski nodalītai informācijas sistēmas daļai (modulim) un informācijas sistēmā elektroniski apstrādājamo informācijas resursu veidam ir **identificējis lietotāju grupas**, izvērtējot lietotāju nepieciešamību piekļūt informācijas resursam
Lūdzu, veidlapas pielikumā pievienot ekrānšāviņu vai dokumentu, kas to apliecina

☐ Jā – Norādīt pielikumu, kurā identificētas lietotāju grupas:

☐ Nē – Norādīt iemeslu:

■ **0702** Subjekts katrai identificētajai lietotāju grupai ir noteicis **piekļuves tiesību līmeni** un **autentifikācijas metodes**, ņemot vērā informācijas resursa veidu un informācijas sistēmas drošības klasi
Lūdzu, veidlapas pielikumā pievienot ekrānšāviņu vai dokumentu, kas to apliecina

☐ Jā – Norādīt pievienoto pielikumu, kurā katrai identificētajai lietotāju grupai noteikts piekļuves tiesību līmenis:

☐ Nē – Norādīt iemeslu:

■ **0703** Subjekts ir ieviesis atbilstošas procedūras, lai nodrošinātu, ka piekļuves tiesības lietotāju kontiem tiek piešķirtas, ievērojot principu **"nepieciešamība zināt"** un **mazāko privilēģiju principu**
Lūdzu, veidlapas pielikumā pievienot ekrānšāviņu vai dokumentu, kas to apliecina

☐ Jā – Norādīt pielikumu, kurā noteiktas minētās procedūras:

☐ Nē – Norādīt iemeslu:

■ **0704** Subjekts ir nodrošinājis, ka lietotājs var veikt darbības ar informācijas resursiem informācijas sistēmā tikai **pēc veiksmīgas autentifikācijas** ar viņam piešķirto lietotāja kontu
Lūdzu, veidlapas pielikumā pievienot ekrānšāviņu vai dokumentu, kas to apliecina

☐ Jā – Norādīt, kā tika nodrošināta minētās prasības izpilde (kādi autentifikācijas risinājumi):

☐ Nē – Norādīt iemeslu:

■ **0705** Subjekts ir nodrošinājis, ka **sistēmkontiem** ir tikai tādas tiesības tehniskajos resursos, kādas nepieciešamas, lai nodrošinātu tīkla vai informācijas sistēmas darbību, tehniskā resursa funkciju vai pakalpojumu
Lūdzu, veidlapas pielikumā pievienot ekrānšāviņu vai dokumentu, kas to apliecina

☐ Jā

☐ Nē – Norādīt iemeslu:

■ **0706** Subjekts ir nodrošinājis, ka informācijas sistēmas tehniskajos resursos ir iestrādāti **kontroles mehānismi**, lai novērstu iespēju lietotājiem lietot sistēmkontus
Lūdzu, veidlapas pielikumā pievienot ekrānšāviņu vai dokumentu, kas to apliecina>

☐ Jā – Norādīt, kādi kontroles mehānismi ieviesti:

☐ Nē – Norādīt iemeslu:

■ **0707** Subjekts ir nodrošinājis, ka **standarta lietotāja konti** netiek izmantoti tīklu, informācijas sistēmu vai tehnisko resursu administrēšanai
Lūdzu, veidlapas pielikumā pievienot ekrānšāviņu vai dokumentu, kas to apliecina

☐ Jā – Norādīt, kā tika nodrošināta minētās prasības izpilde (kādi risinājumi, kādi kontroles mehānismi ir ieviesti):

☐ Nē – Norādīt iemeslu:

■ **0708** Subjekts ir nodrošinājis, ka **administratoru lietotāju konti** netiek izmantoti ikdienas darbam ar informācijas sistēmu vai IKT resursu
Lūdzu, veidlapas pielikumā pievienot ekrānšāviņu vai dokumentu, kas to apliecina

☐ Jā – Norādīt, kā tika nodrošināta minētās prasības izpilde (kādi risinājumi, kādi kontroles mehānismi ir ieviesti):

☐ Nē – Norādīt iemeslu:

■ **0709** Subjektam ir tehniskas iespējas **apturēt jebkura konta darbību**, ja tas ir nepieciešams drošības apsvērumu dēļ:

☐ Jā – Norādīt, kā tiek nodrošināta minētās prasības izpilde (kādi risinājumi tiek izmantoti):

☐ Nē – Norādīt iemeslu:

0710 Subjekts ir nodrošinājis, ka **A klases informācijas sistēmas** administratora un lietotāja kontam var piekļūt tikai, izmantojot daudzfaktoru autentifikāciju
Lūdzu, veidlapas pielikumā pievienot ekrānšāviņu vai dokumentu, kas to apliecina

☐ Jā – Norādīt, kā tiek nodrošināta minētās prasības izpilde (kādi autentifikācijas faktori):

☐ Nē – Norādīt iemeslu:

☐ N/A (Prasība neattiecas uz subjektu, jo tā īpašumā un valdījumā nav nevienas A klases informācijas sistēmas)

0711 Subjekts ir nodrošinājis, ka **B klases informācijas sistēmas** administratora lietotāja kontam var piekļūt tikai, izmantojot daudzfaktoru autentifikāciju:

☐ Jā – Norādīt, kā tiek nodrošināta minētās prasības izpilde (kādi autentifikācijas faktori):

☐ Nē – Norādīt iemeslu:

☐ N/A (Prasība neattiecas uz subjektu, jo tā īpašumā un valdījumā nav nevienas B klases informācijas sistēmas)

0712 Subjekts ir nodrošinājis, ka **B klases informācijas sistēmas** standarta lietotāja kontam, izmantojot attālinātu piekļuvi, var piekļūt tikai, izmantojot daudzfaktoru autentifikāciju:

☐ Jā – Norādīt, kā tiek nodrošināta minētās prasības izpilde (kādi autentifikācijas faktori):

☐ Nē – Norādīt iemeslu:

☐ N/A (Standarta lietotāji nevar piekļūt informācijas sistēmai attālināti)

☐ N/A (Prasība neattiecas uz subjektu, jo tā īpašumā un valdījumā nav nevienas B klases informācijas sistēmas)

■ **0713** Subjekts ir nodrošinājis, ka *(atzīmēt visus atbilstošos atbilžu variantus)*:
Lūdzu, pielikumā pievienot žurnālu vai dokumentu, kas to apliecina

☐ Visi reģistrētie informācijas sistēmas lietotāji ir informēti par informācijas sistēmas lietošanas noteikumiem pirms informācijas sistēmas lietošanas uzsākšanas

☐ Informācijas sistēmas lietošanas noteikumi ir pieejami reģistrētajiem informācijas sistēmas lietotājiem visā informācijas sistēmas lietošanas laikā

>> Norādīt iemeslu, ja kāda no norādītajām prasībām nav izpildīta:

■ **0799** Cita relevanta informācija par lietotāju un piekļuves tiesību pārvaldību, ko pats subjekts vēlas sniegt uzraudzības iestādei:

8. Tīklu pārvaldība

Lūdzu, atzīmējiet atbilstošos atbilžu variantus un sniedziet papildu informāciju, ja nepieciešams

■ **0801** Subjekts ir nodrošinājis, ka **tīkls ir sadalīts loģiskos segmentos** atbilstoši subjekta darbības specifikai un elektroniski apstrādājamo informācijas resursu drošības klasēm
Lūdzu, veidlapas pielikumā pievienot tīkla loģisko shēmu

☐ Jā – Norādīt, kā tiek nodrošināta tīkla segmentācija (kādi segmenti):

☐ Nē – Norādīt iemeslu:

■ **0802** Subjekts ir nodrošinājis, **viesu (apmeklētāju) piekļuve internetam** tiek nodrošināta, izmantojot no iekšējā tīkla fiziski vai loģiski atdalītu tīklu ar atsevišķu reālo IP adresi
Lūdzu veidlapas pielikumā pievienot ekrānšāviņu vai papildu informāciju par dalījumu

☐ Jā – Norādīt viesu tīklu IP adrešu diapazonus:

☐ Nē – Norādīt iemeslu:

☐ N/A (Subjekts nenodrošina viesiem (apmeklētājiem) piekļuvi internetam)

■ **0803** Subjekts ir nodrošinājis, ka **tīkla iekārtas** un cita **aparatūra, kas nav paredzēta tiešai lietotāju izmantošanai**, ir loģiski atdalīta, izmantojot atsevišķus virtuālos tīklus, nodrošinot tai piekļuvi tikai pilnvarotam IKT personālam
Lūdzu veidlapas pielikumā pievienot tīkla loģisko shēmu vai citu skaidrojošu informāciju

☐ Jā – Norādīt, kā tiek nodrošināta minētās prasības izpilde:

☐ Nē – Norādīt iemeslu:

■ **0804** Subjekts ir nodrošinājis, ka **iekšējā bezvadu tīklā** tiek izmantots WPA2, WPA3 vai jaunāks bezvadu drošības protokols ar līdzvērtīgu vai augstāku aizsardzības līmeni
Lūdzu, veidlapas pielikumā pievienot ekrānšāviņu, kas to apliecina

☐ Jā – Norādīt drošības protokolu (piem., WPA2, WPA3):

☐ Nē – Norādīt iemeslu:

☐ N/A (Subjektam nav iekšējā bezvadu tīkla)

■ **0805** Subjekts ir nodrošinājis, ka iekšējais tīkls ir **fiziski vai loģiski nodalīts** no ārēja tīkla:

☐ Jā

☐ Nē – Norādīt iemeslu:

☐ N/A (Prasība neattiecas uz subjektu – svarīgo pakalpojumu sniedzēju)

■ **0806** Subjekts ir nodrošinājis, ka iekšējā tīklā tehnisko resursu administrēšanai paredzētās datu plūsmas (**administratīvais segments**) ir nodalītas no lietotāju ikdienas darbam ar informācijas sistēmu paredzētās datu plūsmas (**lietotāju segments**)
Lūdzu, veidlapas pielikumā pievienot skaidrojošu informāciju

☐ Jā

☐ Nē – Norādīt iemeslu:

☐ N/A (Prasība neattiecas uz subjektu – svarīgo pakalpojumu sniedzēju)

■ **0807** Subjekts ir nodrošinājis, ka datu pārraide starp iekšējo un ārējo tīklu, kā arī starp iekšējā tīkla segmentiem notiek caur **kontrolējamām iekārtām** (piemēram, ugunsmūriem, starpniekserveriem), kas ļauj uzraudzīt un ierobežot neatļautu datu plūsmu (piemēram, izmantojot reāllaika kiberuzbrukumu novēršanas un atklāšanas sistēmu)
Lūdzu, veidlapas pielikumā pievienot tīkla shēmu ar skaidrojošu informāciju par tīkla dalījumu un iekārtām

☐ Jā

☐ Nē – Norādīt iemeslu:

☐ N/A (Prasība neattiecas uz subjektu – svarīgo pakalpojumu sniedzēju)

■ **0808** Subjekts ir nodrošinājis, ka piekļuve iekšējā tīklā esošiem informācijas resursiem ārpus iekšējā tīkla ir iespējama tikai, izmantojot **šifrētu virtuālā privātā tīkla (VPN) risinājumu** ar stingru autentifikāciju
Lūdzu, veidlapas pielikumā pievienot ekrānšāviņu, kas to apliecina

☐ Jā

☐ Nē – Norādīt iemeslu:

☐ N/A (Prasība neattiecas uz subjektu – svarīgo pakalpojumu sniedzēju)

■ **0899** Cita relevanta informācija par tīklu pārvaldību, ko pats subjekts vēlas sniegt uzraudzības iestādei:

9. Žurnālfailu pārvaldība

Lūdzu, atzīmējiet atbilstošos atbilžu variantus un sniedziet papildu informāciju, ja nepieciešams

■ **0901** Subjekts nodrošina **informācijas sistēmu žurnālfailu** un **tīkla plūsmas žurnālfailu** veidošanu:

☐ Jā – Norādīt, kā tiek nodrošināta minētās prasības izpilde (kādi risinājumi):

☐ Nē – Norādīt iemeslu:

■ **0902** Žurnālfaili tiek uzglabāti:
• A klases informācijas sistēmai – vismaz 18 mēnešus;
• B klases informācijas sistēmai – vismaz 12 mēnešus;
• C klases informācijas sistēmai – vismaz 6 mēnešus.
Lūdzu, veidlapas pielikumā pievienot ekrānšāviņu kas to apliecina

☐ Jā – Norādīt, kā tiek nodrošināta minētās prasības izpilde:

☐ Nē – Norādīt iemeslu un to, kāds šobrīd ir žurnālfailu uzglabāšanas laiks:

■ **0903** Subjekts ir nodrošinājis, ka **informācijas sistēmas žurnālfailos** tiek ietverta informācija par šādiem informācijas sistēmas notikumiem *(atzīmēt visus atbilstošos atbilžu variantus): Lūdzu, veidlapas pielikumā pievienot ekrānšāviņus ar piemēriem*

☐ Informācijas sistēmas ieslēgšana un izslēgšana

☐ Kontu izveide, grozīšana vai dzēšana, kontu piekļuves tiesību izmaiņas

☐ Kontu piekļuves mēģinājumi informācijas resursiem

☐ Datu pievienošana, izmaiņas un dzēšana

☐ Tehnisko resursu konfigurāciju izmaiņas

☐ Informācijas sistēmas paziņojumi, brīdinājumi un citi IKT notikumi, kas varētu liecināt par iespējamo kiberincidentu vai citu apdraudējumu informācijas sistēmas vai informācijas resursa drošībai

>> Norādīt iemeslu, ja informācijas sistēmas žurnālfailos netiek ietverta informācija par kādā no punktiem minētajiem notikumiem:

■ **0904** Subjekts ir nodrošinājis, ka **informācijas sistēmas žurnālfailos** tiek fiksēta šāda informācija *(atzīmēt visus atbilstošos atbilžu variantus):*
Lūdzu, veidlapas pielikumā pievienot ekrānšāviņus ar piemēriem

☐ Notikuma laiks, kas sinhronizēts ar augstas precizitātes (vismaz STRATUM 2) tīkla laika protokola (NTP) serveri

☐ IP adrese vai cits identifikators iekārtai, no kuras veikta darbība

☐ Darbības apraksts

☐ Informācija par darbības iniciatoru (piemēram, lietotāja identifikators, pieslēguma metadati)

>> Norādīt iemeslu, ja informācijas sistēmas žurnālfailos netiek fiksēta kādā no punktiem minētā informācija:

■ **0905** Subjekts ir nodrošinājis, ka **tīkla plūsmas žurnālfailos** tiek fiksēta šāda informācija *(atzīmēt visus atbilstošos atbilžu variantus):*
Lūdzu, veidlapas pielikumā pievienot ekrānšāviņus ar piemēriem

☐ Notikuma laiks, kas sinhronizēts ar augstas precizitātes tīkla laika protokola (NTP) serveri

☐ Datu nosūtītāja (avota) un saņēmēja (galamērķa) IP adreses

☐ Avota un galamērķa izmantotie aplikāciju līmeņa protokoli, kas norāda, kādi pakalpojumi vai lietojumprogrammas bija iesaistītas datu pārsūtīšanā (piemēram, HTTP, HTTPS, FTP)

☐ Avota unikālais identifikators (MAC adrese)

☐ Izmantotais tīkla transporta protokols (piemēram, TCP, UDP)

☐ Pārsūtīto datu apjoms

>> Norādīt iemeslu, ja tīkla plūsmas žurnālfailos netiek fiksēta kādā no punktiem minētā informācija:

■ **0906** Subjekts ir nodrošinājis **žurnālfailu aizsardzību** pret neautorizētu piekļuvi, ierakstu izmainīšanu un dzēšanu:

☐ Jā – Norādīt, kā tiek nodrošināta minētās prasības izpilde (piem., kādi risinājumi):

☐ Nē – Norādīt iemeslu:

■ **0907** Subjekts iekšējos normatīvajos aktos ir noteicis **žurnālfailu pārvaldības prasības un kārtību**, tostarp žurnālfailu ierakstu analīzes, pārbaužu kārtību un regularitāti, atbildīgos par žurnālfailu pārvaldību, kā arī žurnālfailu aizsardzības prasības

☐ Jā – Norādīt dokumentus:

☐ Nē – Norādīt iemeslu:

■ **0908** Subjekta **kiberdrošības pārvaldnieks** ir nodrošinājis žurnālfailu pārvaldības un aizsardzības prasību ievērošanas kontroli:

☐ Jā – Norādīt, kā tiek nodrošināta minētās prasības izpilde (piem., kādas pārbaudes, ar kādu periodiskumu):

☐ Nē – Norādīt iemeslu:

■ **0999** Cita relevanta informācija par žurnālfailu pārvaldību, ko pats subjekts vēlas sniegt uzraudzības iestādei:

10. Rezerves kopiju pārvaldība

Lūdzu, atzīmējiet atbilstošos atbilžu variantus un sniedziet papildu informāciju, ja nepieciešams.

■ **1001** Subjekts katrai tā īpašumā un valdījumā esošajai informācijas sistēmai ir nodrošinājis **rezerves kopiju veidošanu**

☐ Jā

☐ Nē – Norādīt iemeslu:

☐ N/A (Prasība neattiecas uz subjektu, jo tā īpašumā un valdījumā nav nevienas A vai B klases informācijas sistēmas)

■ **1002** Subjekts ir nodrošinājis, ka **rezerves kopijas satur visus nepieciešamos datus**, lai varētu atjaunot informācijas sistēmas darbību pilnā apjomā uz to brīdi, kad tika izveidota rezerves kopija, tai skaitā informācijas sistēmā glabātos datus, izpildāmo kodu, atbalsta programmatūru, automatizēto darbību skriptus, tehniskajos resursos regulāri veicamās darbības, operētājsistēmas uzdevumu pārvaldnieka komandas un izpildāmās datnes
Lūdzu, veidlapas pielikumā pievienot ekrānšāviņu ar piemēru - rezerves kopiju dalījumu pa tipiem

☐ Jā – Norādīt, kā tika nodrošināta minētās prasības izpilde (kādi risinājumi tiek izmantoti):

☐ Nē – Norādīt iemeslu:

☐ N/A (Prasība neattiecas uz subjektu, jo tā īpašumā un valdījumā nav nevienas A vai B klases informācijas sistēmas)

■ **1003** Subjekts ir nodrošinājis, ka rezerves kopijas **informācijas sistēmas versijai ir pieejamas** *(atzīmēt visus atbilstošos atbilžu variantus)*:

☐ Informācijas sistēmas tehniskās dokumentācijas rezerves kopijas

☐ Informācijas sistēmas versijas un saistīto bibliotēku versiju pirmkoda (*source code*) rezerves kopijas

☐ Informācijas sistēmas darbību nodrošinošo tehnisko resursu konfigurāciju rezerves kopijas, ja vien tas ir tehniski iespējams

>> Norādīt iemeslu, ja nav pieejama kādā no punktiem minētā informācija:

☐ N/A (Prasība neattiecas uz subjektu, jo tā īpašumā un valdījumā nav nevienas A vai B klases informācijas sistēmas)

■ **1004** Subjekts ir nodrošinājis, ka rezerves kopiju veidošanas **periodiskums un uzglabāšanas laiks** ļauj atjaunot informācijas sistēmas vai informācijas resursa versiju vismaz tādā stāvoklī, kāds bija:
• A klases informācijas sistēmai – iepriekšējā dienā, pirms nedēļas (7-31 diena), pirms mēneša (30-365 dienas), iepriekšējā gadā (vecāku par 365 dienām);
• B klases informācijas sistēmai – pēdējās nedēļas laikā (1-7 dienas), pirms nedēļas (7-31 diena), pirms mēneša (30-365 dienas), iepriekšējā gadā (vecāku par 365 dienām);
• C klases informācijas sistēmai – pirms pēdējām nozīmīgām izmaiņām informācijas sistēmā (piem., pirms migrācijas uz jaunu tehnoloģisku platformu), bet ne senāk kā pirms 6 mēnešiem.
Lūdzu, veidlapas pielikumā pievienot ekrānšāviņu ar konfigurācijas piemēru

☐ Jā – Norādīt, kā tika nodrošināta minētās prasības izpilde (kāds ir rezerves kopiju veidošanas cikls, periodiskums, uzglabāšanas laiks):

☐ Nē – Norādīt iemeslu:

☐ N/A (Prasība neattiecas uz subjektu, jo tā īpašumā un valdījumā nav nevienas A vai B klases informācijas sistēmas)

■ **1005** Subjekts ir nodrošinājis, ka par katru rezerves kopijas izveides gadījumu tiek veikts atbilstošs **ieraksts žurnālfailos**
Lūdzu, veidlapas pielikumā pievienot ekrānšāviņu ar konfigurācijas piemēru

☐ Jā

☐ Nē – Norādīt iemeslu:

☐ N/A (Prasība neattiecas uz subjektu, jo tā īpašumā un valdījumā nav nevienas A vai B klases informācijas sistēmas)

■ **1006** Subjekts ir nodrošinājis, ka par rezerves kopijām atbildīgais personāls un kiberdrošības pārvaldnieks tiek **nekavējoties brīdināti**, ja kārtējā rezerves kopijas izveide nav izdevusies
Lūdzu, veidlapas pielikumā pievienot ekrānšāviņu ar konfigurācijas piemēru

☐ Jā – Norādīt, kā tiek nodrošināta minētās prasības izpilde (kādi risinājumi tiek izmantoti):

☐ Nē – Norādīt iemeslu:

☐ N/A (Prasība neattiecas uz subjektu, jo tā īpašumā un valdījumā nav nevienas A vai B klases informācijas sistēmas)

■ **1007** Subjekts katrai tā īpašumā un valdījumā esošajai A un B klases informācijas sistēmai nodrošina, ka pēc rezerves kopijas izveides tiek izveidota **rezerves kopijas satura kontrolsumma**:

☐ Jā – Norādīt, kā tiek nodrošināta minētās prasības izpilde (kādi risinājumi tiek izmantoti):

☐ Nē – Norādīt iemeslu:

☐ N/A (Prasība neattiecas uz subjektu, jo tā īpašumā un valdījumā nav nevienas A klases informācijas sistēmas)

■ **1008** Subjekts ir nodrošinājis, ka rezerves kopijām **gan fiziski, gan elektroniskajā vidē var piekļūt** tikai par rezerves kopijām atbildīgais personāls un kiberdrošības pārvaldnieks:

☐ Jā – Norādīt, kā tiek nodrošināta minētās prasības izpilde (kādi piekļuves ierobežojumi vai kontroles mehānismi):

☐ Nē – Norādīt iemeslu:

☐ N/A (Prasība neattiecas uz subjektu, jo tā īpašumā un valdījumā nav nevienas A vai B klases informācijas sistēmas)

■ **1009** Subjekts ir nodrošinājis, ka A klases informācijas sistēmai **vismaz viena pilna rezerves kopija** tiek uzglabāta no informācijas sistēmas atdalītos tehniskajos resursos (piem., datu nesējos), ģeogrāfiski nodalītā vietā, telpās, kas aizsargātas pret nesankcionētu piekļuvi un aprīkotas ar automātisko ugunsgrēka atklāšanas un trauksmes signalizācijas sistēmu:

☐ Jā

☐ Nē – Norādīt iemeslu:

☐ N/A (Prasība neattiecas uz subjektu, jo tā īpašumā un valdījumā nav nevienas A klases informācijas sistēmas)

■ **1010** Subjekts nodrošina, ka A klases informācijas sistēmai pēc rezerves kopijas pārvietošanas citā datu nesējā **tiek pārbaudīta rezerves kopijas integritāte** (piemēram, pārbaudot tās satura kontrolsummu):

☐ Jā – Norādīt, kā tiek pārbaudīta rezerves kopijas integritāte (kādi risinājumi):

☐ Nē – Norādīt iemeslu:

☐ N/A (Prasība neattiecas uz subjektu, jo tā īpašumā un valdījumā nav nevienas A klases informācijas sistēmas)

■ **1011** Subjekts **iekšējos normatīvajos aktos** ir noteicis rezerves kopiju veidošanas, glabāšanas, pārbaudes un dzēšanas prasības un kārtību, tostarp kārtību, kādā pārbauda, vai, izmantojot rezerves kopijas, iespējams atjaunot informācijas resursus un informācijas sistēmas darbību:

☐ Jā – Norādīt dokumentus, kuros noteikta rezerves kopiju veidošanas, glabāšanas, pārbaudes un dzēšanas prasības un kārtība:

☐ Nē – Norādīt iemeslu:

☐ N/A (Prasība neattiecas uz subjektu, jo tā īpašumā un valdījumā nav nevienas A vai B klases informācijas sistēmas)

■ **1012** Subjekta **kiberdrošības pārvaldnieks** ir nodrošinājis rezerves kopiju pārvaldības un aizsardzības prasību ievērošanas kontroli, tostarp rezerves kopiju pārbaudi izlases kārtā:

☐ Jā – Norādīt, kā tiek nodrošināta minētās prasības izpilde (piem., kādas pārbaudes, ar kādu periodiskumu):

☐ Nē – Norādīt iemeslu:

☐ N/A (Prasība neattiecas uz subjektu, jo tā īpašumā un valdījumā nav nevienas A vai B klases informācijas sistēmas)

■ **1099** Cita relevanta informācija par rezerves kopiju pārvaldību, ko pats subjekts vēlas sniegt uzraudzības iestādei:

11. Kiberhigiēnas pasākumi

Lūdzu, atzīmējiet atbilstošos atbilžu variantus un sniedziet papildu informāciju, ja nepieciešams

■ **1101** Pārskata periodā tika nodrošinātas **sākotnējās instruktāžas** kiberdrošības jautājumos subjekta nodarbinātajiem, kuri lieto IKT resursus, uzsākot darba (dienesta) attiecības:

☐ Jā

☐ Nē – Norādīt iemeslu:

■ **1102** Pārskata periodā vismaz reizi gadā tika veikta subjekta nodarbināto, kuri lieto IKT resursus, **kārtējā instruktāža** kiberdrošības jautājumos:

☐ Jā – Norādīt pēdējā gada laikā organizētās kārtējās instruktāžas:

Instruktāžas datums:	Instruktāžas nosaukums/tēma:

Nepieciešamības gadījumā pievienot tabulai jaunas rindiņas

☐ Nē – Norādīt iemeslu:

■ **1103** Pārskata periodā tika nodrošinātas **ārkārtas instruktāžas** kiberdrošības jautājumos subjekta nodarbinātajiem, kuri lieto IKT resursus (piemēram, identificējot jaunu būtisku risku, ievainojamību vai kiberapdraudējumu, paredzot normatīvo aktu prasību izmaiņas vai veicot nozīmīgas izmaiņas IKT infrastruktūrā, programmatūrā vai biznesa procesos):

☐ Jā

☐ Nē

■ **1104** Pārskata periodā vismaz reizi gadā tika organizētas subjekta nodarbinātā **IKT personāla apmācības** kiberrisku pārvaldības un IKT darbības nepārtrauktības pasākumu efektīvai īstenošanai:

☐ Jā

☐ Nē – Norādīt iemeslu:

■ **1105** Pārskata periodā **apmācību saturs tika pārskatīts** un nepieciešamības gadījumā aktualizēts vismaz reizi gadā vai, mainoties apstākļiem (piemēram, izceļoties jauniem kiberapdraudējumiem, mainoties kiberriska līmenim, notiekot kiberincidentam):

☐ Jā

☐ Nē

■ **1106** Subjekts ir nodrošinājis, ka visiem tā nodarbinātajiem, kuri lieto IKT resursus, ir pieejami aktuālie **instruktāžu materiāli** (piem., prezentācijas datnes, izdales materiāli):

☐ Jā

☐ Nē

■ **1107** Subjekts ir nodrošinājis organizēto **apmācību uzskaiti**:

☐ Jā

☐ Nē

■ **1108** Subjekts ir ieviesis procesus, lai **novērtētu nodarbināto zināšanas** kiberdrošības jautājumos un īstenoto apmācību efektivitāti:

☐ Jā – Norādīt, kā tiek nodrošināta minētās prasības izpilde (piem., kuros dokumentos šie procesi ir dokumentēti):

☐ Nē – Norādīt iemeslu:

1199 Cita relevanta informācija par kiberhigiēnas pasākumiem, ko pats subjekts vēlas sniegt uzraudzības iestādei:

12. Šifrēšanas prasības

Lūdzu, atzīmējiet atbilstošos atbilžu variantus un sniedziet papildu informāciju, ja nepieciešams

1201 Subjekts pielieto, ja tas ir tehniski iespējams, šifrēšanas risinājumus **A un B konfidencialitātes klases** informācijas resursu **pārsūtīšanai un pārraidei (*in-transit*)** publiskajā vidē un iekšējos IKT infrastruktūras bezvadu tīklos
Lūdzu, veidlapas pielikumā pievienot ekrānšāviņu ar konfigurācijas piemēru

☐ Jā – Norādīt izmantoto šifrēšanas risinājumu:

☐ Nē – Norādīt iemeslu:

☐ N/A (Prasība neattiecas uz subjektu, jo tas nepārsūta un nepārraida A vai B konfidencialitātes klases informācijas resursus publiskajā vidē vai iekšējos IKT infrastruktūras bezvadu tīklos)

1202 Subjekts pielieto, ja tas ir tehniski iespējams, šifrēšanas risinājumus **A konfidencialitātes klases** informācijas resursu **glabāšanai (*at-rest*)**
Ja iespējams, lūdzu, veidlapas pielikumā pievienot ekrānšāviņu ar konfigurācijas piemēru

☐ Jā – Norādīt izmantoto šifrēšanas risinājumu:

☐ Nē – Norādīt iemeslu:

☐ N/A (Prasība neattiecas uz subjektu, jo tas neglabā A konfidencialitātes klases informācijas resursus)

1203 Subjekts iekšējos normatīvajos aktos ir noteicis **minimālo pieļaujamo kriptogrāfijas aizsardzības (noturības) līmeni**, ņemot vērā informācijas resursu konfidencialitātes līmeni un Nacionālā kiberdrošības centra un Satversmes aizsardzības biroja vadlīnijas:

☐ Jā – Aprakstīt izmantoto šifrēšanas aizsardzības līmeni vai veidus:

☐ Nē – Norādīt iemeslu:

■ **1204** Subjekts iekšējos normatīvajos aktos ir **noteicis šifrēšanas atslēgu pārvaldības politiku**, lai nodrošinātu, ka tikai autorizētas personas var atšifrēt datus:

☐ Jā – Aprakstīt pārvaldības politiku:

☐ Nē – Norādīt iemeslu:

■ **1205** Subjekts iekšējos normatīvajos aktos ir noteicis prasības drošai **šifrēšanas atslēgu izveidošanai, uzstādīšanai, glabāšanai, nomaiņai un likvidēšanai**, tai skaitā fiziskās un digitālās drošības prasības:

☐ Jā – Aprakstīt prasību īstenošanu:

☐ Nē – Norādīt iemeslu:

■ **1299** Cita relevanta informācija par šifrēšanas prasībām, ko pats subjekts vēlas sniegt uzraudzības iestādei:

13. IKT infrastruktūras prasības

Lūdzu, atzīmējiet atbilstošos atbilžu variantus un sniedziet papildu informāciju, ja nepieciešams

■ **1301** Subjekts tā īpašumā un valdījumā esošās **A un B klases informācijas sistēmas** uztur *(atzīmēt visus atbilstošos atbilžu variantus)*:

☐ Subjekta IKT infrastruktūrā, kas atbilst Ministru kabineta noteikumiem par minimālajām kiberdrošības prasībām

☐ Datu centrā, kas atbilst Ministra kabineta noteikumiem par informācijas sistēmu izvietošanas un datu centru drošības prasībām

☐ Citur – norādīt, kur:

☐ N/A (Prasība neattiecas uz subjektu, jo tā īpašumā un valdījumā nav nevienas A vai B klases informācijas sistēmas)

■ **1302** Ja A un B klases informācijas sistēmas uztur **subjekta infrastruktūrā**, subjekts ir nodrošinājis, ka *(atzīmēt visus atbilstošos atbilžu variantus)*:

☐ Aparatūra ir izvietota atsevišķā slēdzamā telpā vai slēdzamās statnēs (skapjos)

☐ Katrai telpai vai statnei ir fizisks vai elektronisks apmeklētāju žurnāls

☐ Subjekta vadītājs vai vadītāja pilnvarotā persona ir apstiprinājusi sarakstu ar personām, kurām ir tiesības piekļūt IKT aparatūras telpai un statnēm

☐ Telpas ir nodrošinātas ar atbilstošiem klimata uzraudzības un kontroles mehānismiem

☐ Telpās netiek glabātas ugunsnedrošas mantas vai atkritumi

☐ Telpas ir nodrošinātas ar automātisko ugunsgrēka atklāšanas un trauksmes signalizācijas sistēmu

☐ Atbildīgie nodarbinātie ir informēti par kārtību un rīcību ugunsgrēka gadījumā

☐ Ir izvērtēti elektroapgādes pārtraukuma (pārrāvuma) riski, un IKT infrastruktūra ir aprīkota vismaz ar nepārtrauktās elektrības barošanas iekārtu, rezerves elektrības pieslēgumu vai alternatīvu elektrības padeves rezerves risinājumu

☐ Komunikāciju kabeļi ir aizsargāti pret nejaušu bojāšanu

☐ Atbildīgie nodarbinātie ir informēti par kārtību un rīcību neparedzētu notikumu gadījumā, un viņiem ir zināmi apsardzes, ugunsdzēsības, elektroapgādes un klimata kontroles apkalpojošā personāla vai pakalpojuma sniedzēja kontaktinformācija

>> Norādīt iemeslu, ja kāda no minētajām prasībām netiek ievērota:

☐ N/A (Subjekts neuztur A un B klases informācijas sistēmas savā IKT infrastruktūrā)

☐ N/A (Prasība neattiecas uz subjektu, jo tā īpašumā un valdījumā nav nevienas A vai B klases informācijas sistēmas)

■ **1399** Cita relevanta informācija par IKT infrastruktūras prasībām, ko pats subjekts vēlas sniegt uzraudzības iestādei

14. Cita informācija

■ **9900** Cita informācija par subjekta kiberdrošību, ko pats subjekts vēlas sniegt uzraudzības iestādei saistībā ar subjekta atbilstības pašvērtējumu

14. Informācija par ziņojuma iesniedzēju un apliecinājums

Ziņojuma iesniedzēja vārds, uzvārds:

Ziņojuma iesniedzēja amats:

Ziņojuma iesniedzēja e-pasts:

Ziņojuma iesniedzēja tālruņa Nr.:

☐ Apliecinu, ka šajā ziņojumā norādītā informācija par subjekta kiberdrošību ir pilnīga un patiesa. Apņemos pēc kompetentās iestādes pieprasījuma bez nepamatotas kavēšanas iesniegt papildu informāciju, kas nepieciešama subjekta kiberdrošības uzraudzībai.

© Oficiālais izdevējs "Latvijas Vēstnesis"