LIKUMI

Izdevējs: Ministru kabinets
Veids: noteikumi
Numurs: 602
Pieņemts: 29.09.2026.
Stājas spēkā: 01.10.2026.

Publicēts:
Latvijas Vēstnesis, 189, 01.10.2026.
OP numurs: 2026/189.35

Ministru kabineta noteikumi Nr. 602

Rīgā 2026. gada 29. septembrī (prot. Nr. 55 41. §)

Informācijas sistēmu izvietošanas un datu centru drošības prasības

Izdoti saskaņā ar Nacionālās kiberdrošības likuma 30. panta otro daļu

1. Vispārīgie jautājumi

1. Noteikumi nosaka:

1.1. prasības Nacionālās kiberdrošības likuma subjekta informācijas sistēmu izvietošanai datu centros, kā arī datu centru drošības prasības;

1.2. datu centru atbilstības novērtēšanas un uzraudzības kārtību, kā arī datu centra operatoru pienākumus;

1.3. drošības operāciju centru izveides un darbības noteikumus datu centros.

2. Noteikumos lietotie termini:

2.1. subjekts – Nacionālās kiberdrošības likuma 3. panta pirmās daļas 1. punktā minētais būtisko pakalpojumu sniedzējs, svarīgo pakalpojumu sniedzējs vai informācijas un komunikācijas tehnoloģiju kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs;

2.2. subjekta informācijas un komunikācijas tehnoloģiju infrastruktūra – informācijas un komunikācijas tehnoloģiju infrastruktūra, kura atrodas subjekta īpašumā vai tiesiskajā valdījumā un kurā tiek izvietotas subjekta informācijas sistēmas;

2.3. datu centra operators – publisko tiesību juridiskā persona vai privāto tiesību juridiskā persona, kuras īpašumā vai tiesiskajā valdījumā ir datu centrs un kura nodrošina datu centra izmantošanu:

2.3.1. savas informācijas sistēmas vai tās daļas izvietošanai;

2.3.2. citas ar datu centra īpašnieku vai tiesisko valdītāju saistītas organizācijas informācijas sistēmas vai tās daļas izvietošanai;

2.3.3. cita subjekta informācijas sistēmas vai tās daļas izvietošanai;

2.4. telemetrijas dati – kiberapdraudējuma identificēšanai nepieciešami dati, kas iegūti no informācijas sistēmām, operētājsistēmām, lietojumprogrammām vai datortīkla infrastruktūras, tai skaitā žurnālfaili, kā arī dati un metadati par datu plūsmā identificētajiem drošības notikumiem;

2.5. drošības operāciju centrs – kompetentās kiberincidentu novēršanas institūcijas izveidota un pārvaldīta centralizēta kiberdrošības uzraudzības un reaģēšanas funkcija, kas nodrošina kiberdrošības notikumu un kiberapdraudējumu nepārtrauktu uzraudzību, identificēšanu, analīzi un reaģēšanu uz tiem, kā arī telemetrijas datu apstrādi.

3. Šo noteikumu prasības piemēro tiktāl, ciktāl attiecīgo jautājumu neregulē Komisijas 2024. gada 17. oktobra Īstenošanas regula (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 attiecībā uz kiberdrošības risku pārvaldības pasākumu tehniskajām un metodiskajām prasībām un precizē gadījumus, kad incidentu uzskata par būtisku.

4. Šo noteikumu piemērošanai informācijas sistēmas A, B vai C klasi un tās konfidencialitātes, integritātes un pieejamības drošības klasi nosaka saskaņā ar normatīvajiem aktiem par minimālajām kiberdrošības prasībām.

2. Informācijas sistēmas izvietošanas un datu centru drošības prasības

2.1. Vispārējās prasības

5. Ja šajos noteikumos nav noteikts citādi, subjekts informācijas sistēmu vai tās daļu izvieto datu centrā valstī, kas ir Ziemeļatlantijas līguma organizācijas (turpmāk – NATO) dalībvalsts, Eiropas Savienības dalībvalsts vai Eiropas Brīvās tirdzniecības asociācijas (turpmāk – EBTA) dalībvalsts vai kāda no NATO sadarbības valstīm Indijas un Klusā okeāna reģionā (turpmāk – IP4). Subjekts nodrošina, ka datu apstrāde notiek šo valstu teritorijā.

6. Šo noteikumu prasības piemēro, ievērojot Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Regulu (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula), tai skaitā prasības attiecībā uz personas datu nosūtīšanu trešajām valstīm vai starptautiskajām organizācijām, ja saistībā ar informācijas sistēmas vai tās daļas izvietošanu dati tiek nosūtīti trešajām valstīm vai datiem piekļūst attālināti no trešās valsts.

2.2. A klases informācijas sistēmas izvietošanas prasības

7. Šajā apakšnodaļā noteiktās prasības piemēro A klases informācijas sistēmas vai tās daļas izvietošanai datu centrā ārpus subjekta informācijas un komunikācijas tehnoloģiju infrastruktūras.

8. Subjekts A klases informācijas sistēmu vai tās daļu izvieto datu centrā, kura atbilstība ir apliecināta saskaņā ar šo noteikumu 21. punktu.

9. Izņēmuma gadījumā subjektam ir atļauts A klases informācijas sistēmu vai tās daļu, izņemot informācijas un komunikācijas tehnoloģiju kritiskās infrastruktūras īpašnieka vai tiesiskā valdītāja A klases informācijas sistēmu vai tās daļu, izvietot datu centrā, kura atbilstība nav apliecināta saskaņā ar šo noteikumu 21. punktu, ja subjekts ir dokumentējis nepieciešamību izvietot A klases informācijas sistēmu vai tās daļu šādā datu centrā, izvērtējis ar izvietošanu saistītos riskus, noteicis risku mazināšanas pasākumus un pirms izvietošanas atbilstoši Nacionālās kiberdrošības likuma 41. pantā noteiktajam subjektu uzraudzības dalījumam ir saņēmis attiecīgās kompetentās uzraugošās iestādes pozitīvu saskaņojumu.

10. Izvietojot A klases informācijas sistēmu vai tās daļu datu centrā ārpus Latvijas Republikas teritorijas, subjekts nodrošina:

10.1. zināmu un pakalpojuma sniedzēja dokumentācijā norādītu datu apstrādes vietu;

10.2. līgumiskos nosacījumus, kas nodrošina Latvijas Republikas kompetentajām uzraudzības institūcijām tiesības veikt auditēšanu, uzraudzību un pārbaudes, ciktāl tas ir tehniski iespējams un atbilst attiecīgās valsts normatīvajiem aktiem.

11. Ja subjekta, izņemot informācijas un komunikācijas tehnoloģiju kritiskās infrastruktūras īpašnieka vai tiesiskā valdītāja, A klases informācijas sistēmas vai tās daļas izvietošana vairs neatbilst kādai no šo noteikumu 8. vai 10. punktā minētajām prasībām, subjekts 12 mēnešu laikā no dienas, kad attiecīgā prasība vairs netiek izpildīta, atjauno atbilstību šo noteikumu prasībām.

12. Ja informācijas un komunikācijas tehnoloģiju kritiskās infrastruktūras īpašnieka vai tiesiskā valdītāja A klases informācijas sistēmas vai tās daļas izvietošana vairs neatbilst kādai no šo noteikumu 8. vai 10. punktā minētajām prasībām, informācijas un komunikācijas tehnoloģiju kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs nekavējoties informē Satversmes aizsardzības biroju, kā arī atjauno atbilstību šo noteikumu prasībām.

13. Šo noteikumu 8., 11. un 12. punktā minētās prasības neattiecas uz:

13.1. A klases informācijas sistēmas vai tās daļas pagaidu izvietošanu datu centrā ārpus Latvijas Republikas teritorijas ārkārtējās situācijas vai izņēmuma stāvokļa gadījumā vai primārā datu centra nepieejamības gadījumā, ja tas nepieciešams A klases informācijas sistēmas darbības nepārtrauktības nodrošināšanai;

13.2. rezerves kopiju izvietošanu, izņemot informācijas un komunikācijas tehnoloģiju kritiskās infrastruktūras īpašnieka vai tiesiskā valdītāja A klases informācijas sistēmas rezerves kopiju izvietošanu, ja vienlaikus ir izpildīti visi turpmāk minētie nosacījumi:

13.2.1. rezerves kopijas tiek izmantotas tikai A klases informācijas sistēmas darbības atjaunošanai, tai skaitā tās pagaidu izvietošanai citā datu centrā primārā datu centra darbības traucējumu gadījumā;

13.2.2. subjekts nodrošina rezerves kopiju konfidencialitāti, integritāti un pieejamību atbilstoši A klases informācijas sistēmai noteiktajai drošības klasei;

13.2.3. subjekts ir informējis Nacionālo kiberdrošības centru par rezerves kopiju izvietošanas vietu un piekļuves nosacījumiem.

14. Šo noteikumu 13.1. apakšpunktā minētajā gadījumā subjekts informē kompetento kiberincidentu novēršanas institūciju un atbilstoši Nacionālās kiberdrošības likuma 41. pantā noteiktajam subjektu uzraudzības dalījumam attiecīgo kompetento uzraugošo iestādi, iesniedzot šādu informāciju:

14.1. informācijas sistēmas nosaukums;

14.2. datu centra operatora nosaukums;

14.3. datu centra atrašanās vieta;

14.4. datu apstrādes vieta;

14.5. informācijas sistēmas izvietošanas veids un plānotās izvietošanas sākuma datums.

2.3. Īpašās informācijas un komunikācijas tehnoloģiju kritiskās infrastruktūras īpašnieku vai tiesisko valdītāju informācijas sistēmu izvietošanas prasības

15. Informācijas un komunikācijas tehnoloģiju kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs A klases informācijas sistēmu vai tās daļu var izvietot:

15.1. savā īpašumā vai tiesiskajā valdījumā esošā datu centrā, kas atrodas Latvijas Republikas teritorijā, ja datu apstrāde notiek Latvijas Republikas teritorijā;

15.2. Valsts pārvaldes iekārtas likumā noteiktās publiskās personas vai datu centra operatora, kura kapitāla daļu turētājs vai netiešās ietekmes guvējs ir Valsts pārvaldes iekārtas likumā noteiktā publiskā persona, īpašumā vai tiesiskajā valdījumā esošā datu centrā, kas atrodas Latvijas Republikas teritorijā, ja datu apstrāde notiek Latvijas Republikas teritorijā;

15.3. Valsts pārvaldes iekārtas likumā noteiktās publiskās personas vai datu centra operatora, kura kapitāla daļu turētājs vai netiešās ietekmes guvējs ir Valsts pārvaldes iekārtas likumā noteiktā publiskā persona, īpašumā vai tiesiskajā valdījumā esošā datu centrā, kas atrodas NATO, Eiropas Savienības vai EBTA dalībvalstī, ja datu apstrāde notiek NATO, Eiropas Savienības vai EBTA dalībvalsts teritorijā un informācijas un komunikācijas tehnoloģiju kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs pirms informācijas sistēmas izvietošanas par to informē Satversmes aizsardzības biroju;

15.4. juridiskas personas īpašumā vai tiesiskajā valdījumā esošā datu centrā, kas atrodas NATO, Eiropas Savienības vai EBTA dalībvalstī, ja datu apstrāde notiek minēto valstu teritorijā un pirms informācijas sistēmas izvietošanas ir saņemts Satversmes aizsardzības biroja pozitīvs atzinums.

16. Informācijas un komunikācijas tehnoloģiju kritiskās infrastruktūras īpašniekam vai tiesiskajam valdītājam A klases informācijas sistēmu vai tās daļu ir atļauts izvietot datu centrā, tai skaitā savā īpašumā vai tiesiskajā valdījumā esošā datu centrā, kura atbilstība ir apliecināta saskaņā ar šo noteikumu 21. punktu.

17. Informācijas un komunikācijas tehnoloģiju kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs B klases

informācijas sistēmu vai C klases informācijas sistēmu vai tās daļu izvieto:

17.1. savā īpašumā vai tiesiskajā valdījumā esošā datu centrā, kas atrodas Latvijas Republikas teritorijā, ja datu apstrāde notiek Latvijas Republikas teritorijā;

17.2. Valsts pārvaldes iekārtas likumā noteiktās publiskās personas vai datu centra operatora, kura kapitāla daļu turētājs vai netiešās ietekmes guvējs ir Valsts pārvaldes iekārtas likumā noteiktā publiskā persona, īpašumā vai tiesiskajā valdījumā esošā datu centrā, kas atrodas Latvijas Republikas teritorijā, ja datu apstrāde notiek Latvijas Republikas teritorijā;

17.3. Valsts pārvaldes iekārtas likumā noteiktās publiskās personas vai datu centra operatora, kura kapitāla daļu turētājs vai netiešās ietekmes guvējs ir Valsts pārvaldes iekārtas likumā noteiktā publiskā persona, īpašumā vai tiesiskajā valdījumā esošā datu centrā, kas atrodas NATO, Eiropas Savienības vai EBTA dalībvalstī, ja datu apstrāde notiek minēto valstu teritorijā;

17.4. juridiskas personas īpašumā vai tiesiskajā valdījumā esošā datu centrā, kas atrodas NATO, Eiropas Savienības vai EBTA dalībvalstī, ja datu apstrāde notiek minēto valstu teritorijā un subjekts pirms informācijas sistēmas izvietošanas par to informē Satversmes aizsardzības biroju.

18. Informējot Satversmes aizsardzības biroju šo noteikumu 15.3. un 17.4. apakšpunktā minētajā gadījumā, informācijas un komunikācijas tehnoloģiju kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs iesniedz Satversmes aizsardzības birojam šādu informāciju:

18.1. informācijas sistēmas nosaukums;

18.2. informācijas sistēmas drošības klase;

18.3. datu centra operatora nosaukums;

18.4. datu centra atrašanās vieta;

18.5. datu apstrādes vieta;

18.6. informācijas sistēmas izvietošanas veids un plānotās izvietošanas sākuma datums.

19. Šo noteikumu 15.4. apakšpunktā minēto Satversmes aizsardzības biroja atzinumu pieprasa un sniedz normatīvajos aktos par minimālajām kiberdrošības prasībām noteiktajā kārtībā.

20. Informācijas un komunikācijas tehnoloģiju kritiskās infrastruktūras īpašnieka vai tiesiskā valdītāja informācijas sistēmas rezerves kopiju izvietošanai piemēro konkrētas drošības klases informācijas sistēmai noteiktās izvietošanas prasības.

3. Datu centru atbilstības novērtēšana un uzraudzība un datu centru operatoru pienākumi

21. Datu centra atbilstību šo noteikumu prasībām apliecina vienā no šādiem veidiem:

21.1. ar datu centra auditora atzinumu, kas sagatavots, veicot datu centra atbilstības auditu saskaņā ar šo

noteikumu 1. pielikumu, un ir noformēts atbilstoši šo noteikumu 2. pielikumam;

21.2. ar sertifikātu vai citu dokumentu, kas apliecina datu centra atbilstību kādam no šo noteikumu 3. pielikumā minētajiem sertifikācijas modeļiem.

22. Šo noteikumu 21.1. apakšpunktā minēto atzinumu atjauno ne retāk kā reizi divos gados.

23. Šo noteikumu 21.1. apakšpunktā minēto datu centra atbilstības auditu veic datu centra auditors, kuram ir vismaz divu gadu profesionālā pieredze datu centru drošības audita jomā un kurš ir ieguvis un uztur spēkā sertificēta datu centru auditora profesionāļa (*Certified Data Centre Audit Professional* – CDCAP) sertifikātu vai citu līdzvērtīgu starptautiski atzītu sertifikātu datu centru audita vai drošības audita jomā. Ja auditējamā datu centra īpašnieks vai tiesiskais valdītājs ir subjekts, datu centra auditoram jāatbilst normatīvajos aktos par minimālajām kiberdrošības prasībām noteiktajām ārpakalpojumu prasībām.

24. Subjekts, slēdzot ārpakalpojuma līgumu par informācijas sistēmas vai tās daļas izvietošanu datu centrā, ievēro normatīvajos aktos par minimālajām kiberdrošības prasībām noteiktās ārpakalpojumu prasības un līgumā papildus paredz, ka:

24.1. datu centra operators ievēro tam šajos noteikumos noteiktos pienākumus;

24.2. datu centra atrašanās vieta un subjekta datu apstrādes vieta atbilst šo noteikumu 5. punktā minētajām prasībām un, ja attiecināms, šo noteikumu 2.2. un 2.3. apakšnodaļā minētajām prasībām.

25. Subjekts atbilstoši Nacionālās kiberdrošības likuma 41. pantā noteiktajam subjektu uzraudzības dalījumam informē attiecīgo kompetento uzraugošo iestādi par datu centru, kurā izvietota tā informācijas sistēma vai tās daļa, kā arī par attiecīgā datu centra atbilstību šo noteikumu prasībām, iesniedzot pašvērtējuma ziņojumu normatīvajos aktos par minimālajām kiberdrošības prasībām noteiktajā kārtībā.

26. Informācijas un komunikācijas tehnoloģiju kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs nekavējoties, bet ne vēlāk kā piecu darbdienu laikā nosūta Satversmes aizsardzības birojam datu centra auditora atzinumu, kas sagatavots, veicot informācijas un komunikācijas tehnoloģiju kritiskās infrastruktūras īpašnieka vai tiesiskā valdītāja datu centra atbilstības auditu.

27. Datu centra operators nekavējoties, bet ne vēlāk kā piecu darbdienu laikā informē subjektu par situāciju, kas var ietekmēt datu centra, kurā izvietota subjekta informācijas sistēma vai tās daļa, atbilstību šajos noteikumos noteiktajām datu centra drošības prasībām.

28. Atbilstoši Nacionālās kiberdrošības likuma 41. pantā noteiktajam subjektu uzraudzības dalījumam attiecīgā kompetentā uzraugošā iestāde var pieprasīt datu centra operatoram veikt datu centra ārkārtas atbilstības auditu šādos gadījumos:

28.1. A klases informācijas sistēmā noticis nozīmīgs kiberincidents, un tā cēlonis ir saistīts ar datu centru;

28.2. datu centrā notikuši vairāki līdzīgi kiberincidenti vai fiziskās drošības incidenti;

28.3. pastāv pamatotas šaubas, ka datu centrs neatbilst šajos noteikumos paredzētajām datu centru drošības prasībām;

28.4. datu centra operators, uz kuru attiecas normatīvajos aktos par minimālajām kiberdrošības prasībām noteiktais pienākums norīkot kiberdrošības pārvaldnieku, nav norīkojis kiberdrošības pārvaldnieku vai ir norīkojis kiberdrošības pārvaldnieku, kas neatbilst minētajos normatīvajos aktos noteiktajām prasībām.

4. Drošības operāciju centru izveides un darbības noteikumi datu centros

29. Subjekts, kura īpašumā vai valdījumā ir A klases informācijas sistēma vai tās daļa, nodrošina kompetentajai kiberincidentu novēršanas institūcijai:

29.1. piekļuvi telemetrijas datu pirmavotam;

29.2. datu centra operatora apstrādātu telemetrijas datu pieejamību reāllaikā (ar datu pieejamību ne vēlāk kā vienu minūti pēc notikuma) no pirmavota, izmantojot datu apmaiņas un līgumiskos mehānismus.

30. Ja drošības operāciju centrs tiek izvietots informācijas un komunikācijas tehnoloģiju kritiskās infrastruktūras īpašnieka vai tiesiskā valdītāja īpašumā vai tiesiskajā valdījumā esošā datu centrā, kompetentā kiberincidentu novēršanas institūcija pirms drošības operāciju centra izvietošanas informē Satversmes aizsardzības biroju un nodrošina informācijas apmaiņu ar to atbilstoši Satversmes aizsardzības biroja kompetencei.

31. Datu centra operators nodrošina telemetrijas datu pieejamību reāllaikā (ar datu pieejamību ne vēlāk kā vienu minūti pēc notikuma) kompetentajai kiberincidentu novēršanas institūcijai pēc tās pieprasījuma, tai skaitā drošības operāciju centru darbības nodrošināšanai.

5. Noslēguma jautājumi

32. Pēc šo noteikumu spēkā stāšanās dienas subjekts neuzsāk jaunu A klases informācijas sistēmas vai tās daļas izvietošanu, ja tā neatbilst šo noteikumu prasībām, izņemot šo noteikumu 9. un 13. punktā minētos gadījumus.

33. Subjekts, kas līdz šo noteikumu spēkā stāšanās dienai datu centrā izvieto A klases informācijas sistēmu vai tās daļu, līdz 2026. gada 31. decembrim par šādas informācijas sistēmas izvietošanu informē:

33.1. attiecīgo datu centra operatoru, ja datu centra operators nav pats subjekts;

33.2. Satversmes aizsardzības biroju, ja subjekts ir informācijas un komunikācijas tehnoloģiju kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs.

34. Ja šo noteikumu 33. punktā minētā A klases informācijas sistēma vai tās daļa līdz šo noteikumu spēkā stāšanās dienai nav izvietota atbilstoši šo noteikumu prasībām, subjekts var turpināt attiecīgo izvietošanu līdz 2027. gada 31. decembrim, ja tas nodrošina ar attiecīgo izvietošanu saistīto risku pārvaldību un līdz 2026. gada 31. decembrim sagatavo atbilstības nodrošināšanas plānu.

35. Šo noteikumu 34. punktā minētajā atbilstības nodrošināšanas plānā norāda pasākumus, termiņus un atbildīgās personas šo noteikumu prasību izpildei, kā arī risku mazināšanas pasākumus līdz pilnīgas atbilstības nodrošināšanai. Subjekts plānu aktualizē, ja mainās A klases informācijas sistēmas vai tās daļas izvietošanas risinājums vai citi būtiski izvietošanas riski, un pēc pieprasījuma iesniedz to attiecīgajai kompetentajai uzraugošajai iestādei atbilstoši

Nacionālās kiberdrošības likuma 41. pantā noteiktajam subjektu uzraudzības dalījumam.

36. Subjekts pēc 2027. gada 31. decembra neturpina šo noteikumu 34. punktā minēto izvietošanu, ja tā neatbilst šo noteikumu prasībām. Līgumu, starpiestāžu vienošanos vai citu dokumentu, uz kura pamata tiek nodrošināta attiecīgā izvietošana, var pagarināt vai būtiski grozīt tiktāl, ciktāl tas nerada iespēju turpināt neatbilstošu izvietošanu pēc minētā termiņa.

37. Mākoņdatošanas pakalpojuma izmantošana neatbrīvo subjektu no pienākuma nodrošināt šo noteikumu prasību izpildi attiecībā uz mākoņdatošanas pakalpojumā izmantotajiem datu centriem.

38. Noteikumi stājas spēkā 2026. gada 1. oktobrī.

Ministru prezidents *A. Kulbergs*

Aizsardzības ministra pienākumu izpildītājs – satiksmes ministrs *R. Kozlovskis*

1. pielikums
Ministru kabineta
2026. gada 29. septembra
noteikumiem Nr. 602

Datu centra atbilstības audita kontrolsaraksts

I. Organizatoriskās prasības

1. Personāla apmācība

Nr. p. k.	Prasība	Pārbaude
1.1.	Ir noteikta un ieviesta kārtība darbinieku apmācībai drošības jomā. Apmācības drošības jomā (krīžu vadībā – par datu centra infrastruktūras nepārtrauktības un drošības nodrošināšanu, reaģējot uz fiziskiem, loģiskiem vai organizatoriskiem incidentiem; datu aizsardzībā – par klientu datu, operatīvo infrastruktūras datu un drošības konfigurāciju datu aizsardzību) tiek veiktas ne retāk kā reizi sešos mēnešos	Dokumentu pārbaude: apmācību kārtība/politika, gada plāns un grafiks. Pārbaudīt faktiskos pierādījumus par periodiskumu (≥ 1x/6 mēn.). Pierādījumi: apmācību programmas, dalībnieku saraksti/žurnāli, e-mācību izdrukas, sertifikāti
1.2.	Apmācība drošības jomā ietver praktiskus incidentu simulācijas treniņus (piem., APT, datu noplūde)	Pārbaudīt treniņu scenārijus, mācību plānus un norises protokolus. Pārliecināties, vai treniņi tiešām notikuši (datumi, dalībnieki, mērķi) un sagatavots pēctreniņa ziņojums. Pierādījumi: scenāriji (*injects*), apmeklējuma saraksti, foto/ekrānuzņēmumi, pēctreniņa ziņojums
1.3.	Treniņu rezultāti ir analizēti; ir noteikti un īstenoti koriģējošie pasākumi	Pārskatīt pēctreniņa analīzes un lēmumus (mācības, CAPA). Pārliecināties par pasākumu izpildi un pabeigšanu (atbildīgie, termiņi, statusi). Pierādījumi: CAPA žurnāls, uzdevumu izsekošana (*ticketing*), politiku/procedūru grozījumi, atkārtotu pārbaužu ieraksti

2. Fiziskā piekļuves kontrole

Nr. p. k.	Prasība	Pārbaude
2.1.	Datu centra zonas (tai skaitā perimetrs līdz ēkai) ir noteiktas drošības politikā un klasificētas vismaz trijos drošības līmeņos: zemas drošības zona, vidējas drošības zona un augstas drošības zona. Zonu klasifikācija un perimetra apraksts ir dokumentēti	Dokumentu pārbaude: drošības politika, zonējuma shēma, telpu saraksts, perimetra apraksts. Veikt vietas apskati, vai faktiskie marķējumi un piekļuves punkti atbilst dokumentiem. Pierādījumi: drošības politika, zonējuma shēmu kopijas, foto, marķējuma paraugi
2.2.	Piekļuve tiek nodrošināta atbilstoši zonas drošības līmenim:	Politiku un ACS (*Access Control System*) iestatījumu pārbaude; izlases testi vairākās zonās. Pierādījumi: piekļuves politika, ACS

		konfigurāciju ekrānuzņēmumi
2.2.1.	zemas drošības zona – vismaz personas identifikācija vai vienfaktora autentifikācija	Apskates/intervijas pie ieejas punktiem; notikumu žurnālu pārbaude par identifikācijas/1FA izmantošanu. Pierādījumi: žurnāla izraksti, instrukcijas dežurantam
2.2.2.	vidējas drošības zona – vismaz divfaktoru autentifikācija (piem., RFID + PIN vai biometriskie dati)	ACS iestatījumu pārbaude par 2FA izmantošanu; izlases pārbaude piekļuves notikumu žurnāla ierakstiem, kas apliecina 2FA izmantošanu. Pierādījumi: konfigurāciju ekrānuzņēmumi, žurnāla ieraksti par 2FA izmantošanu
2.2.3.	augstas drošības zona – vismaz trīsfaktoru autentifikācija (piem., RFID + PIN + biometriskie dati)	ACS/biometrikas iestatījumu pārbaude par 3FA izmantošanu; žurnālu izlases pārbaude; kontrolēts praktisks tests (ja iespējams). Pierādījumi: konfigurācijas, žurnāli, testa protokols
2.3.	Elektroniskās autentifikācijas dati ir šifrēti, glabāti un aizsargāti atbilstoši normatīvajos aktos par minimālajām kiberdrošības prasībām attiecīgajai drošības kategorijai noteiktajām prasībām	Politiku, sistēmu iestatījumu un arhitektūras aprakstu pārbaude; datubāzes/ACS šifrēšanas parametri; paroļu/biometrisko datu glabāšanas mehānismi. Pierādījumi: konfigurāciju izdrukas, tehniskā dokumentācija, atbilstības matrica
2.4.	Visi fiziskās piekļūšanas notikumi un piekļuves mēģinājumi ir reģistrēti un glabāti vismaz 18 mēnešus	Žurnālu/žurnāla ierakstu glabāšanas termiņu iestatījumu pārbaude; parauga ieraksta vecuma pārbaude (>18 mēn. robeža). Pierādījumi: glabāšanas termiņu politika, žurnālu izgūšanas ekrānuzņēmumi ar datumiem
2.5.	Piekļuves notikumu ierakstus pārskata ne retāk kā reizi mēnesī. Pārskatīšanu veic kiberdrošības pārvaldnieks vai pilnvarota persona. Pārskatīšanas fakts ir dokumentēts	Procedūras pārbaude; pārskatu (*review*) pierakstu esība katram mēnesim; paraksti un datumi. Pierādījumi: mēneša pārskata žurnāls, kontroles saraksts, atbildīgās personas apstiprinājums
2.6.	Nodrošināta transportlīdzekļu iebraukšanas/ izbraukšanas kontrole apsardzes perimetrā. Reģistrē vismaz reģistrācijas numuru, iebraukšanas/ izbraukšanas laiku un saistīto personu	Apskates/intervijas pie vārtiem; žurnāla/parakstu grāmatas vai elektronisko ierakstu pārbaude; izlases verifikācija ar video/ACS datiem. Pierādījumi: žurnāla izraksti, sistēmas ekrānuzņēmumi, video laika zīmogi

3. Darbības nepārtrauktības plāns

Nr. p. k.	**Prasība**	**Pārbaude**
3.1.	Ir aktuāls darbības nepārtrauktības plāns, kurā ietverta riska analīze, atkopšanas stratēģijas un datu centra darbības atjaunošanas pasākumi (sk. 19. punktu)	Dokumentu pārbaude: plāna versija, apstiprinājums, darbības joma, risku analīze, atjaunošanas stratēģijas un procedūras. Pārliecināties, vai plāns aptver kritiskos pakalpojumus un to savstarpējo atkarību. Pierādījumi: plāna kopija, riska analīze, atjaunošanas procedūras

3.2.	Darbības nepārtrauktības plāna pārbaudes notiek ne retāk kā reizi sešos mēnešos, aptverot vismaz šādus elementus:	Dokumentu pārbaude: gada/pusgada testu grafiks. Pārskatīt testu protokolus un pēctestu ziņojumus. Pierādījumi: grafiks, protokoli, dalībnieku saraksti, secinājumi
3.2.1.	personāla lomu sadalījuma pārbaude; darbinieki zina un izprot savu lomu/atbildību plāna īstenošanā un incidentu vadībā	Intervijas; uzdevumu matricas un kontaktpersonu sarakstu pārbaude; dežūru grafiki. Pierādījumi: lomu/atbildību matrica, kontaktpersonu saraksts, apmācību ieraksti
3.2.2.	elektroapgādes nepārtrauktības pārbaude – testē nepārtrauktās barošanas sistēmas (UPS), ģeneratoru un rezerves enerģijas avotu funkcionalitāti (sk. 8. punktu)	Testa plāni un protokoli; pārslēgšanās žurnāli; ģeneratoru un UPS testu ieraksti. Pierādījumi: protokoli, žurnālu izraksti, iekārtu ekrānuzņēmumi
3.2.3.	dzesēšanas sistēmu nepārtrauktības pārbaude (sk. 9. punktu)	Testa plāni; trauksmju/robežvērtību sasniegšanas brīdinājumu ieraksti; dzesēšanas iekārtu darbības protokoli. Pierādījumi: protokoli, monitoringa izdrukas, žurnāli
3.2.4.	tīkla infrastruktūras rezerves ceļu un datu pārraides sistēmu pārbaude; primārā tīkla atteices gadījumā tiek aktivizēti rezerves sakaru kanāli (sk. 10. punktu)	Praktiska pārslēgšanās pārbaude (plānots tests); maršrutēšanas/pārslēgšanās žurnāli; topoloģijas atbilstība. Pierādījumi: testa protokoli, BGP/ maršrutēšanas žurnāli, shēmas
3.2.5.	ugunsdrošības sistēmas un avārijas reaģēšanas procedūru pārbaude, ieskaitot ugunsgrēka simulāciju un atkopšanas procedūras (sk. 15. punktu)	Testa plāni; signalizācijas un dzēšanas sistēmu testu ieraksti; evakuācijas un darbību protokoli. Pierādījumi: protokoli, sistēmu žurnāli, apmācību ieraksti
3.2.6.	drošības incidentu un fiziskās drošības pārbaude, ieskaitot piekļuves kontroles un videonovērošanas sistēmu pārbaudes (sk. 11. un 14. punktu)	ACS un videonovērošanas testu protokoli; piekļuves noteikumu pārbaude; izlases žurnāli. Pierādījumi: konfigurāciju izdrukas, žurnālu izraksti, testa apraksti
3.2.7.	datu centra pārvaldības informācijas sistēmu atjaunošanas procedūru testēšana, simulējot datu un darbības atjaunošanas plānus (sk. 19. punktu)	Atjaunošanas testa plāni; atjaunošanas laiku un datu atjaunošanas mērķu (RTO/RPO) sasniegšanas pieraksti. Pierādījumi: testa protokoli, laika mērījumi, atjaunoto datu pārbaudes ieraksti
3.3.	Pārbaudes rezultāti ir dokumentēti; konstatētās nepilnības ir analizētas un novērstas	Pārskatīt pēctestu ziņojumus un koriģējošo pasākumu plānu; pārliecināties par pasākumu izpildi un pabeigšanu (atbildīgie, termiņi, statuss). Pierādījumi: ziņojumi, uzdevumu saraksts, statusa pārskati

4. Incidentu pārvaldība

Nr. p. k.	**Prasība**	**Pārbaude**
4.1.	Tiek uzturēts incidentu reģistrs (apraksts, ietekme, novēršana, laiki, lēmumi) (sk. arī 18. punktu)	Dokumentu pārbaude: incidentu pārvaldības kārtība, izmantotā sistēma (piem., servisa pieteikumu rīks). Paraugu pārbaude: izlases kārtā pārskatīt pēdējo 6–12 mēnešu incidentu ierakstus. Pārliecināties, vai katrā ierakstā ir norādīts apraksts, ietekme, novēršanas pasākumi, laika

		atzīmes (konstatēšana/reaģēšanas sākums/ novēršana) un pieņemtais lēmums. Ja incidents ietekmējis pieejamību, pārbaudīt, vai ietekmes ilgums atspoguļots pieejamības uzskaitē (sk. 16.2.2. apakšpunktu). Pierādījumi: izdrukas/ ekrānuzņēmumi no reģistra, pārskati, CAPA ieraksti
4.2.	Incidentu reģistrs tiek regulāri pārskatīts (ne retāk kā reizi nedēļā vai atbilstoši riska izvērtējumā noteiktajam biežumam); pārskatīšanas fakts ir dokumentēts	Pārskatīšanas grafika un atbildīgo noteikšana; pārskatīšanas protokoli/pieraksti ar datumu un parakstu; konstatēto problēmu un uzdevumu saraksts ar statusu. Pārbaudīt paraugus, vai pēdējo triju mēnešu pārskatīšanas pieraksti atbilst noteiktajam biežumam. Pierādījumi: protokoli, uzdevumu saraksti (*ticket*), atbildīgo apstiprinājumi

5. Dokumentācija

Nr. p. k.	Prasība	Pārbaude
5.1.	Datu centra dokumentācija ir strukturēta tematiskajās sadaļās (5.1.1.–5.1.12. apakšpunkts), un tiek uzturēts dokumentu reģistrs. Dokumentu reģistrā norāda katras sadaļas dokumentu sarakstu (nosaukums, versija, apstiprinājuma datums, dokumenta īpašnieks, nākamās pārskatīšanas datums):	Pārbaudīt, vai dokumentu reģistrā ir iekļautas visas tematiskās sadaļas (5.1.1.–5.1.12. apakšpunkts) un vai norādītie dokumenti pastāv. Pārbaudīt piekļuvi dokumentu aktuālajām versijām un arhīvu esību. Pierādījumi: dokumentu reģistrs, saites/dokumentu ekrānuzņēmumi, arhīva ieraksti
5.1.1.	pārvaldība un dokumentu kontrole – dokumentu pārvaldības kārtība (versiju kontrole, īpašnieks, apstiprināšana, pārskatīšanas cikls) un atbildības sadalījums	Pārbaudīt dokumentu pārvaldības politiku/ procedūru; pārliecināties, vai tā atbilst reģistrā norādītajam (sk. 5.1. apakšpunktu) un tiek piemērota praksē. Pierādījumi: politika/procedūra, apstiprinājumi, piemēru pārbaude vairākām dokumentu vienībām
5.1.2.	riska pārvaldība un atbilstība – riska novērtēšanas metodika un rezultāti; atbilstības matrica normatīvo aktu un šī pielikuma prasībām	Pārskatīt pēdējā riska novērtējuma dokumentāciju, metodiku un riska apstiprināšanas lēmumu; pārbaudīt atbilstības matricu, kur sasaistītas prasības, kontrole un atbilstību apliecinošie pierādījumi. Pierādījumi: riska novērtējums, atbilstības matrica
5.1.3.	fiziskā drošība – drošības politika, zonējuma shēma un telpu/perimetra apraksts; piekļuves kontroles kārtība (tai skaitā tiesību pārskatīšana); apmeklētāju/transportlīdzekļu plūsma; videonovērošanas kārtība (sk. 2., 11. un 14. punktu)	Pārbaudīt dokumentus un veikt vietas apskati: zonējuma atbilstība, piekļuves noteikumi, pārskatīšanas biežums, videonovērošanas zonas. Pierādījumi: politika, shēmas, procedūras, žurnāli
5.1.4.	Infrastruktūra:	
5.1.4.1.	elektroapgāde – UPS/ģeneratoru shēmas; testi un uzturēšanas grafiki/protokoli; degvielas nodrošinājums (sk. 8. punktu)	Pārbaudīt shēmas, grafikus, testu protokolus; aplūkot degvielas rezerves un piegādes kārtību. Pierādījumi: shēmas, protokoli, līgumi
5.1.4.2.	dzesēšana – konfigurācijas, robežvērtības/ uzraudzība; uzturēšana un testu protokoli (sk. 9.	Pārbaudīt konfigurāciju aprakstus, monitoringa iestatījumus, uzturēšanas/testu protokolus.

	punktu)	Pierādījumi: dokumentācija, brīdinājumu iestatījumi, protokoli
5.1.4.3.	tīkls un savienojumi – topoloģijas (fiziskā/loģiskā), segmentācija, rezerves ceļi, automātiskā pārslēgšanās (sk. 10. punktu)	Pārskatīt topoloģijas shēmas, segmentācijas aprakstu, BGP/rezerves ceļu iestatījumus, pārslēgšanās testu protokolus. Pierādījumi: shēmas, konfigurācijas, testu ieraksti
5.1.4.4.	ugunsdrošība un noplūžu noteikšana – sistēmu apraksti, testu grafiki un protokoli, avārijas rīcības kārtība (sk. 12. un 15. punktu)	Pārbaudīt procedūras, testu protokolus, trauksmju pārraidi un atbildīgo sarakstus. Pierādījumi: protokoli, plāni, žurnāli
5.1.5.	uzraudzība un mērījumi – monitoringa un trauksmju iestatījumi; pieejamības mērīšanas un aprēķina kārtība (sk. 16. un 21. punktu)	Pārbaudīt monitoringa iestatījumus, trauksmju sliekšņus, pieejamības aprēķina metodiku un pārskatus. Pierādījumi: iestatījumu izdrukas, pārskatu paraugi
5.1.6.	incidentu un problēmu pārvaldība – incidentu pārvaldības kārtība; incidentu reģistra uzturēšana; eskalācijas process un saziņa; problēmu analīzes (cēloņanalīzes) kārtība (sk. 4. un 18. punktu)	Pārbaudīt politikas/procedūras, reģistra ierakstus, eskalācijas ķēdes, pēctestu ziņojumus. Pierādījumi: procedūras, reģistra izdrukas, CAPA ieraksti
5.1.7.	darbības nepārtrauktība un atjaunošana (BCP/DRP) – RTO/RPO/MTO; testu plāni/grafiki un pārskati (sk. 3. un 19. punktu)	Pārbaudīt plānus, testu grafikus un protokolus; pārskatīt mērķu sasniegšanu (RTO/RPO). Pierādījumi: plāni, protokoli, mērījumi
5.1.8.	izmaiņu un uzturēšanas pārvaldība – izmaiņu pieprasīšana/apstiprināšana; plānoto darbu paziņošana; atteices/atgriešanās plāni (sk. 17. un 20. punktu)	Pārskatīt izmaiņu procesu, paziņojumu paraugus klientiem, atcelšanas/atgriešanās plānus. Pierādījumi: CAB protokoli, paziņojumi, plāni
5.1.9.	aktīvu un konfigurāciju pārvaldība – CMDB/aktīvu saraksts, konfigurāciju apraksti; marķēšanas standarts (tai skaitā kabeļu marķēšana), rezerves daļas (sk. 10.3.4. apakšpunktu)	Pārbaudīt CMDB/aktīvu sarakstu atbilstību faktiskajam stāvoklim; kabeļu marķējuma un identifikācijas atbilstību objektā. Pierādījumi: saraksti, foto, shēmas
5.1.10.	datu nesēju dzīves cikls – iegāde, lietošana, glabāšana, transportēšana, atkārtota izmantošana, iznīcināšana; iznīcināšanas dokumentēšana (sk. 23. punktu)	Pārskatīt datu nesēju dzīves cikla kārtību, iznīcināšanas protokolus un sertifikātus; izlases pārbaude par pēdējiem gadījumiem. Pierādījumi: procedūras, protokoli, sertifikāti
5.1.11.	pakalpojumu līmeņi un saziņa ar klientiem – SLA; pieejamības/incidentu pārskati; paziņošanas kārtība (sk. 20. un 22. punktu)	Pārbaudīt SLA tekstus, pārskatu paraugus, paziņošanas termiņus/kanālus; salīdzināt ar faktiskajiem pārskatiem. Pierādījumi: līgumi, pārskati, paziņojumi
5.1.12.	ierakstu (žurnālu) saglabāšanas kārtība – vienots žurnālu un testu rezultātu saglabāšanas termiņu grafiks (piem., piekļuves notikumi – 18 mēn.; monitorings – 12 mēn.; ugunsdrošības pārbaudes – ≥ 3 gadi); atbildība par saglabāšanu, integritāti un pieejamību (sk. 2.4., 21.3. un 15.2. apakšpunktu)	Pārbaudīt saglabāšanas grafiku un to ievērošanu, tai skaitā sistēmu iestatījumus; pārskatīt parauga ierakstus, kas pārsniedz noteikto termiņu; nemaināmības iestatījumus un piekļuves tiesības, ja attiecināms. Pierādījumi: politika/grafiks, ekrānuzņēmumi, paraugi
5.2.	Visi šī pielikuma 5.1. apakšpunktā minētie dokumenti tiek pārskatīti un atjaunināti ne retāk kā reizi 12 mēnešos vai pēc būtiskām izmaiņām; dokumentu reģistrā norādīti aktuālās versijas dati, īpašnieks un nākamās pārskatīšanas datums; iepriekšējās versijas ir arhivētas	Pārbaudīt pēdējos pārskatīšanas/apstiprināšanas datumus, izmaiņu žurnālu un izplatīšanas kārtību; pārliecināties par piekļuvi dokumentu aktuālajām versijām un arhīvu esību. Pierādījumi: reģistrs, izmaiņu žurnāli, piekļuves norādes

6. Personāla drošības pārbaudes

Nr. p. k.	Prasība	Pārbaude
6.1.	Darbinieku drošības pārbaudes tiek veiktas pirms darbinieka pieņemšanas darbā un turpmāk ne retāk kā reizi divos gados	Pārbaudīt personāla drošības pārbaužu kārtību un grafiku. Pārskatīt izlases kārtā personu lietas vai sistēmas ierakstus par veikto pārbaudi un pārbaudes datumu. Pārliecināties par atbilstību noteiktajam pārbaužu biežumam. Pierādījumi: kārtība/politika, pārbaužu reģistrs, paraugu izdrukas ar datumiem
6.2.	Darbinieku drošības pārbaudes attiecas uz šādām darbinieku kategorijām:	
6.2.1.	darbinieki ar fizisku vai plānotu fizisku piekļuvi datu centra infrastruktūrai (datu centra klientu aparatūras telpas, drošības vadības telpas, augstas drošības zonas)	Pārbaudīt, vai minētajiem darbiniekiem ir veikta drošības pārbaude. Salīdzināt piekļuves tiesību sarakstus ar pārbaužu reģistru. Pierādījumi: piekļuves saraksti, pārbaužu reģistrs
6.2.2.	darbinieki ar loģisku vai plānotu loģisku piekļuvi datu centra pārvaldības/uzraudzības sistēmām	Pārbaudīt, vai minētajiem darbiniekiem ir veikta drošības pārbaude. Salīdzināt lietotāju/ administratoru sarakstus ar pārbaužu reģistru. Pierādījumi: lietotāju saraksti, pārbaužu reģistrs
6.2.3.	drošības personāls ar pastāvīgām piekļuves tiesībām augstas drošības zonām	Pārbaudīt, vai drošības personālam ir veikta drošības pārbaude. Salīdzināt pastāvīgo piekļuves tiesību sarakstu ar pārbaužu reģistru. Pierādījumi: piekļuves saraksti, pārbaužu reģistrs
6.3.	Pirms darbinieka nodarbināšanas ir pārbaudīta viņa profesionālā atbilstība un sodāmības neesība atbilstoši piemērojamajam regulējumam	Pārbaudīt pirmsnodarbināšanas pārbaužu kārtību un paraugus (profesionālās atbilstības apliecinājumi, sodāmības neesības pārbaudes kārtība). Pārliecināties, vai pastāv tiesiskais pamats datu apstrādei un vai dokumenti ir noformēti. Pierādījumi: procedūra, paraugu ieraksti/personu lietu izraksti, atbildīgo apstiprinājumi
6.4.	Regulārā pārskatīšanā vērtē vismaz piekļuves tiesību atbilstību amata pienākumiem, drošības politikas ievērošanu un apmācību apmeklējumu	Pārskatīt periodisko pārskatīšanu pierakstus (piem., piekļuves tiesību pārskatīšanas un apstiprināšanas protokoli, disciplīnas pārkāpumu/ noviržu uzskaite, apmācību reģistri). Pārliecināties, vai konstatētie trūkumi ir novērsti un ir atzīmes par pabeigšanu. Pierādījumi: atkārtotas sertifikācijas audits un sertifikāta atjaunošana (sertifikāta kopija, audita ziņojums), apmācību reģistri, koriģējošo pasākumu ieraksti

II. Tehniskās prasības

7. Klimata kontrole

Nr. p. k.	Prasība	Pārbaude

7.1.	Datu centra telpās tiek uzturēts iekārtu ražotāja noteiktais temperatūras režīms, un t. s. aukstajā koridorā temperatūra nepārsniedz +27 °C	Pārbaudīt sensoru/monitoringa iestatījumus un vēsturiskos datus (robežvērtības, trauksmes). Vietas apskate: izlases mērījumi t. s. aukstajos/karstajos koridoros. Pierādījumi: monitoringa ekrānuzņēmumi/pārskati, temperatūras žurnāli, konfigurāciju izdrukas
7.2.	Tiek uzturēts iekārtu ražotāja noteiktais relatīvā mitruma režīms; nodrošināti pasākumi pret kondensāciju un statisko elektrību	Pārbaudīt mitruma uzraudzību un robežvērtības, apskatīt mitrināšanas/atmitrināšanas risinājumus un ESD pasākumus (grīdas, zemējums, ESD brīdinājumi). Pierādījumi: monitoringa dati, tehniskā dokumentācija, uzturēšanas protokoli, ESD kontroles apraksti

8. Enerģijas pārvaldība

Nr. p. k.	Prasība	Pārbaude
8.1.	Datu centram ir nodrošināta nepārtraukta elektroapgāde (piem., nepārtrauktās barošanas sistēma (UPS))	Pārbaudīt shēmas un jaudas aprēķinus; pārbaudīt UPS konfigurāciju un veselības pārskatus. Pierādījumi: shēmas, UPS pārskati, trauksmju žurnāli
8.2.	Nodrošināts rezerves elektroapgādes risinājums; degvielas krājumi vismaz 24 stundu autonomai darbībai; nodrošināti risinājumi savlaicīgai degvielas piegādei	Pārbaudīt ģeneratoru specifikācijas un degvielas apjomu uzskaiti; pārbaudīt līgumus/piekrišanas vēstules par piegādi un piegādes plānu. Pierādījumi: degvielas žurnāli, piegādes līgumi, ģeneratora pārskati
8.3.	Rezerves elektroapgādes risinājums nodrošina automātisku un nepārtrauktu pārslēgšanos no primārā barošanas avota uz rezerves barošanas avotu, izmantojot sinhronizētu pāreju vai pārslēgšanos bez pārrāvuma	Pārbaudīt automātiskās pārslēgšanās (ATS/STS) iestatījumus un testu protokolus; parauga tests, ja iespējams. Pierādījumi: testu protokoli, ATS/STS konfigurācijas, traucējumu žurnāli
8.4.	Rezerves elektroapgādes izmantošana neietekmē šī pielikuma 16. punktā noteikto pieejamības rādītāju (sk. 16. punktu)	Pārskatīt pieejamības pārskatus periodos, kad darbojies rezerves barošanas avots; pārliecināties, vai šie periodi nav uzskaitīti kā dīkstāve. Pierādījumi: pieejamības aprēķini, incidentu/enerģijas notikumu žurnāli
8.5.	Rezerves elektroapgādes darbspēja tiek pārbaudīta atbilstoši ražotāja prasībām un normatīvajiem aktiem; pārbaudes fakts un rezultāti ir dokumentēti	Pārskatīt regulāro testu grafikus un protokolus (aukstie/karstie testi, slodzes bankas, pārslēgšanās testi). Pierādījumi: grafiki, protokoli, konstatējumu un labošanas ieraksti

9. Dzesēšanas sistēma

Nr. p. k.	Prasība	Pārbaude
9.1.	Dzesēšanas sistēma ir projektēta un uzturēta, nodrošinot rezervēšanu un darbības nepārtrauktību atbilstoši šī pielikuma 16. punktā noteiktajam pieejamības līmenim (sk. 16. punktu)	Pārbaudīt rezervēšanas shēmu (piem., N+1/2N) dokumentāciju un reālo izvietojumu; trauksmju un pārslēgšanās darbību. Pierādījumi: shēmas, konfigurāciju apraksti, testu protokoli

9.2.	Dzesēšanas sistēmas konfigurācija un savietojamība ar citām drošības sistēmām ir dokumentēta	Pārbaudīt integrāciju ar ugunsdrošības/monitoringa sistēmām (piem., avārijas izslēgšanas funkcija, trauksmju pāradresācija). Pierādījumi: integrācijas shēmas, procedūras
9.3.	Dzesēšanas sistēmas pārvaldība un monitorings nodrošināts reāllaikā ar attālinātu uzraudzību un automātiskiem brīdinājumiem (piem., robežvērtību pārsniegšana)	Pārbaudīt monitoringa iestatījumus, trauksmju sliekšņus un nosūtīšanas kanālus; vēsturiskās trauksmes. Pierādījumi: iestatījumu ekrānuzņēmumi, trauksmju žurnāli
9.4.	Dzesēšanas sistēmas darbspēja tiek pārbaudīta atbilstoši ražotāja prasībām; pārbaudes fakts un rezultāti ir dokumentēti	Pārskatīt testu grafikus un protokolus (sūkņi, kompresori, vārsti, liekie resursi). Pierādījumi: grafiki, protokoli, labošanas darbi

10. Tīkla infrastruktūra

Nr. p. k.	Prasība	Pārbaude
10.1.	Tīkla infrastruktūras tehniskie līdzekļi ir rezervēti un atbilst šī pielikuma 16. punktā noteiktajām pieejamības prasībām (sk. 16. punktu)	Pārbaudīt aparatūras/tīkla savienojumu rezervēšanu (divkāršus maršrutētājus/slēdžus, dublējošas elektroapgādes ķēdes); pārslēgšanās testu ierakstus. Pierādījumi: shēmas, konfigurācijas, testu protokoli
10.2.	Tīkla drošības kontroles atbilst paaugstinātas drošības kategorijas informācijas sistēmu prasībām, kas noteiktas normatīvajos aktos par minimālajām kiberdrošības prasībām	Pārskatīt atbilstības matricu normatīvo aktu prasībām; tīkla segmentāciju, ugunsmūrus, piekļuves kontroli, žurnālus. Pierādījumi: tīkla drošības politika, konfigurāciju izdrukas, atbilstības matrica, žurnāli
10.3.	Tīkla infrastruktūra atbilst vismaz šādām prasībām:	
10.3.1.	datu pārraides kabeļi ir izbūvēti atsevišķās, ugunsdrošās un fiziski nodalītās trasēs, izvairoties no to šķērsošanās ar energoapgādes kabeļiem	Vietas apskate; projekta/izpildes shēmas; fotofiksācija. Pierādījumi: shēmas, foto, būvprojekta sadaļas
10.3.2.	datu pārraides kabeļi ir novietoti paaugstinātā grīdā vai speciālās aizsargkonstrukcijās, nodrošinot to mehānisko aizsardzību	Vietas apskate; tehniskās pases un kanālu/tekņu specifikācijas. Pierādījumi: foto, specifikācijas
10.3.3.	uzstādītas elektrostatiskās izlādes aizsardzības sistēmas	Pārbaudīt ESD risinājumus (zemējums, materiāli, kontroles). Pierādījumi: zemējuma mērījumi, ESD dokumentācija
10.3.4.	Datu pārraides kabeļi ir marķēti atbilstoši dokumentācijai, nodrošinot to nepārprotamu identificēšanu un atbilstību tīkla topoloģijas shēmai	Vietas apskate (paraugi vairākās zonās); salīdzināt marķējumu ar topoloģijas shēmām/CMDB ierakstiem. Pierādījumi: foto, shēmas, CMDB izraksti
10.4.	Ārējo tīklu savienojumi atbilst šādām prasībām:	
10.4.1.	saziņai ar operatoru tīkliem un publisko internetu nodrošināti vismaz divi neatkarīgi datu pārraides kanāli, izmantojot neatkarīgus optiskās šķiedras ievadus ēku kompleksā	Pārbaudīt līgumus/paketes ar diviem neatkarīgiem pakalpojumu sniedzējiem; vietas apskate šķiedru ievadiem/trasēm. Pierādījumi: līgumi, trases shēmas, foto
10.4.2.	tīkla pieslēgumi nodrošina automātisku pārslēgšanos uz alternatīvo maršrutu primārā savienojuma atteices gadījumā (piem., BGP vai cits	Pārbaudīt maršrutēšanas/pārslēgšanās iestatījumus un testu protokolus; kontrolēts pārslēgšanās tests, ja iespējams. Pierādījumi:

	piemērots risinājums)	BGP/OSPF konfigurācijas, testu ieraksti, žurnāli

III. Fiziskās drošības prasības

11. Videonovērošana

Nr. p. k.	Prasība	Pārbaude
11.1.	Datu centrā ir uzstādīta videonovērošanas sistēma, kas nodrošina reāllaika uzraudzību un ierakstīšanu kritiskajās zonās (tai skaitā telpās ar piekļuves kontroli un tehniskajās telpās)	Pārbaudīt zonējuma shēmu un kameru izvietojumu; veikt izlases kārtā videoierakstu atskaņošanu kritiskajās zonās; salīdzināt ar zonu sarakstu. Pierādījumi: zonējuma/kameru plāns, paraugu ieraksti ar laika zīmogiem, piekļuves tiesību saraksts VNS
11.2.	Videonovērošanas sistēma un ar to saistītie risinājumi atbilst normatīvajiem aktiem par minimālajām kiberdrošības prasībām, nodrošinot šifrēšanu, lietotāju darbību auditāciju, drošu glabāšanu un datu aizsardzību	Pārbaudīt konfigurācijas (šifrēšanu pārvadē/ glabāšanā), lietotāju piekļuvi un audita žurnālus, glabāšanas termiņus un vietu. Pierādījumi: iestatījumu izdrukas, audita žurnāli, saglabāšanas politika, arhīva pieejamības pārbaude

12. Risinājumi šķidrumu radīto bojājumu riska mazināšanai

Nr. p. k.	Prasība	Pārbaude
12.1.	Datu centrs ir aprīkots ar šķidruma noplūdes noteikšanas sensoriem zonās ar paaugstinātu šķidruma noplūdes risku:	Pārbaudīt sensoru izvietojuma plānu un faktiskās uzstādīšanas vietas. Pierādījumi: plāns, foto, iekārtu saraksti
12.1.1.	sensori dzesēšanas sistēmas komponentēs (piem., caurules, kondensāta izplūdes punkti)	Vietas apskate; salīdzināt ar plānu. Pierādījumi: foto, plāna atzīmes
12.1.2.	sensori mitrināšanas iekārtās un ūdens padeves sistēmās	Vietas apskate; uzturēšanas ieraksti. Pierādījumi: foto, protokoli
12.1.3.	sensori telpās ar augstu šķidruma ieplūdes risku	Vietas apskate; riska novērtējums. Pierādījumi: foto, riska kartes
12.2.	Noplūdes noteikšanas sistēmas nodrošina nepārtrauktu uzraudzību un automātiskus brīdinājumus; identificētie noplūdes gadījumi ir reģistrēti	Pārbaudīt monitoringa iestatījumus, trauksmju kanālus un žurnālus; paraugu gadījumu pārskats. Pierādījumi: trauksmju žurnāli, iestatījumu ekrānuzņēmumi, incidentu ieraksti
12.3.	Sensoru un sistēmu darbspēja tiek regulāri pārbaudīta saskaņā ar ražotāja noteiktajiem termiņiem; pārbaudes fakts un rezultāti ir dokumentēti	Pārskatīt testu grafikus un protokolus; pārbaudīt pēdējo pārbaužu datumus. Pierādījumi: grafiki, protokoli, labošanas darbi
12.4.	Datu centrs ir projektēts un uzturēts, lai nodrošinātu aizsardzību pret ārējās vides šķidruma riskiem (piem., plūdiem)	Pārskatīt būvniecības/teritorijas dokumentus, plūdu riska kartes, drenāžas risinājumus. Pierādījumi: projektēšanas dokumenti, kartes, uzturēšanas apraksti

13. Ģeogrāfiskais izvietojums

Nr. p. k.	Prasība	Pārbaude
13.1.	Datu centra atrašanās vietai ir veikts riska novērtējums:	Pārskatīt riska novērtējuma dokumentu un tā apstiprinājumu. Pierādījumi: riska novērtējums, apstiprinājums
13.1.1.	novērtēti dabas riski (plūdu iespējamība, citi dabas katastrofu draudi, ņemot vērā vēsturisko informāciju)	Pārbaudīt izmantotās kartes/datus, vēsturiskos ierakstus. Pierādījumi: plūdu/riska kartes, datu avoti
13.1.2.	novērtēti cilvēku radīti riski (publisku vietu tuvums, satiksmes intensitāte, rūpniecisko avāriju riski, bīstamu objektu tuvums)	Pārbaudīt attālumu/apkaimes analīzi un pieņēmumus. Pierādījumi: karšu izdrukas, aprēķini, foto
13.1.3.	novērtēti infrastruktūras pieejamības riski (elektroapgāde, telekomunikācijas, ūdensapgāde)	Pārskatīt pieslēgumu shēmas, pakalpojumu sniedzēju līgumus, rezerves risinājumus. Pierādījumi: līgumi, shēmas
13.2.	Riska novērtējums tiek veikts ne retāk kā reizi trijos gados vai būtisku izmaiņu gadījumā	Pārbaudīt pēdējo novērtējumu datumus un uzsākšanas kritērijus pēc izmaiņām. Pierādījumi: plāns/grafiks, atjaunošanas ieraksti

14. Apsardze

Nr. p. k.	Prasība	Pārbaude
14.1.	Apsardze tiek nodrošināta atbilstoši Apsardzes darbības likumam un citiem normatīvajiem aktiem, sadarbojoties ar sertificētiem pakalpojumu sniedzējiem vai valsts iestādēm	Pārbaudīt līgumus/sertifikātus, apsardzes licences, sadarbības kārtību ar iestādēm. Pierādījumi: līgumi, licences, kontaktpersonu saraksts
14.2.	Apsardzes organizācija nodrošina:	
14.2.1.	darbinieku kvalifikāciju un sertifikāciju atbilstoši normatīvajiem aktiem	Pārbaudīt personāla sertifikātus, apmācību reģistru
14.2.2.	darbinieku apmācību ne retāk kā reizi sešos mēnešos, ja apsardzi nodrošina datu centra operatora personāls; apmācības aptver darbu ar drošības un piekļuves sistēmām un incidentu pārvaldību	Pārbaudīt apmācību grafikus, programmas un apmeklējumu; pēctreniņa ziņojumus
14.2.3.	tehnoloģisko risinājumu (tai skaitā piekļuves kontroles) uzturēšanu un integrāciju ar drošības pārvaldības sistēmu, kā arī piekļuvi šiem risinājumiem apsardzes personālam	Pārbaudīt integrācijas aprakstus, piekļuves tiesības, darbspējas pierakstus
14.3.	Apsardzes nodrošināšana atbilst šādām prasībām:	
14.3.1.	objektā apsardzes personāls nodrošina 24/7 fizisku klātbūtni vai izmanto attālinātas uzraudzības risinājumus	Pārbaudīt dežūru grafikus, līgumus, attālinātas uzraudzības pierādījumus

14.3.2.	reaģēšanas laiks pēc incidenta vai trauksmes signāla nepārsniedz 15 minūtes. Ja apsardzes pakalpojums ir ārpakalpojums, reaģēšanas laiku nosaka līgumā	Pārskatīt incidentu žurnālus ar laika zīmogiem; salīdzināt ar līguma nosacījumiem
14.4.	Apsardzes darbība tiek dokumentēta, tai skaitā dežūru grafiki, incidentu pieteikumi un reaģēšanas laiks	Pārbaudīt dokumentus un paraugu ierakstus; salīdzināt ar notikumu žurnāliem

15. Ugunsdrošības sistēmas, to pārbaude un uzraudzība

Nr. p. k.	Prasība	Pārbaude
15.1.	Datu centrā ir uzstādītas ugunsdrošības sistēmas, kas ietver:	Vietas apskate; sistēmu dokumentācijas pārbaude
15.1.1.	ugunsgrēka atklāšanas detektorus (piem., dūmu vai karstuma detektorus), kas laikus identificē ugunsgrēka riskus	Pārbaudīt detektoru tipus, izvietojumu, jutības iestatījumus un testu protokolus
15.1.2.	automātiskās ugunsdzēšanas sistēmas, kas piemērotas datu centra telpām	Pārbaudīt dzēšanas aģentu atbilstību telpu tipiem, aktivizācijas nosacījumus, slēgventiļu/zonu shēmas
15.1.3.	manuālās ugunsdzēšanas ierīces, kas izvēlētas atbilstoši aizsargājamajām telpām (piem., serveru un elektrosadales telpas ar CO_2 aparātiem)	Pārbaudīt ierīču tipu, marķējumu, derīguma termiņus, pieejamību vietās
15.2.	Ugunsdrošības sistēmas tiek pārbaudītas atbilstoši ražotāja dokumentācijai un normatīvajiem aktiem, ievērojot biežāko piemērojamo pārbaudes intervālu; pārbaudes ietver detektoru, dzēšanas sistēmu un manuālo ierīču testēšanu; rezultāti tiek dokumentēti un glabāti vismaz trīs gadus	Pārskatīt testu grafikus/protokolus; pārliecināties par testu veikšanu noteiktajos termiņos un rezultātu glabāšanu. Pierādījumi: grafiki, protokoli, arhīva ieraksti
15.3.	Ugunsdrošības sistēmas tiek nepārtraukti uzraudzītas, izmantojot:	Pārbaudīt uzraudzības un trauksmju nosūtīšanas mehānismus
15.3.1.	reāllaika uzraudzības sistēmas, kas nosūta trauksmes signālus par dūmu, paaugstinātas temperatūras vai ugunsgrēka pazīmēm ugunsdrošības risinājumu vai drošības pārvaldības sistēmai un atbildīgajām personām	Pārbaudīt trauksmju konfigurāciju, adresātu sarakstus, pēdējo trauksmju žurnālus
15.3.2.	alternatīvus risinājumus (piem., skaņas signalizāciju vai GSM trauksmes ziņošanu), kas nodrošina sistēmu darbību elektroapgādes traucējumu vai citu bojājumu gadījumā	Pārbaudīt rezerves barošanas avotu darbību, GSM/alternatīvo sakaru kanālu darbību; testa protokolus

IV. Pieejamības prasības

16. Datu centra pieejamība

Nr. p. k.	Prasība	Pārbaude

16.1.	Datu centrs nodrošina vismaz 99,982 % pieejamību kalendāra gadā, kas atbilst maksimāli pieļaujamam pārtraukuma laikam – aptuveni 7,8 minūtes 30 dienu periodā (precīza vērtība atkarīga no perioda ilguma) (sk. 16.2. apakšpunktu)	Pārskatīt pieejamības pārskatus par pilnu kalendāra gadu; pārliecināties, vai aprēķins veikts saskaņā ar šī pielikuma 16.2. apakšpunktā minēto formulu un dati iegūti no uzticama uzraudzības avota. Pierādījumi: pārskati, izejas dati, aprēķinu izklājlapas
16.2.	Pieejamība tiek aprēķināta, izmantojot šādu formulu (*Total Time* − *Downtime*) / *Total Time* × 100, kur:	Pārbaudīt aprēķina formulu un ievaddatus; pārliecināties, vai definīcijas, kas minētas šī pielikuma 16.2.1. un 16.2.2. apakšpunktā, ir piemērotas. Pierādījumi: metodika, aprēķinu paraugi
16.2.1.	*Total Time* – kopējais novērtējamais laiks minūtēs attiecīgajā kalendāra gadā (365 vai 366 dienas)	Pārbaudīt, vai izmantots faktiskā gada minūšu skaits (365/366). Pierādījumi: aprēķina ievaddati
16.2.2.	*Downtime* – kopējais datu centra nepieejamības laiks kalendāra gadā, izteikts minūtēs, ietverot plānotus un neparedzētus pārtraukumus, izņemot tādus plānotos uzturēšanas darbus, kuru laikā klientiem tiek nodrošināti rezerves risinājumi (sk. 17. punktu)	Pārbaudīt incidentu un plānoto darbu žurnālus; salīdzināt no pieejamības izslēgtos (neieskaitītos) gadījumus ar šī pielikuma 17. punktā minētajiem nosacījumiem. Pierādījumi: plānoto darbu paziņojumi, rezerves risinājumu apraksti, incidentu žurnāli

17. Tehniskā apkope un plānotie uzturēšanas darbi

Nr. p. k.	**Prasība**	**Pārbaude**
17.1.	Apkopes un remontdarbi tiek veikti, izmantojot rezerves sistēmas un komponentes, lai nepieļautu darbības pārtraukumus	Pārskatīt apkopes procedūras un pēdējo darbu protokolus; pārbaudīt, vai apkopes darbi veikti, izmantojot rezerves ceļu/sistēmu. Pierādījumi: procedūras, pārslēgšanās protokoli, monitoringa izdrukas apkopes laikā
17.2.	Plānotie uzturēšanas darbi tiek veikti pēc iepriekš apstiprinātiem grafikiem, saskaņojot laikus un rezerves risinājumus ar ietekmēto iekārtu īpašniekiem/klientiem	Pārbaudīt grafikus, saskaņojumus un apstiprinājumus; salīdzināt ar faktisko izpildi. Pierādījumi: grafiki, e-pasta paziņojumi/ apstiprinājumi, darba akti
17.3.	Par darbiem, kas var ietekmēt klientu iekārtas, klienti tiek informēti rakstveidā ne vēlāk kā piecas darbdienas pirms darbu uzsākšanas	Pārbaudīt paziņojumu paraugus, nosūtīšanas datumus un adresātu sarakstus. Pierādījumi: paziņojumu izdrukas, sistēmas žurnāli
17.4.	Plānoto darbu dokumentācijā norāda:	Pārbaudīt, vai norādītie elementi ir visos ierakstos
17.4.1.	darba sākuma un beigu laiku	Pārskatīt ierakstus
17.4.2.	darbu veidu un ietekmētās iekārtas	Pārskatīt ierakstus
17.4.3.	risinājumus darbības atjaunošanai incidentu gadījumā (sk. 19. punktu)	Pārskatīt rezerves/atgriešanās plānus; salīdzināt ar īstenoto praksē

18. Incidenti un neparedzēti pārtraukumi

Nr. p. k.	**Prasība**	**Pārbaude**

18.1.	Incidenta novēršana tiek uzsākta ne vēlāk kā 15 minūšu laikā pēc incidenta konstatēšanas	Pārbaudīt incidentu ierakstu laika zīmogus no incidenta konstatēšanas līdz reaģēšanas uzsākšanai un salīdzināt ar 15 min. prasību. Pierādījumi: incidentu žurnāli, dežūrkomandas pieraksti
18.2.	Incidenta ierakstā iekļauj incidenta konstatēšanas laiku, aprakstu, reaģēšanas laiku, novēršanas laiku, veiktās darbības, incidenta cēloni un ietekmētos infrastruktūras elementus (tai skaitā klientu iekārtas) (sk. arī 4. punktu)	Pārskatīt paraugus no pēdējiem 6–12 mēn.; pārliecināties, vai visi lauki ir aizpildīti. Pierādījumi: reģistra izdrukas, CAPA ieraksti
18.3.	Ja incidents ietekmē pieejamību, ietekmes ilgums ir norādīts un ieskaitīts šī pielikuma 16.2.2. apakšpunktā minētajā *Downtime* aprēķinā	Pārbaudīt incidentus, kas radījuši dīkstāvi; salīdzināt ar pieejamības aprēķinu. Pierādījumi: incidentu un pieejamības pārskati

19. Datu centra pārvaldības informācijas sistēmu darbības atjaunošanas plāns

Nr. p. k.	Prasība	Pārbaude
19.1.	Ir izstrādāts un uzturēts informācijas sistēmu darbības atjaunošanas plāns, kura efektivitāte un saskaņotība ar darbības nepārtrauktības plānu (BCP) tiek pārbaudīta vismaz reizi sešos mēnešos	Pārbaudīt plānu, testu grafiku un pēctestu ziņojumus; sasaisti ar BCP (sk. 3. punktu). Pierādījumi: plāns, protokoli, konstatējumi
19.2.	RTO (atjaunošanas laika mērķis) ≤ 1 stunda	Pārbaudīt testa protokolus un laika mērījumus; salīdzināt ar mērķi
19.3.	RPO (atjaunošanas punkta mērķis) ≤ 15 minūtes vai atbilst stingrākām prasībām, ja tas noteikts normatīvajos aktos attiecīgās sistēmas drošības klasei	Pārbaudīt dublēšanas/žurnālu iestatījumus un testa rezultātus; salīdzināt ar mērķi un normatīviem
19.4.	MTO (maksimālais pieļaujamais pārtraukuma laiks) izriet no šī pielikuma 16.1. apakšpunktā noteiktā pieejamības līmeņa un nedrīkst to pārsniegt (sk. 16. punktu)	Pārskatīt MTO noteikšanas metodiku un dokumentēto vērtību; salīdzināt ar šī pielikuma 16.1. apakšpunktā noteikto prasību un faktiskajiem testiem

V. Informācijas un komunikācijas tehnoloģiju pakalpojumu prasības
20. SLA līgumi

Nr. p. k.	Prasība	Pārbaude
20.1.	Datu centra operators ar klientu noslēdz informācijas un komunikācijas tehnoloģiju pakalpojumu līgumu (SLA), kurā ietver prasības par pieejamību, reaģēšanas laiku, incidentu novēršanas laiku, uzraudzību, incidentu informācijas apmaiņu un ziņošanas kārtību. Ja starp datu centra operatoru un klientu netiek noslēgts līgums, minētās prasības un pušu pienākumu sadalījumu nosaka starpiestāžu vienošanās dokumentā vai citā pusēm saistošā dokumentā	Pārskatīt SLA tekstus: rādītāji, mērījuma metode, aprēķina periods, ziņošanas kārtība. Pierādījumi: SLA līgumi/pielikumi, pārskatu paraugi

20.2.	SLA noteiktās prasības ir saskaņotas ar šī pielikuma 18. punktā noteiktajām reaģēšanas prasībām un 19. punktā noteiktajiem RTO/RPO/MTO	Salīdzināt SLA noteiktos reaģēšanas laikus ar šī pielikuma 18.1. un 18.2. apakšpunktu; atjaunošanas mērķus ar šī pielikuma 19.2., 19.3. un 19.4. apakšpunktu. Pierādījumi: SLA izraksti, iekšējās procedūras, testu protokoli
20.3.	SLA noteiktās pieejamības prasības nav zemākas par šī pielikuma 16.1. apakšpunktā noteikto pieejamības līmeni	Pārbaudīt SLA noteikto pieejamības mērķi un formulu atbilstoši šī pielikuma 16.1. un 16.2. apakšpunktam. Pierādījumi: SLA pielikumi, aprēķina metodika

21. Pārvaldības un uzraudzības rīki

Nr. p. k.	Prasība	Pārbaude
21.1.	Datu centrs nodrošina automatizētus pārvaldības un uzraudzības rīkus infrastruktūras stāvokļa un drošības notikumu reāllaika uzraudzībai atbilstoši šī pielikuma 16. punktā noteiktajām pieejamības prasībām	Pārbaudīt monitoringa sistēmu, uzraudzības parametrus un trauksmju iestatījumus. Pierādījumi: iestatījumu izdrukas, trauksmju saraksti, ekrānuzņēmumi
21.2.	Rīki nodrošina pieejamību ietekmējošo notikumu un mērījumu uzskaiti, analīzi un iespēju pierādīt atbilstību noteiktajam pieejamības līmenim (sk. 16. punktu un 18.3. apakšpunktu)	Pārskatīt notikumu/mērījumu pārskatus un pieejamības aprēķinu izsekojamību. Pierādījumi: žurnāli, pārskati, aprēķinu datnes
21.3.	Uzraudzības rīku dati tiek glabāti vismaz 12 mēnešus un ir pieejami auditam un līgumsaistībām	Pārbaudīt uzraudzības rīku datu saglabāšanas politiku un sistēmu iestatījumus; parauga ieraksts ≥ 12 mēn. Pierādījumi: uzraudzības rīku datu saglabāšanas politika, ekrānuzņēmumi, žurnāli

22. Klientiem sniegto pakalpojumu incidentu žurnāls

Nr. p. k.	Prasība	Pārbaude
22.1.	Datu centra operators nodrošina klientiem pieeju incidentu žurnāla ierakstiem par klientiem sniegtajiem pakalpojumiem	Pārbaudīt piekļuves kārtību (portāls/pārskati), saturu un pieejamības termiņus; pārliecināties par datu aizsardzību. Pierādījumi: piekļuves instrukcija, pārskatu paraugi, tiesību apraksts

23. Datu nesēju pārvaldība

Nr. p. k.	Prasība	Pārbaude
23.1.	Datu centra operators nodrošina datu nesēju uzskaiti un pārraudzību visā to dzīves ciklā (iegāde, lietošana, transportēšana, atkārtota izmantošana, glabāšana, iznīcināšana)	Pārbaudīt uzskaites/CMDB ierakstus un procedūras; izlases pārbaude uz vietas
23.2.	Datu nesēju iznīcināšana tiek dokumentēta, norādot metodi un laiku	Pārskatīt datu nesēju iznīcināšanas protokolus/sertifikātus; salīdzināt ar uzskaiti

23.3.	Bojāti vai neizmantojami datu nesēji tiek iznīcināti 30 dienu laikā pēc to darbības pārtraukšanas, izmantojot drošu iznīcināšanas metodi, kas atbilst apstrādātās informācijas klasifikācijas līmenim un starptautiskajiem standartiem (piem., NIST 800-88)	Pārbaudīt datu nesēju iznīcināšanas termiņus un metodes; piegādātāja kompetenci apliecinošus dokumentus, ja tiek sniegti ārpakalpojumi

Piezīme. Šo pielikumu izmanto, veicot datu centra atbilstības auditu Ministru kabineta 2026. gada 29. septembra noteikumu Nr. 602 "Informācijas sistēmu izvietošanas un datu centru drošības prasības" (turpmāk – noteikumi) 21.1. apakšpunktā minētā auditora atzinuma sagatavošanai. Auditors pārbauda šajā pielikumā norādīto pārbaudes pozīciju izpildi, novērtē datu centra atbilstību šo noteikumu prasībām un secinājumus ietver auditora atzinumā.

Saīsinājumu skaidrojumi

ACS (*Access Control System*) – piekļuves kontroles sistēma

APT (*Advanced Persistent Threat*) – ilgstošs mērķēts kiberuzbrukums

ATS (*Automatic Transfer Switch*) – automātiskās pārslēgšanas slēdzis (tīkla pārslēgšana/elektropārslēgšana)

BCP (*Business Continuity Plan*) – darbības nepārtrauktības plāns

BGP (*Border Gateway Protocol*) – robežvārteju maršrutēšanas protokols

CAB (*Change Advisory Board*) – izmaiņu izvērtēšanas padome

CAPA (*Corrective and Preventive Actions*) – koriģējošie un preventīvie pasākumi

CCTV/VNS (*Closed-Circuit Television*) – videonovērošanas sistēma

CMDB (*Configuration Management Database*) – konfigurāciju pārvaldības datubāze

CO_2 – ogļskābā gāze (ugunsdzēsības iekārtās)

DC – datu centrs

DRP (*Disaster Recovery Plan*) – darbības atjaunošanas plāns

ELK (*Elasticsearch*, *Logstash*, *Kibana*) – žurnālu/telemetrijas platforma

ESD (*Electrostatic Discharge*) – elektrostatiskā izlāde

GSM (*Global System for Mobile Communications*) – globālā mobilo sakaru sistēma

IS – informācijas sistēma

MTO (*Maximum Tolerable Outage*) – maksimālais pieļaujamais pārtraukuma laiks

NIST SP 800-88 (*Guidelines for Media Sanitization*) – NIST vadlīnijas datu nesēju drošai iznīcināšanai

NTP (*Network Time Protocol*) – tīkla laika protokols

OSPF (*Open Shortest Path First*) – maršrutēšanas protokols

PIN (*Personal Identification Number*) – personas identifikācijas numurs

RFID (*Radio-Frequency Identification*) – radiofrekvenču identifikācija

RPO (*Recovery Point Objective*) – atjaunošanas punkta mērķis

RTO (*Recovery Time Objective*) – atjaunošanas laika mērķis

SIEM (*Security Information and Event Management*) – drošības informācijas un notikumu pārvaldība

SLA (*Service Level Agreement*) – pakalpojuma līmeņa līgums

STS (*Static Transfer Switch*) – statiskās pārslēgšanas slēdzis (elektrobarošanā)

UPS (*Uninterruptible Power Supply*) – nepārtrauktās barošanas sistēma

UTC (*Coordinated Universal Time*) – koordinētais pasaules laiks

WORM (*Write Once, Read Many*) – vienreiz rakstāma, daudzkārt lasāma glabāšana (nemaināma glabāšana)

Apzīmējumi rezerves līmenim (papildu skaidrojumi)

N+1 – pie N darba komponentēm ir viena rezerves komponente

2N – pilns dublējums (divas neatkarīgas komponenšu kopas)

2N+1 – pilns dublējums ar papildu rezerves komponenti

2. pielikums
Ministru kabineta
2026. gada 29. septembra
noteikumiem Nr. 602

Auditora atzinums par datu centra atbilstību prasībām

I. Vispārīgā informācija			
Datu centra nosaukums		Datu centra operatora nosaukums	
Datu centra adrese		Datu centra operatora reģistrācijas Nr.	
Audita veikšanas datums			
Audita veicēja (kvalificētā auditora) kontaktinformācija			

II. Atbilstības novērtējuma kopsavilkums						
	Organizatoriskās prasības	Tehniskās prasības	Fiziskās drošības prasības	Pieejamības prasības	IKT pakalpojumu prasības	Piezīmes
Prasības izpildītas	▢	▢	▢	▢	▢	
Nepieciešami uzlabojumi	▢	▢	▢	▢	▢	

▢ Atzīmē, ja prasības ir izpildītas vai ja nepieciešami uzlabojumi

III. Atbilstības novērtējumam pievienotie dokumenti		
Nr. p. k.	Dokumenta nosaukums	Īss kopsavilkums

IV. Secinājumi		
Kopējais novērtējums	▢ Atbilst / ▢ Neatbilst	▢ Nepieciešami uzlabojumi
Papildu ieteikumi (ieteikumi pirms nākamā audita)		

V. Audita veicēja paraksts	
Auditors (Vārds, Uzvārds)	
Paraksts*	
Datums*	

Piezīme. * Dokumenta rekvizītus "Paraksts" un "Datums" neaizpilda, ja elektroniskais dokuments ir sagatavots atbilstoši normatīvajiem aktiem par elektronisko dokumentu noformēšanu.

3. pielikums
Ministru kabineta
2026. gada 29. septembra
noteikumiem Nr. 602

Starptautiskās sertifikācijas modeļi

1. Datu centra atbilstību šo noteikumu prasībām var apliecināt ar sertifikātu vai citu dokumentu, kas apliecina atbilstību kādam no šajā pielikumā norādītajiem starptautiskās sertifikācijas modeļiem, ja ir izpildīti visi šajā pielikumā attiecīgajam sertifikācijas modelim noteiktie nosacījumi.

2. *Uptime Institute* sertifikāts:
2.1. Tier III vai Tier IV līmeņa sertifikācija ekspluatācijā esošam datu centram ("Uzcelts" (*Build*), "Objekts" (*Facility*), "Būvniecība" (*Construction*));
2.2. projektēšanas līmeņa (*Design*) sertifikācija netiek atzīta;
2.3. papildus iesniedzams datu centra auditora atzinums par datu centra atbilstību šo noteikumu 1. pielikuma I sadaļā "Organizatoriskās prasības", II sadaļā "Tehniskās prasības" un III sadaļā "Fiziskās drošības prasības" norādītajām pārbaudes pozīcijām. Atzinums ir derīgs divus gadus.

3. TIA-942 sertifikāts:
3.1. *Rated-3* vai *Rated-4* sertifikācijas līmenis ar datu centra fiziskās infrastruktūras pārbaudi uz vietas.

4. EN 50600 sertifikāts:
4.1. sertifikācija aptver pilnu infrastruktūras atbilstības pārbaudi;
4.2. sertifikācija aptver minimālās prasības, sākot no EN 50600-2-1 līdz EN 50600-2-5 un nodrošinot vismaz 3. pieejamības klasi (*Availability Class 3*) un 2. aizsardzības klasi (*Protection Class 2*) attiecīgajās jomās:

4.2.1. EN 50600-2-1 – standartā noteiktās minimālās prasības (*Requirements*);
4.2.2. EN 50600-2-2 – vismaz 3. pieejamības klase (*Availability Class 3*);
4.2.3. EN 50600-2-3 – vismaz 3. pieejamības klase (*Availability Class 3*);
4.2.4. EN 50600-2-4 – vismaz 3. pieejamības klase (*Availability Class 3*);
4.2.5. EN 50600-2-5 vismaz šādas prasības:
4.2.5.1. aizsardzība pret neatļautu piekļuvi – vismaz četras drošības zonas;
4.2.5.2. aizsardzība pret iekļūšanu datu centra telpās – vismaz 2. aizsardzības klase (*Protection Class 2*);
4.2.5.3. aizsardzība pret iekšējiem ugunsgrēkiem – vismaz 2. aizsardzības klase (*Protection Class 2*);
4.2.5.4. aizsardzība pret iekšējās vides apdraudējumiem – vismaz 2. aizsardzības klase (*Protection Class 2*);
4.2.5.5. aizsardzība pret ārējās vides apdraudējumiem – vismaz 2. aizsardzības klase (*Protection Class 2*).

5. ISO/IEC TS 22237 sertifikāts:
5.1. ieviešanas (*Implementation*) vai sertifikācijas (*Certification*) līmenis;
5.2. koncepcijas (*Concept*) un projektēšanas (*Design*) līmeņa sertifikācija netiek atzīta;
5.3. minimālās prasības, sākot no ISO/IEC 22237-2 līdz ISO/IEC 22237-6 un nodrošinot vismaz 3. pieejamības klasi (*Availability Class 3*) un 2. aizsardzības klasi (*Protection Class 2*) attiecīgajās jomās, un drošības zonējuma ievērošana:

5.3.1. ISO/IEC 22237-2 – nodrošina standartā noteiktās minimālās prasības (*Requirements*);
5.3.2. ISO/IEC 22237-3 – vismaz 3. pieejamības klase (*Availability Class 3*) un 2. detalizācijas līmenis (*Granularity Level 2*);
5.3.3. ISO/IEC 22237-4 – vismaz 3. pieejamības klase (Availability Class 3) un 2. detalizācijas līmenis (*Granularity Level 2*);
5.3.4. ISO/IEC TS 22237-5 – vismaz 3. pieejamības klase (*Availability Class 3*);
5.3.5. ISO/IEC 22237-6 – nodrošina teritorijas un telpu drošības zonējuma principu, piemērojot atbilstošu aizsardzības klasi katrai drošības zonai (*Protection Class*).

6. Citi starptautiski atzīti sertifikāti:

6.1. sertifikāti, kurus Nacionālais kiberdrošības centrs savā oficiālajā tīmekļvietnē atzinis par atbilstošiem.

© Oficiālais izdevējs "Latvijas Vēstnesis"