Aizsardzības ministrija

Kiberdrošības normatīvais regulējums

Progress un aktualitātes

Edgars Kiukucāns
Nacionālā kiberdrošības centra ģenerāldirektora vietnieks

Aizsardzības ministrija

NIS2 direktīva

Direktīvas mērķis

nodrošināt vienādi augstu kiberdrošības līmeni visā Eiropas Savienībā

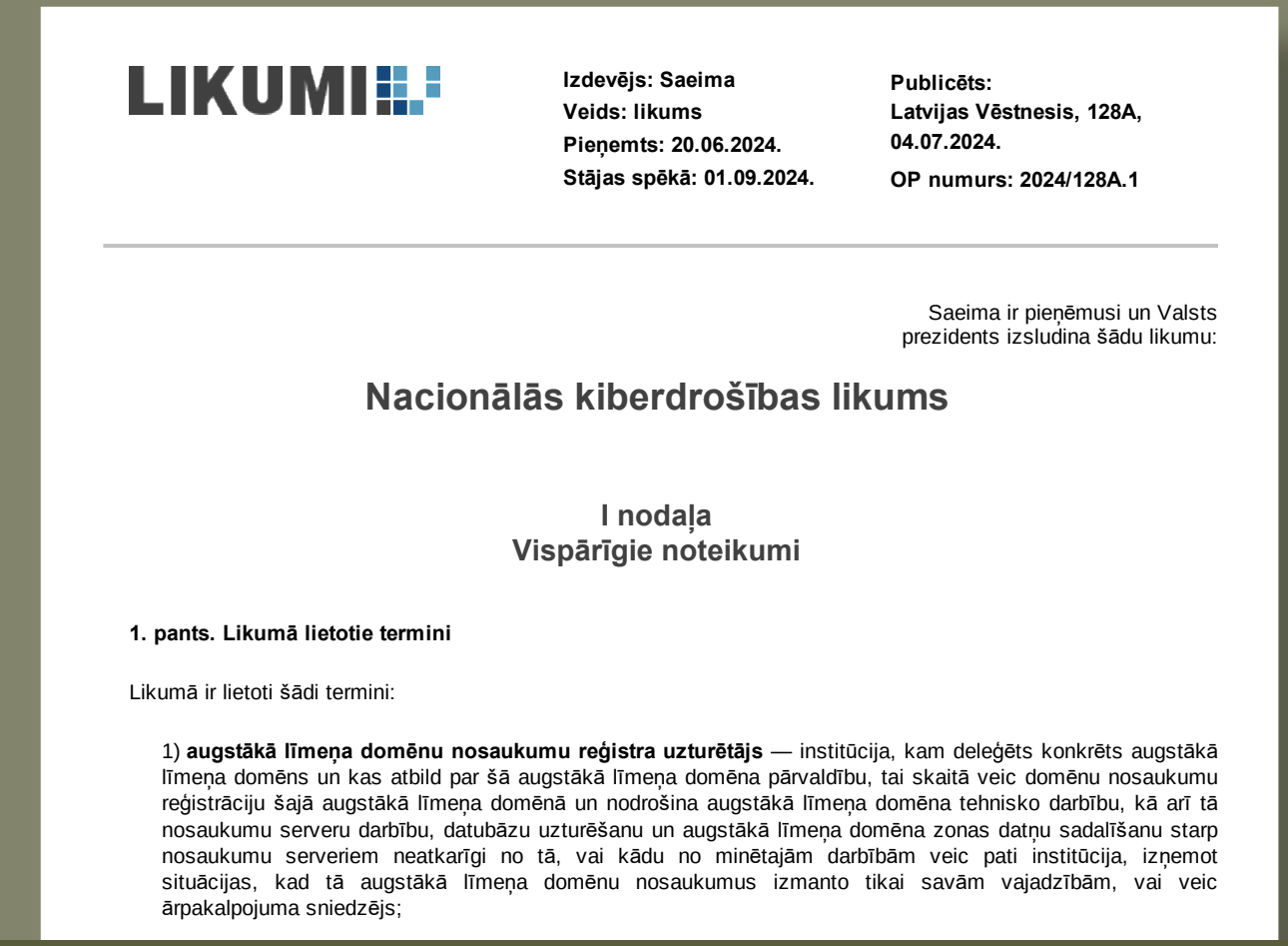
Atbilstības un ziņošanas pienākumi

Saskaņota kiberrisku pārvaldība

Direktīvas subjektu uzraudzība

Aizsardzības ministrija

Nacionālās kiberdrošības likums



LIKUMI

Izdevējs: Saeima
Veids: likums
Pieņemts: 20.06.2024.
Stājas spēkā: 01.09.2024.

Publicēts:
Latvijas Vēstnesis, 128A, 04.07.2024.
OP numurs: 2024/128A.1

Saeima ir pieņēmusi un Valsts prezidents izsludina šādu likumu:

Nacionālās kiberdrošības likums

I nodaļa
Vispārīgie noteikumi

1. pants. Likumā lietotie termini

Likumā ir lietoti šādi termini:

1) **augstākā līmeņa domēnu nosaukumu reģistra uzturētājs** — institūcija, kam deleģēts konkrēts augstākā līmeņa domēns un kas atbild par šā augstākā līmeņa domēna pārvaldību, tai skaitā veic domēnu nosaukumu reģistrāciju šajā augstākā līmeņa domēnā un nodrošina augstākā līmeņa domēna tehnisko darbību, kā arī tā nosaukumu serveru darbību, datubāzu uzturēšanu un augstākā līmeņa domēna zonas datņu sadalīšanu starp nosaukumu serveriem neatkarīgi no tā, vai kādu no minētajām darbībām veic pati institūcija, izņemot situācijas, kad tā augstākā līmeņa domēnu nosaukumus izmanto tikai savām vajadzībām, vai veic ārpakalpojuma sniedzējs;

Pieņemts

20.06.2024.

Stājies spēkā

01.09.2024.

Aizsardzības ministrija

NKDL pakārtotie MK noteikumi

Minimālās kiberdrošības prasības	Saskaņošanā
Informācijas sistēmu izvietošanas un datu centru drošības prasības	Saskaņošanā
Noteikumi par centralizētu aizsardzību pret pakalpojumatteices kiberuzbrukumiem	Stājās spēkā
Vienotā valsts interneta plūsmu apmaiņas punkta darbības noteikumi	Stājās spēkā
Augstākā līmeņa domēna ".lv" reģistra un elektroniskās numurēšanas sistēmas uzturētājam izvirzāmās prasības un tā atzīšanas kārtība, un prasības domēnu vārdu reģistrācijas datubāzei	Stājās spēkā
Agrās brīdināšanas sensoru obligātas uzstādīšanas noteikumi	Izstrādē
Kiberincidentu attiecināšanas kritēriji un kārtība (IP)	Saskaņošanā
Noteikumi par kārtību, kādā nosakāms finanšu gada neto apgrozījums, no kura aprēķina soda naudu, un soda naudas apmēra noteikšanas kritēriji	Iesniegts MK

Aizsardzības ministrija

NKDL subjekta kalendārs 2025

1.aprīlis *Reģistrācija*

- Iekļaušana BPS/SPS sarakstā
- NKDC sarakstu apstiprina DDUK un iesniedz EK
- Informācija par uzraugošo iestādi

1.oktobris *Kiberdrošības pārvaldnieka noteikšana*

- Kritiskā infrastruktūra – saskaņo ar VDI
- Atbilstība MK noteikumu prasībām

1.oktobris *Pašvērtējuma anketas iesniegšana*

- Dokumentācijas sagatavošana (risku izvērtējums, darbības nepārtrauktības plāns
- Veidlapas aizpilde

Aizsardzības ministrija

NKDL subjekti

20. pants

Būtisko pakalpojumu sniedzēji

+

21. pants

Svarīgo pakalpojumu sniedzēji

+

24. pants

Kritiskā IKT infrastruktūra

saskaņā ar Nacionālās drošības likumu

valsts un pašvaldību iestādes + lielie un vidējie uzņēmumi***

Aizsardzības ministrija

NKDL subjekti

20. pants

Būtisko pakalpojumu sniedzēji

Liels saimnieciskās darbības veicējs

- Nodarbina vismaz 250 nodarbinātos
- Neto apgrozījums pārsniedz 50 milj. euro
- Gada bilances kopsumma pārsniedz 43 milj. euro

+

21. pants

Svarīgo pakalpojumu sniedzēji

Vidējs saimnieciskās darbības veicējs

- Nodarbina līdz 249 nodarbināto
- Neto apgrozījums pārsniedz 10 milj. euro (nesasniedz 50 milj. euro)
- Gada bilances kopsumma pārsniedz 10 milj. euro (nesasniedz 43 milj. euro)

+

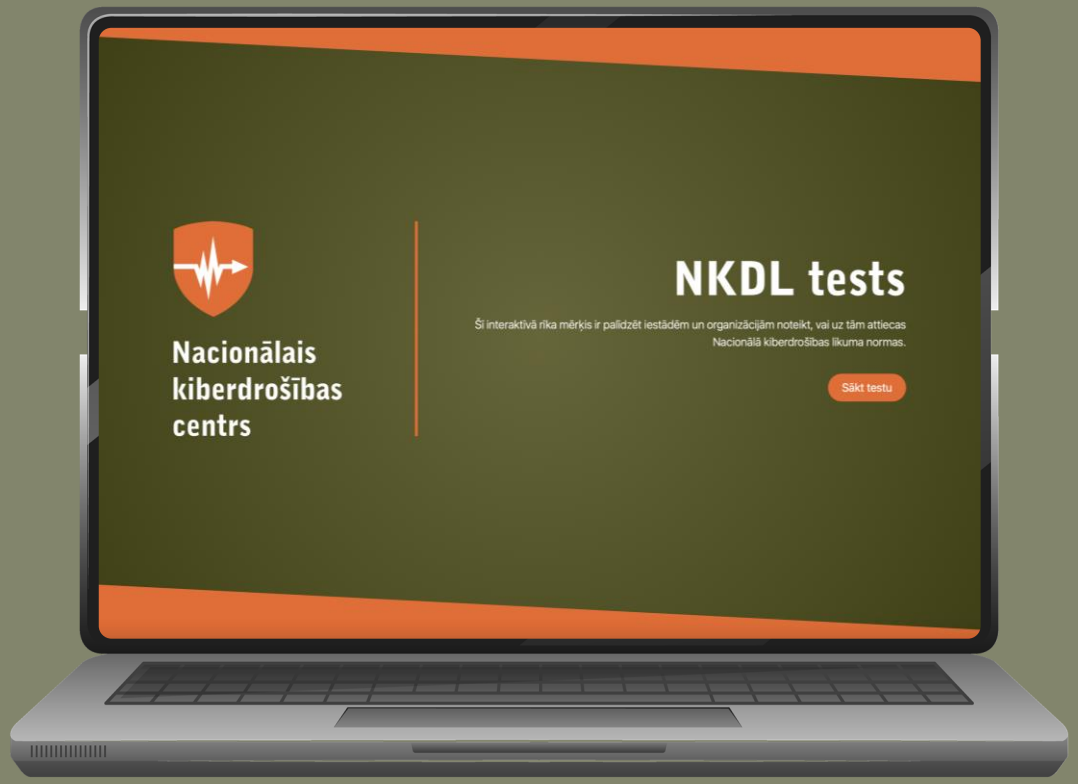
24. pants

Kritiskā IKT infrastruktūra

Atbilstoši sarakstam

Aizsardzības ministrija

Interaktīvais rīks

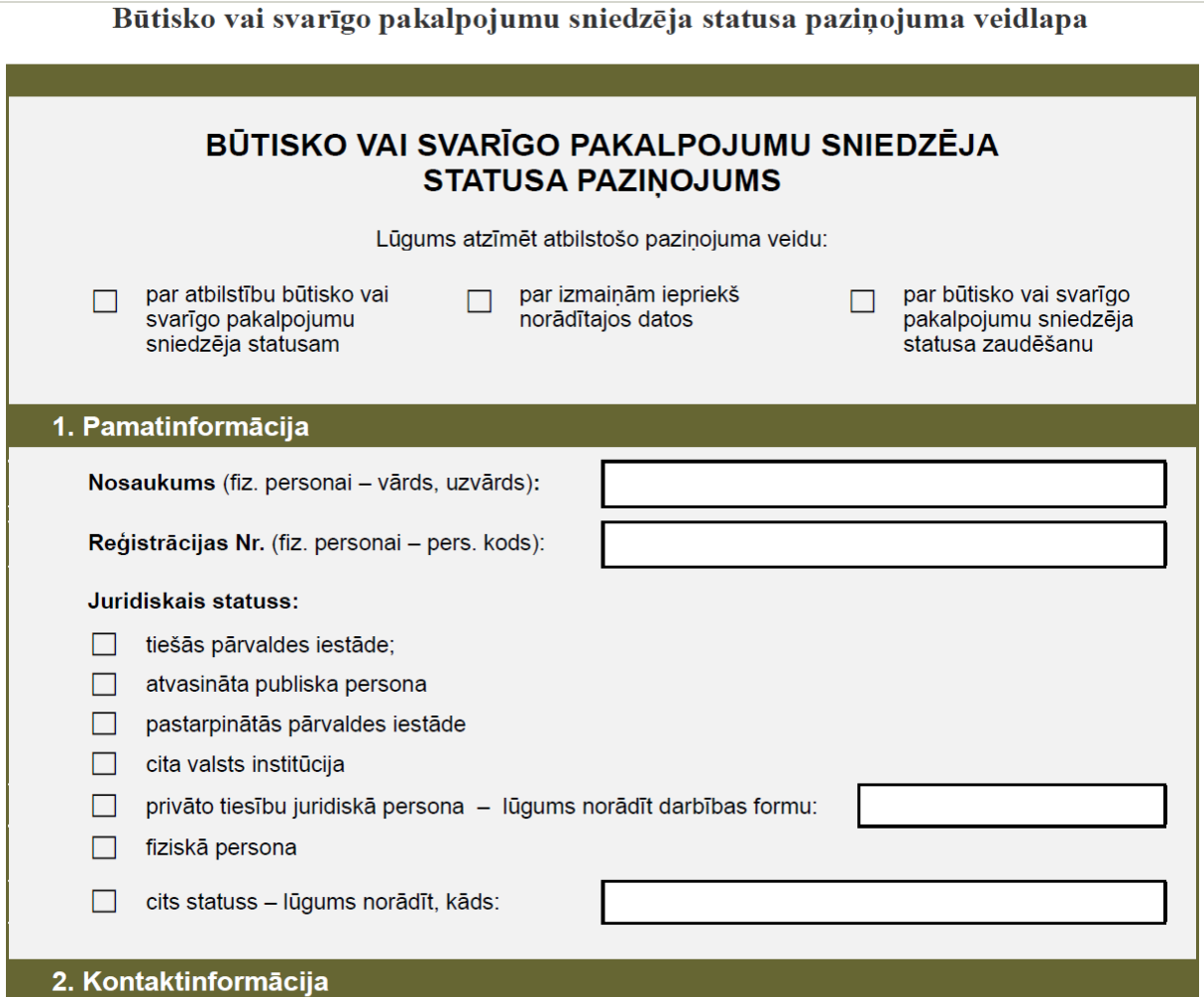


Mērķis – palīdzēt organizācijām noteikt, vai uz tām atteiksies NKDL normas

Rīks publicēts AM mājaslapā
https://www.mod.gov.lv/lv/kiberdrosiba/nkdl

Aizsardzības ministrija

Kā informēt NKDC? 1/2



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:

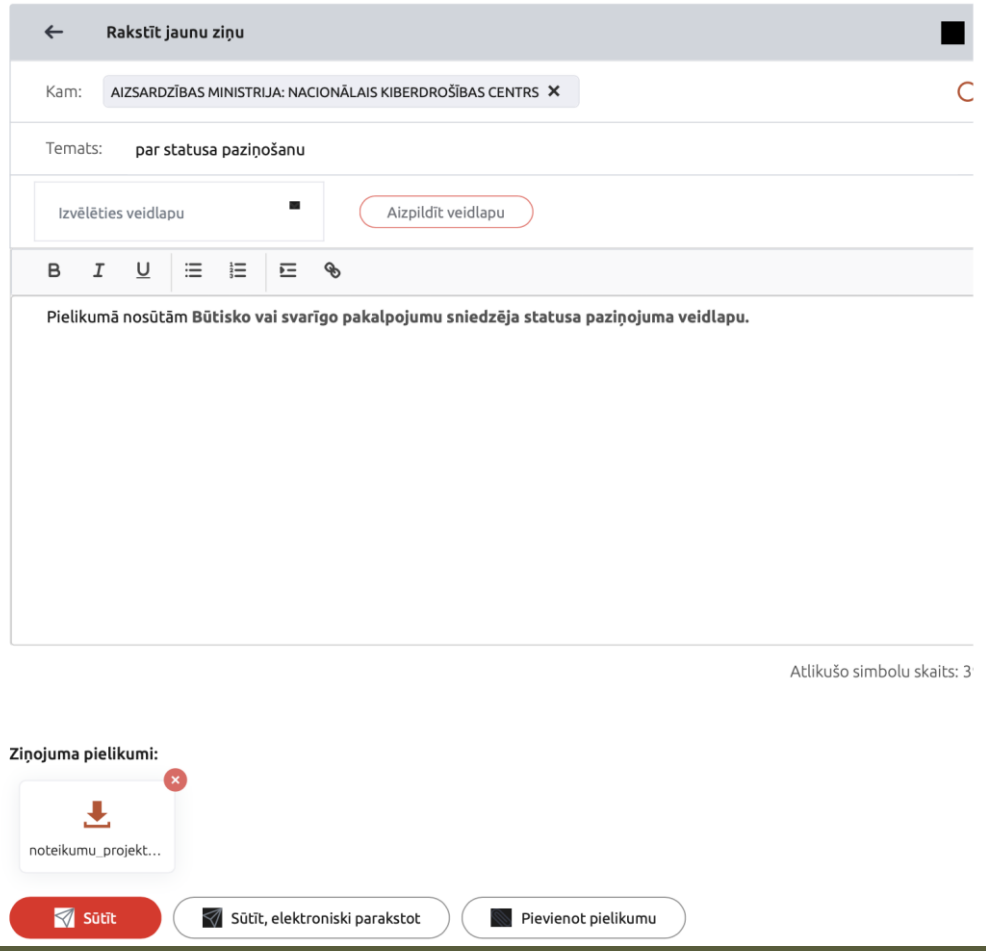
☐ tiešās pārvaldes iestāde;
☐ atvasināta publiska persona
☐ pastarpinātās pārvaldes iestāde
☐ cita valsts institūcija
☐ privāto tiesību juridiskā persona – lūgums norādīt darbības formu:
☐ fiziskā persona
☐ cits statuss – lūgums norādīt, kāds:

2. Kontaktinformācija

1. Pamata informācija par subjektu;
2. Kontaktinformācija;
3. Atzīme par statusu;
4. Darbības joma(s);
5. Valstis, kurās darbojas;
6. IP adrešu diapazoni;
7. Kontaktpersona

Aizsardzības ministrija

Kā informēt NKDC? 2/2



- **Izmanto oficiālo elektronisko adresi (e-adrese) adresātam *"Aizsardzības ministrija: Nacionālais kiberdrošības centrs"***

- **Veidlapa kā pielikums**
- **Nosūta elektroniski parakstot**

- Pēc MK noteikumu par minimālajām kiberdrošības prasībām pieņemšanas plānoti informatīvi semināri par veidlapu sagatavošanu un nosūtīšanu

Aizsardzības ministrija

Minimālās kiberdrošības prasības

- **Vispārīgie jautājumi**
- **Statusa paziņošanas kārtība**
- **Pamatprasības subjektiem**
  - Kiberdrošības pārvaldnieks
  - Kiberdrošības pārvaldības dokumentācija
  - Kiberdrošības politika
  - IKT resursu un informācijas sistēmu katalogs
  - Kiberrisku pārvaldības un IKT darbības nepārtrauktības plāns
  - Kiberincidentu pārvaldība un kiberincidentu žurnāls
  - Lietotāju un piekļuves tiesību pārvaldība
  - Tīklu pārvaldība
  - Žurnālfailu pārvaldība
  - Rezerves kopiju pārvaldība
  - Kiberhigiēnas pasākumi
  - Šifrēšanas prasības
- **Ārpakalpojumu prasības**
  - Vispārīgās ārpakalpojumu prasības
  - Īpašās ārpakalpojumu prasības IKT kritiskajai infrastruktūrai
  - Īpašās ārpakalpojumu prasības būtisko pakalpojumu sniedzējiem
- **Papildu prasības IKT kritiskajai infrastruktūrai**
- **Papildu prasības kiberincidentu novēršanas institūcijām**
- **Kiberincidentu vadība**
- **Subjektu kiberdrošības uzraudzība**
  - Atbilstības audits
  - Ielaušanās testi un drošības skenēšana
  - Pašvērtējuma ziņojums
  - Neatbilstību novēršana valsts un pašvaldību institūcijās
  - Piekļuves slēgšana elektronisko sakaru tīklam
- **Noslēguma jautājumi**

Aizsardzības ministrija

Prasības kiberdrošības pārvaldniekam

PILSONĪBA

IKT kritiskā infrastruktūra	Būtisko pakalpojumu vai svarīgo pakalpojumu sniedzējs
• Latvijas pilsonis	• Eiropas Savienības, Eiropas Brīvās tirdzniecības asociācijas vai NATO dalībvalsts pilsonis

Aizsardzības ministrija

Prasības kiberdrošības pārvaldniekam

VISPĀRĪGAS PRASĪBAS

<table>
<tr><th>IKT kritiskā infrastruktūra</th><th>Būtisko pakalpojumu sniedzējs</th><th>Svarīgo pakalpojumu sniedzējs</th></tr>
<tr><td colspan="3">• Pilngadīgs</td></tr>
<tr><td colspan="3">• Nav nodibināta aizgādnība</td></tr>
<tr><td colspan="2">• Nav sodīts par tīšu noziedzīgu nodarījumu, izņemot, ja persona ir reabilitēta, vai sodāmība ir noņemta vai dzēsta</td><td></td></tr>
</table>

Aizsardzības ministrija

Prasības kiberdrošības pārvaldniekam

KVALIFIKĀCIJAS PRASĪBAS

IKT kritiskā infrastruktūra	Būtisko pakalpojumu sniedzējs	Svarīgo pakalpojumu sniedzējs
• Spēkā esošs, starptautiski atzīts sertifikāts (piem., CISM, CISSP) **vai** • Vidējā profesionālā vai augstākā izglītība kiberdrošības pārvaldībā vai saistītā jomā **un** vismaz 2 gadu darba pieredze kiberdrošības pārvaldībā, kas iegūta pēdējo 5 gadu laikā	• Spēkā esošs, starptautiski atzīts sertifikāts (piem., CISM, CISSP) **vai** • Vidējā profesionālā vai augstākā izglītība kiberdrošības pārvaldībā vai saistītā jomā **vai** • Vismaz 2 gadu darba pieredze kiberdrošības pārvaldībā, kas iegūta pēdējo 5 gadu laikā	• Spēkā esošs, starptautiski atzīts sertifikāts (piem., CISM, CISSP) **vai** • Vidējā profesionālā vai augstākā izglītība kiberdrošības pārvaldībā vai saistītā jomā **vai** • Vismaz 2 gadu darba pieredze kiberdrošības pārvaldībā

Aizsardzības ministrija

Prasības kiberdrošības pārvaldniekam

PAPILDU PRASĪBAS IKT KI KIBERDROŠĪBAS PĀRVALDNIEKIEM

- nav un nav bijis PSRS, Latvijas PSR vai kādas ārvalsts drošības dienesta, izlūkdienesta vai pretizlūkošanas dienesta štata vai ārštata darbinieks, aģents, rezidents vai konspiratīvā dzīvokļa turētājs;
- nav un nav bijis ar Latvijas Republikas likumiem, Augstākās padomes lēmumiem vai tiesas nolēmumiem aizliegto organizāciju dalībnieks (biedrs) pēc šo organizāciju aizliegšanas;
- nepieder pie organizētās noziedzības grupējuma, nelikumīga militarizēta vai bruņota formējuma;
- nav diagnosticēti psihiski traucējumi vai alkohola, narkotisko, psihotropo vai toksisko vielu atkarība, kas dod pamatu apšaubīt fiziskās personas uzticamību;
- Satversmes aizsardzības birojs nav konstatējis drošības riskus.

IKT KI pārvaldnieka kandidātu pirms noteikšanas pārbauda SAB!

Aizsardzības ministrija

Prasības kiberdrošības pārvaldniekam

PIENĀKUMU APVIENOŠANAS IEROBEŽOJUMI

IKT kritiskā infrastruktūra	Būtisko pakalpojumu sniedzējs	Svarīgo pakalpojumu sniedzējs
• Ne vairāk kā 1 IKT kritiskās infrastruktūras subjektā	• Ne vairāk kā 5 būtisko pakalpojumu sniedzējos*	• Nav ierobežojumu

Ierobežojums neattiecas uz:

- būtisko pakalpojumu sniedzēja pakļautībā esošiem būtisko pakalpojumu sniedzējiem
- būtisko pakalpojumu sniedzējiem, kuru kapitāldaļu īpašnieks vai turētais ir attiecīgais būtisko pakalpojumu sniedzējs

(Piemēram, ministrijai un tās pakļautības iestādēm var būt viens kopīgs kiberdrošības pārvaldnieks)

Aizsardzības ministrija

Dokumentācijas prasības

Kiberdrošības politika
Stratēģiskā līmeņa dokuments – kiberdrošības pārvaldības ietvars

Kiberrisku pārvaldības un IKT darbības nepārtrauktības plāns
Risku analīze + mazināšanas pasākumu plāns + rīcības plāns krīzes gadījumā

Resursu un IS katalogs
Aktuāls programmatūras, aparatūras un IS saraksts

Kiberincidentu žurnāls
Ziņas par konstatētajiem incidentiem un to risināšanas aktuālo statusu

Aizsardzības ministrija

Kiberincidentu ziņošanas prasības

kiberincidenta gadījumā

Informē CERT, ievēro rekomendācijas
Nekavējoties

+ papildus nozīmīga kiberincidenta gadījumā

Agrīnais brīdinājums
24 stundu laikā

Sākotnējais ziņojums
72 stundu laikā

Gala ziņojums
1 mēneša laikā (vai pēc incidenta atrisināšanas)

Progresa ziņojums*
(*ja 1 mēneša laikā incidentu nevar atrisināt)

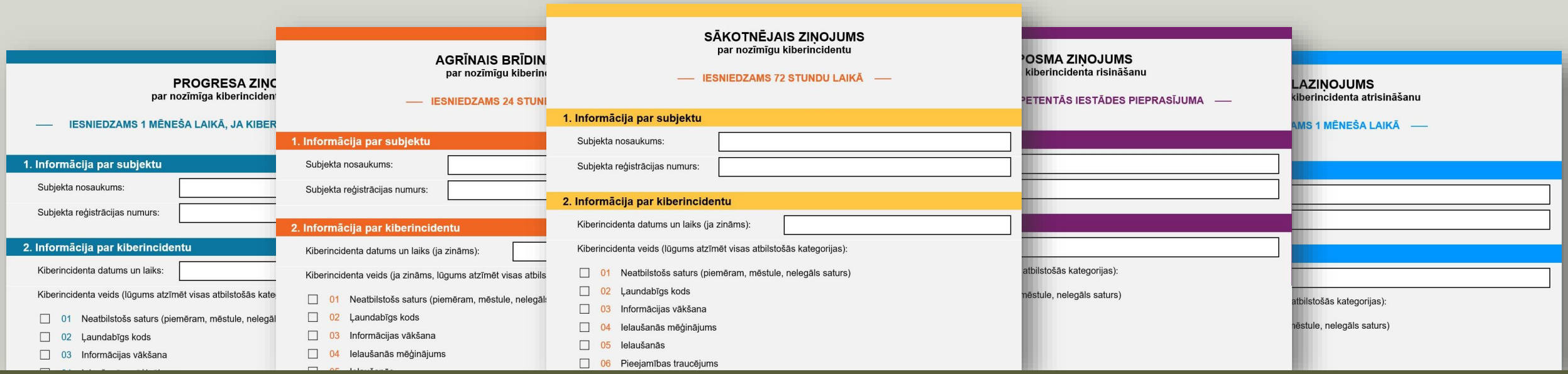
Kiberincidentu nozīmīguma kritēriji būs iekļauti MK noteikumu projektā

Aizsardzības ministrija

Ziņošanas kārtība + veidlapas

Ziņojumu veidlapas ir pievienotas MK noteikumu projekta pielikumā

(nākotnē – valsts informācijas sistēma)

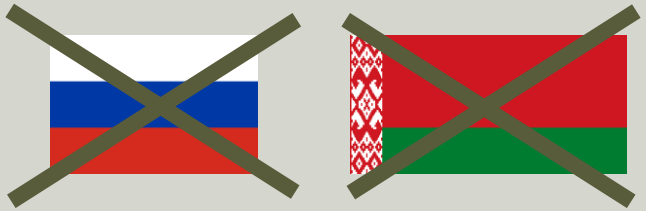


Aizsardzības ministrija

Ārpakalpojumu drošības prasības

ĀRPAKALPOJUMA LĪGUMU AIZLIEGTS SLĒGT

- Ja ārpakalpojuma sniedzējs ir juridiska persona, kas reģistrēta Krievijā, Baltkrievijā vai valstī, kuru Eiropas Parlaments vai Saeima ir atzinusi par terorismu atbalstošu valsti,
- Ja ārpakalpojuma sniedzējs, tā dalībnieks, kapitāla daļu īpašnieks vai patiesais labuma guvējs ir minētās valsts pilsonis vai publiska persona,
- Ja ārpakalpojuma sniedzēja juridiskās personas valde un padome sastāv no fiziskām personām, kuras ir minētās valsts pilsoņi, **vai**
- Ja iegādājama IKT resursa ražotājs ir minētajā valstī reģistrēta juridiska persona vai šīs valsts pilsonis.



Aizsardzības ministrija

Īpašās ārpakalpojumu drošības prasības

ĀRPAKALPOJUMA LĪGUMU ATĻAUTS SLĒGT

- IKT kritiskās infrastruktūras īpašniekam vai tiesiskajam valdītājam, un
- Būtisko pakalpojumu sniedzējam saistībā ar A klases informācijas sistēmu:

EFTA

IP4
Indo-Pacific
Four

- No citām valstīm (ārpus ES, EFTA, NATO, IP4) **drīkst ar SAB atzinumu** (katru gadījumu vērtē individuāli)

IKT KI subjekti jebkuru ārpakalpojumu saistībā ar IKT KI informācijas sistēmu saskaņo ar SAB!
(izņēmums – ja ārpakalpojuma sniedzējs ir publiskā persona, piem., valsts kapitālsabiedrība)

Aizsardzības ministrija

Subjektu uzraudzība

Uzraudzības iestādes (NKDC un SAB) būs tiesīgas veikt subjektu dokumentu un IKT infrastruktūras pārbaudes un vajadzības gadījumā izteikt subjektam brīdinājumu vai uzdot:

- novērst konstatētās neatbilstības,
- veikt ārēju auditu,
- informēt pakalpojumu saņēmējus par kiberapdraudējumu.

Ja minētie pasākumi nebūs efektīvi, uzraudzības iestādes būs tiesīgas:

- apturēt informācijas sistēmas, resursa vai e-pakalpojuma darbību līdz neatbilstību novēršanai,
- apturēt produkta tirdzniecību vai pakalpojuma sniegšanu līdz neatbilstību novēršanai,
- noteikt pagaidu aizliegumu subjekta vadītājam pildīt pienākumus līdz neatbilstību novēršanai.

Aizsardzības ministrija

Subjektu uzraudzība

Aizsardzības ministrija

Sankcijas par prasību neievērošanu

VALSTS UN PAŠVALDĪBU INSTITŪCIJAS

Ziņošana amatpersonai, kura lemj par disciplinārsoda piemērošanu

PRIVĀTO TIESĪBU JURIDISKĀS PERSONAS

Administratīvā akta piespiedu izpilde vai soda nauda

par valsts institūcijām	par pašvaldību institūcijām	būtisko pakalpojumu sniedzējiem un IKT KI	svarīgo pakalpojumu sniedzējiem
			
ziņo atbildīgajam Ministru kabineta loceklim un informē Ministru kabinetu	ziņo pašvaldības domes priekšsēdētājam un informē VARAM	līdz 10 miljoniem eiro vai līdz 2% no kopējā gada apgrozījuma pasaulē	līdz 7 miljoniem eiro vai līdz 1,4 % no kopējā gada apgrozījuma pasaulē

Aizsardzības ministrija

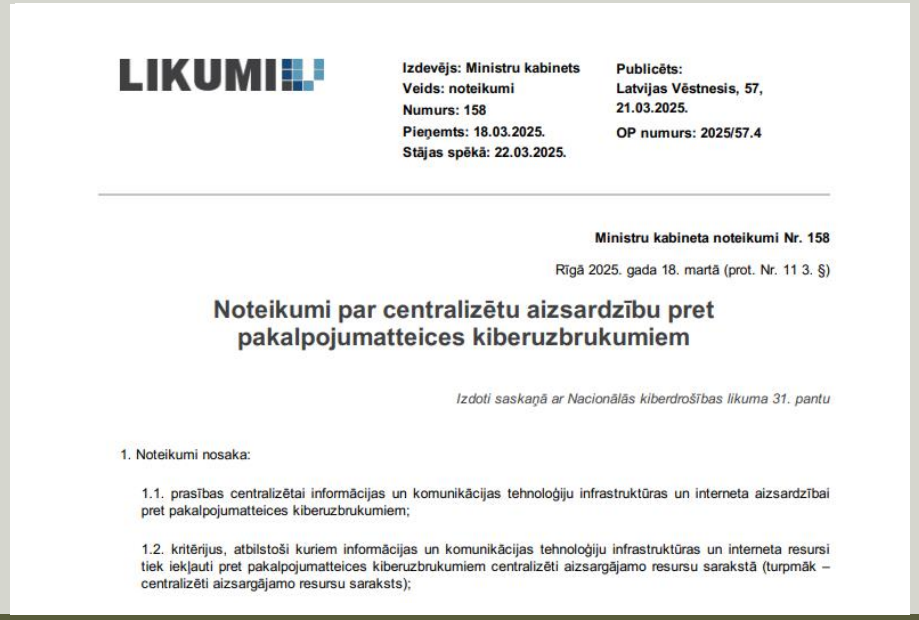
Pieejamie atbalsta pasākumi

- Draudu medību operācijas
- Centralizētā DDoS aizsardzība
- Pentesti un phishing kampaņas
- GLV-IX

- DNS ugunsmūris
- Agrās brīdināšanas sensori
- CERT.LV SOC
- Koordinēta ievainojamību atklāšana

Aizsardzības ministrija

Centralizēta aizsardzība pret DDOS



LIKUMI

Izdevējs: Ministru kabinets
Veids: noteikumi
Numurs: 158
Pieņemts: 18.03.2025.
Stājas spēkā: 22.03.2025.

Publicēts:
Latvijas Vēstnesis, 57, 21.03.2025.
OP numurs: 2025/57.4

Ministru kabineta noteikumi Nr. 158

Rīgā 2025. gada 18. martā (prot. Nr. 11 3. §)

Noteikumi par centralizētu aizsardzību pret pakalpojumatteices kiberuzbrukumiem

Izdoti saskaņā ar Nacionālās kiberdrošības likuma 31. pantu

1. Noteikumi nosaka:

1.1. prasības centralizētai informācijas un komunikācijas tehnoloģiju infrastruktūras un interneta aizsardzībai pret pakalpojumatteices kiberuzbrukumiem;

1.2. kritērijus, atbilstoši kuriem informācijas un komunikācijas tehnoloģiju infrastruktūras un interneta resursi tiek iekļauti pret pakalpojumatteices kiberuzbrukumiem centralizēti aizsargājamo resursu sarakstā (turpmāk – centralizēti aizsargājamo resursu saraksts);

Kā pieteikties aizsardzībai?

Iestādes, organizācijas un uzņēmumi, kuri vai kuru resursi atbilst MK noteikumu 5. punktā minētajiem kritērijiem

1. Iesniedz NKDC* aizpildītu pieteikuma veidlapu

Pieteikuma veidlapu nosūta uz oficiālo elektronisko adresi adresātam «Aizsardzības ministrija Nacionālais kiberdrošības centrs»

2. Starpinstitūciju komisija izvērtē pieteikumu

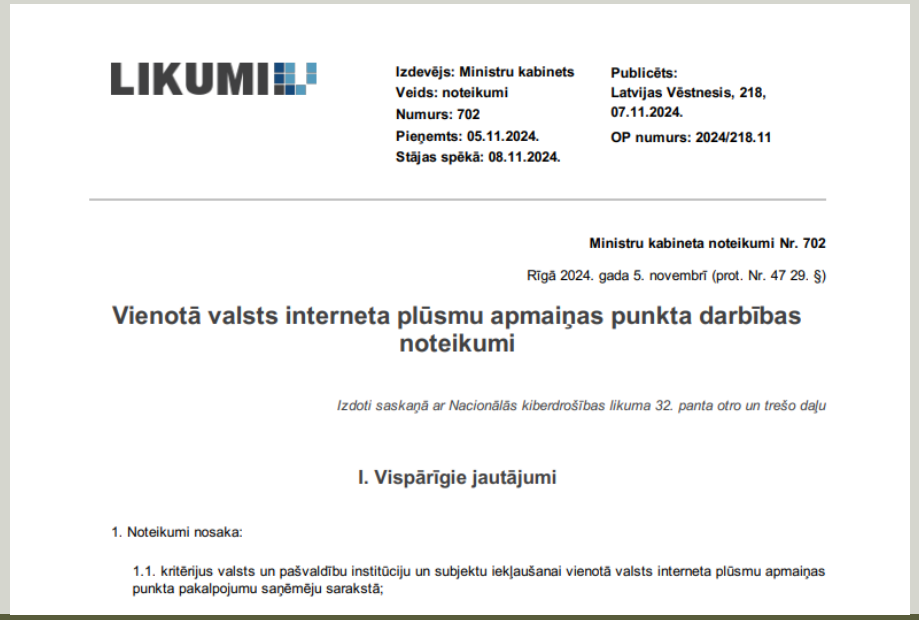
3. NKDC informē pieteikuma iesniedzēju par pieņemto lēmumu

Labvēlīga lēmuma gadījumā tiek noslēgta vienošanās starp pakalpojuma sniedzēju un saņēmēju

*Nacionālais kiberdrošības centrs

Aizsardzības ministrija

Valsts interneta plūsmu apmaiņas punkts



LIKUMI

Izdevējs: Ministru kabinets
Veids: noteikumi
Numurs: 702
Pieņemts: 05.11.2024.
Stājas spēkā: 08.11.2024.

Publicēts:
Latvijas Vēstnesis, 218, 07.11.2024.
OP numurs: 2024/218.11

Ministru kabineta noteikumi Nr. 702

Rīgā 2024. gada 5. novembrī (prot. Nr. 47 29. §)

Vienotā valsts interneta plūsmu apmaiņas punkta darbības noteikumi

Izdoti saskaņā ar Nacionālās kiberdrošības likuma 32. panta otro un trešo daļu

I. Vispārīgie jautājumi

1. Noteikumi nosaka:

1.1. kritērijus valsts un pašvaldību institūciju un subjektu iekļaušanai vienotā valsts interneta plūsmu apmaiņas punkta pakalpojumu saņēmēju sarakstā;

Kā pieslēgties GLV-IX?

Subjektiem, kuriem GLV-IX pakalpojuma saņemšana ir <u>obligāta</u>

1. Iesniedz pieteikumu NKDC*

Pieteikumu nosūta uz kiberdrosiba@mod.gov.lv, norādot:
1) juridiskās personas nosaukumu
2) kontaktpersonu, kas atbild par vienošanās slēgšanas jautājumiem
3) kontaktpersonu tehniskajos jautājumos

2. NKDC izvērtē atbilstību un nosūta pieteikumu GLV-IX pakalpojuma sniedzējam

3. Tiek noslēgta vienošanās starp pakalpojuma sniedzēju un saņēmēju

*Nacionālais kiberdrošības centrs

Aizsardzības ministrija

Paldies par uzmanību!

NIS2@mod.gov.lv