



LATVIJAS REPUBLIKA

Preiļu novada pašvaldība

Reģ. Nr. 90000065720

Raiņa bulvāris 19, Preiļi, Preiļu novads, LV-5301, tālr. - 65322766,
e-pasts - dome@preili.lv

konts Nr.LV08UNLA0026000130630, A/s SEB banka, kods UNLALV2X,
konts Nr. LV81HABA0551019925560, A/s SWEDBANK, kods HABALV22

APSTIPRINĀTS
ar Preiļu novada domes
2025.gada 25.septembra
sēdes lēmumu (protokols Nr.21., 29.§)

Preiļu novada pašvaldības Kiberdrošības politika

*Izdots saskaņā ar
Nacionālo kiberdrošības likumu,
2025. gada 25. jūnija Ministru kabineta
noteikumiem Nr. 397
"Minimālās kiberdrošības prasības"
21.punktu*

I. Vispārīgie jautājumi

1. Kiberdrošības politika nosaka Preiļu novada pašvaldības (turpmāk – Pašvaldība) vispārējo pieeju kiberdrošības pārvaldībai un kalpo kā pamats iekšējai drošības kontrolei, riska pārvaldībai un atbilstības nodrošināšanai attiecībā uz Pašvaldības esošo informācijas un komunikācijas tehnoloģijas (turpmāk - IKT) kiberdrošību, informācijas un informācijas sistēmu pieejamību, integritāti un konfidencialitāti.

2. Kiberdrošības politika ir izstrādāta saskaņā Nacionālo kiberdrošības likumu un uz šī likumu pamata izstrādātajiem Ministru kabineta noteikumiem, t.sk. Ministru kabineta 2025. gada 25. jūnija noteikumu Nr.397 "Minimālās kiberdrošības prasības" 28.punktu un 29.punktu.

3. Kiberdrošības politikā lietotie termini:

- 3.1. **Preiļu novada pašvaldība** – subjekts, kas, ievērojot Nacionālā kiberdrošības likuma nosacījumus, atbilst Būtiskā pakalpojuma sniedzēja statusam.
- 3.2. **Informācijas resurss** - strukturēta digitālo datu vienība.
- 3.3. **Informācijas sistēma** – organizēta sistēma, kas paredzēta informācijas resursu pārvaldībai un elektroniskajai apstrādei, izmantojot tehniskos resursus.
- 3.4. **Informācijas un komunikācijas tehnoloģijas (IKT)** – tehnoloģijas, kuras tām paredzēto uzdevumu izpildei ar tehnisko līdzekļu palīdzību veic informācijas elektronisko apstrādi, tai skaitā izveidošanu, izmainīšanu, dzēšanu, glabāšanu,

Šis dokuments ir parakstīts ar drošu elektronisko parakstu un satur laika zīmogu

- attēlošanu, pārsūtīšanu vai pārraidīšanu (turpmāk — elektroniskā apstrāde), un nodrošina tehnoloģijas izmantotāju savstarpējo komunikāciju.
- 3.5. **IKT resursi** - tehnisko resursu un informācijas resursu kopums.
 - 3.6. **Integritāte** - informācijas resursa un tā elektroniskās apstrādes metožu precizitāte, pareizība un pilnīgums.
 - 3.7. **Konfidencialitāte** – piekļuve informācijas resursam tikai autorizētiem IKT procesiem un lietotājiem.
 - 3.8. **Pieejamība** – iespēja lietotājam lietot informācijas sistēmu vai informācijas resursu noteiktā laikā un vietā.
 - 3.9. **Kiberdrošības pārvaldnieks** – ar Pašvaldības rīkojumu iecelts Pašvaldības darbinieks vai ārpalpojuma sniedzējs, kas atbild par Pašvaldības kiberdrošības pasākumu izstrādi, ieviešanu, uzturēšanu un uzraudzību.
 - 3.10. **Kiberapdraudējums** - jebkādi iespējami apstākļi, notikums vai darbība, kas varētu radīt bojājumus vai traucējumus vai citādi negatīvi ietekmēt tīklu un informācijas sistēmas, to lietotājus un citas personas.
 - 3.11. **Kiberdrošības incidents (turpmāk — kiberincidents)** — notikums, kas apdraud apstrādātus datus vai tādu pakalpojumu pieejamību, autentiskumu, integritāti vai konfidencialitāti, kurus piedāvā tīklu un informācijas sistēmas vai kuri pieejami ar tīklu un informācijas sistēmu starpniecību.
 - 3.12. **Kiberrisks** — kiberincidenta izraisītu zaudējumu vai pakalpojumu traucējumu iespējamība, ko izsaka kā šādu zaudējumu vai traucējumu ietekmes un minētā incidenta varbūtības apvienojumu.
 - 3.13. **IKT resursu īpašnieks** - persona, kuras kompetencē atrodas konkrētas Informācijas sistēmas darbības procesa organizēšana.
 - 3.14. **IKT tehnisko resursu turētājs** – persona vai ārpalpojuma sniedzējs, kas veic datortīklu, serveru un to saistīto iekārtu uzturēšanu un administrēšanu un / vai Informācijas sistēmas lietotāju datoru uzstādīšanu un administrēšanu.
 - 3.15. **Informācijas sistēmas lietotājs** – persona, kurai ir piešķirtas piekļuves tiesības Pašvaldības IKT resursiem un / vai informācijas sistēmām.
 - 3.16. **Fiziskā aizsardzība** – IKT aizsardzība pret fiziskas iedarbības radītiem bojājumiem.
 - 3.17. **Loģiskā aizsardzība** – IKT aizsardzība, kuru realizē ar programmatūras līdzekļiem.

II. Vispārīga informācija par subjekta darbības jomu, sniegtajiem pakalpojumiem un procesiem, kurus var ietekmēt kiberapdraudējums

4. Pašvaldība ir atvasināta publiska persona — vietējā pārvalde —, kurai ir iedzīvotāju ievēlēta lēmējinstītūcija — dome — un kura patstāvīgi nodrošina tai tiesību aktos noteikto funkciju un uzdevumu izpildi savas administratīvās teritorijas iedzīvotāju interesēs un ir atbildīga par to saskaņā ar ārējiem normatīvie aktiem, tai skaitā Pašvaldības likumu un Pašvaldības nolikumu, un saskaņā ar likumu noslēgtiem publisko tiesību līgumiem.

5. Pašvaldības sniegtie pakalpojumi ir cieši saistīti ar IKT resursu un informācijas sistēmu izmantošanu, kas ir pakļauti kiberriskiem un kurus var ietekmēt iespējams kiberapdraudējums.

III. Kiberdrošības politikas principi un pamatnostādnes

6. Pašvaldības pienākums ir nodrošināt, lai tās rīcībā esošā informācija tiktu apstrādāta, glabāta un pārvaldīta droši un pārbaudāmi, sniedzot tās darbiniekiem un lietotājiem skaidri noteiktas prasības IKT resursu izmantošanā, un nodrošinot Informācijas

sistēmas aizsardzību no ārējiem un iekšējiem, apzinātiem un nejaušiem kiberapdraudējumiem.

7. Kiberdrošības politika attiecas uz visiem Pašvaldības Informācijas sistēmas lietotājiem, kuri veic darbības ar IKT resursiem (piemēram, informācijas sistēmām, informāciju, kas tiek saņemta, apstrādāta, ievadīta, pārsūtīta vai uzglabāta) un tehniskajiem resursiem (piemēram, datoru sistēmām, datoru tīkliem), t.sk.:

6.1. Pašvaldības darbiniekiem neatkarīgi no to ieņemamā amata.

6.2. lietotājiem, kuri ir noslēguši līgumu ar Pašvaldības par datu lietošanu vai kuri uz pieprasījuma pamata saņem datus no Pašvaldības izmantotām informācijas sistēmām.

8. Informācijas sistēmas lietotājs atbild par Kiberdrošības politikas nosacījumu un prasību ievērošanu, kas ir minēti šādos dokumentos:

7.1. Kiberdrošības politikā.

7.2. Informācijas sistēmu lietošanas noteikumos.

9. Informācijas sistēmu lietotājs par iepazīšanos ar augstāk minētajiem dokumentiem un to ievērošanu paraksta 1.Pielikumu "Informācijas sistēmas lietotāja apliecinājums par "Kiberdrošības politikas" prasību ievērošanu".

10. Kiberdrošības pārvaldnieks sadarbībā ar atbilstošās IKT resursu īpašnieku un IKT tehnisko resursu turētāju atbild par Kiberdrošības politikas nosacījumu un prasību ievērošanu, kas ir minēti šādos dokumentos:

10.1. Kiberdrošības politikā.

10.2. Informācijas sistēmu lietošanas noteikumos.

10.3. Kiberincidentu pārvaldības noteikumos.

10.4. Kiberrisku pārvaldības noteikumos.

10.5. IKT darbības nepārtrauktības plānā.

10.6. IKT kiberdrošības noteikumos.

11. Pašvaldības struktūrvienību vadītāji ir atbildīgi par viņu pakļautībā vai uzraudzībā esošajiem Informācijas sistēmas lietotājiem, nodrošinot, ka personāls, uz kuru šī Kiberdrošības politika attiecas daļēji vai pilnā apmērā, ir informēts par politikas esamību un pilda savus darba pienākumus atbilstoši Kiberdrošības politikas prasībām.

12. Kiberdrošība tiek nodrošināta šādu uzdevumu īstenošanai:

12.1. nodrošinātu informācijas IKT pieejamību;

12.2. nodrošinātu informācijas IKT integritāti;

12.3. nodrošinātu informācijas IKT konfidencialitāti;

12.4. aizsargātu IKT informācijas sistēmas un resursus;

12.5. aizsargātu IKT informācijas sistēmas un resursus;

12.6. noteiktu IKT informācijas sistēmu un resursu kiberdrošības apdraudējumu;

12.7. novērtētu IKT informācijas sistēmu un resursu kiberdrošības risku;

12.8. atklātu kiberincidentu;

12.9. atjaunotu IKT informācijas sistēmas un resursu darbību pēc kiberincidenta.

IV. Kiberdrošības pārvaldības struktūra

13. Kiberdrošības organizatoriskās struktūras pamatu veido:

13.1. Pašvaldības vadība, kura kontrolē Kiberdrošības politikas īstenošanu Pašvaldības un nodrošina resursu piešķiršanu Kiberdrošības pārvaldības pilnvērtīgai funkcionēšanai.

- 13.2. Kiberdrošības pārvaldnieks, kurš ir atbildīgs par IKT kiberdrošības pasākumu īstenošanu, koordinēšanu un izpildes uzraudzību, ievērojot šo Kiberdrošības politiku, Nacionālo kiberdrošības likumu un uz šī likuma pamata izdotos Ministru kabineta noteikumus. Kiberdrošības pārvaldnieks veic IKT kiberdrošības incidentu analīzi un izmeklēšanu, apkopojot izanalizēto incidentu rezultātus un, ja nepieciešams, ziņo Pašvaldības vadībai un citas iesaistītās personas un uzraudzības institūcijas.
- 13.3. IKT resursu īpašnieks, kurš nodrošina Informācijas sistēmās izmantojamās informācijas racionālu un pareizu izmantošanu, izskata Informācijas sistēmas lietotāju tiesību piešķiršanas un izmaiņu veikšanas pieteikumus saskaņā ar Informācijas sistēmas lietošanas noteikumiem, glabāšanu, kontroli un uzraudzību, kā arī sniedz konsultācijas un atbalstu Kiberdrošības pārvaldniekam un Informācijas sistēmas iekšējiem lietotājiem attiecībā uz Informācijas sistēmas lietošanu.
- 13.4. IKT tehnisko resursu turētājs, kurš nodrošina IKT resursu racionālu un pareizu izmantošanu, veic datortīklu, serveru un to saistīto iekārtu uzturēšanu un administrēšanu, nodrošina Informācijas sistēmu lietotāju pieejas tiesību izveidošanu, administrēšanu un šo pieprasījumu apkopošanu, nodrošina tehnisko resursu fiziskās un loģiskās aizsardzības pasākumus, nodrošina Informācijas sistēmas atjaunošanas procedūras, ja tehnoloģiskie resursi ir bojāti un informācijas sistēmas funkcionēšana traucēta vai neiespējama saskaņā ar IKT kiberdrošības noteikumiem un IKT darbības atjaunošanas plānu, kā arī nodrošina atbilstošu atbalstu, palīdzību un konsultāciju sniegšanu IKT resursu īpašniekiem, Informācijas sistēmas lietotājiem un IKT ārpakalpojumu sniedzējiem, lai tie varētu pildīt savus pienākumus atbilstoši Kiberdrošības politikas prasībām.
- 13.5. Informācijas sistēmas lietotāji, kuru pienākums ir ievērot Kiberdrošības politikas, uz šīs Kiberdrošības politikas izdoto iekšējo normatīvo aktu un citu iekšējo normatīvo aktu noteikumus, rūpēties par informācijas konfidencialitātes, pieejamības un integritātes saglabāšanu Pašvaldībā, kā arī racionāli un lietderīgi izmantot informācijas sistēmas un to datus sava darbu pienākumu veikšanai. Informācijas sistēmu lietotājs ir atbildīgs par visām savām darbībām, kas veiktas ar viņam piešķirto lietotājevārdu un Pašvaldības informāciju, informācijas sistēmām un tehniskiem resursiem. Informācijas sistēmas lietotāja pienākums ir informēt savu tiešo vadītāju vai kontaktpersonu un Kiberdrošības pārvaldnieku par visiem drošības incidentiem, aizdomīgiem notikumiem vai kiberincidentiem. Informācijas sistēmas iekšējā lietotāja pienākumi un atbildība ir iekļauta Pašvaldības Informācijas sistēmu lietošanas noteikumos.

14. Pašvaldības IKT resursu un informācijas sistēmu atbildīgo darbinieku sarakstu, tajā nosakot IKT resursu īpašniekus, IKT tehnisko resursu turētājus un Kiberdrošības pārvaldnieku apstiprina Pašvaldības vadība. IKT resursu un informācijas sistēmu atbildīgo darbinieku sarakstu jāpārskata vismaz reizi gadā, nepieciešamības gadījumā to aktualizējot.

15. Pašvaldības IKT informācijas sistēmu un resursu atbildīgo darbinieku saraksts ir iekļauts Pašvaldības IKT resursu un informācijas sistēmu katalogā.

16. Kiberdrošības pasākumu organizēšanu un iekšējo normatīvu aktu izstrādi, papildināšanu un atjaunošanu Pašvaldība veic saskaņā ar Kiberdrošības politiku un spēkā esošajiem normatīvajiem aktiem.

V. IKT resursu un informācijas sistēmu klasifikācija

17. Pašvaldības īpašumā un valdījumā esošie IKT resursi un informācijas sistēmas tiek iedalītas drošības klasēs ievērojot 2025. gada 25. jūnija noteikumu Nr. 397 “Minimālās kibernetikas prasības” nosacījumus.

18. Pašvaldības īpašumā un valdījumā esošo IKT resursu un informācijas sistēmu klasifikācijas iedalījuma sarakstu apstiprina Pašvaldības valde.

19. Kibernetikas pārvaldnieks sadarbībā ar IKT resursu īpašnieku un IKT tehnisko resursu turētāju vismaz reizi gadā pārskata Pašvaldības īpašumā un valdījumā esošo IKT resursu un informācijas sistēmu klasifikācijas iedalījumu sarakstu, nepieciešamības gadījumā to aktualizējot un iesniedzot to Pašvaldības vadībai apstiprināšanai.

VI. IKT resursu un informācijas sistēmu kataloga izveidošana un uzturēšana

20. Pašvaldības īpašumā un valdījumā esošos IKT resursus un informācijas sistēmas, kas ir pakļautas kibernetiskiem, apzina un uzskaita IKT tehnisko resursu turētājs, izveidojot IKT resursu un informācijas sistēmu katalogu.

21. IKT resursu un informācijas sistēmu katalogā tiek iekļauta informācija par Pašvaldības īpašumā un valdījumā esošajiem IKT resursu un informāciju sistēmām, šo resursu un informācijas sistēmu atbalstošām sistēmām, servisiem, programmatūru, izmantoto aparātūru, fizisko infrastruktūru, datu nesējiem, kā arī izveidoto tīklu shēmu.

22. IKT tehnisko resursu turētājs uztur IKT resursu un informācijas sistēmu katalogu un izmaiņu gadījumā ne vēlāk kā viena mēneša laikā aktualizē to.

VII. Kibernetiku pārvaldība

23. Pašvaldība veic IKT resursu un informācijas sistēmu kibernetiku pārvaldību, ievērojot Pašvaldības Kibernetiku pārvaldības noteikumus iekļautās prasības, nodrošinot šādas darbības:

- 23.1. kibernetiku identificēšanas un reģistrēšanas kārtību;
- 23.2. ietekmes novērtēšanu;
- 23.3. pasākumu un procedūru ieviešanu kibernetiku risināšanai, ietekmes mazināšanai, un sekas likvidēšanai;
- 23.4. pasākumu un procedūru ieviešanu kibernetiku pirmcēloņu atklāšanai, analīzei un novēršanai, pierādījumu saglabāšanai un drošības pasākumu uzlabošanai pēc kibernetiku.
- 23.5. iekšējās un ārējās komunikācijas plānu kibernetiku gadījumā noteikšanu;
- 23.6. pasākumu un procedūru ieviešanu kibernetikas incidenta paziņojuma iesniegšanai uzraudzības iestādei – Nacionālam kibernetikas centram.
- 23.7. Kibernetiku žurnāla izveidošanai un uzturēšanai.

VIII. Kibernetiku pārvaldība

24. Pašvaldība nepārtraukti īsteno pasākumus informācijas drošības risku novērtēšanai un pārvaldīšanai, kā arī informācijas drošības līmeņa paaugstināšanai.

25. Kibernetiku pārvaldības mērķis ir nodrošināt atbilstošu kibernetikas vadību un kontroles darbības efektivitāti, lai atklātu un novērstu kibernetikus,

kiberapdraudējumus, kļūdas un neprecizitātes, un nepieciešamības gadījumā veiktu labojumus kiberdrošības jomā.

26. Kiberrisku pārvaldīšana Pašvaldībā tiek nodrošināta saskaņā ar Kiberrisku pārvaldības noteikumu prasībām, veicot 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.

27. Ņemot vērā kiberriska novērtējumu, tiek sagatavots kiberrisku mazināšanas pasākumu plāns, 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.

IX. IKT resursu un informācijas sistēmu kiberdrošības prasības

1. Pašvaldības Informācijas sistēmas lietotājiem pieejas tiesību piešķiršana, izmaiņšana un anulēšana tiek veikta atbilstoši Informācijas sistēmas lietošanas noteikumiem.

2. Informācijas sistēmas lietotāju pienākumi attiecībā uz informācijas resursu lietošanu, interneta izmantošanu un tehnisko resursu fizisko drošību ir iekļauti Informācijas sistēmas lietošanas noteikumos.

3. Pašvaldības datortīklu, serveru un to saistīto iekārtu uzturēšanu un administrēšanu, kā arī Informācijas sistēmas lietotāju datoru uzstādīšanu un administrēšanu veic IKT tehnisko resursu turētājs, ievērojot Pašvaldības IKT kiberdrošības noteikumus iekļautās prasības.

X. Darbības nepārtrauktības nodrošināšana

4. Pašvaldības IKT resursiem, t.sk. informācijas sistēmām un elektroniskā veidā saglabātai informācijai, regulāras rezerves kopijas veidošanu nodrošina IKT tehnisko resursu turētājs, ievērojot Kiberdrošības politikā un 2025. gada 25. jūnija noteikumos Nr. 397 "Minimālās kiberdrošības prasības" iekļautās prasības.

5. Katram Informācijas sistēmas lietotājam, kas ir nodarbināts Pašvaldībā, ir jāveic un jānodrošina darbības nepārtrauktību tādā apjomā, kādā tā ir noteikta konkrētā darbinieka pienākumos un cik tas nepieciešams darbinieka tiešajiem darba pienākumiem.

XI. Ārpakalpojumu prasības

6. Slēdzot ārpakalpojuma līgumu par IKT resursa vai pakalpojuma iegādi, Pašvaldība nodrošina, ka ārpakalpojuma sniedzējs atbilst Nacionālā kiberdrošības likumam, t.sk. Ministru kabineta 2025. gada 25. jūnija noteikumu Nr.397 "Minimālās kiberdrošības prasības" 4.1.sadaļā iekļautajām prasībām.

7. Pašvaldība nodrošina, ka ārpakalpojuma sniedzējiem tiek iekļautas IKT resursu un informācijas sistēmu prasības, kas nav zemākas par Pašvaldības Kiberdrošības politikā, uz šīs politikas izstrādātajos iekšējos normatīvajos aktos un citos spēkā esošajos normatīvajos aktos iekļautajām prasībām.

XII. Kiberdrošības apmācības

8. Pašvaldība nodrošina, ka IKT resursu un informācijas sistēmu izmantošanā un uzturēšanā iesaistītām personām tiek nodrošinātas vismaz šādas apmācības:

- 8.1. Informācijas sistēmu lietotājiem un IKT resursu īpašniekiem tiek nodrošinātas sākotnējās kiberdrošības apmācības ne vēlāk kā viena mēneša laikā no šai personai izveidotā lietotāja konta;
- 8.2. Informācijas sistēmu lietotājiem un IKT resursu īpašniekiem tiek nodrošinātas kārtējās kiberdrošības apmācības vismaz reizi gadā.
- 8.3. IKT tehnisko resursu turētājiem, kas ir Pašvaldības darbinieki, tiek nodrošinātas individuāli izvērtētas apmācības kiberdrošības jomā, ņemot vērā šo personu zināšanas un prasmes, kas tiek nodrošinātas vismaz reizi gadā.

9. Vismaz reizi gadā tiek veikta Informācijas sistēmu lietotāju, IKT resursu īpašnieku un IKT tehnisko resursu turētāju zināšanu pārbaudes testēšana kiberdrošības jomā, pārbaudot zināšanas kiberdrošības jautājumos un īstenoto kiberdrošības apmācību efektivitāti.

10. Kiberdrošības pārvaldniekam ir pienākums vismaz reizi gadā ir apmeklēt uzraugošās iestādes - Nacionālā kiberdrošības centra organizētās apmācības kiberdrošības jomā.

Preiļu novada domes priekšsēdētājs

Aldis Adamovičs

**INFORMĀCIJAS SISTĒMAS LIETOTĀJA APLIECINĀJUMS
PAR “KIBERDROŠĪBAS POLITIKAS” PRASĪBU IEVĒROŠANU**

Ar šo es, zemāk parakstīties, apliecinu:

1. Esmu iepazinies(usies), izprotu un apņemos ievērot Kiberdrošības politikas nosacījumus un prasības ievērošanu, kas ir minēti šādos dokumentos:
 - 1.1. Kiberdrošības politikā;
 - 1.2. Informācijas sistēmas lietošanas noteikumos;
2. Apņemos neizmantot konfidenciālu informāciju, kas saņemta no Preiļu novada pašvaldības, savu vai trešo personu interesēs.
3. Es piekrītu, ka pārtraucot darba (līguma) attiecības ar Preiļu novada pašvaldību jebkādu iemeslu dēļ, es nekavējoties nodošu Preiļu novada pašvaldībai manā rīcībā esošos IKT resursus, t.sk. programmatūru un tehnisko aprīkojumu, kā arī manā rīcībā esošos informācijas oriģinālus un kopijas, ko esmu saņēmis(usi) darba (līguma izpildes) laikā, un kas ir manā rīcībā vai kas ir citādi tieši vai netieši manā pārvaldībā.
4. Apņemos saglabāt informācijas konfidencialitāti arī pēc darba (līguma izpildes) tiesisko attiecību izbeigšanas.

Struktūrvienība un
amats

/Paraksts/

Paraksta atšifrējums

Datums