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
Kiberrisku pārvaldības noteikumi

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

I. Vispārīgie jautājumi

1. Kiberrisku pārvaldības noteikumi nosaka Preiļu novada pašvaldības (turpmāk – Pašvaldības) izmantoto Informācijas un komunikācijas tehnoloģijas (turpmāk – IKT) resursu un informācijas sistēmas kiberrisku novērtēšanas metodiku, kiberrisku novērtējumu un kiberrisku pārvaldības pasākuma plāna ieviešanu un to vadību, nodrošinot atbilstošu kiberdrošības vadību un kontroles darbības efektivitāti, lai atklātu un novērstu kiberincidentus, kiberapdraudējumus, kļūdas un neprecizitātes, un nepieciešamības gadījumā veiktu labojumus kiberdrošības jomā.

2. Kiberrisku pārvaldības noteikumi ir izstrādāti 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" 39.punktu.

3. Noteikumos 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, 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 ārpakalpojuma 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 ārpakalpojuma 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.

4. Kiberrisku pārvaldības noteikumi ir saistoši IKT resursu īpašniekiem, IKT tehnisko resursu turētājiem, Informācijas tehnoloģiju nodaļai un kiberdrošības pārvaldniekam.

I. Kiberrisku novērtēšanas metodika

5. Pašvaldības kiberrisku pārvaldība tiek veikta pēc sekojošiem soļiem hronoloģiskā secībā:

5.1. kiberrisku identificēšana.

5.2. kiberrisku novērtēšana.

5.3. kiberrisku vadīšana.

5.4. risku uzraudzība.

6. Kiberrisku vadības procesa ieviešanu, vadību, koordināciju un metodisko vadību veic Kiberdrošības pārvaldnieks, nepieciešamības gadījumā pieaicinot Pašvaldības vadītāju, attiecīgo IKT resursu īpašnieku, IKT tehnisko resursu turētāju, Pašvaldības struktūrvienību vadītājus un / vai atsevišķus Informācijas sistēmas lietotājus un / vai citus konsultantus.

7. Kiberdrošības pārvaldnieks sadarbībā ar Pašvaldības vadību un Nacionālo kiberdrošības centru nodrošina IKT resursu un informācijas sistēmu aktuālo kiberrisku novērtēšanu un pārvaldīšanu.

II. Kiberrisku identificēšana

8. Kiberdrošības pārvaldnieks kopīgā sanāksmē ar pieaicinātiem dalībniekiem, ņemot vērā kopējo dalībnieku kompetenci, zināšanas un pieredzi, veic Pašvaldības funkciju un uzdevumu izpildes procesa posmu izskatīšanu, identificējot tajos iespējamos kiberriskus.

9. Kiberdrošības pārvaldniekam ir pienākums augstāk minētās sanāksmes laikā apkopot identificētos kiberriskus, iekļaujot tos Kiberrisku novērtējuma dokumentā (1. Pielikums "Kiberrisku novērtējums").

III. Kiberrisku novērtēšana

10. Kiberdrošības pārvaldnieks kopā ar pieaicinātiem dalībniekiem arī veic šo kiberrisku novērtēšanu, nosakot kiberrisku rādītāju, kas veidojas no Varbūtības, Ietekmes un Pārvaldības novērtējuma punktu reizinājuma.

11. Varbūtība ir novērtējums par iespējamo situācijas (kiberapdraudējumu) iestāšanos noteiktā laika periodā. Novērtējuma punktu iedalījumu skat. tabulā zemāk:

Novērtējums (punktos)	Raksturojums
1	maz iespējams, ka šāda situācija (kiberapdraudējums) īstenosies
2	vidēji iespējams, ka šāda situācija (kiberapdraudējums) īstenosies
3	ļoti iespējams, ka šāda situācija (kiberapdraudējums) īstenosies

12. Ietekme ir novērtējums par iespējamās situācijas (draudu) iestāšanās būtiskumu noteiktā laika periodā. Novērtējuma punktu iedalījumu skat. tabulā zemāk:

Novērtējums (punktos)	Raksturojums
1	kiberapdraudējumam ir maza ietekme uz datu subjektu un / vai Pašvaldību
2	kiberapdraudējumam ir vidēja ietekme uz datu subjektu un / vai Pašvaldību
3	kiberapdraudējumam ir liela ietekme uz datu subjektu un / vai Pašvaldību

13. Pārvaldība ir novērtējums par esošo pasākuma kontroles mehānismu, kas ļauj līdz minimumam samazināt tās trūkumu negatīvo ietekmi uz Pašvaldību. Novērtējuma punktu iedalījumu skat. tabulā zemāk:

Novērtējums (punktos)	Raksturojums
1	Pašvaldībā ir definētas un ieviestas iekšējās kontroles augstākajā līmenī atbilstoši labākajai praksei
2	Pašvaldībā ir definētas un ieviestas iekšējās kontroles labā līmenī, tomēr vēl ir nepieciešams veikt atsevišķus uzlabojumus tās darbībai
3	Pašvaldībā ir definētas un ieviestas iekšējās kontroles vidējā līmenī, kurai ir nepieciešams būtiskus uzlabojumus tās darbībai.
4	Pašvaldībā ir definētas un ieviestas iekšējās kontroles sliktā līmenī vai tā nemaz nepastāv vispār.

14. Kiberdrošības pārvaldnieks Varbūtības, Ietekmes un Pārvaldības novērtējuma rādītājus apkopo un iekļauj Kiberrisku novērtējuma dokumentā (1.Pielikums "Kiberrisku novērtējums").

15. Jo lielāks ir Kiberrisku rādītājs, jo Kiberriska prioritāte ir augstāka, tādejādi, būtu nepieciešams papildus noteikt darbības un kontroles pasākumus kiberrisku mazināšanai un novēršanai.

16. Kiberriska rādītāja pieņemamais līmenis ir 6 (seši).

IV. Kiberrisku vadīšana

17. Kiberdrošības pārvaldnieks kopā ar pieaicinātiem dalībniekiem atbilstoši Kiberrisku novērtējuma dokumentā iekļautajiem kiberriskiem un to kiberrisku rādītājiem vienojas un nosaka no Pašvaldības puses ieteikumus attiecībā uz veicamajiem pasākumiem kiberrisku mazināšanai un novēršanai.

18. Kiberdrošības pārvaldnieks sagatavo Kiberrisku pārvaldības pasākumu plānu, tajā iekļaujot ieteikumus attiecībā uz veicamajiem pasākumiem kiberrisku mazināšanai un novēršanai, atbildīgiem darbiniekiem un ieteikumu izpildes termiņiem (2.Pielikums "Kiberrisku pārvaldības pasākumu plāns").

19. Kiberdrošības pārvaldnieks Kiberrisku novērtējuma dokumenti un Kiberrisku pārvaldības pasākumu plānu iesniedz Pašvaldības priekšsēdētājam apstiprināšanai.

V. Kiberrisku uzraudzība

20. Kiberrisku uzraudzību veic Kiberdrošības pārvaldnieks balstoties uz Pašvaldības vadības apstiprināto Kiberrisku pārvaldības pasākumu plānu.

21. Kiberdrošības pārvaldniekam ir pienākums informēt Pašvaldības priekšsēdētāju par Kiberrisku pārvaldības pasākumu plāna izpildi.

22. Kiberdrošības pārvaldnieks ne retāk kā reizi gadā veic atkārtotu kiberrisku identificēšanu, novērtēšanu un vadību. Nepieciešamības gadījumā, Pašvaldības priekšsēdētājs, IKT tehnisko resursu turētājs un / vai Kiberdrošības pārvaldnieks var ierosināt rīkot atkārtotu sanāksmi pirms augstāk minētā termiņa.

Novada domes priekšsēdētājs *(personiskais paraksts)* A.Adamovičs

1. PIELIKUMS
Kiberrisku pārvaldības noteikumi
Preiļu novada pašvaldības

PREIĻU NOVADA PAŠVALDĪBAS
KIBERRISKU NOVĒRTĒJUMS

Nr.	Kiberrisku uzskaitījums	Varbūtība	Ietekme	Pārvaldība	Risku rādītājs
1.					
2.					
3.					

2. PIELIKUMS
Preiļu novada pašvaldības
Kiberrisku pārvaldības noteikumi

PREIĻU NOVADA PAŠVALDĪBAS
KIBERRISKU PĀRVALDĪBAS PASĀKUMA PLĀNS

Nr.	Kiberrisku mazināšanas pasākuma apraksts	Termiņš	Atbildīgā amatpersona
1.			
2.			
3.			