

LATVIJAS REPUBLIKA

 **PRIEKUĻU NOVADA PAŠVALDĪBA**

Reģistrācijas Nr. 90000057511, Cēsu prospekts 5, Priekuļi, Priekuļu pagasts, Priekuļu novads, LV-4126

 www.priekuli.lv, tālr. 64107871, e-pasts: dome@priekulunovads.lv

**APSTIPRINĀTS**

Priekuļu novada domes

2020.gada 28.maija domes sēdē,

protokols Nr.10

**INFORMĀCIJAS SISTĒMAS DROŠĪBAS POLITIKA**

1. **Vispārīgie jautājumi**
2. Informācijas sistēmas drošības politika nosaka kārtību, kādā Priekuļu novada pašvaldība un tās iestādes (turpmāk – Pašvaldība) nodrošina pašvaldības izmantotās informācijas sistēmas aizsardzību pret ārējiem un iekšējiem riskiem un nodrošina informācijas sistēmas pieejamību, integritāti un konfidencialitāti saskaņā ar spēkā esošajiem normatīvajiem aktiem.
3. Informācijas sistēmas drošības politika attiecas uz visiem Pašvaldības |Informācijas sistēmu lietotājiem, kuriem ir pieeja kādai no valsts informāciju sistēmām (piemēram, Iedzīvotāju reģistram).
4. Politikā lietotie termini:
	1. **Informācijas sistēma** (turpmāk arī - IS) – strukturizēts informācijas tehnoloģiju un datu bāzu kopums, kuru lietojot tiek nodrošināta valsts funkciju izpildei nepieciešamās informācijas ierosināšana, radīšana, apkopošana, uzkrāšana, apstrādāšana, izmantošana un iznīcināšana.
	2. **Informācijas sistēmas lietotājs –** persona, kurai ir piešķirtas piekļuves tiesības informācijas sistēmās.
	3. **Datorsistēmu un datortīklu administrators** (turpmāk – Datortīklu administrators) – Pašvaldības vai ārpakalpojuma darbinieks, kurš Pašvaldības normatīvajos aktos noteiktā kārtībā veic nepieciešamos datortehnikas apkalpošanas darbus. Ārpakalpojuma gadījumā veicamo darbu apjomu un pienākumus nosaka ārpakalpojuma sniedzēja līguma nosacījumi.
	4. **Informācijas tehnoloģiju administrators** - Pašvaldības vai ārpakalpojuma darbinieks, kurš Pašvaldības normatīvajos aktos noteiktā kārtībā nodrošina IS atbalsta izveidi, uzturēšanu un koordinēšanu. Ārpakalpojuma gadījumā veicamo darbu apjomu un pienākumus nosaka ārpakalpojuma sniedzēja līguma nosacījumi.
5. Informācijas sistēmas drošības politika ir izstrādāta saskaņā ar Informācijas tehnoloģiju drošības likumu, Valsts informācijas sistēmu likumu, Fizisko personu datu apstrādes likumu, 2015.gada 28.jūlija Ministru kabineta noteikumu Nr.442 „[Kārtība, kādā tiek nodrošināta informācijas un komunikācijas](http://likumi.lv/ta/id/275671-kartiba-kada-tiek-nodrosinata-informacijas-un-komunikacijas-tehnologiju-sistemu-atbilstiba-minimalajam-drosibas-prasibam) [tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām](http://likumi.lv/ta/id/275671-kartiba-kada-tiek-nodrosinata-informacijas-un-komunikacijas-tehnologiju-sistemu-atbilstiba-minimalajam-drosibas-prasibam)” 8.punktu un citu normatīvo aktu prasībām, kā arī ievērojot Latvijas standartu LVS ISO/IEC 27001:2013 “Informācijas tehnoloģija. Drošības paņēmieni. Informācijas drošības pārvaldības sistēmas. Prasības”.
6. **Informācijas sistēmas drošības politikas mērķi un pamatnostādnes**
7. Pašvaldības pienākums ir nodrošināt, lai to rīcībā esošā informācija tiktu apstrādāta, glabāta un pārvaldīta droši un pārbaudāmi, sniedzot tās lietotājiem skaidri noteiktas prasības informācijas sistēmas iekārtu un resursu izmantošanā, un nodrošinot Informācijas sistēmas aizsardzību no ārējiem un iekšējiem, apzinātiem un nejaušiem apdraudējumiem.
8. Informācijas sistēmas drošības politika attiecas uz visiem Pašvaldības Informācijas sistēmu lietotājiem, kuri veic darbības ar informācijas resursiem (piemēram, informācijas sistēmām, informāciju, kas tiek saņemta, apstrādāta, ievadīta, pārsūtīta vai uzglabāta) un tehniskajiem resursiem (piemēram, datoru sistēmām, datoru tīkliem), t.sk.:
	1. Pašvaldības darbiniekiem, amatpersonām un personām, ar kurām nodarbinātas līgumattiecības;
	2. Informācijas sistēmas lietotājiem, kuri ir noslēguši līgumu ar pašvaldību par datu lietošanu vai kuri uz pieprasījuma pamata saņem datus no pašvaldības izmantotām informācijas sistēmām.
	3. ārpakalpojumu sniedzējiem vai konsultantiem, kuri strādā Pašvaldības labā.
9. Informācijas sistēmas lietotājs, kas ir nodarbināts Pašvaldībā un ir Pašvaldības darbinieks (pilna darba laika, nepilnas slodzes un līgumdarbiniekiem), atbild par drošības politikas nosacījumu un prasību ievērošanu, kas ir minēti šādos dokumentos:
	1. Informācijas sistēmas drošības politikā;
	2. Informācijas sistēmas lietošanas noteikumos.
10. Informācijas sistēmu lietotājs par iepazīšanos ar augstāk minētajiem dokumentiem un to ievērošanu paraksta 1.Pielikumu “Informācijas sistēmas lietotāja apliecinājums par “Informācijas sistēmas drošības politikas” prasību ievērošanu”.
11. Datortīklu un informācijas tehnoloģiju administrators atbild par drošības politikas nosacījumu un prasību ievērošanu, kas ir minēti šādos dokumentos:
	1. Informācijas sistēmas drošības politikā;
	2. Informācijas sistēmas lietošanas noteikumos;
	3. Informācijas sistēmas drošības noteikumos;
	4. Informācijas sistēmas drošības riska pārvaldības plānā;
	5. Informācijas sistēmu atjaunošanas plānā.
12. Pašvaldības iestāžu un struktūrvienību vadītāji ir atbildīgi par viņu pakļautībā vai uzraudzībā esošajiem Informācijas sistēmu lietotājiem. Pašvaldības iestāžu un struktūrvienību vadītāji nodrošina, ka personāls, uz kuru šī politika attiecas daļēji vai pilnā apmērā, ir informēts par politikas esamību un pilda savus darba pienākumus atbilstoši politikas nostādnēm.
13. Informācijas sistēmas drošība tiek nodrošināta šādu mērķu realizācijai:

11.1. nodrošinātu informācijas pieejamību;

11.2. nodrošinātu informācijas integritāti;

11.3. nodrošinātu informācijas konfidencialitāti;

11.4. aizsargātu sistēmas informācijas resursus;

11.5. aizsargātu sistēmas tehniskos resursus;

11.6. noteiktu sistēmas drošības apdraudējumu;

11.7. novērtētu sistēmas drošības risku;

11.8. atklātu sistēmas drošības incidentu;

11.9. atjaunotu sistēmas darbību pēc sistēmas drošības incidenta.

1. Pašvaldībā izmantotajām informācijas sistēmām ir šādas drošības (pieejamības, integritātes un konfidencialitātes) klases:

12.1. C pieejamības klase - sistēmas nodrošinātā pakalpojuma neplānots pārtraukums sistēmas paredzētajā darba laikā drīkst būt ilgāks par 24 stundām mēnesī (summāri);

12.2. B integritātes klase - sistēmas nodrošinātā pakalpojuma neplānotam pārtraukumam sistēmas paredzētajā darba laikā jābūt ne lielākam par 24 stundām (summāri) mēnesī, bet tas pieļaujams lielāks par četrām stundām (summāri) mēnesī;

12.3 A konfidencialitātes klase - sistēmas nodrošinātā pakalpojuma neplānotam pārtraukumam sistēmas paredzētajā darba laikā jābūt ne lielākam par četrām stundām mēnesī (summāri), kā arī sistēmā tiek apstrādāti sensitīvi personas dati vai sistēmā glabātās informācijas neatļauta izpaušana vai noplūde var radīt smagākas sekas nekā kaitējums Iestādes, citu Iestāžu vai Latvijas Republikas reputācijai.

1. Informācijas tehnoloģiju drošības pārvaldību un Informācijas sistēmas drošības politikas koordināciju pašvaldībā veic Datortīklu administrators.
2. **Informācijas sistēmas drošības organizācija**
3. Informācijas sistēmas drošības organizatoriskās struktūras pamatu veido Informācijas tehnoloģiju administrators un Informācijas sistēmas lietotāji.
4. Datortīklu administrators nodrošina informācijas sistēmas drošības politikas realizāciju, kā arī veic šādas darbības:

15.1. aktualizē drošības politiku, izstrādā ar informācijas sistēmu drošības saistīto iekšējo normatīvo aktu projektus un veic to koordināciju.

15.2. aktualizē Informācijas sistēmas drošības politiku un to saistītos dokumentus vismaz vienu reizi gadā, kā arī šādos gadījumos:

15.2.1. ja izmaiņas informācijas sistēmā var ietekmēt sistēmas drošību;

15.2.2. ja mainījušies vai ir atklāti jauni informācijas sistēmas drošības apdraudējumi;

15.2.3. ja pēkšņi pieaug informācijas sistēmas drošības incidentu skaits vai ir noticis nozīmīgs sistēmas drošības incidents;

15.2.4. ja izmaiņas Pašvaldības organizatoriskajā struktūrā skar informācijas sistēmas drošības vadības organizāciju;

15.2.5. ja izdarīti grozījumi normatīvajos aktos, kas regulē informācijas sistēmas darbību.

1. Informācijas tehnoloģiju administrators:
	1. nodrošina informācijas sistēmās izmantojamās informācijas racionālu un pareizu izmantošanu;
	2. izskata informācijas sistēmas lietotāju tiesību piešķiršanas un izmaiņu veikšanas pieteikumu autorizāciju saskaņā ar Informācijas sistēmas lietošanas noteikumiem;
	3. piedalās Risku vadības procesā saskaņā ar Informācijas drošības riska pārvaldības plānu;
	4. nodrošina atbilstošu atbalstu, palīdzību un konsultāciju sniegšanu personālam, lai tas varētu pildīt savus pienākumus atbilstoši šīs politikas prasībām;
2. Pašvaldības izpilddirektors vai Administratīvās nodaļas vadītājs, Datortīklu administratora vai Informācijas tehnoloģiju administratora prombūtnes gadījumā, ja nepieciešams, tad ieceļ tā pienākumu aizvietotāju.
3. Datortīklu administrators:
	1. nodrošina tehnisko resursu racionālu un pareizu izmantošanu;
	2. nodrošina tehnisko resursu fiziskās un loģiskās aizsardzības pasākumus saskaņā ar Informācijas sistēmas drošības noteikumiem;
	3. nodrošina nepieciešamo tehnisko risinājumu attiecīgajam informācijas resursam;
	4. veic Risku vadības procesa koordināciju Pašvaldībā saskaņā ar Informācijas drošības riska pārvaldības plānu;
	5. izmeklē informācijas drošības incidentus;
	6. veic regulāras pārbaudes, lai pārliecinātos, ka tiek ievērotas Informācijas sistēmas drošības politikas un to saistošo dokumentu prasības;
	7. nodrošina informācijas sistēmu atjaunošanas procedūras, ja tehnoloģiskie resursi ir bojāti un informācijas sistēmu funkcionēšana traucēta vai neiespējama saskaņā ar Informācijas sistēmas drošības noteikumiem un Informācijas sistēmu atjaunošanas plānu;
	8. nodrošina atbilstošu atbalstu, palīdzību un konsultāciju sniegšanu personālam, lai tas varētu pildīt savus pienākumus atbilstoši Informācijas sistēmas drošības politikas prasībām.
4. Informācijas sistēmas lietotāja pienākums ir racionāli un lietderīgi izmantot informācijas sistēmas un to datus sava darbu pienākumu veikšanai.
5. **Informācijas resursu klasifikācija**
6. Visiem Pašvaldības informācijas resursiem (t.sk., darba stacijām, serveriem, tīkla iekārtām un programmatūrai) ir jābūt uzskaitītiem un reģistrētiem, kā arī Informācijas sistēmas datiem ir jābūt klasificētiem.
7. Pašvaldības informācijas resursu klasificēšana tiek veikta atbilstoši Informācijas atklātības likumam.
	1. **Informācijas resursu riska analīze**
8. Informācijas resursu riska analīzes mērķis ir nodrošināt atbilstošu Informācijas sistēmu vadību un kontroles sistēmas darbības efektivitāti, lai atklātu un novērstu kļūdas un neprecizitātes, un nepieciešamības gadījumā veiktu drošības labojumus informāciju sistēmās.
9. Pašvaldības informācijas resursu riska analīze tiek veikta atbilstoši Informācijas sistēmas drošības riska pārvaldības plānam.
10. **Informācijas resursu loģiskā drošība**
11. Pašvaldības Informācijas sistēmas lietotājiem pieejas tiesību piešķiršana, izmainīšana un anulēšana tiek veikta atbilstoši Informācijas sistēmas lietošanas noteikumiem un Informācijas sistēmas drošības noteikumiem.
12. Informācijas sistēmas lietotāju pienākumi attiecībā uz informācijas resursu lietošanu, interneta izmantošanu un tehnisko resursu fizisko drošību ir iekļauti Informācijas sistēmas lietošanas noteikumos.
13. Pašvaldības datortīklu, serveru un to saistīto iekārtu uzturēšanu un administrēšanu, kā arī Informācijas sistēmas lietotāju datoru uzstādīšanu un administrēšanu veic Datortīklu administrators, kura pienākumi ir iekļauti Informācijas sistēmas drošības noteikumos.

1. **Tehnisko resursu fiziskā drošība**
2. Pašvaldības datorsistēmas un tehnika (t.sk. datortīkli, programmatūra, informācijas sistēmas, serveri, datori) tiek aizsargāta ar piemērotu fizisko, tehnisko, organizatorisko un vides kontroļu kopumu.
3. Serveri un datori tiek novietoti aizslēgtās telpās vai serveru skapjos, kurās pieeja ir tikai atbilstošām personām, nodrošinot fizisko aizsardzību no trešajām personām pret piekļūšanu šiem resursiem. Par serveru fizisko drošību Pašvaldībā atbild Datortīklu administrators, savukārt par atbilstošo datoru fizisko drošību atbild attiecīgais Informācijas sistēmas lietotājs.
4. Informācijas sistēmas lietotāju pienākumi attiecībā uz tehnisko resursu fizisko drošību ir iekļauti Informācijas sistēmas lietošanas noteikumos.
5. **Darbības nepārtrauktības nodrošināšana**
6. Pašvaldības iekšējām informācijas sistēmām, serveriem, tīkla iekārtām un elektroniskā veidā saglabātai informācijai regulāras rezerves kopijas veidošanu nodrošina Datortīklu administrators atbilstoši Informācijas sistēmas drošības noteikumiem.
7. 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.
8. Par visām avārijas situācijām (t.sk. ugunsgrēku, plūdiem, nelaimes gadījumiem utt.) Informācijas sistēmas lietotājiem, Datortīklu un Informācijas tehnoloģiju administratoram ir nekavējoši jāpaziņo Pašvaldības izpilddirektoram.
9. Informācijas sistēmas drošības politika stājas spēkā tās apstiprināšanas dienā.

Pielikumā: Priekuļu novada pašvaldības Informācijas sistēmas lietotāja apliecinājums par “Informācijas sistēmas drošības politikas” prasību ievērošanu uz 1 lpp.

Domes priekšsēdētāja (paraksts) Elīna Stapulone

Pielikums

“Priekuļu novada pašvaldības

Informācijas sistēmas drošības politika”

**INFORMĀCIJAS SISTĒMAS LIETOTĀJA APLIECINĀJUMS**

**PAR “INFORMĀCIJAS SISTĒMAS DROŠĪBAS POLITIKAS” PRASĪBU IEVĒROŠANU**

Ar šo es apliecinu:

1. Esmu iepazinies(-usies), izprotu un apņemos ievērot Informācijas drošības politikas nosacījumus un prasības ievērošanu, kas ir minēti šādos dokumentos:

1.1. Informācijas sistēmas drošības politikā;

1.2. Informācijas sistēmas lietošanas noteikumos;

1. Apņemos neizmantot konfidenciālu informāciju, kas saņemta no Priekuļu novada pašvaldības, savu vai trešo personu interesēs, kā arī apņemos ievērot Fizisko personu datu aizsardzības likuma un Informācijas atklātības likuma prasības.
2. Es piekrītu, ka pārtraucot darba (līguma) attiecības ar Priekuļu novada pašvaldību jebkādu iemeslu dēļ, es nekavējoties nodošu Priekuļu novada pašvaldībai manā rīcībā esošo 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.
3. Apņemos saglabāt informācijas konfidencialitāti arī pēc darba (līguma izpildes) tiesisko attiecību izbeigšanas.

|  |  |  |  |
| --- | --- | --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Struktūrvienība un amats | /Paraksts/ | /Paraksta atšifrējums/ | Datums |