

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 NOTEIKUMI**

1. **Vispārīgie jautājumi**
2. Informācijas sistēmas drošības noteikumi ietver kārtību, kādā Priekuļu novada pašvaldības un tās iestādes (turpmāk – Pašvaldība) nodrošina Pašvaldībā izmantoto informācijas sistēmu aizsardzību.
3. Noteikumos lietotie termini:
4. **Informācijas sistēma (turpmāk - 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.
5. **Priekuļu novada pašvaldība** – institūcija, kas normatīvajos aktos noteiktajā kārtībā organizē un vada informācijas sistēmu darbību.
6. **Informācijas sistēmas lietotājs –** persona, kurai ir piešķirtas piekļuves tiesības informācijas sistēmās.
7. **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.
8. **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.
9. Informācijas sistēmas drošības noteikumi ir saistoši Informāciju sistēmu lietotājiem, Datortīklu administratoram un Informācijas tehnoloģiju administratoram. Datortīkla un/vai Informācijas tehnoloģiju administratora funkcijas pilnībā vai daļēji var tikt nodotas ārpakalpojumā. Ja tās tiek nodotas daļēji, tad Pašvaldībai ir pienākums parūpēties par pārējo noteikumu ievērošanu citā veidā, piemēram, deleģējot šos pienākumus citam Pašvaldības darbiniekam. Nododot Datortīkla un/vai Informācijas tehnoloģiju administratora funkcijas ārpakalpojumā, tiek nodotas arī atbilstošas pilnvaras.
10. **Informācijas loģiskā aizsardzība**
11. Pašvaldības datortīklu, serveru un to saistīto iekārtu uzturēšanu un administrēšanu, kā arī Informācijas sistēmas lietotāju datoru uzstādīšanu un administrēšanu veic Datortīklu administrators.
12. Datortīklu administrators ir atbildīgs par piemērotu un efektīvu aizsardzības sistēmas izveidi, lietojot atbilstošu maršrutēšanas un ugunsmūra sistēmu, kā arī nodrošinot pretvīrusu programmatūras uzstādīšanu un uzturēšanu uz Pašvaldības serveriem un datoriem.
13. Datortīklu administratoram ir pienākums regulāri sekot līdzi tīkla ugunsmūra paziņojumiem un reaģēt uz vīrusu uzbrukumiem, nodrošinot konstatēto vīrusu iznīcināšanu.
14. Gadījumā, ja tiek konstatēti ielaušanās mēģinājumi vai būtiski incidenti, Datortīklu administrators veic to reģistrēšanu un izmeklēšanu, kā arī par tās rezultātiem informē Drošības incidentu novēršanas institūciju (CERT.lv).
15. Datortīklu administrators datorvīrusu darbības novēršanai nodrošina antivīrusu programmu automātisku atjauninājumu saņemšanu un vīrusu bloķēšanu un ja nepieciešams, tad pārraudzību, lai pārliecinātos par antivīrusu programmatūras darbību un jaunāko vīrusu definīciju failu esamību.
16. Informācijas tehnoloģiju administrators pēc priekšsēdētāja, izpilddirektora, struktūrvienības, iestāžu vadītāja piekrišanas izveido, veic izmaiņas un anulē Informācijas sistēmas lietotāju tiesības.
17. Informācijas sistēmas lietotājiem, kuri ir Pašvaldības darbinieki, autorizēšanās rekvizītus (lietotājvārdu un paroli) izsniedz Informācijas tehnoloģiju administrators vai arī atbilstošās informācijas sistēmas pakalpojumu sniedzējs.
18. Ja Informācijas sistēmas lietotājs, kas ir Pašvaldības darbinieks, ir aizmirsis savu lietotāja paroli, par to Informācijas sistēmas lietotājs personīgi, telefoniski vai izveidojot pieteikumu iekšējā IT atbalsta sistēmā, informē Informācijas tehnoloģiju administratoru. Informācijas tehnoloģiju administrators identificē atbilstošo informācijas sistēmas lietotāju, izveido jaunu paroli un izsniedz atbilstošajam Informācijas sistēmas lietotājam. Savukārt ārpakalpojumu Informācijas sistēmu lietotājiem jauno paroli izveido atbilstošās informācijas sistēmas pakalpojumu sniedzējs, saskaņojot ar tās administratoru.
19. Paroles politika ir noteikta Pašvaldības Informācijas sistēmas lietošanas noteikumos, taču ārpakalpojumu informāciju sistēmās paroļu politiku nosaka ārpakalpojuma sniedzējs. Informācijas sistēmas lietotāja parole ievades laikā nedrīkst tikt atspoguļota.
20. Datortīklu administrators nodrošina, lai tiktu veidoti un saglabāti auditācijas pieraksti vismaz 6 mēnešus datortīkla maršrutētāju autorizācijai un par informācijas sistēmām, kuras ir izvietotas uz Pašvaldības resursiem vai kuras ir Pašvaldības īpašumā. Auditācijas pierakstos iekļauj visus veiksmīgus un neveiksmīgus pieslēgšanās gadījumus, to datumus un laiku, kā arī šo lietotāju (t.sk. administratora) vārdus vai citu autentifikācijas līdzekli pēc kura var identificēt lietotāju.
21. Datortīklu administrators nodrošina auditācijas pierakstu integritāti un regulāri veido auditācijas pierakstu datu rezerves kopijas.
22. Pašvaldība pirms jaunas informācijas sistēmas pieņemšanas ekspluatācijā pārliecinās vai tā atbilst Ministru kabineta 28.07.2015. Noteikumu Nr. 442 “Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām” (turpmāk - MK 422) drošības prasībām.
23. Datortīklu administrators veic auditācijas pierakstu analīzi šādos gadījumos:

16.1. Informācijas sistēmas lietotāja atkārtota neveiksmīga pieslēgšanās kādai no iekšējām informācijas sistēmām;

16.2. Informācijas sistēmas lietotāja pieslēgšanās kādai no iekšējām informācijas sistēmām ārpus darba laika, ja šāda situācija nav pieļaujama;

16.3. mēģinājumi piekļūt informācijas resursiem, kuriem Datortīklu administrators nav pilnvarojis piekļūt;

16.4. atkārtoti mēģinājumi lietot lietotāja rekvizītus, kuri jau ir atcelti.

1. Datortīklu administratoram ir pienākums informēt Pašvaldības izpilddirektoru par nepieciešamās programmatūras iegādi, kā arī pēc nepieciešamības sniegt arī priekšlikumus un konsultācijas saistībā ar jaunas programmatūras iegādi.
2. Reģistru par iegādātiem un uzstādītiem informācijas tehniskajiem resursiem (t.sk. par darba stacijām, serveriem un tīkla iekārtām) veic Pašvaldības Finanšu un grāmatvedības nodaļa. Vismaz reizi gadā tiek veikta šo resursu inventarizācija, pārliecinoties, ka šis reģistrs ir korekts.
3. Datortīklu vai informāciju tehnoloģiju administrators, tā pilnvarota persona vai ārējs konsultants nodrošina Pašvaldības Informācijas sistēmas lietotāju informēšanu un iepazīstināšanu informācijas sistēmu drošības jomā, izskaidrojot tiem Informācijas sistēmas drošības politikas pamatprincipus un būtiskākos drošības pasākumus datu drošībai.
4. Pašvaldībā tiek nodrošināta datortīkla / iekšējo informācijas sistēmu atbilstība šādām aizsardzības prasībām:

20.1. iekšējo datortīklu nodala no interneta ar ugunsmūra palīdzību;

20.2. ja tehniskais risinājums to pieļauj, nodrošina datortīkla / informācijas sistēmu pretvīrusa aizsardzību;

20.3. izmantojot tikai šifrētu VPN pieslēgumu un ja iespējams, tad daudzfaktoru autentifikāciju, nodrošina attālinātas piekļuves ierobežošanu datortīkla / informācijas sistēmu administrēšanai;

20.4. informācijas sistēmu testēšanai organizē uz servera loģiskā vai fiziskā līmenī individuāli nodalītu testēšanas vidi;

20.5. piekļuvi datortīkla / informācijas sistēmu administrēšanas un pārvaldības funkcionalitātei nodrošina tikai tām personām, kurām datortīkla / informācijas sistēmu esošā informācija atbilstošā apmērā ir nepieciešama darba pienākumu veikšanai;

20.6. informācijas sistēmas lietotāji, kas veic administrēšanas darbu, izmanto īpašus lietotāju kontus (piemēram, sistēmas administratora konts), kas netiek izmantoti ikdienas darbību veikšanai;

20.7. informāciju sistēmās vēlams nodrošināt, lai katrs lietotāja konts ir saistīts ar konkrētu fizisko personu;

20.8. informācijas sistēmu lietotāja paroles aizliegts elektroniski glabāt un transportēt nešifrētā veidā, arī lietotāja autentifikācijas procesa ietvaros;

20.9. informācijas sistēmu lietotāja parole ievadīšanas brīdī lietotājam netiek attēlota;

20.10. informācijas sistēmu lietotāja parole, kas nosūtīta publiskā datu pārraides tīklā nešifrētā veidā, ir lietojama tikai vienu reizi un derīga ne ilgāk kā 72 stundas pēc tās nosūtīšanas;

20.11. informācijas sistēmās un pārlūkprogrammās nav pieļaujama funkcionalitāte, kas atļauj sistēmas lietotājam saglabāt savu paroli tā, lai tā turpmākajās pieslēgšanas reizēs nav jāievada;

20.12. iekārtām, tai skaitā infrastruktūras iekārtām, kas nodrošina informācijas sistēmu funkcionēšanu, netiek izmantotas noklusējuma (ražotāja vai izplatītāja uzstādītās) paroles, piemēram, (admin:admin);

20.13. tiek nodrošināta informācijas sistēmu auditācijas pierakstu (turpmāk – sistēmas pieraksti) veidošana un uzglabāšana vismaz 6 mēnešus pēc ieraksta izdarīšanas;

20.14. informācijas sistēmām, operētājsistēmām un tīkla iekārtām, iespēju robežās, nodrošināt jaunāko pieejamo programmatūras atjauninājumu uzstādīšanu, iepriekš rūpīgi izvērtējot to nepieciešamību;

20.15. visās Pašvaldības valdījumā esošajās galalietotāju iekārtās, kas ikdienā tiek izmantotas, lai pieslēgtos kādai no informācijas sistēmām, jābūt iekļautai pretvīrusu funkcionalitātei;

20.16. informācijas sistēmu lietotāju funkcionalitātei ir jābūt izpildāmai tikai ar pašām nepieciešamākajām tiesībām, atbilstoši darba pienākumu veikšanai, visu pārējo bloķējot;

20.17. piecas secīgas reizes nepareizi ievadot informācijas sistēmu lietotāja konta paroli, šis konts (izņemot sistēmas administratora kontu) nekavējoties tiek bloķēts;

20.18. ar informācijas sistēmu administratora kontu piekļūt iekšējām sistēmām, izmantojot iekārtas, kas atrodas ārpus Pašvaldības telpām, kā arī iekārtas, kas neatrodas Pašvaldības valdījumā, iespējams, tikai izmantojot šifrētu VPN savienojumu;

20.19. fiziski piekļūt serveru skapjos izvietotajām iekārtām, kas nodrošina informācijas sistēmu darbību, atļauts vienīgi Pašvaldības pilnvarotām personām;

20.20. Pašvaldības iekšēji izstrādātajām informācijas sistēmām lietotājiem redzamie kļūdu paziņojumi satur tikai minimāli nepieciešamo informāciju, lai sistēmas lietotājs pašrocīgi vai ar sistēmas atbalsta personāla palīdzību atrisinātu kļūdu;

20.21. plūsma starp informācijas sistēmu un tās lietotājiem, kā arī starp informācijas sistēmu un citām sistēmām tiek kontrolēta, izmantojot ugunsmūri;

20.22. datortīkla servisi (porti), kas netiek izmantoti kādas informācijas sistēmas darbības nodrošināšanai, ir atslēgti;

20.23. veicot jaunas informācijas sistēmas izstrādi un testēšanu, nav pieļaujams radīt apdraudējumu risku citām serverī glabātām sistēmām vai datiem;

1. Pašvaldība nodrošina, ka vismaz reizi gadā Datortīklu un informāciju tehnoloģiju administrators apmeklē nepieciešamās apmācības informācijas tehnoloģiju drošības un attīstības jautājumos.
2. Pašvaldība nodrošina, ka ne retāk kā reizi gadā jāveic institūcijas darbinieku, kuri strādā ar kādu no informācijas sistēmām, instruktāža informācijas tehnoloģiju drošības jautājumos.
3. **Informācijas fiziskā aizsardzība**
4. Informācijas sistēmu serveri, datortīkls un to saistītais aprīkojums tiek ekspluatēts ierobežotas pieejas serveru skapjos, kuriem iespēja piekļūt ir Datortīklu un Informācijas tehnoloģiju administratoram vai izpilddirektoram, nodrošinot aizsardzību pret neautorizētu personu iespēju serverus u.c. iekārtas izslēgt un nesankcionēti mainīt to konfigurāciju.
5. Telpas, kurās atrodas serveru skapji ir aprīkotas ar:

24.1. ugunsgrēka signalizācijas iekārtu;

24.2. ugunsdzēšamo aparātu;

24.3. gaisa kondicionēšanas iekārtu;

24.4. nepārtrauktās barošanas avotu (UPS);

24.5. apsardzes signalizāciju.

1. Nepiederošas personas, t.sk. ārpakalpojumu sniedzēji, serveru telpās drīkst uzturēties tikai Datortīklu administratora, Informācijas tehnoloģiju administratora vai izpilddirektora klātbūtnē.
2. Pazūdot elektrībai, Datortīklu administratoram ir jānoskaidro, cik ilgā laikā elektrības pieslēgums varētu atjaunoties un ja nepieciešams, tad nodrošināt pieslēgumu no cita enerģijas avota vai arī, ja tas nav iespējams un serveriem nav nodrošināta izslēgšanās automātiski, uzsākt manuālu serveru izslēgšanu.
3. Datu nesēju (CD, DVD, USB Flash, ārējais cietais disks vai tml.) fizisko aizsardzību nodrošina katrs Informācijas sistēmas lietotājs, nodrošinot, ka tie tiek glabāti drošās vietās, lai novērstu jebkādu nepilnvaroto personu piekļuvi pie tiem.
4. **Ārpakalpojumu iesaiste**
5. Ja Pašvaldība informācijas sistēmas uzturēšanai slēdz ārpakalpojuma līgumu ar pakalpojuma sniedzēju, līguma izpildi uzrauga atbildīgā persona un līgumā iekļauj vismaz šādas drošības prasības:

28.1. saņemamā ārpakalpojuma aprakstu;

28.2. precīzas prasības attiecībā uz ārpakalpojuma apjomu un kvalitāti;

28.3. Pašvaldības un ārpakalpojuma sniedzēja tiesības un pienākumus, tai skaitā:

28.3.1. Pašvaldības tiesības pastāvīgi uzraudzīt ārpakalpojuma sniegšanas kvalitāti;

28.3.2. Pašvaldības tiesības dot ārpakalpojuma sniedzējam obligāti izpildāmus norādījumus jautājumos, kas saistīti ar ārpakalpojuma godprātīgu, kvalitatīvu, savlaicīgu un normatīvajiem aktiem atbilstošu izpildi;

28.3.3. Pašvaldības tiesības iesniegt ārpakalpojuma sniedzējam pamatotu rakstisku pieprasījumu nekavējoties izbeigt ārpakalpojuma līgumu, ja Pašvaldība konstatējusi, ka ārpakalpojumu sniedzējs nepilda ārpakalpojuma līgumā noteiktās prasības attiecībā uz ārpakalpojuma apjomu vai kvalitāti;

28.3.4. iekļaujot pušu atbildību, atbilstoši jaunās vispārējās datu regulas prasībām, nodrošinot, ka datu saņēmējs/uzglabātājs uzņemas pilnu atbildību par personu datu drošību un apstrādi;

28.4. nepieciešamās izmaiņas lietotāju kontos ir piesakāmas caur ne vairāk kā divām atbildīgajām personām, lai kādas atbildīgās personas atvaļinājuma vai slimības gadījumā būtu nodrošināts šīs personas aizvietotājs.

1. Ja Pašvaldība uzsāk iepirkumu par esošas sistēmas uzlabojumiem, tā nodrošina, ka atbilstošās drošības prasības tiek iekļautas iepirkuma specifikācijā.
2. Ja Pašvaldība uzsāk iepirkumu par jaunas sistēmas izstrādi, tā iepirkuma specifikācijā iekļauj prasības, paredzot:

30.1. noteiktu sistēmas uzturēšanas un atbalsta nodrošināšanas (tai skaitā informācijas sistēmas drošības nepilnību novēršanas) laikposmu;

30.2. sistēmas datorprogrammu pirmkoda un tā izmantošanas tiesību nodošanu Pašvaldībai ne vēlāk kā pēc noteiktā laikposma beigām, kā arī pēc katru izmaiņu vai uzlabojumu veikšanas tajā;

30.3. iespēju noteiktajā laikposmā turpināt informācijas sistēmas ekspluatēšanu ar sistēmas funkcionēšanai obligāti nepieciešamā programmnodrošinājuma (piemēram, operētājsistēma, datubāžu vadības sistēma, interpretators) jaunākām versijām.

1. **Rezerves kopiju veidošanas kārtība**
2. Datortīklu administrators nodrošina Pašvaldības informācijas resursu rezerves kopiju veidošanu tām informācijas sistēmām / resursiem, kas ir izvietoti uz Pašvaldības serveriem / darba stacijām.
3. Rezerves kopijas glabā attālināti no oriģinālajiem datiem, lai novērstu oriģināla un kopijas vienlaicīgas bojāejas iespēju liela apjoma negadījuma situācijā.
4. Datortīklu administrators nosaka vietu, kur tiks glabātas rezerves kopijas.
5. Datortīklu administrators nodrošina Pašvaldības informācijas resursu atjaunošanu no rezerves kopijām.
6. Datortīklu administratoram ir pienākums vismaz reizi gadā veikt pārbaudi par iekšējo informācijas sistēmu atjaunošanas iespējām no rezerves kopijām.
7. **Elektronisko datu nesēju iznīcināšanas procedūra**
8. Pašvaldības darbinieki datu nesējus, kuri satur fiziskas personas datus un kuri paredzēti iznīcināšanai, nogādā Datortīklu administratoram. Datortīklu administrators nodrošina minēto datu nesēju drošu iznīcināšanu šādā kārtībā:

36.1. CD, BlueRay vai DVD matricas tiek iznīcinātas speciālā griezējā, sasmalcinot tās tā, ka nav iespējams atjaunot;

36.2. USB un SD atmiņu kartes atkārtotai lietošanai tiek pārrakstītas ar „0” un „1”, vai - ar defektiem - tiek fiziski iznīcinātas;

36.3. Datoru cietie diski (gan iekšējie, gan ārējie) tiek formatēti un pēc tam pārrakstīti ar „0” un „1” vai - ar defektiem - tiek fiziski iznīcināti.

37. Noteikumi stājas spēkā to apstiprināšanas dienā.

Domes priekšsēdētāja (paraksts) Elīna Stapulone