



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 Informācijas sistēmas lietošanas 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. Informācijas sistēmas lietošanas noteikumi (turpmāk tekstā Noteikumi) nosaka Preiļu novada pašvaldības (turpmāk – Pašvaldība) darbinieku pienākumus un prasības Pašvaldības izmantotās informācijas un komunikācijas tehnoloģijas (turpmāk - IKT) resursu, informācijas sistēmas un interneta lietošanai, kā arī nosaka kārtību, kādā tiek veikta Pašvaldības izmantotās informācijas sistēmas lietotāju pieejas tiesību piešķiršana, izmaiņas un anulēšana.

2. 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" 53.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,

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. **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.
 - 3.11. **IKT resursu īpašnieks** - persona, kuras kompetencē atrodas konkrētas Informācijas sistēmas darbības procesa organizēšana.
 - 3.12. **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.
 - 3.13. **Informācijas sistēmas lietotājs** – persona, kurai ir piešķirtas piekļuves tiesības Pašvaldības IKT resursiem un / vai informācijas sistēmām.

4. Informācijas sistēmas lietošanas noteikumi ir saistoši visiem Pašvaldības darbiniekiem (pilna darba laika, nepilnas slodzes un līgumdarbiniekiem), kuri ir nodarbināti Pašvaldībā un kam ir piekļuve kādai no Pašvaldības informācijas sistēmām.

5. Katra Informācijas sistēmas lietotāja pienākums ir iepazīties ar šiem noteikumiem un ievērot tos ikdienas darbā.

I. Informācijas sistēmas lietotāju administrēšanas kārtība

6. Lai izveidotu informācijas sistēmas lietotāju pieejas tiesības vai veiktu izmaiņas tajās, Pašvaldības darbinieka tiešais vadītājs raksta Informācijas sistēmu tiesību pieprasījumu, ko nosūta uz IT daļas e-pastu: itd@preili.lv.

7. Ja IKT resursu īpašniekam nav piešķirtas lietotāja tiesības attiecīgajā informācijas sistēmā, kas ļautu izveidot vai mainīt lietotāju tiesības darbiniekiem, un IKT resursu īpašnieks piekrīt piešķirt vai mainīt lietotāju tiesības atbilstoši Informācijas sistēmu tiesību pieprasījumam, IKT resursu īpašnieks šo pieprasījumu pārsūta izpildei IT daļai.

8. Gadījumos, kad ir nepieciešamas lietotāju tiesības kādiem no informācijas resursiem vai informācijas sistēmām, kas nav minētas Informācijas sistēmu sarakstā, Informācijas sistēmu tiesību pieprasījumu nosūta IT daļai.

9. Informācijas sistēmas lietotāju pieejas tiesības tiek piešķirtas Pašvaldības darbiniekiem atbilstoši katra atsevišķā darbinieka noteiktajiem darba pienākumiem un specifikai, ievērojot principu “nepieciešamība zināt” un “mazāko privilēģiju” principu, nodrošinot tikai minimāli nepieciešamo piekļuves līmeni informācijas sistēmas lietotāja kontam.

10. Informācijas sistēmas lietotāju pieejas tiesību piešķiršana Pašvaldības informācijas resursiem personām, kuras nav Pašvaldības darbinieki, notiek tikai atsevišķos gadījumos pēc Pašvaldības Informācijas tehnoloģiju daļas vadītāja pieprasījuma (piemēram, gadījumā ja ir noslēgts līgums starp Pašvaldību un atbilstošo personu, kurā ir precīzi noteikti personas pienākumi, pieļaujamie informācijas izmantošanas mērķi, konfidencialitātes prasības un atbildība).

11. Piešķirtās lietotāju pieejas tiesības Pašvaldības IKT resursiem un / vai informācijas sistēmām ir nekavējoties jāanulē šādos gadījumos:

11.1. Darbiniekiem, kuri pārtrauc darbu (līguma) tiesiskās attiecības ar Pašvaldību un / vai tās vairs nav nepieciešamas pienākumu veikšanai.

11.2. Personām, kuras ir izpildījušas savstarpēji noslēgto līgumu ar Pašvaldību vai šī līguma izbeigšanās (atcelšanas) gadījumā.

12. Iestājoties šo noteikumu 11.punktā minētajam gadījumam, atbilstošās struktūrvienības vadītājam, kura pakļautībā ir augstāk minētais darbinieks (vai koordinējošās struktūrvienības vadītājam gadījumos ar trešajām personām), ir pienākums informēt IKT resursu īpašnieku un/vai IKT tehnisko resursu turētāju, kurš veic atbilstošā lietotāja tiesību bloķēšanu.

13. Piešķirtās lietotāju pieejas tiesības var anulēt arī Kiberdrošības pārvaldnieks vai IKT tehnisko resursu turētājs, balstoties uz atbilstošā lietotāja Informācijas sistēmu drošības politikas vai to saistošo dokumentu pārkāpumiem, par to rakstiski informējot Pašvaldības vadību.

14. Kiberdrošības pārvaldnieks sadarbībā ar IKT tehnisko resursu turētāju pēc Pašvaldības vadības pieprasījuma sagatavo un Pašvaldības vadībai iesniedz Lietotāju pieejas tiesību sarakstu.

15. Kiberdrošības pārvaldniekam ir pienākums vismaz reizi gadā sadarbībā ar attiecīgo IKT resursu īpašnieku veikt Lietotāju pieejas tiesību kontroli, pārbaudot un salīdzinot piešķirto lietotāju pieejas tiesību atbilstību darbinieka (personas, kuras darbojas uz līguma pamata) pienākumiem un specifikai.

16. Informācijas sistēmas lietotājiem, autorizēšanās rekvizītus (lietotājevārdu un paroli) izsniedz IKT tehnisko resursu turētājs vai arī atbilstošās IKT resursu īpašnieks.

17. Ja Informācijas sistēmas lietotājs ir aizmirsis savu lietotāja paroli, par to Informācijas sistēmas lietotājs personīgi vai telefoniski informē IKT tehnisko resursu turētāju. IKT tehnisko resursu turētājs identificē atbilstošo informācijas sistēmas lietotāju, izveido jaunu paroli un izsniedz atbilstošajam Informācijas sistēmas lietotājam.

18. IKT tehnisko resursu turētājam, Kiberdrošības pārvaldniekam un Pašvaldības vadībai ir tiesības:

18.1. Pārbaudīt informācijas sistēmu lietotāju kontu sarakstu, tiem piešķirtās piekļuves tiesības un to veiktās darbības informācijas sistēmā, tostarp lietotāju veiktās informācijas resursu izmaiņas un tehnisko resursu konfigurāciju izmaiņas;

18.2. Nodrošināt žurnālfailu ierakstu analīzi par lietotāju veiktajām darbībām;

18.3. Ja noticis kiberincidents vai ja ir pamatotas aizdomas par to, bloķēt vai uzdot IKT tehnisko resursu turētājam bloķēt ar kiberincidentu saistītos lietotāju kontus;

18.4. Pārbaudīt reģistrēto lietotāju zināšanas par informācijas sistēmas lietošanas noteikumiem un nepieciešamības gadījumā organizēt papildu apmācības, lai šīs zināšanas pilnveidotu.

18.5. Pieprasīt no IKT ārpakalpojuma sniedzēja informācijas sistēmas žurnālfailu ierakstus, ja informācijas sistēmu vai tās daļu uzturēšana notiek ārpus subjekta īpašumā vai valdījumā esošās IKT infrastruktūras.

II. Informācijas sistēmas lietotāju tiesības, pienākumi un atbildība

19. Informācijas sistēmas lietotājam ir tiesības izmantot viņam lietošanā nodotos datorus un to programmatūru, kā arī Informācijas sistēmas lietotājam ir tiesības pieprasīt atbalstu gadījumā, ja datoram vai tā programmatūrai ir radušies traucējumi.

20. Informācijas sistēmas lietotājs ir atbildīgs par datortehniku, kas nodota viņa rīcībā, kā arī atbild par darbībām, kas tiek veiktas ar viņam nodoto datortehniku.

21. Informācijas sistēmas lietotājs nedrīkst atļaut piekļūt tam nodotai datortehnikai citām personām, ja tas nav nepieciešams tiešo darba pienākumu pildīšanai un to pilnvarojumu nav devusi Pašvaldības vadība, Kiberdrošības pārvaldnieks, attiecīgais IKT resursu īpašnieks vai IKT tehnisko resursu turētājs.

22. Informācijas sistēmas lietotāja pienākums ir apzināti nepieļaut datorvīrusu iekļūšanu Pašvaldības datorsistēmās un neizmantojot nezināmas izcelsmes datu nesējus. Rodoties aizdomām, ka dators ir inficēts ar datorvīrusu, par to nekavējoties jāinformē IKT tehnisko resursu turētāju un Kiberdrošības pārvaldnieku.

23. Informācijas sistēmas lietotājam ir pienākums jebkuru ienākošo elektronisko informāciju (failus) pirms lietošanas obligāti pārbaudīt ar antivīrusa programmatūru, ja tas netiek nodrošināts automātiski.

24. Gadījumos, kad ir noticis kiberdrošības incidents vai ir pamatotas aizdomas, ka iespējams ir noticis kiberdrošības incidents, Informācijas sistēmas lietotāja pienākums ir šādos gadījumos nekavējoties informēt IKT tehnisko resursu turētāju un Kiberdrošības pārvaldnieku.

25. Nelicencētas programmatūras uzstādīšana un lietošana darba stacijās (lietotāja datoros) ir aizliegta. Patvaļīgi uzstādītas programmatūras lietošana, bez Pašvaldības vadības, Kiberdrošības pārvaldnieka vai IKT tehnisko resursu turētāja atļaujas ir aizliegta.

26. Informācijas sistēmas lietotājs nedrīkst izpaust nepilnvarotām personām ziņas par Pašvaldības datoru tīkla uzbūvi un konfigurāciju.

27. Informācijas sistēmas lietotājs nedrīkst no sava darba datora kopēt failus uz ārējiem datu nesējiem (piemēram, CD, DVD, USB kartēm vai citiem datu nesējiem), ja to nevajag tiešo darba pienākumu pildīšanai vai ja tam pilnvarojumu nav devusi Pašvaldības vadība, IKT tehnisko resursu turētājs vai Kiberdrošības pārvaldnieks.

28. Ārējo datu nesēju, kurā ir iekopēta ierobežotas pieejamības informācija, no Pašvaldības telpām drīkst izņest tikai ar Pašvaldības vadības atļauju. Šajos gadījumos Informācijas sistēmas lietotājs, kurš no Pašvaldības telpām iznes šādu datu nesēju, uzņemas pilnu atbildību par šo informāciju.

29. Informācijas sistēmas lietotājam ir aizliegts patvarīgi pārvietot, demontēt aparatūru, izjaukt, remontēt iekārtas vai veikt citas darbības, kas varētu traucēt IKT resursu darbību.

30. Informācijas sistēmas lietotājam ir aizliegts veikt paroli minēšanu, drošības ievainojamības pārbaudes, kodēto datu atkodēšanu, izmantot noklausīšanās programmas un veikt citas darbības, kas vērstas uz IKT resursu drošības vājināšanu.

III. Interneta un e-pasta lietošana

31. Pieeju Internetam darbiniekiem piešķir vienlaicīgi ar Informācijas sistēmas lietotāja pieejas tiesībām Pašvaldības datortīklā, kas nepieciešams, lai nodrošinātu Pašvaldības darbību un klientiem sniegtos pakalpojumus.

32. Informācijas sistēmas lietotājam darba vajadzībām ir jāizmanto tikai Pašvaldības piešķirtais e-pasts.

33. Informācijas sistēmas lietotājam ir aizliegts, izmantojot Pašvaldības piešķirto e-pastu, reģistrēties dažādos interneta resursos, kas tiek izmantoti privātām vajadzībām.

34. Informācijas sistēmas lietotājam ir aizliegts atvērt e-pasta pielikumus vai atvērt sūtījumā iekļautās Interneta adreses, kas saņemtas no nenoskaidrotiem sūtītājiem.

35. Lietojot Internetu, darbinieki pārstāv Pašvaldību un tie ir atbildīgi, lai Internets tiktu izmantots darba vajadzībām ētiski un atbilstoši likumdošanas prasībām.

36. Darbiniekiem, izmantojot e-pastu, ir jānodrošina, ka visas komunikācijas tiek veiktas profesionālām vajadzībām un netraucē pašu darbinieku darba produktivitāti, kā arī netiek izplatīta vai sūtīta informācija, kas ir aizsargāta ar autortiesībām. Pašvaldība no darbinieka ir tiesīga piedzīt zaudējumus, kas Pašvaldībai var būt radušies maksājot atlīdzību autortiesību īpašniekam par autortiesību pārkāpumu.

37. Darbinieki ir atbildīgi par visu nosūtīto tekstuālo, audio un vizuālo saturu. IKT tehnisko resursu turētājam un / vai Kiberdrošības pārvaldniekam pēc Pašvaldības vadības pieprasījuma ir tiesības pārlūkot darbinieku saņemto un nosūtīto e-pastu saturu, ja uzskata to par nepieciešamu.

38. IKT tehnisko resursu turētājam un / vai Kiberdrošības pārvaldniekam ir tiesības bloķēt atsevišķu interneta resursu izmantošanu, kā arī ir tiesības piekļūt Informācijas sistēmas lietotāja saglabātajai informācijai, kas atrodas uz Informācijas sistēmas lietotāja datoriem vai serveriem, tikai pildot amata pienākumus vai pildot Pašvaldības vadības rīkojumus.

39. Darbiniekiem ir aizliegts sūtīt tā sauktās “ķēdes vēstules” (t.sk. mēstules, reklāmas, aģitācijas un tml.)– elektroniskus ziņojumus ar lūgumu pārsūtīt tos citiem adresātiem, kā arī ir aizliegts atvērt un darbināt no Interneta tīkla saņemtus aizdomīgus failus. Informācijas sistēmas lietotājam ir jāatceras, ka Interneta tīkls nav drošs datu pārraides medijs un nosūtītāja identifikāciju var viegli viltot. Ja par failu rodas šaubas, Informācijas sistēmas lietotājam ir nepieciešams sazināties ar nosūtītāju un noskaidrot, vai šāds dokuments ir ticis nosūtīts.

40. Nodaļu, struktūrvienību vadītāji nodrošina pieejamību informācijai, kura tiek saņemta e-pastā, ar šo informāciju iepazīstinot padotos darbiniekus uz kuriem tā attiecas un kuriem nav piešķirta e-pasta pieeja.

IV. Informācijas sistēmas lietotāja pieejas paroles uzbūve un lietošana

41. Pašvaldības informācijas resursu aizsardzība tiek nodrošināta ar datora paroli datortīkla (domēna) līmenī, kam ir jāatbilst vismaz sekojošām prasībām:

41.1. Minimālam paroles garumam ir jābūt vismaz 9 simboli un tās maksimālais garums nedrīkst pārsniegt 16 simbolus.

41.2. Maksimālais paroles maiņas periods nedrīkst būt ilgāks par 90 dienām, taču paroli aizliegts pašrocīgi mainīt biežāk nekā divas reizes 24 stundu laikā.

41.3. Paroles uzbūvei jābūt komplicētai, izmantojot vismaz vienu lielo latīņu alfabēta burtu, mazo latīņu alfabēta burtu, ciparu un īpašo rakstzīmju kombināciju (kā piemēram, !@#\$%^*()_+).

41.4. Izveidojot paroli, tā nedrīkst sakrist ar nevienu no 5 iepriekšējām parolēm.

42. Informācijas sistēmas lietotājs nedrīkst izpaust savu paroli jebkurām citām trešajām personām vai citiem lietotājiem, izņemot atsevišķos gadījumos savas prombūtnes laikā, ja atļauju ir devis atbilstošās struktūrvienības vadītājs.

43. Informācijas sistēmas lietotājs nedrīkst savu paroli pierakstīt uz papīra, ja šo dokumentu neglabā seifā vai citā vietā ar ierobežotu citu personu piekļuvi.

44. Ja Informācijas sistēmas lietotājam rodas aizdomas, ka viņa paroli ir uzzinājusi jebkura cita persona, Informācijas sistēmas lietotājam ir pienākums pēc iespējas īsākā laikā šo paroli nomainīt patstāvīgi vai lūgt IKT tehnisko resursu turētājam to izdarīt savā vietā.

45. Informācijas sistēmas lietotājs ir atbildīgs par informācijas aizsardzību un tā pienākums ir nodrošināt, ka datoriem Informācijas sistēmas lietotāja prombūtnes laikā ir ieslēgts ar paroli aizsargāts ekrānsaudzētājs vai noslēgta datora klaviatūra.

46. Dienas beigās, beidzot darbu pie datora, tas jāizslēdz.

Novada domes priekšsēdētājs

(personiskais paraksts)

A.Adamovičs