



LATVIJAS REPUBLIKA
INČUKALNA NOVADA DOME

Reģ.Nr.90000068337, Atmodas iela 4, Inčukalns, Inčukalna pagasts, Inčukalna novads, LV-2141

Tālr./fakss 67977310, mob.t. 26181294, e-pasts: dome@incukalns.lv

NOTEIKUMI
Inčukalnā

2019.gada 22.maijā
Nr.7/2019

protokols Nr. 8-
36.§.

Inčukalna novada pašvaldības
Informācijas sistēmas lietošanas noteikumi

I. Vispārīgie jautājumi

1. Informācijas sistēmas lietošanas noteikumi nosaka Inčukalna novada pašvaldība (turpmāk – Pašvaldība) darbinieku pienākumus un prasības pašvaldības izmantotās informācijas sistēmas un interneta lietošanai, kā arī nosaka kārtību, kādā tiek veikta pašvaldības izmantotās informācijas sistēmas lietotāju pieejas tiesību piešķiršana, izmaiņas un anulēšana.

2. Noteikumos lietotie termini:

2.1. **Informācijas sistēma** – strukturizēts informācijas tehnoloģiju un datu bāzu kopums, kuru lietojot tiek nodrošināta valsts funkciju izpildei nepieciešamās informācijas ierosināšana, radīšana, apkopošana, uzkrāšana, apstrādāšana, izmantošana un iznīcināšana.

2.2. **Inčukalna novada pašvaldība** – institūcija, kas normatīvajos aktos noteiktajā kārtībā organizē un vada informācijas sistēmu darbību.

2.3. **Informācijas sistēmas lietotājs** – persona, kurai ir piešķirtas piekļuves tiesības informācijas sistēmās.

2.4. **IS drošības speciālists** - atbildīgie Informācijas sistēmas drošības darbinieki, kuri Inčukalna novada pašvaldības uzdevumā veic informācijas sistēmu drošības pasākumus šo noteikumu izpildē.

3. 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.

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

II. Informācijas sistēmas lietotāju administrēšanas kārtība

5. Pašvaldības katras pašvaldības iestādes un struktūrvienības vadītājs ir atbildīgs par sev un to padotībā esošo darbinieku lietotāju pieejas tiesību piešķiršanu, izmaiņu veikšanu un anulēšanu.

6. Lai izveidotu lietotāju pieejas tiesības vai veiktu izmaiņas tajās, Pašvaldības atbilstošās pašvaldības iestādes un struktūrvienības vadītājs raksta pieprasījumu (1.Pielikums), atzīmējot tajā nepieciešamo Informācijas resursu, ko iesniedz IS drošības speciālistam.

7. Informācijas sistēmas lietotāju pieejas tiesības tiek piešķirtas Pašvaldības darbiniekiem atbilstoši katra atsevišķā darbinieka noteiktajiem darba pienākumiem un specifikai.

8. IS drošības speciālists izskata lietotāju pieejas tiesību piešķiršanas pieprasījumu un izveido atbilstošās informācijas sistēmas lietošanas tiesības un nosūta tās Lietotājam.

9. Informācijas sistēmas lietotāju pieejas tiesību piešķiršana Pašvaldības informācijas resursiem personām, kuras nav Pašvaldības darbinieki, notiek tikai atsevišķos gadījumos pēc IS drošības speciālista 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).

10. IS drošības speciālists ir atbildīgs par Lietotāju pieejas tiesību izveidošanu, administrēšanu un šo pieprasījumu apkopošanu, glabāšanu, kontroli un uzraudzību.

11. Piešķirtās lietotāju pieejas tiesības Pašvaldības informācijas resursiem ir nekavējoties jāanulē šādos gadījumos:

11.1. darbiniekiem, kuri pārtrauc darba (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, Juridiskās daļas juriskonsults personālvadības jautājumos informē IS drošības speciālistu, kas veic atbilstošā lietotāja tiesību bloķēšanu.

13. Piešķirtās lietotāju pieejas tiesības var anulēt IS drošības speciālists, balstoties uz atbilstošā lietotāja Informācijas sistēmas drošības politikas vai to saistošo dokumentu pārkāpumiem, par to rakstiski informējot Pašvaldības izpilddirektoru.

14. IS drošības speciālistam pēc Pašvaldības izpilddirektora pieprasījuma, sagatavot Lietotāju pieejas tiesību sarakstu.

15. IS drošības speciālistam ir pienākums vismaz reizi gadā veikt Lietotāju pieejas tiesību kontroli, pārbaudot un salīdzinot piešķirto lietotāju pieejas tiesību atbilstību darbinieka (personas, kuras darbojas uz līguma pamata) pienākumiem un specifikai.

III. Informācijas sistēmas lietotāju tiesības, pienākumi un atbildība

16. 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.

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

18. Informācijas sistēmas lietotājs nedrīkst atļaut piekļūt tam nodotai datortehnikai citām personām, ja tas nav nepieciešams tiešo darba pienākumu pildīšanai un to pilnvarojumu nav devis Pašvaldības izpilddirektors vai IS drošības speciālists.

19. Informācijas sistēmas lietotāja pienākums ir apzināti nepieļaut datorvīrusu iekļūšanu iestādes datorsistēmās un neizmantojot nezināmas izcelsmes datu nesējus. Rodoties aizdomām, ka dators ir inficēts ar datorvīrusu, par to nekavējoties jāinformē IS drošības speciālists.

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

21. Nelicencētas programmatūras uzstādīšana un lietošana darba stacijās (lietotāja datoros) ir aizliegta. Patvaļīgi uzstādītas programmatūras lietošana, bez Pašvaldības izpilddirektora vai IS drošības speciālista atļaujas ir aizliegta.

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

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

24. Informācijas sistēmas lietotājam ir aizliegts patvaļīgi pārvietot, demontēt aparatūru, izjaukt, remontēt iekārtas vai veikt citas darbības, kas varētu traucēt informācijas un tehnisko resursu darbību.

25. Informācijas sistēmas lietotājam ir aizliegts veikt paroļu minēšanu, drošības ievainojamības pārbaudes, kodēto datu atkodēšanu, izmantot noklausīšanās programmas un veikt citas darbības, kas vērstas uz informācijas un tehnisko resursu drošības vājināšanu.

IV. Interneta un e-pasta lietošana

27. Pieeju Internetam darbiniekiem piešķir vienlaicīgi ar Informācijas sistēmas lietotāja pieejas tiesībām Pašvaldības datortīklam (domēnam), kas nepieciešams, lai nodrošinātu iestādes darbību un klientiem sniegtos pakalpojumus.

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

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

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

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

32. 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 tiesīgs piedzīt zaudējumus, kas Pašvaldībai

var būt radušies maksājot atlīdzību autortiesību īpašniekam par autortiesību pārkāpumu.

33. Darbinieki ir atbildīgi par visu nosūtīto tekstuālo, audio un vizuālo saturu.

34. IS drošības speciālistam ir tiesības ierobežot 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 izpilddirektora rīkojumus.

35. 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.

V. Informācijas sistēmas lietotāja pieejas paroles uzbūve un lietošana

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

37.1. minimālam paroles garumam ir jābūt vismaz 9 simboli un tās maksimālais garums nedrīkst pārsniegt 16 simbolus;

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

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

37.4. izveidojot paroli, tā nedrīkst sakrist ar nevienu no 5 iepriekšējām parolēm.

37. Informācijas sistēmas lietotājs nedrīkst izpaust savu paroli jebkurām citām trešajām personām vai citiem lietotājiem.

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

39. 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 IS drošības speciālistu to izdarīt savā vietā.

40. 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 darbvirsmas ar Windows + L taustiņu kombināciju.

42. Dienas beigās, beidzot darbu pie datora, tas jāizslēdz izmantojot procedūru: Start => Shut Down => Ok.

Inčukalna novada domes priekšsēdētājs
A.Nalivaiko

1.pielikums
2019.gada 22.maija
Inčukalna novada domes noteikumiem Nr.7/2019
„Inčukalna novada
pašvaldības Informācijas
sistēmas lietošanas
noteikumi”

**Inčukalna novada pašvaldības
informācijas resursu lietotāja reģistrācijas anketa**

Vārds, Uzvārds	
Struktūrvienība	
Amats	
Telefona numurs	

Piešķirt pieeju sekojošiem informācijas resursiem, vajadzīgos atzīmēt ar

Dokumentu koplietošanas mape (failu serveris)

E-pasts

Grāmatvedības uzskaites sistēma (Pakalns)

- Personu dzīvesvietas reģistrēšanas sistēma (PERS)**
- Personu dzimtsarakstu reģistrācijas informatīvā sistēma (DZIMTS)**
- Sociālās palīdzības administrēšanas sistēma (SOPA)**
- Nekustamā īpašuma nodokļa administrēšanas sistēma (NINO)**
- Dokumentu vadības sistēma (NAMEJS)**
- E-klase**
- _____
- _____
- _____
- _____

(datums, paraksts)