ROPAŽU NOVADA PAŠVALDĪBA
Reģ. Nr. 90000067986
Institūta iela 1A, Ulbroka, Stopiņu pagasts, Ropažu novads, LV-2130
Tālr. 67910518
novada.dome@ropazi.lv
Ulbrokā

IEKŠĒJIE NOTEIKUMI

2022.gada 21.aprīlī Nr. 10

Ropažu novada pašvaldības Informācijas sistēmas lietošanas noteikumi

Izdoti saskaņā ar
Valsts pārvaldes iekārtas likuma 72.panta pirmās daļas 1.punktu,
Ministru kabineta 2015.gada 28.jūlija noteikumu Nr.442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" 8.3.apakšpunktu

I. Vispārīgie jautājumi

1. Informācijas sistēmas lietošanas noteikumi nosaka Ropažu novada pašvaldības, tās izveidoto iestāžu un pašvaldības aģentūras (turpmāk – institūcija) darbinieku pienākumus un prasības Institūcijas izmantotās informācijas sistēmas un interneta lietošanai, kā arī nosaka kārtību, kādā tiek veikta institūcijas izmantotās informācijas sistēmas lietotāju pieejas tiesību piešķiršana, izmaiņas un anulēšana.

2. Noteikumos lietotie termini:

2.1. **Institūcija** - Ropažu novada pašvaldība (Centrālā administrācija), pašvaldību izveidotās iestādes un pašvaldības aģentūras.

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

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

2.4. **Sistēmas drošības pārvaldnieks** – ar Pašvaldības izpilddirektora vai institūcijas vadītāja rīkojumu iecelta persona, kura atbild par institūcijas informācijas sistēmas drošības pasākumu izstrādi, ieviešanu un uzturēšanu, kā arī rīkojas ar informācijas resursiem.

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

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

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

II. Informācijas sistēmas lietotāju administrēšanas kārtība

5. Katrs institūcijas 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, atbilstošās institūcijas vai struktūrvienības vadītājs (ja institūcijā ir izveidota struktūrvienība, departaments) raksta pieprasījumu (1.Pielikums), atzīmējot tajā nepieciešamo Informācijas resursu, ko iesniedz Sistēmas drošības pārvaldniekam.

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

8. Sistēmas drošības pārvaldnieks izskata lietotāju pieejas tiesību piešķiršanas pieprasījumu un, ja uzskata to par pamatotu, Sistēmas drošības pārvaldnieks pieprasījumu izveidot atbilstošās informācijas sistēmas lietošanas tiesības nosūta Datortīkla administratoram.

9. Informācijas sistēmas lietotāju pieejas tiesību piešķiršana institūcijas informācijas resursiem personām, kuras nav institūcijas darbinieki, notiek tikai atsevišķos gadījumos pēc Sistēmas drošības pārvaldnieka pieprasījuma (piemēram, gadījumā ja ir noslēgts līgums starp institūciju un atbilstošo personu, kurā ir precīzi noteikti personas pienākumi, pieļaujamie informācijas izmantošanas mērķi, konfidencialitātes prasības un atbildība).

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

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

11.1. darbiniekiem, kuri pārtrauc darba (līguma) tiesiskās attiecības ar institūciju un / vai tās vairs nav nepieciešamas pienākumu veikšanai;

11.2. personām, kuras ir izpildījušas savstarpēji noslēgto līgumu ar institūciju vai šī līguma izbeigšanās (atcelšanas) gadījumā;

11.3. citos gadījumos, kad lietotāju tiesības anulēšanu pieprasa Sistēmas drošības pārvaldnieks.

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 Sistēmas drošības pārvaldnieku un Datortīkla administratoru, kas veic atbilstošā lietotāja tiesību bloķēšanu.

13. Piešķirtās lietotāju pieejas tiesības var anulēt arī Sistēmas drošības pārvaldnieks vai Datortīkla administrators, balstoties uz atbilstošā lietotāja Informācijas sistēmas drošības politikas vai to saistošo dokumentu pārkāpumiem, par to rakstiski informējot Pašvaldības izpilddirektoru.

14. Datortīkla administratoram ir pienākums pēc Pašvaldības izpilddirektora vai Sistēmas drošības pārvaldnieka pieprasījuma, sagatavot Lietotāju pieejas tiesību sarakstu.

15. Sistēmas drošības pārvaldniekam 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, Sistēmas drošības pārvaldnieks vai Datortīkla administrators.

19. Informācijas sistēmas lietotāja pienākums ir apzināti nepieļaut datorvīrusu iekļūšanu iestādes datorsistēmās un neizmantot nezināmas izcelsmes datu nesējus. Rodoties aizdomām, ka dators ir inficēts ar datorvīrusu, par to nekavējoties jāinformē Sistēmas drošības pārvaldnieks vai Datortīkla administrators.

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 uzstādīšana bez Pašvaldības izpilddirektora, Sistēmas drošības pārvaldnieka vai Datortīkla administratora atļaujas ir aizliegta.

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

23. 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 devis Pašvaldības izpilddirektors, Sistēmas drošības pārvaldnieks vai Datortīkla administrators.

24. Ārējo datu nesēju, kurā ir iekopēta ierobežotas pieejamības informācija, no institūcijas telpām drīkst iznest 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.

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

26. 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 institūcijas datortīklam (domēnam), kas nepieciešams, lai nodrošinātu iestādes darbību un klientiem sniegtos pakalpojumus.

28.Informācijas sistēmas lietotājam darba vajadzībām ir jāizmanto tikai institūcijas piešķirtais e-pasts. Informācijas sistēmas lietotājam ir aizliegts pāradresēt uz Institūcijas piešķirto epastu saņemtos epastus uz savu privāto vai citu epastu bez Sistēmas drošības pārvaldnieka rakstiskas atļaujas.

29. Informācijas sistēmas lietotājam ir aizliegts, izmantojot institūcijas 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, institūciju 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 vai institūcija no darbinieka ir tiesīga piedzīt zaudējumus, kas institūcijai var būt radušies, maksājot atlīdzību autortiesību īpašniekam par autortiesību pārkāpumu.

33. Darbinieki ir atbildīgi par visu nosūtīto tekstuālo, audio un vizuālo saturu. Datortīkla administrators bez saskaņošanas ar darbinieku patur sev tiesības pārlūkot darbinieku saņemto un nosūtīto e-pastu saturu, ja uzskata to par nepieciešamu.

34. Sistēmas drošības pārvaldniekam vai Datortīkla administratoram 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 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 mēdijs un nosūtītāja identifikāciju var viegli viltot. Ja par saņemto e-pastu 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. Institūcijas informācijas resursu aizsardzība tiek nodrošināta ar datora paroli datortīkla (domēna) līmenī, kam ir jāatbilst vismaz sekojošām prasībām:

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

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

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

36.4. 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, izņemot atsevišķos gadījumos savas prombūtnes laikā, ja atļauju ir devis atbilstošās struktūrvienības vadītājs.

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 Datortīkla administratoru 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 klaviatūra, izvēloties „Lock Computer" izvēlni.

41. Pēc darba laika beigšanas, darbiniekam ir nepieciešams atslēgties no visām Informācijas sistēmām.

VI. Noslēguma jautājums

42. Ar šo noteikumu spēkā stāšanos spēku zaudē Stopiņu novada domes 2020.gada 10.februāra iekšējie noteikumi Nr.9 (apstiprināti ar Stopiņu novada domes 2020.gada 5.februāra sēdes lēmumu, prot. Nr.70, p.4.4) "Informācijas sistēmas lietošanas noteikumi".

Pielikumā: Ropažu novada pašvaldības Informācijas sistēmu tiesību pieprasījums.

Ropažu novada pašvaldības izpilddirektors M.Griščenko

1.pielikums

"Ropažu novada pašvaldības
Informācijas sistēmas lietošanas noteikumi"

ROPAŽU NOVADA PAŠVALDĪBAS
INFORMĀCIJAS RESURSU LIETOTĀJA REĢISTRĀCIJAS ANKETA

Vārds, Uzvārds	
Struktūrvienība	
Amats	
Telefona numurs	

Piešķirt pieeju sekojošiem informācijas resursiem (vajadzīgos atzīmēt ☑).

- ☐ Lietotāju konts Aktīvajā Direktorijā (iekšējā datortīklā)
- ☐ E-pasts
- ☐ Dokumentu vadības sistēma
- ☐ Grāmatvedības uzskaites sistēma
- ☐ Personu dzīvesvietas reģistrēšanas sistēma (PERS)
- ☐ Personu dzimtsarakstu reģistrācijas informatīvā sistēma (DZIMTS)
- ☐ Sociālās palīdzības administrēšanas sistēma (SOPA)
- ☐ Nekustamā īpašuma nodokļa administrēšanas sistēma (NINO)
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____

(Nepieciešamības gadījumā kontaktēties ar Datortīkla administratoru, lai norādītu nepieciešamos informācijas resursus)

_____

(Datums, paraksts)