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. 9

Ropažu novada pašvaldības Informācijas sistēmas drošības 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" 8.2.apakšpunktu

I.Vispārīgie jautājumi

1. Informācijas sistēmas drošības noteikumi ietver kārtību, kādā Ropažu novada pašvaldība, tās izveidotās iestādes un pašvaldības aģentūras (turpmāk – institūcija) nodrošina pašvaldības izmantotās informācijas sistēmas aizsardzību.

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 funkciju izpildei nepieciešamās informācijas ierosināšana, radīšana, apkopošana, uzkrāšana, apstrādāšana, izmantošana un iznīcināšana.

2.4. **Sistēmas drošības pārvaldnieks** – ar pašvaldības izpilddirektora vai institūcijas vadītāja rīkojumuiecelta 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 drošības noteikumi ir saistoši Informācijas sistēmas drošības pārvaldniekam un Datortīkla administratoram.

II. Informācijas loģiskā aizsardzība

4. Institūcijas datortīklu, serveru un to saistīto iekārtu uzturēšanu un administrēšanu, kā arī Informācijas sistēmas lietotāju datoru uzstādīšanu un administrēšanu veic Datortīkla administrators.

5. Datortīkla administrators ir atbildīgi par piemērotu un efektīvu aizsardzības sistēmas izveidi, lietojot atbilstošu maršrutēšanas un ugunsmūra sistēmu, kā arī nodrošinot pretvīrusu programmatūras uzstādīšanu un uzturēšanu uz institūcijas serveriem un datoriem.

6. Datortīkla administratoram ir pienākums regulāri sekot līdzi ugunsmūra paziņojumiem un reaģēt uz vīrusu uzbrukumiem, nodrošinot konstatēto vīrusu iznīcināšanu un būtisko incidentu reģistrēšanu.

7. Gadījumā, ja tiek konstatēti būtiski darbības traucējumi ielaušanās mēģinājumu rezultātā vai arī būtiski incidenti, Datortīkla administrators veic to reģistrēšanu un izmeklēšanu, kā arī par tās rezultātiem informē Sistēmas drošības pārvaldnieku un Drošības incidentu novēršanas institūciju (CERT.lv).

8. Vīrusu darbības novēršanai veic šādus pasākumus:

8.1. Datortīkla administrators veic pasākumus datoru vīrusu darbības novēršanai tehniskajos resursos, izmantojot šim nolūkam paredzētu programmatūru.

8.2. IT Datortīkla administrators veic antivīrusu programmu pārraudzību, lai pārliecinātos par to darbību un jaunāko vīrusu definīciju failu esamību.

9. Datortīkla administrators izveido, veic izmaiņas un anulē Informācijas sistēmas lietotāju tiesības atbilstoši Informācijas sistēmas drošības pārvaldnieka norādījumiem.

10. Informācijas sistēmas lietotājiem, kuri ir institūcijas darbinieki, autorizēšanās rekvizītus (lietotājvārdu un paroli) izsniedz Datortīkla administrators vai arī atbilstošās informācijas sistēmas pakalpojumu sniedzējs.

11. Informācijas sistēmas lietotājiem, kuri nav institūcijas darbinieki, autorizēšanās rekvizītus (lietotājvārdu un paroli) izsniedz Informācijas sistēmas drošības pārvaldnieks pēc atbilstošā Informācijas sistēmas lietotāja identificēšanas.

12. Ja Informācijas sistēmas lietotājs, kas ir institūcijas darbinieks, ir aizmirsis savu lietotāja paroli, par to Informācijas sistēmas lietotājs personīgi vai telefoniski informē Datortīkla administratoru. Datortīkla administrators identificē atbilstošo informācijas sistēmas lietotāju, izveido jaunu paroli un izsniedz atbilstošajam Informācijas sistēmas lietotājam.

13. Ja Informācijas sistēmas lietotājs, kas nav institūcijas darbinieks, ir aizmirsis savu lietotāja paroli, par to Informācijas sistēmas lietotājs personīgi vai telefoniski informē Datortīkla administratoru. Datortīkla administrators identificē atbilstošo informācijas sistēmas lietotāju, izveido jaunu paroli un izsniedz atbilstošajam Informācijas sistēmas lietotājam.

14. Paroles politika ir noteikta Pašvaldības Informācijas sistēmas lietošanas noteikumos.

15. Informācijas sistēmas lietotāja parole pie ievades nedrīkst parādīties uz ekrāna.

16. Datortīkla administrators nodrošina auditācijas pierakstu veidošanu datortīkla autorizācijai un par informācijas sistēmām, kas ir izvietotas uz Pašvaldības un/vai institūcijas

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. Datortīkla administrators nodrošina auditācijas pierakstu integritāti un regulāri veido auditācijas pierakstu datu rezerves kopijas.

17. Institūcija nodrošina, ka pirms jaunas paaugstinātas sistēmas pieņemšanas ekspluatācijā tai ir veikti ielaušanās testi. Ielaušanās testus veic juridiska persona vai Pašvaldības un/vai institūcijas darbinieki, kuri nav piedalījušies sistēmas izstrādē.

18. Datortīkla administrators veic auditācijas pierakstu analīzi šādos gadījumos:
18.1. Informācijas sistēmas lietotāja atkārtota neveiksmīga pieslēgšanās informācijas sistēmai.
18.2. Informācijas sistēmas lietotāja pieslēgšanās informācijas sistēmai ārpus darba laika.
18.3. mēģinājumi piekļūt informācijas resursiem, kuriem Informācijas sistēmas drošības pārvaldnieks nav pilnvarojis piekļūt.
18.4. atkārtoti mēģinājumi lietot lietotāja rekvizītus, kuri jau ir atcelti;
18.5. nesankcionētas programmatūras konfigurācijas maiņas un neatļautas programmatūras uzstādīšana.

19. Datortīkla administrators, sadarbojoties ar Informācijas sistēmas drošības pārvaldnieku, ir pienākums veikt reģistru par iegādātām un izlietotām programmatūras licencēm, kā arī, ja nepieciešams, savlaicīgi informēt Sistēmas drošības pārvaldnieku par nepieciešamību iegādāties papildus licences.

20. Reģistru par iegādātiem un uzstādītiem informācijas tehniskajiem resursiem (t.sk. par darba stacijām, serveriem un perifērijas iekārtām) veic Pašvaldības vai institūcijas grāmatvedība. Vismaz reizi gadā tiek veikta šo resursu inventarizācija, pārliecinoties, ka šis reģistrs ir korekts.

21. Informācijas sistēmas drošības pārvaldnieks, tā pilnvarota persona vai ārējs konsultants nodrošina institūcijas Informācijas sistēmas lietotāju apmācību informācijas sistēmu drošības jomā vismaz reizi gadā, izskaidrojot tiem Informācijas sistēmas drošības politikas pamatprincipus un būtiskākos drošības pasākumus datu drošībai.

22. Institūcijā tiek nodrošināta datortīkla / informācijas sistēmas atbilstība šādām aizsardzības prasībām:
22.1. iekšējo datortīklu nodala no interneta ar ugunsmūra palīdzību;
22.2. ja tehniskais risinājums to pieļauj, nodrošina datortīkla / informācijas sistēmas pretvīrusa aizsardzību;
22.3. nodrošina nepārtrauktu datortīkla / informācijas sistēmas darba vides drošības apdraudējumu novēršanu, izmantojot ielaušanās mēģinājumu noteikšanu un aizsardzības sistēmu;
22.4. izmantojot tikai šifrētu pieslēgumu un daudzfaktoru autentifikāciju, nodrošina attālinātas piekļuves ierobežošanu datortīkla / informācijas sistēmas administrēšanai;
22.5. organizē atsevišķi savietojamās sistēmas un savietotāja uzlabojumu testēšanu šīm vajadzībām izveidotā testa vidē, kas nodalīta no savietojamās sistēmas un savietotāja fiziskā vai loģiskā līmenī.
22.6. piekļuvi datortīkla / informācijas sistēmas administrēšanas un pārvaldības funkcionalitātei nodrošina tikai tām personām, kurām datortīkla / informācijas sistēmas esošā informācija atbilstošā apmērā ir nepieciešama darba pienākumu veikšanai;

22.7. sistēmas lietotāji, kas veic sistēmas administrēšanas darbu, izmanto īpašus lietotāju kontus (piemēram, sistēmas administratora konts), kas netiek izmantoti ikdienas darbību veikšanai;
22.8. katrs lietotāja konts ir saistīts ar konkrētu fizisko personu. Ja sistēmā tiek izmantoti konti, kas nav piesaistāmi konkrētai fiziskai personai, tad sistēmā jābūt iestrādātiem tehniskiem līdzekļiem, kas novērš iespēju lietotājiem izmantot šādus kontus;
22.9. sistēmas lietotāja paroles aizliegts elektroniski glabāt un transportēt nešifrētā veidā, arī lietotāja autentifikācijas procesa ietvaros.
22.10. sistēmas lietotāja parole ievadīšanas brīdī lietotājam netiek pilnībā attēlota;
22.11. sistēmas lietotāja parole, kas nosūtīta publiskā datu pārraides tīklā nešifrētā veidā, ir lietojama vienu reizi un derīga ne ilgāk kā 72 stundas pēc tās nosūtīšanas;
22.12. sistēmā nav pieļaujama funkcionalitāte, kas atļauj sistēmas lietotājam saglabāt savu paroli tā, lai tā turpmākajās pieslēgšanas reizēs nav jāievada;
22.13. iekārtām, tai skaitā infrastruktūras iekārtām, kas nodrošina sistēmas funkcionēšanu, netiek izmantotas noklusējuma (ražotāja vai izplatītāja uzstādītās) paroles;
22.14. tiek nodrošināta sistēmas auditācijas pierakstu (turpmāk – sistēmas pieraksti) veidošana un uzglabāšana vismaz sešus mēnešus pēc ieraksta izdarīšanas;
22.15. jebkura piekļuve sistēmai ir izsekojama līdz konkrētam sistēmas lietotāja kontam vai interneta protokola (IP) adresei;
22.16. sistēmai jābūt uzliktiem visiem pieejamiem programmatūras atjauninājumiem, iepriekš izvērtējot to nepieciešamību;
22.17. visās institūcijas valdījumā esošajās galalietotāju iekārtās, kas ikdienā tiek izmantotas, lai pieslēgtos sistēmai, jābūt iekļautai pretvīrusu funkcionalitātei;
22.18. sistēmas funkcionalitāte ir izpildāma ar minimāli iespējamām tiesībām.
22.19. piecas secīgas reizes nepareizi ievadot sistēmas lietotāja konta paroli, šis konts (izņemot sistēmas administratora kontu) nekavējoties tiek bloķēts;
22.20. ar sistēmas administratora kontu piekļūt sistēmai, izmantojot iekārtas, kas atrodas ārpus iestādes telpām, kā arī iekārtas, kas neatrodas iestādes valdījumā, iespējams, tikai izmantojot daudzfaktoru autentifikāciju;
22.21. fiziski piekļūt iekārtām, kas nodrošina sistēmas darbību, atļauts vienīgi iestādes pilnvarotām personām;
22.22. sistēmas lietotājiem redzamie kļūdu paziņojumi satur tikai minimāli nepieciešamo informāciju, lai sistēmas lietotājs pašrocīgi vai ar sistēmas atbalsta personāla palīdzību atrisinātu kļūdu;
22.23. plūsma starp sistēmu un tās lietotājiem, kā arī starp sistēmu un citām sistēmām tiek kontrolēta, piemēram, izmantojot ugunsmūri;
22.24. datortīkla pakalpojumi, kas netiek izmantoti sistēmas darbības nodrošināšanai, ir atslēgti;
22.25. veicot sistēmas izstrādi un testēšanu, nav pieļaujams radīt apdraudējumu sistēmā glabāto datu integritātei;
22.26. sistēmas izvietošana ārpakalpojuma sniedzēja nodrošinātos resursos atļauta tikai tad, ja pakalpojuma sniedzējs ir juridiska persona, kas reģistrēta Eiropas Savienības vai Eiropas Ekonomikas zonas dalībvalstī, un sistēmā glabātā informācija atrodas vienīgi Eiropas Savienības vai Eiropas Ekonomikas zonas valstu teritorijā.

23. Institūcija nodrošina, ka vismaz reizi gadā tiek veikta informācijas tehnoloģiju drošības pārbaude (t.i. institūcijas izmantotās informācijas sistēmas drošības dokumentācijas un pasākumu atbilstības pārbaude) un atbilstoši tās rezultātiem tiek organizēta atklāto trūkumu novēršana.

24. Institūcija nodrošina, ka vismaz reizi gadā institūcijas pārstāvis apmeklē Drošības incidentu novēršanas institūcijas organizētu apmācību informācijas tehnoloģiju drošības jautājumos.

25. Institūcija nodrošina, ka ne retāk kā reizi gadā veic institūcijas darbinieku instruktāžu informācijas tehnoloģiju drošības jautājumos.

III. Informācijas fiziskā aizsardzība

26. Informācijas sistēmu serveri, datortīkls un ar to saistītais aprīkojums tiek ekspluatēts ierobežotas pieejas telpās (turpmāk - serveru telpas), kurām iespēja piekļūt ir Datortīkla administrators un Informācijas sistēmas drošības pārvaldniekam, nodrošinot aizsardzību pret neautorizētu personu iespēju serverus izslēgt, pārvietot, bojāt un nesankcionēti mainīt to konfigurāciju.

27. Serveru telpas ir aprīkotas ar:
27.1. ugunsgrēka signalizācijas iekārtu.
27.2. ugunsdzēšamo aparātu.
27.3. gaisa kondicionēšanas iekārtu.
27.4. nepārtrauktās barošanas avotu (UPS).
27.5. apsardzes signalizāciju.
27.6. diviem neatkarīgiem elektrības pievadiem.

28. Nepiederošas personas, t.sk. ārējie pakalpojumu sniedzēji, serveru telpās drīkst uzturēties tikai Datortīkla administratora vai Informācijas sistēmas drošības pārvaldnieka klātbūtnē.

29. Pazūdot elektrībai, Datortīkla administratoram vai Informācijas sistēmas drošības pārvaldniekam ir pienākums maksimāli īsā laikā novērst elektrības padeves traucējumus un nodrošināt pieslēgumu no cita enerģijas avota vai arī, ja tas nav iespējams un serveriem nav nodrošināta izslēgšanās automātiski, uzsākt manuālu serveru izslēgšanu.

30. Informācijas sistēmas lietotāju darba stacijas atrodas ierobežotas pieejas telpās, kā arī tās ir pieslēgtas nepārtrauktās barošanas avotam (UPS), ja elektroenerģijas padeves traucējumu risks ir nepieņemami liels.

31. Datu nesēju (t.sk. 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.

IV. Ārpakalpojumu iesaiste

32. Ja Pašvaldība un/vai institūcija sistēmas uzturēšanai slēdz ārpakalpojuma līgumu ar pakalpojuma sniedzēju, līguma izpildi uzrauga atbildīgā persona un līgumā iekļauj vismaz šādas drošības prasības:
32.1. saņemamā ārpakalpojuma aprakstu;
32.2. precīzas prasības attiecībā uz ārpakalpojuma apjomu un kvalitāti;
32.3. institūcijas un ārpakalpojuma sniedzēja tiesības un pienākumus, tai skaitā:
32.3.1. institūcijas tiesības pastāvīgi uzraudzīt ārpakalpojuma sniegšanas kvalitāti;
32.3.2. institūcijas tiesības dot ārpakalpojuma sniedzējam obligāti izpildāmus norādījumus jautājumos, kas saistīti ar ārpakalpojuma godprātīgu, kvalitatīvu, savlaicīgu un normatīvajiem aktiem atbilstošu izpildi;
32.3.3. institūcijas 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;

32.3.4. ārpakalpojuma sniedzēja pienākumu nodrošināt institūcijai iespēju pastāvīgi uzraudzīt ārpakalpojuma sniegšanas kvalitāti.

33. Ja institūcija uzsāk iepirkumu par esošas sistēmas uzlabojumiem, tā nodrošina, ka atbilstošās drošības prasības tiek iekļautas iepirkuma specifikācijā.

34. Ja institūcija uzsāk iepirkumu par jaunas sistēmas izstrādi, tā iepirkuma specifikācijā iekļauj prasības, paredzot:

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

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

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

V. Rezerves kopiju veidošanas kārtība

35. Datortīkla administrators nodrošina institūcijas informācijas resursu rezerves kopiju veidošanu tām informācijas sistēmām / resursiem, kas ir izvietoti uz Pašvaldības un/vai institūcijas serveriem / darba stacijām.

36. Rezerves kopiju ārējos datu nesējus glabā attālināti no oriģinālajiem datiem, lai novērstu oriģināla un kopijas vienlaicīgas bojāejas iespēju liela apjoma negadījuma situācijā.

37. Sistēmas drošības pārvaldnieks nosaka vietu, kur tiks glabātas rezerves kopijas uz ārējā datu nesēja.

38. Datortīkla administrators nodrošina institūcijas informācijas resursu atjaunošanu no rezerves kopijām pēc Sistēmas drošības pārvaldnieka pieprasījuma.

39. Datortīkla administrators sadarbībā ar Sistēmas drošības pārvaldnieku ir pienākums vismaz reizi gadā veikt pārbaudi par informācijas sistēmu atjaunošanas iespējām no rezerves kopijām, par to rezultātiem informējot pašvaldības izpilddirektoru.

VI. Elektronisko datu nesēju iznīcināšanas procedūra

40. Datortīkla administrators organizē elektronisko datu nesēju iznīcināšanu un nodrošina šo iznīcināto elektronisko datu nesēju uzskaiti.

VII. Noslēguma jautājums

41. Ar šo noteikumu spēkā stāšanos spēku zaudē Stopiņu novada domes 2020.gada 10.februāra iekšējie noteikumi Nr.6 (apstiprināti ar Stopiņu novada domes 2020.gada 5.februāra sēdes lēmumu, prot. Nr.70, p.4.4) “Informācijas sistēmas drošības noteikumi”.

Ropažu novada pašvaldības izpilddirektors M.Griščenko