BALVU NOVADA PAŠVALDĪBA
BALVU NOVADA DOME

Reģ.Nr.90009115622, Bērzpils iela 1A, Balvi, Balvu novads, LV-4501, tālrunis +371 64522453
fakss+371 64522453, e-pasts: dome@balvi.lv

Balvos

APSTIPRINĀTI
ar Balvu novada Domes
2022.gada 24.februāra
lēmumu (sēdes protokols Nr.6., 43.§)

NOTEIKUMI

2022.gada 24.februārī Nr.3/2022

Informācijas sistēmu drošības noteikumi

Izdoti saskaņā ar Valsts iekārtas likuma
72.panta pirmās daļas 1.punktu,
likuma „Par pašvaldībām"
41.panta pirmās daļas 2.punktu un
Ministru kabineta 2015. gada 28. jūlija noteikumu Nr. 442
„Kārtība, kādā tiek nodrošināta informācijas un komunikācijas
tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" 8.2. un 11.punktu

I.Vispārīgie jautājumi

1. Informācijas sistēmu drošības noteikumi ietver kārtību, kādā Balvu novada pašvaldība un tās iestādes (turpmāk – Pašvaldība) nodrošina pašvaldības izmantoto informācijas sistēmu aizsardzību.

2. Noteikumos lietotie termini:

2.1. **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.

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

2.3. **Informācijas sistēmas drošības pārvaldnieks** – ar Pašvaldības izpilddirektora rīkojumu iecelta persona, kura atbild par Pašvaldības informācijas sistēmas drošības pasākumu izstrādi, ieviešanu un uzturēšanu, kā arī rīkojas ar informācijas resursiem.

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

3. Informācijas sistēmu drošības noteikumi ir saistoši Informācijas sistēmas drošības pārvaldniekam un Pašvaldības un tās iestāžu datorspeciālistiem (turpmāk tekstā – Datortīkla administrators).

II. Informācijas loģiskā aizsardzība

4. Pašvaldības 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 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.

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 Informācijas 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. 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 Pašvaldības darbinieki, autorizēšanās rekvizītus (lietotājvārdu un paroli) izsniedz Datortīkla administrators vai arī atbilstošās informācijas sistēmas pakalpojumu sniedzējs.

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

12. Ja Informācijas sistēmas lietotājs, kas ir Pašvaldības 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 Pašvaldības 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 sistēmu 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 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. Pašvaldība nodrošina, ka pirms jaunas sistēmas pieņemšanas ekspluatācijā tai ir veikti ielaušanās testi. Ielaušanās testus veic juridiska persona vai Pašvaldības 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 administratoram, sadarbojoties ar Informācijas sistēmas drošības pārvaldnieku, ir pienākums veikt reģistru par iegādātām un izlietotām programmatūras licencēm, kā arī, ja nepieciešams, savlaicīgi informēt Informācijas 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 Balvu novada administrācijas Finanšu plānošanas un centralizētās grāmatvedības nodaļa. 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 Pašvaldības 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. Pašvaldībā 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 Pašvaldības 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 un interneta datu plūsmu virza Eiropas Savienības un Eiropas Ekonomikas zonas teritorijā.
22.27. sistēmās, kas nodrošina elektroniskā pasta saņemšanu no ārējiem resursiem, ienākošo saziņu apstrādā vismaz atbilstoši e-pastu autentifikācijas protokola (DMARC) prasībām, ieviešot e-pasta apstrādi atbilstoši sūtītāja domēna vārda DMARC politikai, atskaites ģenerēšanu un nosūtīšanu DMARC konfigurācijā norādītajam kontaktam;
22.28. institūcija, kas ir elektroniskā pasta domēna īpašnieks, publicē DMARC atbilstošu ierakstu savā domēna vārdu sistēmā (DNS), norādot striktu atteikuma politiku (p=reject), ievieš procedūru DMARC ziņojumu saņemšanai un to analīzei;
22.29. institūcija nodrošina informācijas sistēmās esošo datu rezerves kopiju veidošanu un atjaunošanu.

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

24. Paaugstinātas drošības sistēmām, kas pieejamas, izmantojot publisku datu pārraides tīklu, institūcija nodrošina Pašvaldības informācijas sistēmas drošības pārbaudi, vismaz reizi divos gados pasūtot ārēju drošības dokumentācijas auditu un ielaušanās testu veikšanu.

25. Pasūtot ārējas drošības pārbaudi paaugstinātas drošības sistēmai, institūcija paredz, ka juridiska persona, kas veic auditu, ir reģistrēta NATO, Eiropas Savienības vai Eiropas Ekonomikas zonas dalībvalstī, tās darbinieki, kas iesaistīti drošības audita veikšanā, ir NATO, Eiropas Savienības, Eiropas Ekonomikas zonas valstu pilsoņi vai Latvijas Republikas nepilsoņi, un juridiskā persona apstrādā audita laikā iegūto informāciju vienīgi NATO, Eiropas Savienības un Eiropas Ekonomikas zonas valstu teritorijā.

26. Pašvaldība nodrošina, ka vismaz reizi gadā pašvaldības pārstāvis apmeklē Drošības incidentu novēršanas institūcijas organizētu apmācību informācijas tehnoloģiju drošības jautājumos.

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

III. Informācijas fiziskā aizsardzība

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

29. Serveru telpas ir aprīkotas ar:
29.1. ugunsgrēka signalizācijas iekārtu;

29.2. ugunsdzēšamo aparātu;
29.3. gaisa kondicionēšanas iekārtu;
29.4. nepārtrauktās barošanas avotu (UPS);
29.5. apsardzes signalizāciju;
29.6. diviem neatkarīgiem elektrības pievadiem.

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

31. 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.

32. 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.

33. 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

34. Ja Pašvaldība sistēmas uzturēšanai slēdz ārpakalpojuma līgumu ar pakalpojuma sniedzēju, līguma izpildi uzrauga atbildīgā persona un līgumā iekļauj vismaz šādas drošības prasības:
34.1. saņemamā ārpakalpojuma aprakstu;
34.2. precīzas prasības attiecībā uz ārpakalpojuma apjomu un kvalitāti;
34.3. Pašvaldības un ārpakalpojuma sniedzēja tiesības un pienākumus, tai skaitā:
34.3.1. Pašvaldības tiesības pastāvīgi uzraudzīt ārpakalpojuma sniegšanas kvalitāti;
34.3.2. Pašvaldības tiesības dot ārpakalpojuma sniedzējam obligāti izpildāmus norādījumus jautājumos, kas saistīti ar ārpakalpojuma godprātīgu, kvalitatīvu, savlaicīgu un normatīvajiem aktiem atbilstošu izpildi;
34.3.3. 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;
34.3.4. ārpakalpojuma sniedzēja pienākumu nodrošināt Pašvaldībai iespēju pastāvīgi uzraudzīt ārpakalpojuma sniegšanas kvalitāti.
34.3.5. ārpakalpojuma sniedzēja pienākumu nekavējoties ziņot par informācijas tehnoloģiju drošības incidentu un veikt visas tā novēršanai nepieciešamās darbības;
34.3.6. ārpakalpojuma sniedzēja pienākumu informēt par apakšuzņēmēju un viņa atbilstību šajos noteikumos un līgumā noteiktajām drošības prasībām;
34.4. normatīvajos aktos noteiktās un citas institūcijas vadītāja identificētās sistēmai veicamās drošības pārbaudes;

34.5. piekļuves prasības datiem un to uzglabāšanai, kā arī pienākumu piegādātājam pēc līguma termiņa beigām dzēst viņa rīcībā nonākušos datus, izņemot gadījumu, ja atkārtoti slēdz līgumu ar to pašu pakalpojuma sniedzēju par to pašu līguma priekšmetu.

35. Ja Pašvaldība uzsāk iepirkumu par esošās sistēmas uzlabojumiem, tā nodrošina, ka atbilstošās drošības prasības tiek iekļautas iepirkuma specifikācijā.

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

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

36.2. 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;

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

37. Domes vadība, slēdzot līgumu par informācijas un komunikācijas tehnoloģiju sistēmu izstrādi, ieviešanu vai uzturēšanu, nosaka atbildīgo personu, kas uzrauga informācijas un komunikācijas tehnoloģiju sistēmu izstrādi, ieviešanu un uzturēšanas ārpakalpojuma līguma izpildi.

38. Iegādājoties pakalpojumu, programmatūru vai iekārtu, Pašvaldība iepirkuma specifikācijā un līgumā iekļauj pienākumu pakalpojuma sniedzējam un produkta ražotājam līguma darbības laikā informēt vai publicēt informāciju par atklātajām informācijas un komunikācijas tehnoloģiju produkta vai pakalpojuma ievainojamībām, to novēršanas pasākumiem un termiņiem.

39. Pašvaldība, slēdzot iepirkuma līgumu par maršrutētāju, komutatoru, ārējo ugunsmūru, ielaušanās atklāšanas sistēmu, pretielaušanās sistēmu, antivīrusu programmatūru iegādi, kā arī par pakalpojumiem, programmatūrām vai iekārtām, kas nodrošina pamata drošības sistēmu aizsardzības un uzraudzības funkcijas, ievēro šo noteikumu 36.1 punktā noteiktās prasības. Slēdzot vispārīgo vienošanos, tās noteikumos ietver norādi uz šo noteikumu 36.1 punktā noteiktajiem ierobežojumiem, kas piemērojami, vienošanās ietvaros slēdzot iepirkuma līgumus šajā punktā minēto preču vai pakalpojumu iegādei.

40. Paaugstinātas drošības sistēmu uzturēšanas ārpakalpojuma līgumu atļauts slēgt vienīgi ar:

40.1. juridisku personu:

40.1.1. kas ir reģistrēta NATO, Eiropas Savienības vai Eiropas Ekonomikas zonas dalībvalstī;

40.1.2. kuras patiesais labuma guvējs ir NATO, Eiropas Savienības, Eiropas Ekonomikas zonas valsts pilsonis vai Latvijas Republikas nepilsonis;

40.1.3 kuras pakalpojuma nodrošināšanai izmantoto programmatūru vai iekārtu ražotājs ir juridiska persona, kas reģistrēta NATO, Eiropas Savienības vai Eiropas Ekonomikas zonas dalībvalstī, vai fiziska persona, kas ir Latvijas Republikas

valstspiederīgais, NATO, Eiropas Savienības vai Eiropas Ekonomikas zonas valsts pilsonis;

40.2. fizisku personu, kas ir NATO, Eiropas Savienības, Eiropas Ekonomikas zonas valsts pilsonis vai Latvijas Republikas nepilsonis.

41. Līgumu par pakalpojumu, programmatūru vai iekārtu iegādi paaugstinātas drošības sistēmām atļauts slēgt ar:

41.1. juridisku personu:

41.1.1. kas ir reģistrēta NATO, Eiropas Savienības vai Eiropas Ekonomikas zonas dalībvalstī;

41.1.2. kuras patiesais labuma guvējs ir NATO, Eiropas Savienības, Eiropas Ekonomikas zonas valsts pilsonis vai Latvijas Republikas nepilsonis;

41.1.3. kuras pakalpojuma nodrošināšanai izmantoto programmatūru vai iekārtu ražotājs ir juridiska persona, kas reģistrēta NATO, Eiropas Savienības vai Eiropas Ekonomikas zonas dalībvalstī, vai fiziska persona, kas ir Latvijas Republikas valstspiederīgais, NATO, Eiropas Savienības vai Eiropas Ekonomikas zonas valsts pilsonis;

41.2. fizisku personu, kas ir Latvijas Republikas valstspiederīgais, NATO, Eiropas Savienības vai Eiropas Ekonomikas zonas valsts pilsonis.

V. Rezerves kopiju veidošanas kārtība

42. Datortīkla administrators nodrošina Pašvaldības informācijas resursu rezerves kopiju veidošanu tām informācijas sistēmām/resursiem, kas ir izvietoti uz pašvaldības serveriem/darba stacijām.

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

44. Informācijas sistēmas drošības pārvaldnieks nosaka vietu, kur tiks glabātas rezerves kopijas uz ārējā datu nesēja.

45. Datortīkla administrators nodrošina Pašvaldības informācijas resursu atjaunošanu no rezerves kopijām pēc Informācijas sistēmas drošības pārvaldnieka pieprasījuma.

46. Datortīkla administratoram sadarbībā ar Informācijas sistēmas drošības pārvaldnieku ir pienākums vismaz reizi gadā veikt pārbaudi par informācijas sistēmu atjaunošanas iespējām no rezerves kopijām, par to rezultātiem informējot Informācijas sistēmas drošības pārvaldnieku.

VI. Elektronisko datu nesēju iznīcināšanas procedūra

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

VII. Noslēguma jautājumi

48. Noteikumi stājas spēkā ar 2022.gada 1.martu.

49. Ar šo noteikumu spēkā stāšanos spēku zaudē Viļakas novada Domes 2018.gada 5.jūlija Informācijas tehnoloģiju drošības politika.

Domes priekšsēdētājs Sergejs Maksimovs