



BEVERĪNAS NOVADA PAŠVALDĪBA

Reģistrācijas Nr.90009115285

“Pagastmāja”, Mūrmuiža, Kauguru pag., Beverīnas nov., LV-4224, tālr. 64281737, fax 64220890, e-pasts:pasvaldiba@beverina.lv,

Beverīnas novada Kauguru pagastā

2019.gada 30.maijā

APSTIPRINĀTS

ar Beverīnas novada pašvaldības domes 30.05.2019. sēdes lēmumu Nr.85 (protokols Nr.5, 10.§)

Beverīnas novada pašvaldības Informācijas sistēmas drošības politika

Izdota saskaņā Ministru kabineta 2015. gada 28. jūlija noteikumu Nr. 442 “Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām” 8.1. punktu

I. Vispārīgie jautājumi

1. Informācijas sistēmas drošības politika nosaka politiku, kādā Beverīnas novada pašvaldība (turpmāk – Pašvaldība) nodrošina pašvaldības izmantotās informācijas sistēmas aizsardzību pret ārējiem un iekšējiem riskiem un nodrošina informācijas sistēmas pieejamību, integritāti un konfidencialitāti saskaņā ar spēkā esošajiem normatīvajiem aktiem.
2. Informācijas sistēmas drošības politika ir saistoša Informācijas sistēmu drošības pārvaldniekam un Datortīklu administratoram.
3. Politikā lietotie termini:
 - 3.1. **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.
 - 3.2. **Beverīnas novada pašvaldība** – institūcija, kas normatīvajos aktos noteiktajā kārtībā organizē un vada informācijas sistēmu darbību.
 - 3.3. **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.
 - 3.4. **Informācijas sistēmas lietotājs** – persona, kurai ir piešķirtas piekļuves tiesības informācijas sistēmās.
4. Informācijas sistēmas drošības politika ir izstrādāta saskaņā ar Informācijas tehnoloģiju drošības likumu, Valsts informācijas sistēmu likumu, 2015.gada 28.jūlija Ministru kabineta noteikumu Nr.442 „Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām” 8.1. punktu un citu LR normatīvo aktu prasībām, kā arī ievērojot Latvijas standartu LVS ISO/IEC 27001:2013“

Informācijas tehnoloģija. Drošības paņēmieni. Informācijas drošības pārvaldības sistēmas. Prasības”.

II. Informācijas sistēmas drošības politikas mērķi un pamatnostādnes

5. Pašvaldības pienākums ir nodrošināt, lai to rīcībā esošā informācija tiktu apstrādāta, glabāta un pārvaldīta droši un pārbaudāmi, sniedzot tās darbiniekiem un lietotājiem skaidri noteiktas prasības informācijas sistēmas iekārtu un resursu izmantošanā, un nodrošinot Informācijas sistēmas aizsardzību no ārējiem un iekšējiem, apzinātiem un nejaušiem apdraudējumiem.
6. Informācijas sistēmas drošības politika attiecas uz visiem Pašvaldības Informācijas sistēmas lietotājiem, kuri veic darbības ar informācijas resursiem (piemēram, informācijas sistēmām, informāciju, kas tiek saņemta, apstrādāta, ievadīta, pārsūtīta vai uzglabāta) un tehniskajiem resursiem (piemēram, datoru sistēmām, datoru tīkliem), t.sk.:
 - 6.1. Pilna darba laika, nepilnas slodzes un līgumdarbiniekiem, kuri ir nodarbināti pašvaldībā;
 - 6.2. Lietotājiem, kuri ir noslēguši līgumu ar pašvaldību par datu lietošanu vai kuri uz pieprasījuma pamata saņem datus no pašvaldības izmantotām informācijas sistēmām;
 - 6.3. Ārpakalpojumu sniedzējiem vai konsultantiem, kuri strādā pašvaldības labā.
7. Informācijas sistēmas lietotājs, kurš nodarbināts Pašvaldībā un ir Pašvaldības darbinieks (pilna darba laika, nepilnas slodzes un līgumdarbiniekiem), atbild par drošības politikas nosacījumu un prasību ievērošanu, kas ir minēti šādos dokumentos:
 - 7.1. Informācijas sistēmas drošības politikā;
 - 7.2. Informācijas sistēmas lietošanas noteikumos.
8. Informācijas sistēmu lietotājs par iepazīšanās ar augstāk minētajiem dokumentiem un to ievērošanu paraksta pielikumu “Informācijas sistēmas lietotāja apliecinājums par “Informācijas sistēmas drošības politikas” prasību ievērošanu”.
9. Informācijas sistēmas drošības pārvaldnieks atbild par drošības politikas nosacījumu un prasību ievērošanu.
10. Pašvaldības iestāžu un struktūrvienību vadītāji ir atbildīgi par viņu pakļautībā vai uzraudzībā esošajiem Informācijas sistēmas lietotājiem. Pašvaldības iestāžu un struktūrvienību vadītāji nodrošina, ka personāls, uz kuru šī politika attiecas daļēji vai pilnā apmērā, ir informēts par politikas esamību un pilda savus darba pienākumus atbilstoši politikas nostādņēm.
11. Informācijas sistēmas drošība tiek nodrošināta šādu mērķu realizācijai:
 - 11.1. nodrošinātu informācijas pieejamību;
 - 11.2. nodrošinātu informācijas integritāti;
 - 11.3. nodrošinātu informācijas konfidencialitāti;
 - 11.4. aizsargātu sistēmas informācijas resursus;
 - 11.5. aizsargātu sistēmas tehniskos resursus;
 - 11.6. noteiktu sistēmas drošības apdraudējumu;
 - 11.7. novērtētu sistēmas drošības risku;
 - 11.8. atklātu sistēmas drošības incidentu;
 - 11.9. atjaunotu sistēmas darbību pēc sistēmas drošības incidenta.
12. Pašvaldībā izmantotās informācijas sistēmām ir šādas drošības (pieejamības, integritātes un konfidencialitātes) klases:

- 12.1. C pieejamības klase - sistēmas nodrošinātā pakalpojuma neplānots pārtraukums sistēmas paredzētajā darba laikā drīkst būt ilgāks par 24 stundām mēnesī (summāri);
- 12.2. C integritātes klase - atsevišķu sistēmā glabāto datu integritātes apdraudējums rada risku Pašvaldības pamatfunkciju nodrošināšanai;
- 12.3. A konfidencialitātes klase - sistēmā tiek apstrādāti īpašo kategoriju personas dati vai sistēmā glabātās informācijas neatļauta izpaušana vai noplūde var radīt smagākas sekas nekā kaitējums pašvaldības, citu institūciju vai Latvijas Republikas reputācijai.
13. Pašvaldības būtiskākās informācijas sistēmās (piemēram, Iedzīvotāju reģistrs un Sociālās palīdzības uzskaites sistēma) tiek apstrādāti īpašo kategoriju personas dati, tādejādi tās ir uzskatāmas par paaugstinātam drošības sistēmām.
14. Vienotai un efektīvai informāciju sistēmu drošības pārvaldībai, pašvaldība piemēro paaugstinātas drošības sistēmas prasības arī visām pārējām izmantotajām informācijas sistēmām.
15. Informācijas tehnoloģiju drošības pārvaldību un Informācijas sistēmas drošības politikas koordināciju pašvaldībā veic datortīklu administrators.

III. Informācijas sistēmas drošības organizācija

16. Informācijas sistēmas drošības organizatoriskās struktūras pamatu veido Informācijas sistēmas drošības pārvaldnieks, datortīklu administrators un Informācijas sistēmas lietotāji.
17. Informācijas sistēmas drošības pārvaldnieks nodrošina informācijas sistēmas drošības politikas realizāciju, kā arī veic šādas darbības:
 - 17.1. kopā ar datortīklu administratoru aktualizē drošības politiku, izstrādā ar informācijas sistēmas drošības saistīto iekšējo normatīvo aktu projektus un veic tās koordināciju.
 - 17.2. aktualizē Informācijas sistēmas drošības politiku un to saistītos dokumentus vismaz vienu reizi gadā, kā arī šādos gadījumos:
 - 17.2.1. ja izmaiņas sistēmā var ietekmēt sistēmas drošību;
 - 17.2.2. ja mainījušies vai ir atklāti jauni sistēmas drošības apdraudējumi;
 - 17.2.3. ja pēkšņi pieaug sistēmas drošības incidentu skaits vai ir noticis nozīmīgs sistēmas drošības incidents;
 - 17.2.4. ja izmaiņas Pašvaldības organizatoriskajā struktūrā skar sistēmas drošības vadības organizāciju;
 - 17.2.5. ja izdarīti grozījumi normatīvajos aktos, kas regulē sistēmas darbību.
 - 17.3. nodrošina informācijas sistēmās izmantojamās informācijas racionālu un pareizu izmantošanu.
 - 17.4. izskata informācijas sistēmas lietotāju tiesību piešķiršanas un izmaiņu veikšanas pieteikumu autorizāciju saskaņā ar Informācijas sistēmas lietošanas noteikumiem;
 - 17.5. piedalās Risku vadības procesā saskaņā ar Informācijas drošības riska pārvaldības plānu.
 - 17.6. nodrošina atbilstošu atbalstu, palīdzību un konsultāciju sniegšanu personālam, lai tas varētu pildīt savus pienākumus atbilstoši šīs politikas prasībām.
 - 17.7. Informācijas sistēmas drošības pārvaldnieks vai pašvaldības izpilddirektors Informācijas sistēmas drošības pārvaldnieka prombūtnes gadījumā ieceļ tā pienākumu aizvietotāju.

18. Datortīklu administrators pienākums ir:
 - 18.1.nodrošināt tehnisko resursu racionālu un pareizu izmantošanu.
 - 18.2.nodrošināt tehnisko resursu fiziskās un loģiskās aizsardzības pasākumus saskaņā ar Informācijas sistēmas drošības noteikumiem.
 - 18.3.sadarboties ar informācijas sistēmas drošības pārvaldnieku, nodrošinot nepieciešamo tehnisko risinājumu attiecīgajam informācijas resursam.
 - 18.4.veikt Risku vadības procesa koordināciju pašvaldībā saskaņā ar Informācijas drošības riska pārvaldības plānu.
 - 18.5.palīdzēt Informācijas sistēmas drošības pārvaldniekam izmeklēt informācijas drošības incidentus.
 - 18.6.veikt regulāras pārbaudes, lai pārlicinātos, ka tiek ievērotas Informācijas sistēmas drošības politikas un to saistošo dokumentu prasības.
 - 18.7.nodrošināt informācijas sistēmas atjaunošanas procedūras, ja tehnoloģiskie resursi ir bojāti un informācijas sistēmas funkcionēšana traucēta vai neiespējama saskaņā ar Informācijas sistēmas drošības noteikumiem un Informācijas sistēmu atjaunošanas plānu.
 - 18.8.nodrošināt atbilstošu atbalstu, palīdzību un konsultāciju sniegšanu personālam, lai tas varētu pildīt savus pienākumus atbilstoši Informācijas sistēmas drošības politikas prasībām.
19. Informācijas sistēmas lietotāja pienākums ir racionāli un lietderīgi izmantot informācijas sistēmas un to datus sava darbu pienākumu veikšanai.

IV. Informācijas resursu klasifikācija

20. Visiem Pašvaldības informācijas resursiem (t.sk., darba stacijām, serveriem, perifērijas iekārtām, programmatūrai, Informācijas sistēmas datiem) ir jābūt uzskaitītiem un reģistrētiem, kā arī Informācijas sistēmas datiem ir jābūt klasificētiem.
21. Pašvaldības informācijas resursu klasificēšana tiek veikta atbilstoši Informācijas atklātības likumam un noteikta ar rīkojumu par ierobežotas pieejamības informācijas statusa noteikšanu.

V. Informācijas resursu riska analīze

22. Informācijas resursu riska analīzes mērķis ir nodrošināt atbilstošu Informācijas sistēmas vadību un kontroles sistēmas darbības efektivitāti, lai atklātu un novērstu kļūdas un neprecizitātes, un nepieciešamības gadījumā veiktu labojumus drošības sistēmā.
23. Pašvaldības informācijas resursu riska analīze tiek veikta atbilstoši Informācijas sistēmas drošības riska pārvaldības plānam.

VI. Informācijas resursu loģiskā drošība

24. Pašvaldības Informācijas sistēmas lietotājiem pieejas tiesību piešķiršana, izmainīšana un anulēšana tiek veikta atbilstoši Informācijas sistēmas lietošanas noteikumiem un Informācijas sistēmas drošības noteikumiem.

25. Informācijas sistēmas lietotāju pienākumi attiecībā uz informācijas resursu lietošanu, interneta izmantošanu un tehnisko resursu fizisko drošību ir iekļauti Informācijas sistēmas lietošanas noteikumos.
26. Pašvaldības datortīklu, serveru un to saistīto iekārtu uzturēšanu un administrēšanu, kā arī Informācijas sistēmas lietotāju datoru uzstādīšanu un administrēšanu veic datortīklu administrators, kura pienākumi ir iekļauti Informācijas sistēmas drošības noteikumos.

VII. Tehnisko resursu fiziskā drošība

27. Pašvaldības datorsistēmas un tehnika (t.sk. datortīkli, programmatūra, informācijas sistēmas, serveri, datori) tiek aizsargāta ar piemērotu fizisko, tehnisko, organizatorisko un vides kontroļu kopumu.
28. Serveri un datori tiek novietoti aizslēgtās telpās, kurās pieeja ir tikai atbilstošām personām, nodrošinot fizisko aizsardzību no trešajām personām pret piekļūšanu šiem resursiem. Par serveru fizisko drošību pašvaldībā atbild datortīklu administrators, savukārt par atbilstošo datoru fizisko drošību atbild attiecīgais Informācijas sistēmas lietotājs.
29. Informācijas sistēmas lietotāju pienākumi attiecībā uz tehnisko resursu fizisko drošību ir iekļauti Informācijas sistēmas lietošanas noteikumos.

VIII. Darbības nepārtrauktības nodrošināšana

30. Pašvaldības informācijas sistēmām un elektroniskā veidā saglabātai informācijai regulāras rezerves kopijas veidošanu nodrošina datortīklu administrators atbilstoši Informācijas sistēmas drošības noteikumiem.
31. Katram Informācijas sistēmas lietotājam, kas ir nodarbināts pašvaldībā, ir jāveic un jānodrošina darbības nepārtrauktību tādā apjomā, kādā tā ir noteikta konkrētā darbinieka pienākumos un cik tas nepieciešams darbinieka tiešajiem darba pienākumiem.
32. Par visām avārijas situācijām (t.sk. ugunsgrēku, plūdiem, nelaiemes gadījumiem utt.) Informācijas sistēmas lietotājiem un datortīklu administratoram ir nekavējoši jāpaziņo pašvaldības izpilddirektoram.

Domes priekšsēdētājs

M.Zvirbulis

**INFORMĀCIJAS SISTĒMAS LIETOTĀJA APLIECINĀJUMS
PAR “INFORMĀCIJAS SISTĒMAS DROŠĪBAS POLITIKAS” PRASĪBU
IEVĒROŠANU**

Ar šo es, zemāk parakstījies, apliecinu:

1. Esmu iepazinies(usies), izprotu un apņemos ievērot Informācijas drošības politikas nosacījumus un prasības ievērošanu, kas ir minēti šādos dokumentos:
 - 1.1. Informācijas sistēmas drošības politikā;
 - 1.2. Informācijas sistēmas lietošanas noteikumos;
2. Apņemos neizmantot konfidenciālu informāciju, kas saņemta no Beverīnas novada domes, savu vai trešo personu interesēs, kā arī apņemos ievērot Vispārīgās datu aizsardzības regulas un Informācijas atklātības likuma prasības.
3. Es piekrītu, ka pārtraucot darba tiesiskās attiecības, es nekavējoties nodošu Pašvaldībai manā rīcībā esošo programmatūru un tehnisko aprīkojumu, kā arī manā rīcībā esošos informācijas oriģinālus un kopijas, ko esmu saņēmis(-usi) darba (līguma izpildes) laikā, un kas ir manā rīcībā vai kas ir citādi tieši vai netieši manā pārvaldībā.
4. Apņemos saglabāt informācijas konfidencialitāti arī pēc darba (līguma izpildes)tiesisko attiecību izbeigšanas.

_____ Struktūrvienība un amats	_____ Paraksts	_____ Paraksta atšifrējums	_____ Datums
_____ Struktūrvienība un amats	_____ Paraksts	_____ Paraksta atšifrējums	_____ Datums
_____ Struktūrvienība un amats	_____ Paraksts	_____ Paraksta atšifrējums	_____ Datums
_____ Struktūrvienība un amats	_____ Paraksts	_____ Paraksta atšifrējums	_____ Datums

...