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

APSTIPRINĀTA
ar Balvu novada Domes
2022.gada 24.februāra
lēmumu (sēdes protokols Nr.6., 39.§)

2022.gada 24.februārī

Informācijas sistēmu drošības politika

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" 8.1. un 11.punktu

I. Vispārīgie jautājumi

1. Informācijas sistēmu drošības politika nosaka politiku, kādā Balvu novada pašvaldība un tās iestādes (turpmāk – Pašvaldība) nodrošina pašvaldības izmantoto informācijas sistēmu aizsardzību pret ārējiem un iekšējiem riskiem un nodrošina informācijas sistēmu pieejamību, integritāti un konfidencialitāti saskaņā ar spēkā esošajiem normatīvajiem aktiem.

2. Politikā 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 sistēmas drošības politika ir izstrādāta saskaņā ar Informācijas tehnoloģiju drošības likumu, Valsts informācijas sistēmu likumu, Fizisko personu datu apstrādes likumu, 2015.gada 28.jūlija MK noteikumu Nr.442 „Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" 8.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

4. 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.

5. 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.:

5.1. pilna darba laika, nepilnas slodzes un līgumdarbiniekiem, kuri ir nodarbināti Pašvaldībā;

5.2. lietotājiem, kuri ir noslēguši līgumu ar Pašvaldību par datu lietošanu vai kuri uz pieprasījuma pamata saņem datus no Pašvaldības izmantotām informācijas sistēmām;

5.3. ārpakalpojumu sniedzējiem vai konsultantiem, kuri strādā Pašvaldības labā.

6. Informācijas sistēmas lietotājs, kas ir 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:

6.1. Informācijas sistēmu drošības politikā.

6.2. Informācijas sistēmu lietošanas noteikumos.

7. Informācijas sistēmu lietotājs par iepazīšanos ar augstāk minētajiem dokumentiem un to ievērošanu paraksta Informācijas sistēmas lietotāja apliecinājumu (1.Pielikums "Informācijas sistēmas lietotāja apliecinājums par "Informācijas sistēmas drošības politikas" prasību ievērošanu").

8. Informācijas sistēmas drošības pārvaldnieks atbild par drošības politikas nosacījumu un prasību ievērošanu, kas ir minēti šādos dokumentos:

8.1. Informācijas sistēmu drošības politikā;

8.2. Informācijas sistēmu lietošanas noteikumos;

8.3. Informācijas sistēmu drošības noteikumos;

8.4. Informācijas sistēmu drošības riska pārvaldības plānā;

8.5. Informācijas sistēmu atjaunošanas plānā.

9. 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 nostādnēm.

10. Informācijas sistēmas drošība tiek nodrošināta šādu mērķu realizācijai:
10.1. nodrošinātu informācijas pieejamību;
10.2. nodrošinātu informācijas integritāti;
10.3. nodrošinātu informācijas konfidencialitāti;
10.4. aizsargātu sistēmas informācijas resursus;
10.5. aizsargātu sistēmas tehniskos resursus;
10.6. noteiktu sistēmas drošības apdraudējumu;
10.7. novērtētu sistēmas drošības risku;
10.8. atklātu sistēmas drošības incidentu;
10.9. atjaunotu sistēmas darbību pēc sistēmas drošības incidenta.

11. Pašvaldības informācijas sistēmas tiek iedalītas paaugstinātas drošības un pamata drošības sistēmās atbilstoši to drošības klasei. Pašvaldības informācijas sistēmas iedalījums ir iekļauts 2.Pielikumā "Balvu novada pašvaldības informācijas sistēmu iedalījums".

12. Pašvaldībā tiek izmantotas šādas drošības (pieejamības, integritātes un konfidencialitātes) klases:
12.1. Pieejamība:
12.1.1. ja sistēmas nodrošinātā pakalpojuma neplānots pārtraukums sistēmas paredzētajā darba laikā drīkst būt ilgāks par 24 stundām mēnesī (summāri), sistēmai piešķir C pieejamības klasi;
12.1.2. ja sistēmas nodrošinātā pakalpojuma neplānotam pārtraukumam sistēmas paredzētajā darba laikā jābūt ne lielākam par 24 stundām (summāri) mēnesī, bet tas pieļaujams lielāks par četrām stundām (summāri) mēnesī, sistēmai piešķir B pieejamības klasi;
12.1.3. ja sistēmas nodrošinātā pakalpojuma neplānotam pārtraukumam sistēmas paredzētajā darba laikā jābūt ne lielākam par četrām stundām mēnesī (summāri), sistēmai piešķir A pieejamības klasi;
12.2. Integritāte:
12.2.1. ja sistēmā glabāto datu integritātes apdraudējums nerada risku institūcijas pamatfunkciju nodrošināšanai, sistēmai piešķir C integritātes klasi;
12.2.2. ja atsevišķu sistēmā glabāto datu integritātes apdraudējums rada risku institūcijas pamatfunkciju nodrošināšanai, sistēmai piešķir B integritātes klasi;
12.2.3. ja sistēmā glabāto datu integritātes apdraudējums rada risku institūcijas pamatfunkciju nodrošināšanai vai atsevišķu sistēmā glabāto datu integritātes apdraudējums var apdraudēt Latvijas Republikas nacionālās intereses un pamatvērtības vai izraisīt katastrofu, sistēmai piešķir A integritātes klasi;
12.3. Konfidencialitāte:
12.3.1. ja sistēma satur tikai publiski pieejamu informāciju vai sistēmā glabātās informācijas neatļauta izpaušana vai noplūde nerada risku institūcijai, sistēmai piešķir C konfidencialitātes klasi;
12.3.2. ja sistēmā tiek apstrādāta ierobežotas pieejamības informācija, izņemot sensitīvus personas datus, vai sistēmā glabātās informācijas neatļauta izpaušana vai noplūdes vienīgās sekas ir iespējamais kaitējums institūcijas, citu institūciju vai Latvijas Republikas reputācijai, sistēmai piešķir B konfidencialitātes klasi;

12.3.3. ja sistēmā tiek apstrādāti sensitīvi personas dati vai sistēmā glabātās informācijas neatļauta izpaušana vai noplūde var radīt smagākas sekas nekā kaitējums institūcijas, citu institūciju vai Latvijas Republikas reputācijai, sistēmai piešķir A konfidencialitātes klasi;

12.4. Ja sistēmai piešķirtas trīs B drošības klases vai vismaz viena A drošības klase, sistēma ir uzskatāma par paaugstinātas drošības sistēmu.

13. Vienotai un efektīvai informāciju sistēmu drošības pārvaldībai, pašvaldība piemēro paaugstinātas drošības sistēmas prasības arī visām pārējām izmantotajām informācijas sistēmām.

14. Informācijas tehnoloģiju drošības pārvaldību un Informācijas sistēmu drošības politikas koordināciju Pašvaldībā veic Informācijas sistēmas drošības pārvaldnieks.

III. Informācijas sistēmas drošības organizācija

15. Informācijas sistēmas drošības organizatoriskās struktūras pamatu veido Informācijas sistēmas drošības pārvaldnieks, Pašvaldības un tās iestāžu datorspeciālisti (turpmāk tekstā – Datortīkla administrators) un Informācijas sistēmas lietotāji.

16. Informācijas sistēmas drošības pārvaldnieks nodrošina informācijas sistēmas drošības politikas realizāciju, kā arī veic šādas darbības:

16.1. kopā ar Datortīkla administratoram aktualizē drošības politiku, izstrādā ar informācijas sistēmas drošības saistīto iekšējo normatīvo aktu projektus un veic tās koordināciju;

16.2. aktualizē Informācijas sistēmas drošības politiku un to saistītos dokumentus vismaz vienu reizi gadā, kā arī šādos gadījumos:

16.2.1. ja izmaiņas sistēmā var ietekmēt sistēmas drošību;

16.2.2. ja mainījušies vai ir atklāti jauni sistēmas drošības apdraudējumi;

16.2.3. ja pēkšņi pieaug sistēmas drošības incidentu skaits vai ir noticis nozīmīgs sistēmas drošības incidents;

16.2.4. ja izmaiņas Pašvaldības organizatoriskajā struktūrā skar sistēmas drošības vadības organizāciju;

16.2.5. ja izdarīti grozījumi normatīvajos aktos, kas regulē sistēmas darbību.

16.3. nodrošina informācijas sistēmās izmantojamās informācijas racionālu un pareizu izmantošanu;

16.4. izskata informācijas sistēmas lietotāju tiesību piešķiršanas un izmaiņu veikšanas pieteikumu autorizāciju saskaņā ar Informācijas sistēmu lietošanas noteikumiem;

16.5. piedalās risku vadības procesā saskaņā ar Informācijas drošības riska pārvaldības plānu;

16.6. nodrošina atbilstošu atbalstu, palīdzību un konsultāciju sniegšanu personālam, lai tas varētu pildīt savus pienākumus atbilstoši šīs politikas prasībām;

16.7. Pašvaldības izpilddirektors Informācijas sistēmas drošības pārvaldnieka prombūtnes gadījumā ieceļ tā pienākumu aizvietotāju.

17. Datortīkla administratora pienākumi ir:

17.1. nodrošināt tehnisko resursu racionālu un pareizu izmantošanu;

17.2. nodrošināt tehnisko resursu fiziskās un loģiskās aizsardzības pasākumus saskaņā ar Informācijas sistēmu drošības noteikumiem;

17.3. sadarboties ar Informācijas sistēmas drošības pārvaldnieku, nodrošinot nepieciešamo tehnisko risinājumu attiecīgajam informācijas resursam;

17.4. veikt risku vadības procesa koordināciju pašvaldībā saskaņā ar Informācijas drošības riska pārvaldības plānu;

17.5. palīdzēt Informācijas sistēmas drošības pārvaldniekam izmeklēt informācijas drošības incidentus;

17.6. veikt regulāras pārbaudes, lai pārliecinātos, ka tiek ievērotas Informācijas sistēmas drošības politikas un to saistošo dokumentu prasības;

17.7. 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;

17.8. nodrošināt atbilstošu atbalstu, palīdzību un konsultāciju sniegšanu personālam, lai tas varētu pildīt savus pienākumus atbilstoši Informācijas sistēmas drošības politikas prasībām.

18. Informācijas sistēmas lietotāja pienākums ir racionāli un lietderīgi izmantot informācijas sistēmas un to datus tikai darbu pienākumu veikšanai.

IV. Informācijas resursu klasifikācija

19. 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.

20. 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

21. 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.

22. Pašvaldības informācijas resursu riska analīze tiek veikta atbilstoši Informācijas sistēmu drošības riska pārvaldības plānam.

VI. Informācijas resursu loģiskā drošība

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

24. Informācijas sistēmas lietotāju pienākumi attiecībā uz informācijas resursu lietošanu, interneta izmantošanu un tehnisko resursu fizisko drošību ir iekļauti Informācijas sistēmu lietošanas noteikumos.

25. Pašvaldības datortīklu, serveru un to saistīto iekārtu uzturēšanu un administrēšanu, kā arī Informācijas sistēmas lietotāju datoru uzstādīšanu un administrēšanu veic Datortīkla administrators, kuru pienākumi ir iekļauti Informācijas sistēmu drošības noteikumos.

VII. Tehnisko resursu fiziskā drošība

26. Pašvaldības datorsistēmas un tehnika (t.sk. datortīkli, programmatūra, informācijas sistēmas, serveri, datori) tiek aizsargāta ar piemērotu fizisko, tehnisko, organizatorisko un vides kontroļu kopumu.

27. 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 Datortīkla administrators, savukārt par atbilstošo datoru fizisko drošību atbild attiecīgais Informācijas sistēmas lietotājs.

28. Informācijas sistēmas lietotāju pienākumi attiecībā uz tehnisko resursu fizisko drošību ir iekļauti Informācijas sistēmas lietošanas noteikumos.

VIII. Darbības nepārtrauktības nodrošināšana

29. Pašvaldības informācijas sistēmām un elektroniskā veidā saglabātai informācijai regulāras rezerves kopijas veidošanu nodrošina Datortīkla administrators atbilstoši Informācijas sistēmas drošības noteikumiem vai arī pakalpojuma sniedzējs, balstoties uz savstarpēji noslēgto līgumu.

30. 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.

31. Par visām avārijas situācijām (t.sk. ugunsgrēku, plūdiem, nelaimes gadījumiem utt.) Informācijas sistēmas lietotājiem un Datortīkla administratoram ir nekavējoši jāpaziņo Pašvaldības izpilddirektoram un Informācijas sistēmas drošības pārvaldniekam.

Domes priekšsēdētājs Sergejs Maksimovs

1. Pielikums
"Balvu novada pašvaldības
Informācijas sistēmas drošības politikai"

INFORMĀCIJAS SISTĒMAS LIETOTĀJA APLIECINĀJUMS PAR "INFORMĀCIJAS SISTĒMU DROŠĪBAS POLITIKAS" PRASĪBU IEVĒROŠANU

Ar šo es, zemāk parakstījies, apliecinu:

1. Esmu iepazinies(usies), izprotu un apņemos ievērot Informācijas drošības politikas nosacījumus un prasības, kas ir minētas šādos dokumentos:
   1.1. Informācijas sistēmu drošības politikā;
   1.2. Informācijas sistēmu lietošanas noteikumos.

2. Apņemos neizmantot konfidenciālu informāciju, kas saņemta no Balvu novada pašvaldības, savu vai trešo personu interesēs.

3. Es piekrītu, ka pārtraucot darba (līguma) attiecības ar Balvu novada pašvaldību jebkādu iemeslu dēļ, es nekavējoties nodošu Balvu novada 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.

_____	_____	_____	_____
Iestāde/struktūrvienība un amats	/Paraksts/	Paraksta atšifrējums	Datums

Domes priekšsēdētājs Sergejs Maksimovs

2. Pielikums
“Balvu novada pašvaldības
Informācijas sistēmas drošības politikai”

BALVU NOVADA PAŠVALDĪBAS
INFORMĀCIJAS SISTĒMU IEDALĪJUMS

Nr.	Informācijas sistēmas nosaukums	Pieejamības klase	Integritātes klase	Konfidencialitātes klase	Pamata vai Paaugstinātas drošības sistēma

Domes priekšsēdētājs Sergejs Maksimovs