LATVIJAS REPUBLIKA
INČUKALNA NOVADA DOME

Reģ.Nr.90000068337, Atmodas iela 4, Inčukalns, Inčukalna pagasts, Inčukalna novads, LV-2141
Tālr./fakss 67977310, mob.t. 26181294, e-pasts: dome@incukalns.lv

NOTEIKUMI
Inčukalnā

2019.gada 22.maijā Nr.4/2019
protokols Nr. 8-36.§

.

Informācijas sistēmas drošības politika

I.Vispārīgie jautājumi

1. Informācijas sistēmas drošības politika nosaka politiku, kādā Inčukalna 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 attiecas uz visiem Pašvaldības iestāžu Informācijas sistēmas lietotājiem, kuriem ir pieeja kādai(ām) no valsts informāciju sistēmām (piemēram, Iedzīvotāju reģistram).
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. **Inčukalna novada pašvaldība** – institūcija, kas normatīvajos aktos noteiktajā kārtībā organizē un vada informācijas sistēmu darbību.

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

3.4. **IS drošības speciālists** - atbildīgie Informācijas sistēmas drošības darbinieki, kuri Inčukalna novada pašvaldības uzdevumā veic informācijas sistēmu drošības pasākumus šo noteikumu izpildē.

4. Informācijas sistēmas drošības politika ir izstrādāta saskaņā ar Informācijas tehnoloģiju drošības likumu, Valsts informācijas sistēmu likumu, Fizisko personu datu aizsardzības 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

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, 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:

7.1. Informācijas sistēmas drošības politikā;

7.2. Informācijas sistēmas lietošanas noteikumos.

8. Informācijas sistēmu lietotājs par iepazīšanos ar augstāk minētajiem dokumentiem un to ievērošanu paraksta 1.Pielikumu "Informācijas sistēmas lietotāja apliecinājums par "Informācijas sistēmas drošības politikas" prasību ievērošanu".

9. IS drošības speciālists atbild par drošības politikas nosacījumu un prasību ievērošanu, kas ir minēti šādos dokumentos:

9.1. Informācijas sistēmas lietošanas noteikumos;

9.2. Informācijas sistēmu atjaunošanas plānā;

9.3. Informācijas sistēmas drošības politikā;

9.4. Informācijas sistēmas drošības riska pārvaldības plānā;

9.5. Informācijas sistēmas drošības noteikumos.

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 nostādnēm.

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 sensitīvi 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 būtiskākajās lietošanā esošajās ārpakalpojumu informācijas sistēmās (Iedzīvotāju reģistrs un Sociālās palīdzības uzskaites sistēma) tiek apstrādāti sensitīvi personas dati, tādejādi tās ir uzskatāmas par paaugstinātām 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 IS drošības speciālists.

III. Informācijas sistēmas drošības organizācija

16. Informācijas sistēmas drošības organizatoriskās struktūras pamatu veido IS drošības speciālists un Informācijas sistēmas lietotāji.

17. IS drošības speciālists nodrošina informācijas sistēmas drošības politikas realizāciju, kā arī veic šādas darbības:

17.1. kopā ar IS drošības speciālistu 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.

18. IS drošības speciālista 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. nodrošinot nepieciešamo tehnisko risinājumu attiecīgajam informācijas resursam;

18.4. veikt Risku vadības procesa koordināciju pašvaldībā saskaņā ar Informācijas drošības riska pārvaldības plānu;

18.5. izmeklēt informācijas drošības incidentus;

18.6. veikt regulāras pārbaudes, lai pārliecinātos, 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.

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 IS drošības speciālists, 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 IS drošības speciālists 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, nelaimes gadījumiem utt.) Informācijas sistēmas lietotājiem un IS drošības speciālistam ir nekavējoši jāpaziņo pašvaldības izpilddirektoram.

Inčukalna novada domes priekšsēdētājs A.Nalivaiko

1.pielikums
2019.gada 22.maija
Inčukalna novada domes noteikumiem Nr.4/2019
„Inčukalna novada pašvaldības
Informācijas sistēmas drošības politika”

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 Inčukalna novada pašvaldības, savu vai trešo personu interesēs, kā arī apņemos ievērot Fizisko personu datu aizsardzības likuma un Informācijas atklātības likuma prasības.

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

_____	_____	_____
Struktūrvienība un amats atšifrējums	Paraksts	Paraksta