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. 8

Ropažu novada pašvaldības Informācijas sistēmas drošības politika

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" 8.1.apakšpunktu

I.Vispārīgie jautājumi

1. Informācijas sistēmas drošības politika nosaka politiku, kādā Ropažu novada pašvaldība, tās izveidotās iestādes un pašvaldības aģentūras (turpmāk – Institūcija) 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. Politikā 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 rīkojumu iecelta 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 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. Institūcijas 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 institūcijas 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 institūcijā;

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

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

6. Informācijas sistēmas lietotājs, kas ir nodarbināts institūcijā un ir institūcijas darbinieks (pilna darba laika, nepilnas slodzes un līgumdarbiniekiem), atbild par drošības politikas nosacījumu un prasību ievērošanu, kas ir minēti šādos dokumentos:

6.1. Informācijas sistēmas drošības politikā;

6.2. Informācijas sistēmas lietošanas noteikumos.

7. 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".

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

8.1. Informācijas sistēmas drošības politikā;

8.2. Informācijas sistēmas lietošanas noteikumos;

8.3. Informācijas sistēmas drošības noteikumos;

8.4. Informācijas sistēmas drošības riska pārvaldības plānā;

8.5. Informācijas sistēmu atjaunošanas plānā.

9. Institūcijasvadītāji ir atbildīgi par viņu pakļautībā vai uzraudzībā esošajiem Informācijas sistēmas lietotājiem. institūcijasvadītāji 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. Institūcijas informācijas sistēmas tiek iedalītas paaugstinātas drošības un pamata drošības sistēmās atbilstoši to drošības klasei. Institūcijas informācijas sistēmas iedalījums ir iekļauts 2.pielikumā.

12. Institūcijā 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, institūcija piemēro paaugstinātas drošības sistēmas prasības arī visām pārējām izmantotajām informācijas sistēmām.

14. Informācijas tehnoloģiju drošības pārvaldību un Informācijas sistēmas drošības politikas koordināciju institūcijā veic Sistēmas drošības pārvaldnieks.

III. Informācijas sistēmas drošības organizācija

15. Informācijas sistēmas drošības organizatoriskās struktūras pamatu veido Sistēmas drošības pārvaldnieks, Datortīkla administrators un Informācijas sistēmas lietotāji.

16. 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 institūcijas 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 sistēmas 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 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 sistēmas drošības noteikumiem;

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

17.4. veikt Risku vadības procesa koordināciju institūcijā saskaņā ar Informācijas drošības riska pārvaldības plānu;

17.5. palīdzēt 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 institūcijas 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. Institūcijas 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. Institūcijas informācijas resursu riska analīze tiek veikta atbilstoši Informācijas sistēmas drošības riska pārvaldības plānam.

VI. Informācijas resursu loģiskā drošība

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

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

25. Institūcijas 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 sistēmas drošības noteikumos.

VII. Tehnisko resursu fiziskā drošība

26. Institūcijas 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 institūcijā 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. Institūcijas 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 institūcijā, 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, institūcijas vadītājam un Sistēmas drošības pārvaldniekam.

IX. Noslēguma jautājums

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

Pielikumā:

1. Ropažu novada pašvaldības Informācijas sistēmas lietotāja apliecinājums par "Informācijas sistēmas drošības politikas" prasību ievērošanu;
2. Ropažu novada pašvaldības Informācijas sistēmas iedalījums.

Ropažu novada pašvaldības izpilddirektors M.Griščenko

1.pielikums

Ropažu novada pašvaldības iekšējiem noteikumiem
"Ropažu 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, kas ir minētas šādos dokumentos:
   1.1. Informācijas sistēmas drošības politikā;
   1.2. Informācijas sistēmas lietošanas noteikumos;

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

3. Es piekrītu, ka pārtraucot darba (līguma) attiecības ar Ropažu novada pašvaldību jebkādu iemeslu dēļ, es nekavējoties nodošu Ropažu 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	/Paraksts/	Paraksta atšifrējums	Datums

2.pielikums

Ropažu novada pašvaldības iekšējiem noteikumiem
"Ropažu novada pašvaldības
Informācijas sistēmas drošības politika"

INSTITŪCIJAS INFORMĀCIJAS SISTĒMU IEDALĪJUMS

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