LATVIJAS REPUBLIKA
KRUSTPILS NOVADA PAŠVALDĪBA
Reģ.Nr.90009118116
Rīgas ielā 150a, Jēkabpilī, LV-5202
Tālrunis 65237635, Fakss 65237611, e-pasts: novads@krustpils.lv

Jēkabpilī

15.03.2017.

APSTIPRINĀTI
ar Krustpils novada domes
15.03.2017. sēdes lēmumu
(protokols Nr.5.,17.p.)

Pielikums Nr.1

Krustpils novada pašvaldības Informācijas sistēmas drošības noteikumi

I.Vispārīgie jautājumi

1. Informācijas sistēmas drošības noteikumi ietver kārtību, kādā Krustpils novada pašvaldība (turpmāk – Pašvaldība) nodrošina pašvaldības izmantotās informācijas sistēmas aizsardzību.

2. Noteikumos lietotie termini:

2.1. **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.

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

2.3. **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.

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

3. Informācijas sistēmas drošības noteikumi ir saistoši Informācijas sistēmas drošības pārvaldniekam un Datortīklu administratoram.

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 Datortīklu administrators.

5. Datortīklu 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. Datortīklu 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 ielaušanās mēģinājumi vai būtiski incidenti, Datortīklu administrators veic to reģistrēšanu un izmeklēšanu, kā arī par tās rezultātiem informē Sistēmas drošības pārvaldnieku un Drošības incidentu novēršanas institūciju (CERT.lv).

8. Vīrusu darbības novēršanai veic šādus pasākumus:

8.1. Datortīklu administrators veic pasākumus datoru vīrusu darbības novēršanai tehniskajos resursos, izmantojot šim nolūkam paredzētu programmatūru.

8.2. Datortīklu administrators veic antivīrusu programmu pārraudzību, lai pārliecinātos par to darbību un jaunāko vīrusu definīciju failu esamību.

9. Datortīklu 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 Datortīklu 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 Datortīklu administratoru. Datortīklu 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 Datortīklu administratoru. Datortīklu administrators identificē atbilstošo informācijas sistēmas lietotāju, izveido jaunu paroli un izsniedz atbilstošajam Informācijas sistēmas lietotājam.

14. Paroles politika ir noteikta Pašvaldības Informācijas sistēmas lietošanas noteikumos.

15. Informācijas sistēmas lietotāja parole pie ievades nedrīkst parādīties uz ekrāna.

16. Datortīklu 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. Datortīklu 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. Datortīklu 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. Datortīklu administratoram, sadarbojoties ar Informācijas sistēmas drošības pārvaldnieku, ir pienākums veikt reģistru par iegādātām un izlietotām programmatūras licencēm, kā arī, ja nepieciešams, savlaicīgi informēt 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 Pašvaldības grāmatvedība. 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, 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.

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

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

III. Informācijas fiziskā aizsardzība

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

27. Serveru telpas ir aprīkotas ar:
27.1. ugunsgrēka signalizācijas iekārtu.
27.2. ugunsdzēšamo aparātu.
27.3. gaisa kondicionēšanas iekārtu.
27.4. nepārtrauktās barošanas avotu (UPS).
27.5. apsardzes signalizāciju.

28. Nepiederošas personas, t.sk. ārējie pakalpojumu sniedzēji, serveru telpās drīkst uzturēties tikai Informācijas sistēmas drošības pārvaldnieka klātbūtnē.

29. Pazūdot elektrībai, 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.

30. Informācijas sistēmas lietotāju darba stacijas atrodas ierobežotas pieejas telpās, kā arī uz tām ir uzstādīts nepārtrauktās barošanas avots (UPS), ja elektroenerģijas padeves traucējumu risks ir nepieņemami liels.

31. 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

32. Ja Pašvaldība sistēmas uzturēšanai slēdz ārpakalpojuma līgumu ar pakalpojuma sniedzēju, līguma izpildi uzrauga atbildīgā persona un līgumā iekļauj vismaz šādas drošības prasības:

32.1. saņemamā ārpakalpojuma aprakstu;

32.2. precīzas prasības attiecībā uz ārpakalpojuma apjomu un kvalitāti;

32.3. Pašvaldības un ārpakalpojuma sniedzēja tiesības un pienākumus, tai skaitā:

32.3.1. Pašvaldības tiesības pastāvīgi uzraudzīt ārpakalpojuma sniegšanas kvalitāti;

32.3.2. Pašvaldības tiesības dot ārpakalpojuma sniedzējam obligāti izpildāmus norādījumus jautājumos, kas saistīti ar ārpakalpojuma godprātīgu, kvalitatīvu, savlaicīgu un normatīvajiem aktiem atbilstošu izpildi;

32.3.3. 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;

32.3.4. ārpakalpojuma sniedzēja pienākumu nodrošināt Pašvaldībai iespēju pastāvīgi uzraudzīt ārpakalpojuma sniegšanas kvalitāti.

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

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

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

34.2. 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;

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

V. Rezerves kopiju veidošanas kārtība

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

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

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

38. Datortīklu administrators nodrošina Pašvaldības informācijas resursu atjaunošanu no rezerves kopijām pēc Sistēmas drošības pārvaldnieka pieprasījuma.
39. Datortīklu 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 Sistēmas drošības pārvaldnieku.

VI. Elektronisko datu nesēju iznīcināšanas procedūra

40. Datortīklu administrators organizē elektronisko datu nesēju iznīcināšanu un nodrošina šo iznīcināto elektronisko datu nesēju uzskaiti.

Domes priekšsēdētājs K.Pabērzs

LATVIJAS REPUBLIKA
KRUSTPILS NOVADA PAŠVALDĪBA
Reģ.Nr.90009118116
Rīgas ielā 150a, Jēkabpilī, LV-5202
Tālrunis 65237635, Fakss 65237611, e-pasts: novads@krustpils.lv

Jēkabpilī

15.03.2017.

APSTIPRINĀTI
ar Krustpils novada domes
15.03.2017. sēdes lēmumu
(protokols Nr.5.,17.p.)
Pielikums Nr. 2.

Informācijas sistēmas drošības politika

I.Vispārīgie jautājumi

1. Informācijas sistēmas drošības politika nosaka politiku, kādā Krustpils 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 šādu Pašvaldības iestāžu Informācijas sistēmas lietotājiem, kuriem ir pieeja kādai(ām) no valsts informāciju sistēmām (piemēram, Iedzīvotāju reģistram):
   2.1. Pašvaldības administrācija;
   2.2. Atašienes pagastu pārvalde;
   2.3. Krustpils pagastu pārvalde;
   2.4. Kūku pagastu pārvalde;
   2.5. Mežāres pagastu pārvalde;
   2.6. Variešu pagastu pārvalde;
   2.7. Vīpes pagastu pārvalde;
   2.8. Dzimtsarakstu nodaļa;
   2.9. Bāriņtiesa;
   2.10. Sociālais dienests.

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

9.1. Informācijas sistēmas drošības politikā.
9.2. Informācijas sistēmas lietošanas noteikumos.
9.3. Informācijas sistēmas drošības noteikumos.
9.4. Informācijas sistēmas drošības riska pārvaldības plānā.
9.5. Informācijas sistēmu atjaunošanas plānā.

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 būtiskākās informācijas sistēmās (piemēram, Iedzīvotāju reģistrs un Sociālās palīdzības uzskaites sistēma) tiek apstrādāti sensitīvi 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 administratora 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 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. Pašvaldības datortīklu, serveru un to saistīto iekārtu uzturēšanu un administrēšanu, kā arī Informācijas sistēmas lietotāju datoru uzstādīšanu un administrēšanu veic Datortīklu administrators, kuras 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, nelaimes gadījumiem utt.) Informācijas sistēmas lietotājiem un Datortīklu administratoram ir nekavējoši jāpaziņo pašvaldības izpilddirektoram.

Pielikumā:

1. Krustpils novada pašvaldības Informācijas sistēmas lietotāja apliecinājums par “Informācijas sistēmas drošības politikas” prasību ievērošanu uz 1 lp.

Domes priekšsēdētājs K.Pabērzs

1. PIELIKUMS
"Krustpils 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 Krustpils 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 Krustpils novada pašvaldību jebkādu iemeslu dēļ, es nekavējoties nodošu Krustpils 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

LATVIJAS REPUBLIKA
KRUSTPILS NOVADA PAŠVALDĪBA
Reģ.Nr.90009118116
Rīgas ielā 150a, Jēkabpilī, LV-5202
Tālrunis 65237635, Fakss 65237611, e-pasts: novads@krustpils.lv

Jēkabpilī

15.03.2017.

APSTIPRINĀTI
ar Krustpils novada domes
15.03.2017. sēdes lēmumu
(protokols Nr.5.,17.p.)
Pielikums Nr.3.

Krustpils novada pašvaldības Informācijas sistēmas darbības atjaunošanas plāns

I.Vispārīgie jautājumi

1. Informācijas sistēmas darbības atjaunošanas plāns ietver kārtību, kādā Krustpils novada pašvaldība (turpmāk – Pašvaldība) nodrošina pašvaldības izmantotās informācijas sistēmas, kas ir izvietotas uz pašvaldības serveriem, atjaunošanu darbības traucējumu gadījumā.

2. Noteikumos lietotie termini:
   2.1. **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.
   2.2. **Krustpils novada pašvaldība** – institūcija, kas normatīvajos aktos noteiktajā kārtībā organizē un vada informācijas sistēmu darbību.
   2.3. **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.
   2.4. **Informācijas sistēmas lietotājs –** persona, kurai ir piešķirtas piekļuves tiesības informācijas sistēmās.

3. Informācijas sistēmu atjaunošanas plāna mērķis ir nodrošināt Pašvaldības darbības turpināšanu, iespējamo zaudējumu minimizēšanu, saistību izpildi gadījumos, kad darbība ir traucēta ārēju vai iekšēju faktoru gadījumā, kas, piemēram, ir informācijas sistēmas bojājumi, personāla kļūdas, ļaunprātīga rīcība, datu pārraides sistēmu bojājumi, elektrības padeves traucējumi, ugunsgrēks, plūdi, daļēji vai pilnīgi telpu postījumi vai tml.

4. Sistēmas drošības pārvaldnieks veic pārraudzību par darbības atjaunošanas plānošanu, piešķirot nepieciešamos personāla, tehnoloģiskos un finanšu resursus kārtības izstrādei un realizācijai.

5. Informācijas sistēmas darbības atjaunošanas plāns ir saistošs Informācijas sistēmas drošības pārvaldniekam, Datortīklu administratoram un visiem Pašvaldības struktūrvienību vadītājiem.

II. Darbības traucējuma identificēšana

6. Īslaicīgs informācijas sistēmas darbības traucējums ir situācija, kas atbilst šādiem nosacījumiem:
   6.1. pārtraukta vai daļēji pārtraukta informācijas sistēmas darbība, kas nepārsniedz 2 (divas) stundas;
   6.2. identificējot šo traucējumu, Datortīklu administratoram ir saprotami darbības traucējuma iemesli un ir pamatota pārliecība, ka šis traucējums tiks novērsts 2 (divu) stundu laikā.

7. Ilglaicīgs darbības traucējums ir situācija, kas atbilst šādiem nosacījumiem:
   7.1. pārtraukta vai daļēji pārtraukta informācijas sistēmas darbība, kas pārsniedz 2 (divas) stundas; vai
   7.2. identificējot šo traucējumu, Datortīklu administratoram ir saprotami darbības traucējumu iemesli, apzinoties, ka to novēršanai būs nepieciešams laiks ilgāks par 2 (divām) stundām; vai

8. Informācijas sistēmas darbības traucējums var rasties, ja:
   8.1. ir pilnīgi vai daļēji pārtraukta Pašvaldības pakalpojumu sniegšana.
   8.2. ir konstatēts, ka pakalpojumu sniegšanu nevar atjaunot nepieciešamajā apjomā un kvalitātē.

III. Darbības traucējuma novēršana

9. Pēc darbības traucējuma atklāšanas pirmais uzdevums ir noteikt, vai situācijas bīstamības līmenis prasa personāla evakuāciju. Ja radusies situācija, kas rezultātā izraisīti būtiski ēku un iekārtu bojājumi, situāciju konstatējušajam Pašvaldības darbiniekam nekavējoties jāinformē Sistēmas drošības pārvaldnieku.

10. Informācijas sistēmas drošības pārvaldnieks pēc darbības traucējuma identificēšanas pārņem situācijas vadību un informē par darbības traucējumu iesaistītos Pašvaldības struktūrvienību vadītājus.

11. Rīcība atsevišķos ārkārtas situāciju gadījumos un turpmāko bojājumu novēršanā:
   11.1. ugunsgrēka trauksmes, atklātas uguns vai piedūmojuma gadījumā jārīkojas atbilstoši „Rīcības plāns ugunsgrēka gadījumā".
   Ugunsgrēka gadījumā nekavējoties zvanīt 01 vai 112.
   Atbildīgā persona ugunsdrošības jautājumos Edgars Līcis, tālr., 29556842.
   11.2. elektrības padeves pārrāvumu gadījumā, pazūdot apgaismojumam (būtiski telpām bez āra apgaismojuma piekļuves vai diennakts tumšajā laikā), jāatstāj darba vietu.
   11.3. serveri elektroapgādes traucējumu gadījumiem ir pieslēgti pie nepārtrauktās barošanas avotiem (turpmāk - UPS).
   11.4. ilgstošu elektroapgādes pārtraukumu gadījumā Sistēmas drošības pārvaldnieks dod nepieciešamos rīkojumus par turpmākajām darbībām.

12. Darbinieku evakuācija atbilstoši izstrādātām evakuācijas shēmām un norādēm tiek veikta, iestājoties vienam no sekojošiem apstākļiem:
   12.1. ieslēdzoties ugunsgrēka trauksmes signalizācijai.
   12.2. ugunsgrēka gadījumā.
   12.3. pēc Pašvaldības rīkojuma.
   12.4. pēc Sistēmas drošības pārvaldnieka vai tā pilnvarotas personas rīkojuma.

13. Gadījumos, ja tas ir nepieciešams, Sistēmas drošības pārvaldnieks izveido Negadījumu seku novēršanas un atjaunošanas grupu, kuras sastāvā iekļauj -Informācijas sistēmas drošības pārvaldnieku, Datortīklu administratoru un / vai citus struktūrvienību vadītājus vai Pašvaldības speciālistus.

14. Negadījumu seku novēršanas un atjaunošanas grupas pienākumi:

14.1. pieņemt lēmumu par konkrētām reaģējošām darbībām negadījumu seku novēršanai.
14.2. novērtēt darbinieku apdraudējumu, telpu un iekārtu bojājumu pakāpi un stāvokli.
14.3. identificēt un novērtēt bojātās sistēmas nozīmīgumu Pašvaldības darbībai, noteikt apdraudējuma vai darbības pārtraukuma iemeslus.
14.4. novērtēt Pašvaldības radītos zaudējumus infrastruktūras un informācijas sistēmu atjaunošanai.
14.5. noteikt apdraudēto vai skarto teritoriju. Pieņemt lēmumu par darbības atjaunošanu esošajās telpās vai pārvietot to uz citām telpām.
14.6. noteikt turpmākās darbības sistēmas atjaunošanai, to prioritāro kārtību, nepieciešamās darbības datu bāžu vai atsevišķu failu atjaunošanai, kā arī noteikt paredzamo darbības atjaunošanai nepieciešamo laiku.
14.7. sadarbībā ar Datortīklu administratoru sastādīt aizvietošanai nepieciešamā aprīkojuma sarakstu (aparatūra, programmatūra, palīgmateriāli).

15. Datortīklu administratoram ir pienākums nodrošināt iesaistītiem darbiniekiem atbilstošas apmācības informācijas sistēmu darbības nepārtrauktības nodrošināšanai.

Domes priekšsēdētājs K.Pabērzs

LATVIJAS REPUBLIKA
KRUSTPILS NOVADA PAŠVALDĪBA
Reģ.Nr.90009118116
Rīgas ielā 150a, Jēkabpilī, LV-5202
Tālrunis 65237635, Fakss 65237611, e-pasts: novads@krustpils.lv

Jēkabpilī

15.03.2017.

APSTIPRINĀTI
ar Krustpils novada domes
15.03.2017. sēdes lēmumu
(protokols Nr.5.,17.p.)
Pielikums Nr.4.

Krustpils novada pašvaldības Informācijas sistēmas drošības riska pārvaldības plāns

I.Vispārīgie jautājumi

1. Informācijas sistēmas drošības riska pārvaldības plāns nosaka Krustpils novada pašvaldība (turpmāk – Pašvaldība) pašvaldības izmantotās informācijas sistēmas risku vadības procesa ieviešanu un to vadību, nodrošinot atbilstošu vadības un kontroles sistēmas darbības efektivitāti, atklājot un novēršot kļūdas un neprecizitātes, kā arī nepieciešamības gadījumā, veicot drošības labojumus informācijas sistēmās.

2. Noteikumos lietotie termini:

2.1. **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.

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

2.3. **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.

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

3. Pašvaldības informācijas risku analīze tiek veikta pēc sekojošiem soļiem hronoloģiskā secībā:

3.1. risku identificēšana.
3.2. risku novērtēšana.
3.3. risku vadīšana.
3.4. risku uzraudzība.

4. Risku vadības procesa ieviešanu un vadību veic Informācijas sistēmas drošības pārvaldnieks, nepieciešamības gadījumā pieaicinot Pašvaldības vadītāju, Datortīklu administratoru, Pašvaldības struktūrvienību vadītājus un / vai atsevišķus Informācijas sistēmas lietotājus vai citus konsultantus.

5. Risku vadības procesa koordināciju un metodisko vadību veic Datortīklu administrators.

II. Informācijas resursu risku identificēšana

6. Datortīklu administrators kopīgā sanāksmē ar pieaicinātiem dalībniekiem, ņemot vērā kopējo dalībnieku kompetenci, zināšanas un pieredzi, veic Pašvaldības funkciju un uzdevumu izpildes procesa posmu izskatīšanu, identificējot tajos iespējamos informācijas resursu riskus.

7. Datortīklu administratoram ir pienākums augstāk minētās sanāksmes laikā apkopot identificētos informāciju resursu riskus, iekļaujot tos Risku reģistrā (1. Pielikums "Informācijas resursu risku reģistrs").

III. Informācijas resursu risku novērtēšana

8. Datortīklu administrators kopā ar pieaicinātiem dalībniekiem arī veic šo risku novērtēšanu, nosakot Risku rādītāju, kas veidojas no Varbūtības, Ietekmes un Pārvaldības novērtējuma punktu reizinājuma.

9. Varbūtība ir novērtējums par iespējamo situācijas (apdraudējumu) iestāšanos noteiktā laika periodā. Novērtējuma punktu iedalījumu skat. tabulā zemāk:

Novērtējums (punktos)	Raksturojums
1	maz iespējams, ka šāda situācija (apdraudējums) īstenosies
2	vidēji iespējams, ka šāda situācija (apdraudējums) īstenosies
3	ļoti iespējams, ka šāda situācija (apdraudējums) īstenosies

10. Ietekme ir novērtējums par iespējamās situācijas (draudu) iestāšanās būtiskumu noteiktā laika periodā. Novērtējuma punktu iedalījumu skat. tabulā zemāk:

Novērtējums (punktos)	Raksturojums
1	apdraudējumam ir maza ietekme uz datu subjektu un / vai pašvaldību
2	apdraudējumam ir vidēja ietekme uz datu subjektu un / vai pašvaldību
3	apdraudējumam ir liela ietekme uz datu subjektu un / vai pašvaldību

11. Pārvaldība ir novērtējums par esošo izveidoto personas datu apstrādes aizsardzības mehānismu, kas ļauj līdz minimumam samazināt tās trūkumu negatīvo ietekmi uz pašvaldību. Novērtējuma punktu iedalījumu skat. tabulā zemāk:

Novērtējums (punktos)	Raksturojums
1	Personas datu apstrādes vadība ir izveidota augstākajā līmenī atbilstoši labākajai praksei
2	Personas datu apstrādes vadība ir izveidota labā līmenī, tomēr vēl ir nepieciešams veikt atsevišķus uzlabojumus tās darbībai
3	Personas datu apstrādes vadība ir izveidota vidējā līmenī, kurai ir nepieciešams būtiskus uzlabojumus tās darbībai.
4	Personas datu apstrādes vadība ir izveidota sliktā līmenī vai tā nemaz nepastāv vispār.

12. Datortīklu administratoram ir pienākums sanāksmes laikā apkopot grupas dalībnieku Varbūtības, Ietekmes un Pārvaldības novērtējuma rādītājus un pēc vidējā aritmētiskā tos iekļaut Risku reģistrā (1.Pielikums "Informācijas resursu risku reģistrs").

13. Jo lielāks ir Risku rādītājs, jo informācijas resursu riska prioritāte ir augstāka, tādejādi, būtu nepieciešams papildus noteikt darbības un kontroles pasākumus risku mazināšanai un novēršanai.

14. Informācijas sistēmas drošības Riska rādītāja pieņemamais līmenis ir 6 (seši). Gadījumā, ja Riska rādītājs pārsniedz pieņemamo līmeni ir nepieciešams nekavējoši sasaukt atkārtotu sanāksmi un pēc iespējas ātrākā laikā veikt pasākumus risku mazināšanai un novēršanai tā, lai Risku rādītājs nepārsniegtu pieņemamo līmeni.

IV. Informācijas resursu risku vadīšana

15. Datortīklu administrators kopā ar pieaicinātiem dalībniekiem atbilstoši Risku reģistrā iekļautajiem riskiem un to risku rādītājiem vienojas un nosaka no Pašvaldības puses veicamos iespējamos pasākumus risku mazināšanai un novēršanai.

16. Datortīklu administrators sagatavo sarakstu ar veicamajiem pasākumiem risku mazināšanai un novēršanai, nosakot atbildīgās personas un to ieviešanas termiņus (2.Pielikums "Pārskats par pasākumiem risku mazināšanai un novēršanai").

V. Informācijas resursu risku uzraudzība

17. Informācijas resursu risku uzraudzību veic Datortīklu administrators balstoties uz atbildīgo personu par pasākumiem risku mazināšanai un novēršanai sniegto informāciju.

18. Datortīklu administratoram ir pienākums Risku reģistru un Pārskatu par pasākumiem risku mazināšanai un novēršanai iesniegt Pašvaldības vadītājam, kā arī regulāri informēt Pašvaldības vadītāju par risku mazināšanas un novēršanas veikto pasākumu norisi.

19. Datortīklu administrators ne retāk kā reizi gadā veic atkārtotu Informācijas resursu risku identificēšanu, novērtēšanu un vadību. Nepieciešamības gadījumā, Pašvaldības vadītājs, Informācijas sistēmas drošības pārvaldnieks vai Datortīklu administrators var ierosināt rīkot atkārtotu sanāksmi pirms augstāk minētā termiņa.

Pielikumā:

1. Krustpils novada pašvaldības informācijas resursu risku reģistrs uz 1 lp.
2. Krustpils novada pašvaldības pārskats par pasākumiem risku mazināšanai un novēršanai uz 1 lp.

Domes priekšsēdētājs K.Pabērzs

1. PIELIKUMS
"Krustpils novada pašvaldības
Informācijas sistēmas drošības riska pārvaldības plāns"

KRUSTPILS NOVADA PAŠVALDĪBAS
INFORMĀCIJAS RESURSU RISKU REĢISTRS

Nr.	Informācijas resursu risku nosaukums (raksturojums)	Varbūtība	Ietekme	Pārvaldība	Risku rādītājs
1.					
2.					
3.					

2. PIELIKUMS
"Krustpils novada pašvaldības
Informācijas sistēmas drošības riska pārvaldības plāns"

KRUSTPILS NOVADA PAŠVALDĪBAS
PĀRSKATS PAR PASĀKUMIEM RISKU MAZINĀŠANAI UN NOVĒRŠANAI

Nr.	Pasākuma apraksts	Termiņš	Atbildīgā amatpersona
1.			
2.			
3.			

LATVIJAS REPUBLIKA
KRUSTPILS NOVADA PAŠVALDĪBA
Reģ.Nr.90009118116
Rīgas ielā 150a, Jēkabpilī, LV-5202
Tālrunis 65237635, Fakss 65237611, e-pasts: novads@krustpils.lv

Jēkabpilī

15.03.2017.

APSTIPRINĀTI
ar Krustpils novada domes
15.03.2017. sēdes lēmumu
(protokols Nr.5.,17.p.)
Pielikums Nr.5.

Krustpils novada pašvaldības administrācijas Informācijas sistēmas lietošanas noteikumi

I.Vispārīgie jautājumi

1. Informācijas sistēmas lietošanas noteikumi nosaka Krustpils novada pašvaldība (turpmāk – Pašvaldība) darbinieku pienākumus un prasības pašvaldības izmantotās informācijas sistēmas un interneta lietošanai, kā arī nosaka kārtību, kādā tiek veikta pašvaldības izmantotās informācijas sistēmas lietotāju pieejas tiesību piešķiršana, izmaiņas un anulēšana.

2. Noteikumos lietotie termini:
   2.1. **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.
   2.2. **Krustpils novada pašvaldība** – institūcija, kas normatīvajos aktos noteiktajā kārtībā organizē un vada informācijas sistēmu darbību.
   2.3. **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.
   2.4. **Informācijas sistēmas lietotājs –** persona, kurai ir piešķirtas piekļuves tiesības informācijas sistēmās.

3. Informācijas sistēmas lietošanas noteikumi ir saistoši visiem pašvaldības darbiniekiem (pilna darba laika, nepilnas slodzes un līgumdarbiniekiem), kuri ir nodarbināti pašvaldībā un kam ir piekļuve kādai no pašvaldības informācijas sistēmām.

4. Katra pašvaldības Informācijas sistēmas lietotāja pienākums ir iepazīties ar šiem noteikumiem un ievērot tos ikdienas darbā.

II. Informācijas sistēmas lietotāju administrēšanas kārtība

5. Pašvaldības katras pašvaldības iestādes un struktūrvienības vadītājs ir atbildīgs par sev un to padotībā esošo darbinieku lietotāju pieejas tiesību piešķiršanu, izmaiņu veikšanu un anulēšanu.

6. Lai izveidotu lietotāju pieejas tiesības vai veiktu izmaiņas tajās, Pašvaldības atbilstošās pašvaldības iestādes un struktūrvienības vadītājs raksta pieprasījumu (1.Pielikums), atzīmējot tajā nepieciešamo Informācijas resursu, ko iesniedz Informācijas sistēmas drošības pārvaldniekam.

7. Informācijas sistēmas lietotāju pieejas tiesības tiek piešķirtas Pašvaldības darbiniekiem atbilstoši katra atsevišķā darbinieka noteiktajiem darba pienākumiem un specifikai.

8. Informācijas sistēmas drošības pārvaldnieks izskata lietotāju pieejas tiesību piešķiršanas pieprasījumu un, ja uzskata to par pamatotu, Informācijas sistēmas drošības pārvaldnieks pieprasījumu izveidot atbilstošās informācijas sistēmas lietošanas tiesības nosūta Datortīklu administratoram.

9. Informācijas sistēmas lietotāju pieejas tiesību piešķiršana Pašvaldības informācijas resursiem personām, kuras nav Pašvaldības darbinieki, notiek tikai atsevišķos gadījumos pēc Sistēmas drošības pārvaldnieka pieprasījuma (piemēram, gadījumā ja ir noslēgts līgums starp pašvaldību un atbilstošo personu, kurā ir precīzi noteikti personas pienākumi, pieļaujamie informācijas izmantošanas mērķi, konfidencialitātes prasības un atbildība).

10. Informācijas sistēmas drošības pārvaldnieks ir atbildīgs par Lietotāju pieejas tiesību izveidošanu, administrēšanu un šo pieprasījumu apkopošanu, glabāšanu, kontroli un uzraudzību.

11. Piešķirtās lietotāju pieejas tiesības Pašvaldības informācijas resursiem ir nekavējoties jāanulē šādos gadījumos:

11.1. darbiniekiem, kuri pārtrauc darba (līguma) tiesiskās attiecības ar pašvaldību un / vai tās vairs nav nepieciešamas pienākumu veikšanai.

11.2. personām, kuras ir izpildījušas savstarpēji noslēgto līgumu ar pašvaldību vai šī līguma izbeigšanās (atcelšanas) gadījumā.

12. Iestājoties šo noteikumu 11.punktā minētajam gadījumam, atbilstošās struktūrvienības vadītājam, kura pakļautībā ir augstāk minētais darbinieks (vai koordinējošās struktūrvienības vadītājam gadījumos ar trešajām personām), ir pienākums informēt Datortīklu administratoru, kas veic atbilstošā lietotāja tiesību bloķēšanu.

13. Piešķirtās lietotāju pieejas tiesības var anulēt arī Informācijas sistēmas drošības pārvaldnieks vai Datortīklu administrators, balstoties uz atbilstošā lietotāja Informācijas sistēmas drošības politikas vai to saistošo dokumentu pārkāpumiem, par to rakstiski informējot Pašvaldības izpilddirektoru.

14. Datortīklu administratoram pēc Pašvaldības izpilddirektora vai Informācijas sistēmas drošības pārvaldnieka pieprasījuma, sagatavot Lietotāju pieejas tiesību sarakstu.

15. Datortīklu administratoram sadarbībā ar Informācijas sistēmas drošības pārvaldnieku ir pienākums vismaz reizi gadā veikt Lietotāju pieejas tiesību kontroli, pārbaudot un salīdzinot piešķirto lietotāju pieejas tiesību atbilstību darbinieka (personas, kuras darbojas uz līguma pamata) pienākumiem un specifikai.

III. Informācijas sistēmas lietotāju tiesības, pienākumi un atbildība

16. Informācijas sistēmas lietotājam ir tiesības izmantot viņam lietošanā nodotos datorus un to programmatūru, kā arī Informācijas sistēmas lietotājam ir tiesības pieprasīt atbalstu gadījumā, ja datoram vai tā programmatūrai ir radušies traucējumi.

17. Informācijas sistēmas lietotājs ir atbildīgs par datortehniku, kas nodota viņa rīcībā, kā arī atbild par darbībām, kas tiek veiktas ar viņam nodoto datortehniku.

18. Informācijas sistēmas lietotājs nedrīkst atļaut piekļūt tam nodotai datortehnikai citām personām, ja tas nav nepieciešams tiešo darba pienākumu pildīšanai un to pilnvarojumu nav devis Pašvaldības izpilddirektors, Informācijas sistēmas drošības pārvaldnieks vai Datortīklu administrators.

19. Informācijas sistēmas lietotāja pienākums ir apzināti nepieļaut datorvīrusu iekļūšanu iestādes datorsistēmās un neizmantot nezināmas izcelsmes datu nesējus. Rodoties aizdomām, ka dators ir inficēts ar datorvīrusu, par to nekavējoties jāinformē Informācijas sistēmas drošības pārvaldnieks vai Datortīklu administrators.

20. Informācijas sistēmas lietotājam ir pienākums jebkuru ienākošo elektronisko informāciju (failus) pirms lietošanas obligāti pārbaudīt ar antivīrusa programmatūru, ja tas netiek nodrošināts automātiski.

21. Nelicencētas programmatūras uzstādīšana un lietošana darba stacijās (lietotāja datoros) ir aizliegta. Patvaļīgi uzstādītas programmatūras lietošana, bez Pašvaldības izpilddirektora, Informācijas sistēmas drošības pārvaldnieka vai Datortīklu administratora atļaujas ir aizliegta.

22. Informācijas sistēmas lietotājs nedrīkst izpaust nepilnvarotām personām ziņas par Pašvaldības datoru tīkla uzbūvi un konfigurāciju.

23. Informācijas sistēmas lietotājs nedrīkst no sava darba datora kopēt failus uz ārējiem datu nesējiem (piemēram, CD, DVD, USB kartēm vai citiem datu nesējiem), ja to nevajag tiešo darba pienākumu pildīšanai vai ja tam pilnvarojumu nav devis Pašvaldības izpilddirektors, Informācijas sistēmas drošības pārvaldnieks vai Datortīklu administrators.

24. Ārējo datu nesēju, kurā ir iekopēta ierobežotas pieejamības informācija, no Pašvaldības telpām drīkst iznest tikai ar Pašvaldības izpilddirektora RAKSTISKU atļauju. Šajos gadījumos Informācijas sistēmas lietotājs, kurš no iestādes telpām iznes šādu datu nesēju, uzņemas pilnu atbildību par šo informāciju.

25. Informācijas sistēmas lietotājam ir aizliegts patvarīgi pārvietot, demontēt aparatūru, izjaukt, remontēt iekārtas vai veikt citas darbības, kas varētu traucēt informācijas un tehnisko resursu darbību.

26. Informācijas sistēmas lietotājam ir aizliegts veikt paroļu minēšanu, drošības ievainojamības pārbaudes, kodēto datu atkodēšanu, izmantot noklausīšanās programmas un veikt citas darbības, kas vērstas uz informācijas un tehnisko resursu drošības vājināšanu.

IV. Interneta un e-pasta lietošana

27. Pieeju Internetam darbiniekiem piešķir vienlaicīgi ar Informācijas sistēmas lietotāja pieejas tiesībām Pašvaldības datortīklam (domēnam), kas nepieciešams, lai nodrošinātu iestādes darbību un klientiem sniegtos pakalpojumus.

28. Informācijas sistēmas lietotājam darba vajadzībām ir jāizmanto tikai Pašvaldības piešķirtais e-pasts.

29. Informācijas sistēmas lietotājam ir aizliegts, izmantojot Pašvaldības piešķirto e-pastu, reģistrēties dažādos interneta resursos, kas tiek izmantoti privātām vajadzībām.

30. Informācijas sistēmas lietotājam ir aizliegts atvērt e-pasta pielikumus vai atvērt sūtījumā iekļautās Interneta adreses, kas saņemtas no nenoskaidrotiem sūtītājiem.

31. Lietojot Internetu, darbinieki pārstāv pašvaldību un tie ir atbildīgi, lai Internets tiktu izmantots darba vajadzībām ētiski un atbilstoši likumdošanas prasībām.

32. Darbiniekiem, izmantojot e-pastu, ir jānodrošina, ka visas komunikācijas tiek veiktas profesionālām vajadzībām un netraucē pašu darbinieku darba produktivitāti, kā arī netiek izplatīta vai sūtīta informācija, kas ir aizsargāta ar autortiesībām. Pašvaldība no darbinieka ir tiesīgs piedzīt zaudējumus, kas Pašvaldībai var būt radušies maksājot atlīdzību autortiesību īpašniekam par autortiesību pārkāpumu.

33. Darbinieki ir atbildīgi par visu nosūtīto tekstuālo, audio un vizuālo saturu. Datortīklu administrators bez saskaņošanas ar darbinieku patur sev tiesības pārlūkot darbinieku saņemto un nosūtīto e-pastu saturu, ja uzskata to par nepieciešamu.

34. Informācijas sistēmas drošības pārvaldniekam vai Datortīklu administratoram ir tiesības bloķēt atsevišķu interneta resursu izmantošanu, kā arī ir tiesības piekļūt Informācijas sistēmas lietotāja saglabātajai informācijai, kas atrodas uz Informācijas sistēmas lietotāja datoriem vai serveriem, tikai pildot amata pienākumus vai pildot izpilddirektora rīkojumus.

35. Darbiniekiem ir aizliegts sūtīt tā sauktās "ķēdes vēstules" (t.sk. mēstules, reklāmas, aģitācijas un tml.)– elektroniskus ziņojumus ar lūgumu pārsūtīt tos citiem adresātiem, kā arī ir aizliegts atvērt un darbināt no Interneta tīkla saņemtus aizdomīgus failus. Informācijas sistēmas lietotājam ir jāatceras, ka Interneta tīkls nav drošs datu pārraides mēdijs un nosūtītāja identifikāciju var viegli viltot. Ja par failu rodas šaubas, Informācijas sistēmas lietotājam ir nepieciešams sazināties ar nosūtītāju un noskaidrot, vai šāds dokuments ir ticis nosūtīts.

V. Informācijas sistēmas lietotāja pieejas paroles uzbūve un lietošana

36. Pašvaldības informācijas resursu aizsardzība tiek nodrošināta ar datora paroli datortīkla (domēna) līmenī, kam ir jāatbilst vismaz sekojošām prasībām:

36.1. minimālam paroles garumam ir jābūt vismaz 8 simboli un tās maksimālais garums nedrīkst pārsniegt 16 simbolus.

36.2. maksimālais paroles maiņas periods nedrīkst būt ilgāks par 90 dienām, taču paroli aizliegts pašrocīgi mainīt biežāk nekā divas reizes 24 stundu laikā.

36.3. paroles uzbūvei jābūt komplicētai, izmantojot vismaz vienu lielo latīņu alfabēta burtu, mazo latīņu alfabēta burtu, ciparu un īpašo rakstzīmju kombināciju (kā piemēram, !@#$%^*()_+).

36.4. izveidojot paroli, tā nedrīkst sakrist ar nevienu no 5 iepriekšējām parolēm.

37. Informācijas sistēmas lietotājs nedrīkst izpaust savu paroli jebkurām citām trešajām personām vai citiem lietotājiem, izņemot atsevišķos gadījumos savas prombūtnes laikā, ja atļauju ir devis atbilstošās struktūrvienības vadītājs.

38. Informācijas sistēmas lietotājs nedrīkst savu paroli pierakstīt uz papīra, ja šo dokumentu neglabā seifā vai citā vietā ar ierobežotu citu personu piekļuvi.

39. Ja Informācijas sistēmas lietotājam rodas aizdomas, ka viņa paroli ir uzzinājusi jebkura cita persona, Informācijas sistēmas lietotājam ir pienākums pēc iespējas īsākā laikā šo paroli nomainīt patstāvīgi vai lūgt Datortīklu administratoru to izdarīt savā vietā.

40. Informācijas sistēmas lietotājs ir atbildīgs par informācijas aizsardzību un tā pienākums ir nodrošināt, ka datoriem Informācijas sistēmas lietotāja prombūtnes laikā ir ieslēgts ar paroli aizsargāts ekrānsaudzētājs vai noslēgta datora klaviatūra ar Ctrl-Alt-Del funkcijas palīdzību, izvēloties „Lock Computer" izvēlni.

41. Dienas beigās, beidzot darbu pie datora, tas jāizslēdz izmantojot procedūru: Start =>Shut Dowm =>Ok.

Pielikumā:

1. Krustpils novada pašvaldības Informācijas sistēmu tiesību pieprasījums uz 1 lp.

Domes priekšsēdētājs K.Pabērzs

1. PIELIKUMS
"Krustpils novada pašvaldības
Informācijas sistēmas lietošanas noteikumi"

KRUSTPILS NOVADA PAŠVALDĪBAS
INFORMĀCIJAS RESURSU LIETOTĀJA REĢISTRĀCIJAS ANKETA

Vārds, Uzvārds	
Struktūrvienība	
Amats	
Telefona numurs	

Piešķirt pieeju sekojošiem informācijas resursiem. vajadzīgos atzīmēt ar). ☑

- ☐ **Dokumentu koplietošanas mape (failu serveris)**
- ☐ **E-pasts**
- ☐ **Grāmatvedības uzskaites sistēma (GVEDIS)**
- ☐ **Personu dzīvesvietas reģistrēšanas sistēma (PERS)**
- ☐ **Personu dzimtsarakstu reģistrācijas informatīvā sistēma (DZIMTS)**
- ☐ **Sociālās palīdzības administrēšanas sistēma (SOPA)**
- ☐ **Nekustamā īpašuma nodokļa administrēšanas sistēma (NINO)**
- ☐ **D**okumentu vadības sistēma **(NAMEJS)**
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _

_____

_____

(Datums, paraksts)

LATVIJAS REPUBLIKA
KRUSTPILS NOVADA PAŠVALDĪBA
Reģ.Nr.90009118116
Rīgas ielā 150a, Jēkabpilī, LV-5202
Tālrunis 65237635, Fakss 65237611, e-pasts: novads@krustpils.lv

Jēkabpilī

15.03.2017.

APSTIPRINĀTI
ar Krustpils novada domes
15.03.2017. sēdes lēmumu
(protokols Nr.5.,17.p.)
Pielikums Nr.6.

Krustpils novada pašvaldība
Krustpils pagasta pārvalde
Informācijas sistēmas lietošanas noteikumi

I.Vispārīgie jautājumi

1. Informācijas sistēmas lietošanas noteikumi nosaka Krustpils novada pašvaldība (turpmāk – Pašvaldība) darbinieku pienākumus un prasības pašvaldības izmantotās informācijas sistēmas un interneta lietošanai, kā arī nosaka kārtību, kādā tiek veikta pašvaldības izmantotās informācijas sistēmas lietotāju pieejas tiesību piešķiršana, izmaiņas un anulēšana.

2. Noteikumos lietotie termini:
2.1. **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.
2.2. **Krustpils novada pašvaldība** – institūcija, kas normatīvajos aktos noteiktajā kārtībā organizē un vada informācijas sistēmu darbību.
2.3. **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.
2.4. **Informācijas sistēmas lietotājs –** persona, kurai ir piešķirtas piekļuves tiesības informācijas sistēmās.

3. Informācijas sistēmas lietošanas noteikumi ir saistoši visiem pašvaldības darbiniekiem (pilna darba laika, nepilnas slodzes un līgumdarbiniekiem), kuri ir nodarbināti pašvaldībā un kam ir piekļuve kādai no pašvaldības informācijas sistēmām.

4. Katra pašvaldības Informācijas sistēmas lietotāja pienākums ir iepazīties ar šiem noteikumiem un ievērot tos ikdienas darbā.

II. Informācijas sistēmas lietotāju administrēšanas kārtība

5. Pašvaldības katras pašvaldības iestādes un struktūrvienības vadītājs ir atbildīgs par sev un to padotībā esošo darbinieku lietotāju pieejas tiesību piešķiršanu, izmaiņu veikšanu un anulēšanu.

6. Lai izveidotu lietotāju pieejas tiesības vai veiktu izmaiņas tajās, Pašvaldības atbilstošās pašvaldības iestādes un struktūrvienības vadītājs raksta pieprasījumu (1.Pielikums), atzīmējot tajā nepieciešamo Informācijas resursu, ko iesniedz Informācijas sistēmas drošības pārvaldniekam.

7. Informācijas sistēmas lietotāju pieejas tiesības tiek piešķirtas Pašvaldības darbiniekiem atbilstoši katra atsevišķā darbinieka noteiktajiem darba pienākumiem un specifikai.

8. Informācijas sistēmas drošības pārvaldnieks izskata lietotāju pieejas tiesību piešķiršanas pieprasījumu un, ja uzskata to par pamatotu, Informācijas sistēmas drošības pārvaldnieks pieprasījumu izveidot atbilstošās informācijas sistēmas lietošanas tiesības nosūta Datortīklu administratoram.

9. Informācijas sistēmas lietotāju pieejas tiesību piešķiršana Pašvaldības informācijas resursiem personām, kuras nav Pašvaldības darbinieki, notiek tikai atsevišķos gadījumos pēc Sistēmas drošības pārvaldnieka pieprasījuma (piemēram, gadījumā ja ir noslēgts līgums starp pašvaldību un atbilstošo personu, kurā ir precīzi noteikti personas pienākumi, pieļaujamie informācijas izmantošanas mērķi, konfidencialitātes prasības un atbildība).

10. Informācijas sistēmas drošības pārvaldnieks ir atbildīgs par Lietotāju pieejas tiesību izveidošanu, administrēšanu un šo pieprasījumu apkopošanu, glabāšanu, kontroli un uzraudzību.

11. Piešķirtās lietotāju pieejas tiesības Pašvaldības informācijas resursiem ir nekavējoties jāanulē šādos gadījumos:

11.1. darbiniekiem, kuri pārtrauc darba (līguma) tiesiskās attiecības ar pašvaldību un / vai tās vairs nav nepieciešamas pienākumu veikšanai.

11.2. personām, kuras ir izpildījušas savstarpēji noslēgto līgumu ar pašvaldību vai šī līguma izbeigšanās (atcelšanas) gadījumā.

12. Iestājoties šo noteikumu 11.punktā minētajam gadījumam, atbilstošās struktūrvienības vadītājam, kura pakļautībā ir augstāk minētais darbinieks (vai koordinējošās struktūrvienības vadītājam gadījumos ar trešajām personām), ir pienākums informēt Datortīklu administratoru, kas veic atbilstošā lietotāja tiesību bloķēšanu.

13. Piešķirtās lietotāju pieejas tiesības var anulēt arī Informācijas sistēmas drošības pārvaldnieks vai Datortīklu administrators, balstoties uz atbilstošā lietotāja Informācijas sistēmas drošības politikas vai to saistošo dokumentu pārkāpumiem, par to rakstiski informējot Pašvaldības izpilddirektoru.

14. Datortīklu administratoram pēc Pašvaldības izpilddirektora vai Informācijas sistēmas drošības pārvaldnieka pieprasījuma, sagatavot Lietotāju pieejas tiesību sarakstu.

15. Datortīklu administratoram sadarbībā ar Informācijas sistēmas drošības pārvaldnieku ir pienākums vismaz reizi gadā veikt Lietotāju pieejas tiesību kontroli, pārbaudot un salīdzinot piešķirto lietotāju pieejas tiesību atbilstību darbinieka (personas, kuras darbojas uz līguma pamata) pienākumiem un specifikai.

III. Informācijas sistēmas lietotāju tiesības, pienākumi un atbildība

16. Informācijas sistēmas lietotājam ir tiesības izmantot viņam lietošanā nodotos datorus un to programmatūru, kā arī Informācijas sistēmas lietotājam ir tiesības pieprasīt atbalstu gadījumā, ja datoram vai tā programmatūrai ir radušies traucējumi.

17. Informācijas sistēmas lietotājs ir atbildīgs par datortehniku, kas nodota viņa rīcībā, kā arī atbild par darbībām, kas tiek veiktas ar viņam nodoto datortehniku.

18. Informācijas sistēmas lietotājs nedrīkst atļaut piekļūt tam nodotai datortehnikai citām personām, ja tas nav nepieciešams tiešo darba pienākumu pildīšanai un to pilnvarojumu nav devis Pašvaldības izpilddirektors, Informācijas sistēmas drošības pārvaldnieks vai Datortīklu administrators.

19. Informācijas sistēmas lietotāja pienākums ir apzināti nepieļaut datorvīrusu iekļūšanu iestādes datorsistēmās un neizmantot nezināmas izcelsmes datu nesējus. Rodoties aizdomām, ka dators ir inficēts ar datorvīrusu, par to nekavējoties jāinformē Informācijas sistēmas drošības pārvaldnieks vai Datortīklu administrators.

20. Informācijas sistēmas lietotājam ir pienākums jebkuru ienākošo elektronisko informāciju (failus) pirms lietošanas obligāti pārbaudīt ar antivīrusa programmatūru, ja tas netiek nodrošināts automātiski.

21. Nelicencētas programmatūras uzstādīšana un lietošana darba stacijās (lietotāja datoros) ir aizliegta. Patvaļīgi uzstādītas programmatūras lietošana, bez Pašvaldības izpilddirektora, Informācijas sistēmas drošības pārvaldnieka vai Datortīklu administratora atļaujas ir aizliegta.

22. Informācijas sistēmas lietotājs nedrīkst izpaust nepilnvarotām personām ziņas par Pašvaldības datoru tīkla uzbūvi un konfigurāciju.

23. Informācijas sistēmas lietotājs nedrīkst no sava darba datora kopēt failus uz ārējiem datu nesējiem (piemēram, CD, DVD, USB kartēm vai citiem datu nesējiem), ja to nevajag tiešo darba pienākumu pildīšanai vai ja tam pilnvarojumu nav devis Pašvaldības izpilddirektors, Informācijas sistēmas drošības pārvaldnieks vai Datortīklu administrators.

24. Ārējo datu nesēju, kurā ir iekopēta ierobežotas pieejamības informācija, no Pašvaldības telpām drīkst iznest tikai ar Pašvaldības izpilddirektora RAKSTISKU atļauju. Šajos gadījumos Informācijas sistēmas lietotājs, kurš no iestādes telpām iznes šādu datu nesēju, uzņemas pilnu atbildību par šo informāciju.

25. Informācijas sistēmas lietotājam ir aizliegts patvarīgi pārvietot, demontēt aparatūru, izjaukt, remontēt iekārtas vai veikt citas darbības, kas varētu traucēt informācijas un tehnisko resursu darbību.

26. Informācijas sistēmas lietotājam ir aizliegts veikt paroļu minēšanu, drošības ievainojamības pārbaudes, kodēto datu atkodēšanu, izmantot noklausīšanās programmas un veikt citas darbības, kas vērstas uz informācijas un tehnisko resursu drošības vājināšanu.

IV. Interneta un e-pasta lietošana

27. Pieeju Internetam darbiniekiem piešķir vienlaicīgi ar Informācijas sistēmas lietotāja pieejas tiesībām Pašvaldības datortīklam (domēnam), kas nepieciešams, lai nodrošinātu iestādes darbību un klientiem sniegtos pakalpojumus.

28. Informācijas sistēmas lietotājam darba vajadzībām ir jāizmanto tikai Pašvaldības piešķirtais e-pasts.

29. Informācijas sistēmas lietotājam ir aizliegts, izmantojot Pašvaldības piešķirto e-pastu, reģistrēties dažādos interneta resursos, kas tiek izmantoti privātām vajadzībām.

30. Informācijas sistēmas lietotājam ir aizliegts atvērt e-pasta pielikumus vai atvērt sūtījumā iekļautās Interneta adreses, kas saņemtas no nenoskaidrotiem sūtītājiem.

31. Lietojot Internetu, darbinieki pārstāv pašvaldību un tie ir atbildīgi, lai Internets tiktu izmantots darba vajadzībām ētiski un atbilstoši likumdošanas prasībām.

32. Darbiniekiem, izmantojot e-pastu, ir jānodrošina, ka visas komunikācijas tiek veiktas profesionālām vajadzībām un netraucē pašu darbinieku darba produktivitāti, kā arī netiek izplatīta vai sūtīta informācija, kas ir aizsargāta ar autortiesībām. Pašvaldība no darbinieka ir tiesīgs piedzīt zaudējumus, kas Pašvaldībai var būt radušies maksājot atlīdzību autortiesību īpašniekam par autortiesību pārkāpumu.

33. Darbinieki ir atbildīgi par visu nosūtīto tekstuālo, audio un vizuālo saturu. Datortīklu administrators bez saskaņošanas ar darbinieku patur sev tiesības pārlūkot darbinieku saņemto un nosūtīto e-pastu saturu, ja uzskata to par nepieciešamu.

34. Informācijas sistēmas drošības pārvaldniekam vai Datortīklu administratoram ir tiesības bloķēt atsevišķu interneta resursu izmantošanu, kā arī ir tiesības piekļūt Informācijas sistēmas lietotāja saglabātajai informācijai, kas atrodas uz Informācijas sistēmas lietotāja datoriem vai serveriem, tikai pildot amata pienākumus vai pildot izpilddirektora rīkojumus.

35. Darbiniekiem ir aizliegts sūtīt tā sauktās "ķēdes vēstules" (t.sk. mēstules, reklāmas, aģitācijas un tml.)– elektroniskus ziņojumus ar lūgumu pārsūtīt tos citiem adresātiem, kā arī ir aizliegts atvērt un darbināt no Interneta tīkla saņemtus aizdomīgus failus. Informācijas sistēmas lietotājam ir jāatceras, ka Interneta tīkls nav drošs datu pārraides mēdijs un nosūtītāja identifikāciju var viegli viltot. Ja par failu rodas šaubas, Informācijas sistēmas lietotājam ir nepieciešams sazināties ar nosūtītāju un noskaidrot, vai šāds dokuments ir ticis nosūtīts.

V. Informācijas sistēmas lietotāja pieejas paroles uzbūve un lietošana

36. Pašvaldības informācijas resursu aizsardzība tiek nodrošināta ar datora paroli datortīkla (domēna) līmenī, kam ir jāatbilst vismaz sekojošām prasībām:

36.1. minimālam paroles garumam ir jābūt vismaz 8 simboli un tās maksimālais garums nedrīkst pārsniegt 16 simbolus.

36.2. maksimālais paroles maiņas periods nedrīkst būt ilgāks par 90 dienām, taču paroli aizliegts pašrocīgi mainīt biežāk nekā divas reizes 24 stundu laikā.

36.3. paroles uzbūvei jābūt komplicētai, izmantojot vismaz vienu lielo latīņu alfabēta burtu, mazo latīņu alfabēta burtu, ciparu un īpašo rakstzīmju kombināciju (kā piemēram, !@#$%^*()_+).

36.4. izveidojot paroli, tā nedrīkst sakrist ar nevienu no 5 iepriekšējām parolēm.

37. Informācijas sistēmas lietotājs nedrīkst izpaust savu paroli jebkurām citām trešajām personām vai citiem lietotājiem, izņemot atsevišķos gadījumos savas prombūtnes laikā, ja atļauju ir devis atbilstošās struktūrvienības vadītājs.

38. Informācijas sistēmas lietotājs nedrīkst savu paroli pierakstīt uz papīra, ja šo dokumentu neglabā seifā vai citā vietā ar ierobežotu citu personu piekļuvi.

39. Ja Informācijas sistēmas lietotājam rodas aizdomas, ka viņa paroli ir uzzinājusi jebkura cita persona, Informācijas sistēmas lietotājam ir pienākums pēc iespējas īsākā laikā šo paroli nomainīt patstāvīgi vai lūgt Datortīklu administratoru to izdarīt savā vietā.

40. Informācijas sistēmas lietotājs ir atbildīgs par informācijas aizsardzību un tā pienākums ir nodrošināt, ka datoriem Informācijas sistēmas lietotāja prombūtnes laikā ir ieslēgts ar paroli aizsargāts ekrānsaudzētājs vai noslēgta datora klaviatūra ar Ctrl-Alt-Del funkcijas palīdzību, izvēloties „Lock Computer" izvēlni.

41. Dienas beigās, beidzot darbu pie datora, tas jāizslēdz izmantojot procedūru: Start =>Shut Dowm =>Ok.

Pielikumā:
1. Krustpils novada pašvaldības Informācijas sistēmu tiesību pieprasījums uz 1 lp.

Domes priekšsēdētājs: K.Pabērzs

1. PIELIKUMS
"Krustpils novada pašvaldības
Informācijas sistēmas lietošanas noteikumi"

KRUSTPILS NOVADA PAŠVALDĪBAS
INFORMĀCIJAS RESURSU LIETOTĀJA REĢISTRĀCIJAS ANKETA

Vārds, Uzvārds	
Struktūrvienība	
Amats	
Telefona numurs	

Piešķirt pieeju sekojošiem informācijas resursiem (vajadzīgos atzīmēt ar). ☑

- ☐ **Dokumentu koplietošanas mape (failu serveris)**
- ☐ **E-pasts**
- ☐ **Grāmatvedības uzskaites sistēma**
- ☐ **Personu dzīvesvietas reģistrēšanas sistēma (PERS)**
- ☐ **Personu dzimtsarakstu reģistrācijas informatīvā sistēma (DZIMTS)**
- ☐ **Sociālās palīdzības administrēšanas sistēma (SOPA)**
- ☐ **Nekustamā īpašuma nodokļa administrēšanas sistēma (NINO)**
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____

_____

(Datums, paraksts)

LATVIJAS REPUBLIKA
KRUSTPILS NOVADA PAŠVALDĪBA
Reģ.Nr.90009118116
Rīgas ielā 150a, Jēkabpilī, LV-5202
Tālrunis 65237635, Fakss 65237611, e-pasts: novads@krustpils.lv

Jēkabpilī

15.03.2017.

APSTIPRINĀTI
ar Krustpils novada domes
15.03.2017. sēdes lēmumu
(protokols Nr.5.,17.p.)
Pielikums Nr.7.

Krustpils novada pašvaldība
Kūku pagasta pārvalde
Informācijas sistēmas lietošanas noteikumi

I.Vispārīgie jautājumi

1. Informācijas sistēmas lietošanas noteikumi nosaka Krustpils novada pašvaldība, Kūku pagasta pārvaldes (turpmāk – Pašvaldība) darbinieku pienākumus un prasības pašvaldības izmantotās informācijas sistēmas un interneta lietošanai, kā arī nosaka kārtību, kādā tiek veikta pašvaldības izmantotās informācijas sistēmas lietotāju pieejas tiesību piešķiršana, izmaiņas un anulēšana.

2. Noteikumos lietotie termini:
2.1. **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.
2.2. **Krustpils novada pašvaldība** – institūcija, kas normatīvajos aktos noteiktajā kārtībā organizē un vada informācijas sistēmu darbību.
2.3. **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.
2.4. **Informācijas sistēmas lietotājs –** persona, kurai ir piešķirtas piekļuves tiesības informācijas sistēmās.

3. Informācijas sistēmas lietošanas noteikumi ir saistoši visiem pašvaldības darbiniekiem (pilna darba laika, nepilnas slodzes un līgumdarbiniekiem), kuri ir nodarbināti pašvaldībā un kam ir piekļuve kādai no pašvaldības informācijas sistēmām.

4. Katra pašvaldības Informācijas sistēmas lietotāja pienākums ir iepazīties ar šiem noteikumiem un ievērot tos ikdienas darbā.

II. Informācijas sistēmas lietotāju administrēšanas kārtība

5. Pašvaldības katras pašvaldības iestādes un struktūrvienības vadītājs ir atbildīgs par sev un to padotībā esošo darbinieku lietotāju pieejas tiesību piešķiršanu, izmaiņu veikšanu un anulēšanu.

6. Lai izveidotu lietotāju pieejas tiesības vai veiktu izmaiņas tajās, Pašvaldības atbilstošās pašvaldības iestādes un struktūrvienības vadītājs raksta pieprasījumu (1.Pielikums), atzīmējot tajā nepieciešamo Informācijas resursu, ko iesniedz Informācijas sistēmas drošības pārvaldniekam.

7. Informācijas sistēmas lietotāju pieejas tiesības tiek piešķirtas Pašvaldības darbiniekiem atbilstoši katra atsevišķā darbinieka noteiktajiem darba pienākumiem un specifikai.

8. Informācijas sistēmas drošības pārvaldnieks izskata lietotāju pieejas tiesību piešķiršanas pieprasījumu un, ja uzskata to par pamatotu, Informācijas sistēmas drošības pārvaldnieks pieprasījumu izveidot atbilstošās informācijas sistēmas lietošanas tiesības nosūta Datortīklu administratoram.

9. Informācijas sistēmas lietotāju pieejas tiesību piešķiršana Pašvaldības informācijas resursiem personām, kuras nav Pašvaldības darbinieki, notiek tikai atsevišķos gadījumos pēc Sistēmas drošības pārvaldnieka pieprasījuma (piemēram, gadījumā ja ir noslēgts līgums starp pašvaldību un atbilstošo personu, kurā ir precīzi noteikti personas pienākumi, pieļaujamie informācijas izmantošanas mērķi, konfidencialitātes prasības un atbildība).

10. Informācijas sistēmas drošības pārvaldnieks ir atbildīgs par Lietotāju pieejas tiesību izveidošanu, administrēšanu un šo pieprasījumu apkopošanu, glabāšanu, kontroli un uzraudzību.

11. Piešķirtās lietotāju pieejas tiesības Pašvaldības informācijas resursiem ir nekavējoties jāanulē šādos gadījumos:

11.1. darbiniekiem, kuri pārtrauc darba (līguma) tiesiskās attiecības ar pašvaldību un / vai tās vairs nav nepieciešamas pienākumu veikšanai.

11.2. personām, kuras ir izpildījušas savstarpēji noslēgto līgumu ar pašvaldību vai šī līguma izbeigšanās (atcelšanas) gadījumā.

12. Iestājoties šo noteikumu 11.punktā minētajam gadījumam, atbilstošās struktūrvienības vadītājam, kura pakļautībā ir augstāk minētais darbinieks (vai koordinējošās struktūrvienības vadītājam gadījumos ar trešajām personām), ir pienākums informēt Datortīklu administratoru, kas veic atbilstošā lietotāja tiesību bloķēšanu.

13. Piešķirtās lietotāju pieejas tiesības var anulēt arī Informācijas sistēmas drošības pārvaldnieks vai Datortīklu administrators, balstoties uz atbilstošā lietotāja Informācijas sistēmas drošības politikas vai to saistošo dokumentu pārkāpumiem, par to rakstiski informējot Pašvaldības izpilddirektoru.

14. Datortīklu administratoram pēc Pašvaldības izpilddirektora vai Informācijas sistēmas drošības pārvaldnieka pieprasījuma, sagatavot Lietotāju pieejas tiesību sarakstu.

15. Datortīklu administratoram sadarbībā ar Informācijas sistēmas drošības pārvaldnieku ir pienākums vismaz reizi gadā veikt Lietotāju pieejas tiesību kontroli, pārbaudot un salīdzinot piešķirto lietotāju pieejas tiesību atbilstību darbinieka (personas, kuras darbojas uz līguma pamata) pienākumiem un specifikai.

III. Informācijas sistēmas lietotāju tiesības, pienākumi un atbildība

16. Informācijas sistēmas lietotājam ir tiesības izmantot viņam lietošanā nodotos datorus un to programmatūru, kā arī Informācijas sistēmas lietotājam ir tiesības pieprasīt atbalstu gadījumā, ja datoram vai tā programmatūrai ir radušies traucējumi.

17. Informācijas sistēmas lietotājs ir atbildīgs par datortehniku, kas nodota viņa rīcībā, kā arī atbild par darbībām, kas tiek veiktas ar viņam nodoto datortehniku.

18. Informācijas sistēmas lietotājs nedrīkst atļaut piekļūt tam nodotai datortehnikai citām personām, ja tas nav nepieciešams tiešo darba pienākumu pildīšanai un to pilnvarojumu nav devis Pašvaldības izpilddirektors, Informācijas sistēmas drošības pārvaldnieks vai Datortīklu administrators.

19. Informācijas sistēmas lietotāja pienākums ir apzināti nepieļaut datorvīrusu iekļūšanu iestādes datorsistēmās un neizmantot nezināmas izcelsmes datu nesējus. Rodoties aizdomām, ka dators ir inficēts ar datorvīrusu, par to nekavējoties jāinformē Informācijas sistēmas drošības pārvaldnieks vai Datortīklu administrators.

20. Informācijas sistēmas lietotājam ir pienākums jebkuru ienākošo elektronisko informāciju (failus) pirms lietošanas obligāti pārbaudīt ar antivīrusa programmatūru, ja tas netiek nodrošināts automātiski.

21. Nelicencētas programmatūras uzstādīšana un lietošana darba stacijās (lietotāja datoros) ir aizliegta. Patvaļīgi uzstādītas programmatūras lietošana, bez Pašvaldības izpilddirektora, Informācijas sistēmas drošības pārvaldnieka vai Datortīklu administratora atļaujas ir aizliegta.

22. Informācijas sistēmas lietotājs nedrīkst izpaust nepilnvarotām personām ziņas par Pašvaldības datoru tīkla uzbūvi un konfigurāciju.

23. Informācijas sistēmas lietotājs nedrīkst no sava darba datora kopēt failus uz ārējiem datu nesējiem (piemēram, CD, DVD, USB kartēm vai citiem datu nesējiem), ja to nevajag tiešo darba pienākumu pildīšanai vai ja tam pilnvarojumu nav devis Pašvaldības izpilddirektors, Informācijas sistēmas drošības pārvaldnieks vai Datortīklu administrators.

24. Ārējo datu nesēju, kurā ir iekopēta ierobežotas pieejamības informācija, no Pašvaldības telpām drīkst iznest tikai ar Pašvaldības izpilddirektora RAKSTISKU atļauju. Šajos gadījumos Informācijas sistēmas lietotājs, kurš no iestādes telpām iznes šādu datu nesēju, uzņemas pilnu atbildību par šo informāciju.

25. Informācijas sistēmas lietotājam ir aizliegts patvarīgi pārvietot, demontēt aparatūru, izjaukt, remontēt iekārtas vai veikt citas darbības, kas varētu traucēt informācijas un tehnisko resursu darbību.

26. Informācijas sistēmas lietotājam ir aizliegts veikt paroļu minēšanu, drošības ievainojamības pārbaudes, kodēto datu atkodēšanu, izmantot noklausīšanās programmas un veikt citas darbības, kas vērstas uz informācijas un tehnisko resursu drošības vājināšanu.

IV. Interneta un e-pasta lietošana

27. Pieeju Internetam darbiniekiem piešķir vienlaicīgi ar Informācijas sistēmas lietotāja pieejas tiesībām Pašvaldības datortīklam (domēnam), kas nepieciešams, lai nodrošinātu iestādes darbību un klientiem sniegtos pakalpojumus.

28. Informācijas sistēmas lietotājam darba vajadzībām ir jāizmanto tikai Pašvaldības piešķirtais e-pasts.

29. Informācijas sistēmas lietotājam ir aizliegts, izmantojot Pašvaldības piešķirto e-pastu, reģistrēties dažādos interneta resursos, kas tiek izmantoti privātām vajadzībām.

30. Informācijas sistēmas lietotājam ir aizliegts atvērt e-pasta pielikumus vai atvērt sūtījumā iekļautās Interneta adreses, kas saņemtas no nenoskaidrotiem sūtītājiem.

31. Lietojot Internetu, darbinieki pārstāv pašvaldību un tie ir atbildīgi, lai Internets tiktu izmantots darba vajadzībām ētiski un atbilstoši likumdošanas prasībām.

32. Darbiniekiem, izmantojot e-pastu, ir jānodrošina, ka visas komunikācijas tiek veiktas profesionālām vajadzībām un netraucē pašu darbinieku darba produktivitāti, kā arī netiek izplatīta vai sūtīta informācija, kas ir aizsargāta ar autortiesībām. Pašvaldība no darbinieka ir tiesīgs piedzīt zaudējumus, kas Pašvaldībai var būt radušies maksājot atlīdzību autortiesību īpašniekam par autortiesību pārkāpumu.

33. Darbinieki ir atbildīgi par visu nosūtīto tekstuālo, audio un vizuālo saturu. Datortīklu administrators bez saskaņošanas ar darbinieku patur sev tiesības pārlūkot darbinieku saņemto un nosūtīto e-pastu saturu, ja uzskata to par nepieciešamu.

34. Informācijas sistēmas drošības pārvaldniekam vai Datortīklu administratoram ir tiesības bloķēt atsevišķu interneta resursu izmantošanu, kā arī ir tiesības piekļūt Informācijas sistēmas lietotāja saglabātajai informācijai, kas atrodas uz Informācijas sistēmas lietotāja datoriem vai serveriem, tikai pildot amata pienākumus vai pildot izpilddirektora rīkojumus.

35. Darbiniekiem ir aizliegts sūtīt tā sauktās "ķēdes vēstules" (t.sk. mēstules, reklāmas, aģitācijas un tml.)– elektroniskus ziņojumus ar lūgumu pārsūtīt tos citiem adresātiem, kā arī ir aizliegts atvērt un darbināt no Interneta tīkla saņemtus aizdomīgus failus. Informācijas sistēmas lietotājam ir jāatceras, ka Interneta tīkls nav drošs datu pārraides mēdijs un nosūtītāja identifikāciju var viegli viltot. Ja par failu rodas šaubas, Informācijas sistēmas lietotājam ir nepieciešams sazināties ar nosūtītāju un noskaidrot, vai šāds dokuments ir ticis nosūtīts.

V. Informācijas sistēmas lietotāja pieejas paroles uzbūve un lietošana

36. Pašvaldības informācijas resursu aizsardzība tiek nodrošināta ar datora paroli datortīkla (domēna) līmenī, kam ir jāatbilst vismaz sekojošām prasībām:

36.1. minimālam paroles garumam ir jābūt vismaz 8 simboli un tās maksimālais garums nedrīkst pārsniegt 16 simbolus.

36.2. maksimālais paroles maiņas periods nedrīkst būt ilgāks par 90 dienām, taču paroli aizliegts pašrocīgi mainīt biežāk nekā divas reizes 24 stundu laikā.

36.3. paroles uzbūvei jābūt komplicētai, izmantojot vismaz vienu lielo latīņu alfabēta burtu, mazo latīņu alfabēta burtu, ciparu un īpašo rakstzīmju kombināciju (kā piemēram, !@#$%^*()_+).

36.4. izveidojot paroli, tā nedrīkst sakrist ar nevienu no 5 iepriekšējām parolēm.

37. Informācijas sistēmas lietotājs nedrīkst izpaust savu paroli jebkurām citām trešajām personām vai citiem lietotājiem, izņemot atsevišķos gadījumos savas prombūtnes laikā, ja atļauju ir devis atbilstošās struktūrvienības vadītājs.

38. Informācijas sistēmas lietotājs nedrīkst savu paroli pierakstīt uz papīra, ja šo dokumentu neglabā seifā vai citā vietā ar ierobežotu citu personu piekļuvi.

39. Ja Informācijas sistēmas lietotājam rodas aizdomas, ka viņa paroli ir uzzinājusi jebkura cita persona, Informācijas sistēmas lietotājam ir pienākums pēc iespējas īsākā laikā šo paroli nomainīt patstāvīgi vai lūgt Datortīklu administratoru to izdarīt savā vietā.

40. Informācijas sistēmas lietotājs ir atbildīgs par informācijas aizsardzību un tā pienākums ir nodrošināt, ka datoriem Informācijas sistēmas lietotāja prombūtnes laikā ir ieslēgts ar paroli aizsargāts ekrānsaudzētājs vai noslēgta datora klaviatūra ar Ctrl-Alt-Del funkcijas palīdzību, izvēloties „Lock Computer" izvēlni.

41. Dienas beigās, beidzot darbu pie datora, tas jāizslēdz izmantojot procedūru: Start =>Shut Dowm =>Ok.

Pielikumā:

1. Krustpils novada pašvaldības Informācijas sistēmu tiesību pieprasījums uz 1 lp.

Domes priekšsēdētājs K.Pabērzs

1. PIELIKUMS
"Krustpils novada pašvaldības
Informācijas sistēmas lietošanas noteikumi"

KRUSTPILS NOVADA PAŠVALDĪBAS
INFORMĀCIJAS RESURSU LIETOTĀJA REĢISTRĀCIJAS ANKETA

Vārds, Uzvārds	
Struktūrvienība	
Amats	
Telefona numurs	

Piešķirt pieeju sekojošiem informācijas resursiem (vajadzīgos atzīmēt ar). ☑

- ☐ **Dokumentu koplietošanas mape (failu serveris)**
- ☐ **E-pasts**
- ☐ **Grāmatvedības uzskaites sistēma**
- ☐ **Personu dzīvesvietas reģistrēšanas sistēma (PERS)**
- ☐ **Personu dzimtsarakstu reģistrācijas informatīvā sistēma (DZIMTS)**
- ☐ **Sociālās palīdzības administrēšanas sistēma (SOPA)**
- ☐ **Nekustamā īpašuma nodokļa administrēšanas sistēma (NINO)**
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____

_____

(Datums, paraksts)

LATVIJAS REPUBLIKA
KRUSTPILS NOVADA PAŠVALDĪBA
Reģ.Nr.90009118116
Rīgas ielā 150a, Jēkabpilī, LV-5202
Tālrunis 65237635, Fakss 65237611, e-pasts: novads@krustpils.lv

Jēkabpilī

15.03.2017.

APSTIPRINĀTI
ar Krustpils novada domes
15.03.2017. sēdes lēmumu
(protokols Nr.5.,17.p.)
Pielikums Nr.8.

Krustpils novada pašvaldība
Mežāres pagasta pārvalde
Informācijas sistēmas lietošanas noteikumi

I.Vispārīgie jautājumi

1. Informācijas sistēmas lietošanas noteikumi nosaka Krustpils novada pašvaldība, Mežāres pagasta pārvaldes (turpmāk – Pašvaldība) darbinieku pienākumus un prasības pašvaldības izmantotās informācijas sistēmas un interneta lietošanai, kā arī nosaka kārtību, kādā tiek veikta pašvaldības izmantotās informācijas sistēmas lietotāju pieejas tiesību piešķiršana, izmaiņas un anulēšana.

2. Noteikumos lietotie termini:

2.1. **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.

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

2.3. **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.

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

3. Informācijas sistēmas lietošanas noteikumi ir saistoši visiem pašvaldības darbiniekiem (pilna darba laika, nepilnas slodzes un līgumdarbiniekiem), kuri ir nodarbināti pašvaldībā un kam ir piekļuve kādai no pašvaldības informācijas sistēmām.

4. Katra pašvaldības Informācijas sistēmas lietotāja pienākums ir iepazīties ar šiem noteikumiem un ievērot tos ikdienas darbā.

II. Informācijas sistēmas lietotāju administrēšanas kārtība

5. Pašvaldības katras pašvaldības iestādes un struktūrvienības vadītājs ir atbildīgs par sev un to padotībā esošo darbinieku lietotāju pieejas tiesību piešķiršanu, izmaiņu veikšanu un anulēšanu.

6. Lai izveidotu lietotāju pieejas tiesības vai veiktu izmaiņas tajās, Pašvaldības atbilstošās pašvaldības iestādes un struktūrvienības vadītājs raksta pieprasījumu (1.Pielikums), atzīmējot tajā nepieciešamo Informācijas resursu, ko iesniedz Informācijas sistēmas drošības pārvaldniekam.

7. Informācijas sistēmas lietotāju pieejas tiesības tiek piešķirtas Pašvaldības darbiniekiem atbilstoši katra atsevišķā darbinieka noteiktajiem darba pienākumiem un specifikai.

8. Informācijas sistēmas drošības pārvaldnieks izskata lietotāju pieejas tiesību piešķiršanas pieprasījumu un, ja uzskata to par pamatotu, Informācijas sistēmas drošības pārvaldnieks pieprasījumu izveidot atbilstošās informācijas sistēmas lietošanas tiesības nosūta Datortīklu administratoram.

9. Informācijas sistēmas lietotāju pieejas tiesību piešķiršana Pašvaldības informācijas resursiem personām, kuras nav Pašvaldības darbinieki, notiek tikai atsevišķos gadījumos pēc Sistēmas drošības pārvaldnieka pieprasījuma (piemēram, gadījumā ja ir noslēgts līgums starp pašvaldību un atbilstošo personu, kurā ir precīzi noteikti personas pienākumi, pieļaujamie informācijas izmantošanas mērķi, konfidencialitātes prasības un atbildība).

10. Informācijas sistēmas drošības pārvaldnieks ir atbildīgs par Lietotāju pieejas tiesību izveidošanu, administrēšanu un šo pieprasījumu apkopošanu, glabāšanu, kontroli un uzraudzību.

11. Piešķirtās lietotāju pieejas tiesības Pašvaldības informācijas resursiem ir nekavējoties jāanulē šādos gadījumos:

11.1. darbiniekiem, kuri pārtrauc darba (līguma) tiesiskās attiecības ar pašvaldību un / vai tās vairs nav nepieciešamas pienākumu veikšanai.

11.2. personām, kuras ir izpildījušas savstarpēji noslēgto līgumu ar pašvaldību vai šī līguma izbeigšanās (atcelšanas) gadījumā.

12. Iestājoties šo noteikumu 11.punktā minētajam gadījumam, atbilstošās struktūrvienības vadītājam, kura pakļautībā ir augstāk minētais darbinieks (vai koordinējošās struktūrvienības vadītājam gadījumos ar trešajām personām), ir pienākums informēt Datortīklu administratoru, kas veic atbilstošā lietotāja tiesību bloķēšanu.

13. Piešķirtās lietotāju pieejas tiesības var anulēt arī Informācijas sistēmas drošības pārvaldnieks vai Datortīklu administrators, balstoties uz atbilstošā lietotāja Informācijas sistēmas drošības politikas vai to saistošo dokumentu pārkāpumiem, par to rakstiski informējot Pašvaldības izpilddirektoru.

14. Datortīklu administratoram pēc Pašvaldības izpilddirektora vai Informācijas sistēmas drošības pārvaldnieka pieprasījuma, sagatavot Lietotāju pieejas tiesību sarakstu.

15. Datortīklu administratoram sadarbībā ar Informācijas sistēmas drošības pārvaldnieku ir pienākums vismaz reizi gadā veikt Lietotāju pieejas tiesību kontroli, pārbaudot un salīdzinot piešķirto lietotāju pieejas tiesību atbilstību darbinieka (personas, kuras darbojas uz līguma pamata) pienākumiem un specifikai.

III. Informācijas sistēmas lietotāju tiesības, pienākumi un atbildība

16. Informācijas sistēmas lietotājam ir tiesības izmantot viņam lietošanā nodotos datorus un to programmatūru, kā arī Informācijas sistēmas lietotājam ir tiesības pieprasīt atbalstu gadījumā, ja datoram vai tā programmatūrai ir radušies traucējumi.

17. Informācijas sistēmas lietotājs ir atbildīgs par datortehniku, kas nodota viņa rīcībā, kā arī atbild par darbībām, kas tiek veiktas ar viņam nodoto datortehniku.

18. Informācijas sistēmas lietotājs nedrīkst atļaut piekļūt tam nodotai datortehnikai citām personām, ja tas nav nepieciešams tiešo darba pienākumu pildīšanai un to pilnvarojumu nav devis Pašvaldības izpilddirektors, Informācijas sistēmas drošības pārvaldnieks vai Datortīklu administrators.

19. Informācijas sistēmas lietotāja pienākums ir apzināti nepieļaut datorvīrusu iekļūšanu iestādes datorsistēmās un neizmantot nezināmas izcelsmes datu nesējus. Rodoties aizdomām, ka dators ir inficēts ar datorvīrusu, par to nekavējoties jāinformē Informācijas sistēmas drošības pārvaldnieks vai Datortīklu administrators.

20. Informācijas sistēmas lietotājam ir pienākums jebkuru ienākošo elektronisko informāciju (failus) pirms lietošanas obligāti pārbaudīt ar antivīrusa programmatūru, ja tas netiek nodrošināts automātiski.

21. Nelicencētas programmatūras uzstādīšana un lietošana darba stacijās (lietotāja datoros) ir aizliegta. Patvaļīgi uzstādītas programmatūras lietošana, bez Pašvaldības izpilddirektora, Informācijas sistēmas drošības pārvaldnieka vai Datortīklu administratora atļaujas ir aizliegta.

22. Informācijas sistēmas lietotājs nedrīkst izpaust nepilnvarotām personām ziņas par Pašvaldības datoru tīkla uzbūvi un konfigurāciju.

23. Informācijas sistēmas lietotājs nedrīkst no sava darba datora kopēt failus uz ārējiem datu nesējiem (piemēram, CD, DVD, USB kartēm vai citiem datu nesējiem), ja to nevajag tiešo darba pienākumu pildīšanai vai ja tam pilnvarojumu nav devis Pašvaldības izpilddirektors, Informācijas sistēmas drošības pārvaldnieks vai Datortīklu administrators.

24. Ārējo datu nesēju, kurā ir iekopēta ierobežotas pieejamības informācija, no Pašvaldības telpām drīkst iznest tikai ar Pašvaldības izpilddirektora RAKSTISKU atļauju. Šajos gadījumos Informācijas sistēmas lietotājs, kurš no iestādes telpām iznes šādu datu nesēju, uzņemas pilnu atbildību par šo informāciju.

25. Informācijas sistēmas lietotājam ir aizliegts patvarīgi pārvietot, demontēt aparatūru, izjaukt, remontēt iekārtas vai veikt citas darbības, kas varētu traucēt informācijas un tehnisko resursu darbību.

26. Informācijas sistēmas lietotājam ir aizliegts veikt paroļu minēšanu, drošības ievainojamības pārbaudes, kodēto datu atkodēšanu, izmantot noklausīšanās programmas un veikt citas darbības, kas vērstas uz informācijas un tehnisko resursu drošības vājināšanu.

IV. Interneta un e-pasta lietošana

27. Pieeju Internetam darbiniekiem piešķir vienlaicīgi ar Informācijas sistēmas lietotāja pieejas tiesībām Pašvaldības datortīklam (domēnam), kas nepieciešams, lai nodrošinātu iestādes darbību un klientiem sniegtos pakalpojumus.

28. Informācijas sistēmas lietotājam darba vajadzībām ir jāizmanto tikai Pašvaldības piešķirtais e-pasts.

29. Informācijas sistēmas lietotājam ir aizliegts, izmantojot Pašvaldības piešķirto e-pastu, reģistrēties dažādos interneta resursos, kas tiek izmantoti privātām vajadzībām.

30. Informācijas sistēmas lietotājam ir aizliegts atvērt e-pasta pielikumus vai atvērt sūtījumā iekļautās Interneta adreses, kas saņemtas no nenoskaidrotiem sūtītājiem.

31. Lietojot Internetu, darbinieki pārstāv pašvaldību un tie ir atbildīgi, lai Internets tiktu izmantots darba vajadzībām ētiski un atbilstoši likumdošanas prasībām.

32. Darbiniekiem, izmantojot e-pastu, ir jānodrošina, ka visas komunikācijas tiek veiktas profesionālām vajadzībām un netraucē pašu darbinieku darba produktivitāti, kā arī netiek izplatīta vai sūtīta informācija, kas ir aizsargāta ar autortiesībām. Pašvaldība no darbinieka ir tiesīgs piedzīt zaudējumus, kas Pašvaldībai var būt radušies maksājot atlīdzību autortiesību īpašniekam par autortiesību pārkāpumu.

33. Darbinieki ir atbildīgi par visu nosūtīto tekstuālo, audio un vizuālo saturu. Datortīklu administrators bez saskaņošanas ar darbinieku patur sev tiesības pārlūkot darbinieku saņemto un nosūtīto e-pastu saturu, ja uzskata to par nepieciešamu.

34. Informācijas sistēmas drošības pārvaldniekam vai Datortīklu administratoram ir tiesības bloķēt atsevišķu interneta resursu izmantošanu, kā arī ir tiesības piekļūt Informācijas sistēmas lietotāja saglabātajai informācijai, kas atrodas uz Informācijas sistēmas lietotāja datoriem vai serveriem, tikai pildot amata pienākumus vai pildot izpilddirektora rīkojumus.

35. Darbiniekiem ir aizliegts sūtīt tā sauktās "ķēdes vēstules" (t.sk. mēstules, reklāmas, aģitācijas un tml.)– elektroniskus ziņojumus ar lūgumu pārsūtīt tos citiem adresātiem, kā arī ir aizliegts atvērt un darbināt no Interneta tīkla saņemtus aizdomīgus failus. Informācijas sistēmas lietotājam ir jāatceras, ka Interneta tīkls nav drošs datu pārraides mēdijs un nosūtītāja identifikāciju var viegli viltot. Ja par failu rodas šaubas, Informācijas sistēmas lietotājam ir nepieciešams sazināties ar nosūtītāju un noskaidrot, vai šāds dokuments ir ticis nosūtīts.

V. Informācijas sistēmas lietotāja pieejas paroles uzbūve un lietošana

36. Pašvaldības informācijas resursu aizsardzība tiek nodrošināta ar datora paroli datortīkla (domēna) līmenī, kam ir jāatbilst vismaz sekojošām prasībām:

36.1. minimālam paroles garumam ir jābūt vismaz 8 simboli un tās maksimālais garums nedrīkst pārsniegt 16 simbolus.

36.2. maksimālais paroles maiņas periods nedrīkst būt ilgāks par 90 dienām, taču paroli aizliegts pašrocīgi mainīt biežāk nekā divas reizes 24 stundu laikā.

36.3. paroles uzbūvei jābūt komplicētai, izmantojot vismaz vienu lielo latīņu alfabēta burtu, mazo latīņu alfabēta burtu, ciparu un īpašo rakstzīmju kombināciju (kā piemēram, !@#$%^*()_+).

36.4. izveidojot paroli, tā nedrīkst sakrist ar nevienu no 5 iepriekšējām parolēm.

37. Informācijas sistēmas lietotājs nedrīkst izpaust savu paroli jebkurām citām trešajām personām vai citiem lietotājiem, izņemot atsevišķos gadījumos savas prombūtnes laikā, ja atļauju ir devis atbilstošās struktūrvienības vadītājs.

38. Informācijas sistēmas lietotājs nedrīkst savu paroli pierakstīt uz papīra, ja šo dokumentu neglabā seifā vai citā vietā ar ierobežotu citu personu piekļuvi.

39. Ja Informācijas sistēmas lietotājam rodas aizdomas, ka viņa paroli ir uzzinājusi jebkura cita persona, Informācijas sistēmas lietotājam ir pienākums pēc iespējas īsākā laikā šo paroli nomainīt patstāvīgi vai lūgt Datortīklu administratoru to izdarīt savā vietā.

40. Informācijas sistēmas lietotājs ir atbildīgs par informācijas aizsardzību un tā pienākums ir nodrošināt, ka datoriem Informācijas sistēmas lietotāja prombūtnes laikā ir ieslēgts ar paroli aizsargāts ekrānsaudzētājs vai noslēgta datora klaviatūra ar Ctrl-Alt-Del funkcijas palīdzību, izvēloties „Lock Computer" izvēlni.

41. Dienas beigās, beidzot darbu pie datora, tas jāizslēdz izmantojot procedūru: Start =>Shut Dowm =>Ok.

Pielikumā:

1. Krustpils novada pašvaldības Informācijas sistēmu tiesību pieprasījums uz 1 lp.

Domes priekšsēdētājs: K.Pabērzs

1. PIELIKUMS
"Krustpils novada pašvaldības
Informācijas sistēmas lietošanas noteikumi"

KRUSTPILS NOVADA PAŠVALDĪBAS
INFORMĀCIJAS RESURSU LIETOTĀJA REĢISTRĀCIJAS ANKETA

Vārds, Uzvārds	
Struktūrvienība	
Amats	
Telefona numurs	

Piešķirt pieeju sekojošiem informācijas resursiem (vajadzīgos atzīmēt ar). ☑

- ☐ **Dokumentu koplietošanas mape (failu serveris)**
- ☐ **E-pasts**
- ☐ **Grāmatvedības uzskaites sistēma**
- ☐ **Personu dzīvesvietas reģistrēšanas sistēma (PERS)**
- ☐ **Personu dzimtsarakstu reģistrācijas informatīvā sistēma (DZIMTS)**
- ☐ **Sociālās palīdzības administrēšanas sistēma (SOPA)**
- ☐ **Nekustamā īpašuma nodokļa administrēšanas sistēma (NINO)**
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____

_____

(Datums, paraksts)

LATVIJAS REPUBLIKA
KRUSTPILS NOVADA PAŠVALDĪBA
Reģ.Nr.90009118116
Rīgas ielā 150a, Jēkabpilī, LV-5202
Tālrunis 65237635, Fakss 65237611, e-pasts: novads@krustpils.lv

Jēkabpilī

15.03.2017.

APSTIPRINĀTI
ar Krustpils novada domes
15.03.2017. sēdes lēmumu
(protokols Nr.5.,17.p.)
Pielikums Nr.9.

Krustpils novada pašvaldība
Variešu pagasta pārvalde
Informācijas sistēmas lietošanas noteikumi

I.Vispārīgie jautājumi

1. Informācijas sistēmas lietošanas noteikumi nosaka Krustpils novada pašvaldība, Variešu pagasta pārvaldes (turpmāk – Pašvaldība) darbinieku pienākumus un prasības pašvaldības izmantotās informācijas sistēmas un interneta lietošanai, kā arī nosaka kārtību, kādā tiek veikta pašvaldības izmantotās informācijas sistēmas lietotāju pieejas tiesību piešķiršana, izmaiņas un anulēšana.

2. Noteikumos lietotie termini:
2.1. **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.
2.2. **Krustpils novada pašvaldība** – institūcija, kas normatīvajos aktos noteiktajā kārtībā organizē un vada informācijas sistēmu darbību.
2.3. **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.
2.4. **Informācijas sistēmas lietotājs –** persona, kurai ir piešķirtas piekļuves tiesības informācijas sistēmās.

3. Informācijas sistēmas lietošanas noteikumi ir saistoši visiem pašvaldības darbiniekiem (pilna darba laika, nepilnas slodzes un līgumdarbiniekiem), kuri ir nodarbināti pašvaldībā un kam ir piekļuve kādai no pašvaldības informācijas sistēmām.

4. Katra pašvaldības Informācijas sistēmas lietotāja pienākums ir iepazīties ar šiem noteikumiem un ievērot tos ikdienas darbā.

II. Informācijas sistēmas lietotāju administrēšanas kārtība

5. Pašvaldības katras pašvaldības iestādes un struktūrvienības vadītājs ir atbildīgs par sev un to padotībā esošo darbinieku lietotāju pieejas tiesību piešķiršanu, izmaiņu veikšanu un anulēšanu.

6. Lai izveidotu lietotāju pieejas tiesības vai veiktu izmaiņas tajās, Pašvaldības atbilstošās pašvaldības iestādes un struktūrvienības vadītājs raksta pieprasījumu (1.Pielikums), atzīmējot tajā nepieciešamo Informācijas resursu, ko iesniedz Informācijas sistēmas drošības pārvaldniekam.

7. Informācijas sistēmas lietotāju pieejas tiesības tiek piešķirtas Pašvaldības darbiniekiem atbilstoši katra atsevišķā darbinieka noteiktajiem darba pienākumiem un specifikai.

8. Informācijas sistēmas drošības pārvaldnieks izskata lietotāju pieejas tiesību piešķiršanas pieprasījumu un, ja uzskata to par pamatotu, Informācijas sistēmas drošības pārvaldnieks pieprasījumu izveidot atbilstošās informācijas sistēmas lietošanas tiesības nosūta Datortīklu administratoram.

9. Informācijas sistēmas lietotāju pieejas tiesību piešķiršana Pašvaldības informācijas resursiem personām, kuras nav Pašvaldības darbinieki, notiek tikai atsevišķos gadījumos pēc Sistēmas drošības pārvaldnieka pieprasījuma (piemēram, gadījumā ja ir noslēgts līgums starp pašvaldību un atbilstošo personu, kurā ir precīzi noteikti personas pienākumi, pieļaujamie informācijas izmantošanas mērķi, konfidencialitātes prasības un atbildība).

10. Informācijas sistēmas drošības pārvaldnieks ir atbildīgs par Lietotāju pieejas tiesību izveidošanu, administrēšanu un šo pieprasījumu apkopošanu, glabāšanu, kontroli un uzraudzību.

11. Piešķirtās lietotāju pieejas tiesības Pašvaldības informācijas resursiem ir nekavējoties jāanulē šādos gadījumos:

11.1. darbiniekiem, kuri pārtrauc darba (līguma) tiesiskās attiecības ar pašvaldību un / vai tās vairs nav nepieciešamas pienākumu veikšanai.

11.2. personām, kuras ir izpildījušas savstarpēji noslēgto līgumu ar pašvaldību vai šī līguma izbeigšanās (atcelšanas) gadījumā.

12. Iestājoties šo noteikumu 11.punktā minētajam gadījumam, atbilstošās struktūrvienības vadītājam, kura pakļautībā ir augstāk minētais darbinieks (vai koordinējošās struktūrvienības vadītājam gadījumos ar trešajām personām), ir pienākums informēt Datortīklu administratoru, kas veic atbilstošā lietotāja tiesību bloķēšanu.

13. Piešķirtās lietotāju pieejas tiesības var anulēt arī Informācijas sistēmas drošības pārvaldnieks vai Datortīklu administrators, balstoties uz atbilstošā lietotāja Informācijas sistēmas drošības politikas vai to saistošo dokumentu pārkāpumiem, par to rakstiski informējot Pašvaldības izpilddirektoru.

14. Datortīklu administratoram pēc Pašvaldības izpilddirektora vai Informācijas sistēmas drošības pārvaldnieka pieprasījuma, sagatavot Lietotāju pieejas tiesību sarakstu.

15. Datortīklu administratoram sadarbībā ar Informācijas sistēmas drošības pārvaldnieku ir pienākums vismaz reizi gadā veikt Lietotāju pieejas tiesību kontroli, pārbaudot un salīdzinot piešķirto lietotāju pieejas tiesību atbilstību darbinieka (personas, kuras darbojas uz līguma pamata) pienākumiem un specifikai.

III. Informācijas sistēmas lietotāju tiesības, pienākumi un atbildība

16. Informācijas sistēmas lietotājam ir tiesības izmantot viņam lietošanā nodotos datorus un to programmatūru, kā arī Informācijas sistēmas lietotājam ir tiesības pieprasīt atbalstu gadījumā, ja datoram vai tā programmatūrai ir radušies traucējumi.

17. Informācijas sistēmas lietotājs ir atbildīgs par datortehniku, kas nodota viņa rīcībā, kā arī atbild par darbībām, kas tiek veiktas ar viņam nodoto datortehniku.

18. Informācijas sistēmas lietotājs nedrīkst atļaut piekļūt tam nodotai datortehnikai citām personām, ja tas nav nepieciešams tiešo darba pienākumu pildīšanai un to pilnvarojumu nav devis Pašvaldības izpilddirektors, Informācijas sistēmas drošības pārvaldnieks vai Datortīklu administrators.

19. Informācijas sistēmas lietotāja pienākums ir apzināti nepieļaut datorvīrusu iekļūšanu iestādes datorsistēmās un neizmantot nezināmas izcelsmes datu nesējus. Rodoties aizdomām, ka dators ir inficēts ar datorvīrusu, par to nekavējoties jāinformē Informācijas sistēmas drošības pārvaldnieks vai Datortīklu administrators.

20. Informācijas sistēmas lietotājam ir pienākums jebkuru ienākošo elektronisko informāciju (failus) pirms lietošanas obligāti pārbaudīt ar antivīrusa programmatūru, ja tas netiek nodrošināts automātiski.

21. Nelicencētas programmatūras uzstādīšana un lietošana darba stacijās (lietotāja datoros) ir aizliegta. Patvaļīgi uzstādītas programmatūras lietošana, bez Pašvaldības izpilddirektora, Informācijas sistēmas drošības pārvaldnieka vai Datortīklu administratora atļaujas ir aizliegta.

22. Informācijas sistēmas lietotājs nedrīkst izpaust nepilnvarotām personām ziņas par Pašvaldības datoru tīkla uzbūvi un konfigurāciju.

23. Informācijas sistēmas lietotājs nedrīkst no sava darba datora kopēt failus uz ārējiem datu nesējiem (piemēram, CD, DVD, USB kartēm vai citiem datu nesējiem), ja to nevajag tiešo darba pienākumu pildīšanai vai ja tam pilnvarojumu nav devis Pašvaldības izpilddirektors, Informācijas sistēmas drošības pārvaldnieks vai Datortīklu administrators.

24. Ārējo datu nesēju, kurā ir iekopēta ierobežotas pieejamības informācija, no Pašvaldības telpām drīkst iznest tikai ar Pašvaldības izpilddirektora RAKSTISKU atļauju. Šajos gadījumos Informācijas sistēmas lietotājs, kurš no iestādes telpām iznes šādu datu nesēju, uzņemas pilnu atbildību par šo informāciju.

25. Informācijas sistēmas lietotājam ir aizliegts patvarīgi pārvietot, demontēt aparatūru, izjaukt, remontēt iekārtas vai veikt citas darbības, kas varētu traucēt informācijas un tehnisko resursu darbību.

26. Informācijas sistēmas lietotājam ir aizliegts veikt paroļu minēšanu, drošības ievainojamības pārbaudes, kodēto datu atkodēšanu, izmantot noklausīšanās programmas un veikt citas darbības, kas vērstas uz informācijas un tehnisko resursu drošības vājināšanu.

IV. Interneta un e-pasta lietošana

27. Pieeju Internetam darbiniekiem piešķir vienlaicīgi ar Informācijas sistēmas lietotāja pieejas tiesībām Pašvaldības datortīklam (domēnam), kas nepieciešams, lai nodrošinātu iestādes darbību un klientiem sniegtos pakalpojumus.

28. Informācijas sistēmas lietotājam darba vajadzībām ir jāizmanto tikai Pašvaldības piešķirtais e-pasts.

29. Informācijas sistēmas lietotājam ir aizliegts, izmantojot Pašvaldības piešķirto e-pastu, reģistrēties dažādos interneta resursos, kas tiek izmantoti privātām vajadzībām.

30. Informācijas sistēmas lietotājam ir aizliegts atvērt e-pasta pielikumus vai atvērt sūtījumā iekļautās Interneta adreses, kas saņemtas no nenoskaidrotiem sūtītājiem.

31. Lietojot Internetu, darbinieki pārstāv pašvaldību un tie ir atbildīgi, lai Internets tiktu izmantots darba vajadzībām ētiski un atbilstoši likumdošanas prasībām.

32. Darbiniekiem, izmantojot e-pastu, ir jānodrošina, ka visas komunikācijas tiek veiktas profesionālām vajadzībām un netraucē pašu darbinieku darba produktivitāti, kā arī netiek izplatīta vai sūtīta informācija, kas ir aizsargāta ar autortiesībām. Pašvaldība no darbinieka ir tiesīgs piedzīt zaudējumus, kas Pašvaldībai var būt radušies maksājot atlīdzību autortiesību īpašniekam par autortiesību pārkāpumu.

33. Darbinieki ir atbildīgi par visu nosūtīto tekstuālo, audio un vizuālo saturu. Datortīklu administrators bez saskaņošanas ar darbinieku patur sev tiesības pārlūkot darbinieku saņemto un nosūtīto e-pastu saturu, ja uzskata to par nepieciešamu.

34. Informācijas sistēmas drošības pārvaldniekam vai Datortīklu administratoram ir tiesības bloķēt atsevišķu interneta resursu izmantošanu, kā arī ir tiesības piekļūt Informācijas sistēmas lietotāja saglabātajai informācijai, kas atrodas uz Informācijas sistēmas lietotāja datoriem vai serveriem, tikai pildot amata pienākumus vai pildot izpilddirektora rīkojumus.

35. Darbiniekiem ir aizliegts sūtīt tā sauktās "ķēdes vēstules" (t.sk. mēstules, reklāmas, aģitācijas un tml.)– elektroniskus ziņojumus ar lūgumu pārsūtīt tos citiem adresātiem, kā arī ir aizliegts atvērt un darbināt no Interneta tīkla saņemtus aizdomīgus failus. Informācijas sistēmas lietotājam ir jāatceras, ka Interneta tīkls nav drošs datu pārraides mēdijs un nosūtītāja identifikāciju var viegli viltot. Ja par failu rodas šaubas, Informācijas sistēmas lietotājam ir nepieciešams sazināties ar nosūtītāju un noskaidrot, vai šāds dokuments ir ticis nosūtīts.

V. Informācijas sistēmas lietotāja pieejas paroles uzbūve un lietošana

36. Pašvaldības informācijas resursu aizsardzība tiek nodrošināta ar datora paroli datortīkla (domēna) līmenī, kam ir jāatbilst vismaz sekojošām prasībām:

36.1. minimālam paroles garumam ir jābūt vismaz 8 simboli un tās maksimālais garums nedrīkst pārsniegt 16 simbolus.

36.2. maksimālais paroles maiņas periods nedrīkst būt ilgāks par 90 dienām, taču paroli aizliegts pašrocīgi mainīt biežāk nekā divas reizes 24 stundu laikā.

36.3. paroles uzbūvei jābūt komplicētai, izmantojot vismaz vienu lielo latīņu alfabēta burtu, mazo latīņu alfabēta burtu, ciparu un īpašo rakstzīmju kombināciju (kā piemēram, !@#$%^*()_+).

36.4. izveidojot paroli, tā nedrīkst sakrist ar nevienu no 5 iepriekšējām parolēm.

37. Informācijas sistēmas lietotājs nedrīkst izpaust savu paroli jebkurām citām trešajām personām vai citiem lietotājiem, izņemot atsevišķos gadījumos savas prombūtnes laikā, ja atļauju ir devis atbilstošās struktūrvienības vadītājs.

38. Informācijas sistēmas lietotājs nedrīkst savu paroli pierakstīt uz papīra, ja šo dokumentu neglabā seifā vai citā vietā ar ierobežotu citu personu piekļuvi.

39. Ja Informācijas sistēmas lietotājam rodas aizdomas, ka viņa paroli ir uzzinājusi jebkura cita persona, Informācijas sistēmas lietotājam ir pienākums pēc iespējas īsākā laikā šo paroli nomainīt patstāvīgi vai lūgt Datortīklu administratoru to izdarīt savā vietā.

40. Informācijas sistēmas lietotājs ir atbildīgs par informācijas aizsardzību un tā pienākums ir nodrošināt, ka datoriem Informācijas sistēmas lietotāja prombūtnes laikā ir ieslēgts ar paroli aizsargāts ekrānsaudzētājs vai noslēgta datora klaviatūra ar Ctrl-Alt-Del funkcijas palīdzību, izvēloties „Lock Computer" izvēlni.

41. Dienas beigās, beidzot darbu pie datora, tas jāizslēdz izmantojot procedūru: Start =>Shut Dowm =>Ok.

Pielikumā:

1. Krustpils novada pašvaldības Informācijas sistēmu tiesību pieprasījums uz 1 lp.

Domes priekšsēdētājs K.Pabērzs

1. PIELIKUMS
"Krustpils novada pašvaldības
Informācijas sistēmas lietošanas noteikumi"

KRUSTPILS NOVADA PAŠVALDĪBAS
INFORMĀCIJAS RESURSU LIETOTĀJA REĢISTRĀCIJAS ANKETA

Vārds, Uzvārds	
Struktūrvienība	
Amats	
Telefona numurs	

Piešķirt pieeju sekojošiem informācijas resursiem (vajadzīgos atzīmēt ar ☑).

- ☐ **Dokumentu koplietošanas mape (failu serveris)**
- ☐ **E-pasts**
- ☐ **Grāmatvedības uzskaites sistēma**
- ☐ **Personu dzīvesvietas reģistrēšanas sistēma (PERS)**
- ☐ **Personu dzimtsarakstu reģistrācijas informatīvā sistēma (DZIMTS)**
- ☐ **Sociālās palīdzības administrēšanas sistēma (SOPA)**
- ☐ **Nekustamā īpašuma nodokļa administrēšanas sistēma (NINO)**
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____

_____

(Datums, paraksts)

LATVIJAS REPUBLIKA
KRUSTPILS NOVADA PAŠVALDĪBA
Reģ.Nr.90009118116
Rīgas ielā 150a, Jēkabpilī, LV-5202
Tālrunis 65237635, Fakss 65237611, e-pasts: novads@krustpils.lv

Jēkabpilī

15.03.2017.

APSTIPRINĀTI
ar Krustpils novada domes
15.03.2017. sēdes lēmumu
(protokols Nr.5.,17.p.)
Pielikums Nr.10.

Krustpils novada pašvaldība Vīpes pagasta pārvalde Informācijas sistēmas lietošanas noteikumi

I.Vispārīgie jautājumi

1. Informācijas sistēmas lietošanas noteikumi nosaka Krustpils novada pašvaldība, Vīpes pagasta pārvaldes (turpmāk – Pašvaldība) darbinieku pienākumus un prasības pašvaldības izmantotās informācijas sistēmas un interneta lietošanai, kā arī nosaka kārtību, kādā tiek veikta pašvaldības izmantotās informācijas sistēmas lietotāju pieejas tiesību piešķiršana, izmaiņas un anulēšana.

2. Noteikumos lietotie termini:

2.1. **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.

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

2.3. **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.

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

3. Informācijas sistēmas lietošanas noteikumi ir saistoši visiem pašvaldības darbiniekiem (pilna darba laika, nepilnas slodzes un līgumdarbiniekiem), kuri ir nodarbināti pašvaldībā un kam ir piekļuve kādai no pašvaldības informācijas sistēmām.

4. Katra pašvaldības Informācijas sistēmas lietotāja pienākums ir iepazīties ar šiem noteikumiem un ievērot tos ikdienas darbā.

II. Informācijas sistēmas lietotāju administrēšanas kārtība

5. Pašvaldības katras pašvaldības iestādes un struktūrvienības vadītājs ir atbildīgs par sev un to padotībā esošo darbinieku lietotāju pieejas tiesību piešķiršanu, izmaiņu veikšanu un anulēšanu.

6. Lai izveidotu lietotāju pieejas tiesības vai veiktu izmaiņas tajās, Pašvaldības atbilstošās pašvaldības iestādes un struktūrvienības vadītājs raksta pieprasījumu (1.Pielikums), atzīmējot tajā nepieciešamo Informācijas resursu, ko iesniedz Informācijas sistēmas drošības pārvaldniekam.

7. Informācijas sistēmas lietotāju pieejas tiesības tiek piešķirtas Pašvaldības darbiniekiem atbilstoši katra atsevišķā darbinieka noteiktajiem darba pienākumiem un specifikai.

8. Informācijas sistēmas drošības pārvaldnieks izskata lietotāju pieejas tiesību piešķiršanas pieprasījumu un, ja uzskata to par pamatotu, Informācijas sistēmas drošības pārvaldnieks pieprasījumu izveidot atbilstošās informācijas sistēmas lietošanas tiesības nosūta Datortīklu administratoram.

9. Informācijas sistēmas lietotāju pieejas tiesību piešķiršana Pašvaldības informācijas resursiem personām, kuras nav Pašvaldības darbinieki, notiek tikai atsevišķos gadījumos pēc Sistēmas drošības pārvaldnieka pieprasījuma (piemēram, gadījumā ja ir noslēgts līgums starp pašvaldību un atbilstošo personu, kurā ir precīzi noteikti personas pienākumi, pieļaujamie informācijas izmantošanas mērķi, konfidencialitātes prasības un atbildība).

10. Informācijas sistēmas drošības pārvaldnieks ir atbildīgs par Lietotāju pieejas tiesību izveidošanu, administrēšanu un šo pieprasījumu apkopošanu, glabāšanu, kontroli un uzraudzību.

11. Piešķirtās lietotāju pieejas tiesības Pašvaldības informācijas resursiem ir nekavējoties jāanulē šādos gadījumos:

11.1. darbiniekiem, kuri pārtrauc darba (līguma) tiesiskās attiecības ar pašvaldību un / vai tās vairs nav nepieciešamas pienākumu veikšanai.

11.2. personām, kuras ir izpildījušas savstarpēji noslēgto līgumu ar pašvaldību vai šī līguma izbeigšanās (atcelšanas) gadījumā.

12. Iestājoties šo noteikumu 11.punktā minētajam gadījumam, atbilstošās struktūrvienības vadītājam, kura pakļautībā ir augstāk minētais darbinieks (vai koordinējošās struktūrvienības vadītājam gadījumos ar trešajām personām), ir pienākums informēt Datortīklu administratoru, kas veic atbilstošā lietotāja tiesību bloķēšanu.

13. Piešķirtās lietotāju pieejas tiesības var anulēt arī Informācijas sistēmas drošības pārvaldnieks vai Datortīklu administrators, balstoties uz atbilstošā lietotāja Informācijas sistēmas drošības politikas vai to saistošo dokumentu pārkāpumiem, par to rakstiski informējot Pašvaldības izpilddirektoru.

14. Datortīklu administratoram pēc Pašvaldības izpilddirektora vai Informācijas sistēmas drošības pārvaldnieka pieprasījuma, sagatavot Lietotāju pieejas tiesību sarakstu.

15. Datortīklu administratoram sadarbībā ar Informācijas sistēmas drošības pārvaldnieku ir pienākums vismaz reizi gadā veikt Lietotāju pieejas tiesību kontroli, pārbaudot un salīdzinot piešķirto lietotāju pieejas tiesību atbilstību darbinieka (personas, kuras darbojas uz līguma pamata) pienākumiem un specifikai.

III. Informācijas sistēmas lietotāju tiesības, pienākumi un atbildība

16. Informācijas sistēmas lietotājam ir tiesības izmantot viņam lietošanā nodotos datorus un to programmatūru, kā arī Informācijas sistēmas lietotājam ir tiesības pieprasīt atbalstu gadījumā, ja datoram vai tā programmatūrai ir radušies traucējumi.

17. Informācijas sistēmas lietotājs ir atbildīgs par datortehniku, kas nodota viņa rīcībā, kā arī atbild par darbībām, kas tiek veiktas ar viņam nodoto datortehniku.

18. Informācijas sistēmas lietotājs nedrīkst atļaut piekļūt tam nodotai datortehnikai citām personām, ja tas nav nepieciešams tiešo darba pienākumu pildīšanai un to pilnvarojumu nav devis Pašvaldības izpilddirektors, Informācijas sistēmas drošības pārvaldnieks vai Datortīklu administrators.

19. Informācijas sistēmas lietotāja pienākums ir apzināti nepieļaut datorvīrusu iekļūšanu iestādes datorsistēmās un neizmantot nezināmas izcelsmes datu nesējus. Rodoties aizdomām, ka dators ir inficēts ar datorvīrusu, par to nekavējoties jāinformē Informācijas sistēmas drošības pārvaldnieks vai Datortīklu administrators.

20. Informācijas sistēmas lietotājam ir pienākums jebkuru ienākošo elektronisko informāciju (failus) pirms lietošanas obligāti pārbaudīt ar antivīrusa programmatūru, ja tas netiek nodrošināts automātiski.

21. Nelicencētas programmatūras uzstādīšana un lietošana darba stacijās (lietotāja datoros) ir aizliegta. Patvaļīgi uzstādītas programmatūras lietošana, bez Pašvaldības izpilddirektora, Informācijas sistēmas drošības pārvaldnieka vai Datortīklu administratora atļaujas ir aizliegta.

22. Informācijas sistēmas lietotājs nedrīkst izpaust nepilnvarotām personām ziņas par Pašvaldības datoru tīkla uzbūvi un konfigurāciju.

23. Informācijas sistēmas lietotājs nedrīkst no sava darba datora kopēt failus uz ārējiem datu nesējiem (piemēram, CD, DVD, USB kartēm vai citiem datu nesējiem), ja to nevajag tiešo darba pienākumu pildīšanai vai ja tam pilnvarojumu nav devis Pašvaldības izpilddirektors, Informācijas sistēmas drošības pārvaldnieks vai Datortīklu administrators.

24. Ārējo datu nesēju, kurā ir iekopēta ierobežotas pieejamības informācija, no Pašvaldības telpām drīkst iznest tikai ar Pašvaldības izpilddirektora RAKSTISKU atļauju. Šajos gadījumos Informācijas sistēmas lietotājs, kurš no iestādes telpām iznes šādu datu nesēju, uzņemas pilnu atbildību par šo informāciju.

25. Informācijas sistēmas lietotājam ir aizliegts patvarīgi pārvietot, demontēt aparatūru, izjaukt, remontēt iekārtas vai veikt citas darbības, kas varētu traucēt informācijas un tehnisko resursu darbību.

26. Informācijas sistēmas lietotājam ir aizliegts veikt paroļu minēšanu, drošības ievainojamības pārbaudes, kodēto datu atkodēšanu, izmantot noklausīšanās programmas un veikt citas darbības, kas vērstas uz informācijas un tehnisko resursu drošības vājināšanu.

IV. Interneta un e-pasta lietošana

27. Pieeju Internetam darbiniekiem piešķir vienlaicīgi ar Informācijas sistēmas lietotāja pieejas tiesībām Pašvaldības datortīklam (domēnam), kas nepieciešams, lai nodrošinātu iestādes darbību un klientiem sniegtos pakalpojumus.

28. Informācijas sistēmas lietotājam darba vajadzībām ir jāizmanto tikai Pašvaldības piešķirtais e-pasts.

29. Informācijas sistēmas lietotājam ir aizliegts, izmantojot Pašvaldības piešķirto e-pastu, reģistrēties dažādos interneta resursos, kas tiek izmantoti privātām vajadzībām.

30. Informācijas sistēmas lietotājam ir aizliegts atvērt e-pasta pielikumus vai atvērt sūtījumā iekļautās Interneta adreses, kas saņemtas no nenoskaidrotiem sūtītājiem.

31. Lietojot Internetu, darbinieki pārstāv pašvaldību un tie ir atbildīgi, lai Internets tiktu izmantots darba vajadzībām ētiski un atbilstoši likumdošanas prasībām.

32. Darbiniekiem, izmantojot e-pastu, ir jānodrošina, ka visas komunikācijas tiek veiktas profesionālām vajadzībām un netraucē pašu darbinieku darba produktivitāti, kā arī netiek izplatīta vai sūtīta informācija, kas ir aizsargāta ar autortiesībām. Pašvaldība no darbinieka ir tiesīgs piedzīt zaudējumus, kas Pašvaldībai var būt radušies maksājot atlīdzību autortiesību īpašniekam par autortiesību pārkāpumu.

33. Darbinieki ir atbildīgi par visu nosūtīto tekstuālo, audio un vizuālo saturu. Datortīklu administrators bez saskaņošanas ar darbinieku patur sev tiesības pārlūkot darbinieku saņemto un nosūtīto e-pastu saturu, ja uzskata to par nepieciešamu.

34. Informācijas sistēmas drošības pārvaldniekam vai Datortīklu administratoram ir tiesības bloķēt atsevišķu interneta resursu izmantošanu, kā arī ir tiesības piekļūt Informācijas sistēmas lietotāja saglabātajai informācijai, kas atrodas uz Informācijas sistēmas lietotāja datoriem vai serveriem, tikai pildot amata pienākumus vai pildot izpilddirektora rīkojumus.

35. Darbiniekiem ir aizliegts sūtīt tā sauktās "ķēdes vēstules" (t.sk. mēstules, reklāmas, aģitācijas un tml.)– elektroniskus ziņojumus ar lūgumu pārsūtīt tos citiem adresātiem, kā arī ir aizliegts atvērt un darbināt no Interneta tīkla saņemtus aizdomīgus failus. Informācijas sistēmas lietotājam ir jāatceras, ka Interneta tīkls nav drošs datu pārraides mēdijs un nosūtītāja identifikāciju var viegli viltot. Ja par failu rodas šaubas, Informācijas sistēmas lietotājam ir nepieciešams sazināties ar nosūtītāju un noskaidrot, vai šāds dokuments ir ticis nosūtīts.

V. Informācijas sistēmas lietotāja pieejas paroles uzbūve un lietošana

36. Pašvaldības informācijas resursu aizsardzība tiek nodrošināta ar datora paroli datortīkla (domēna) līmenī, kam ir jāatbilst vismaz sekojošām prasībām:

36.1. minimālam paroles garumam ir jābūt vismaz 8 simboli un tās maksimālais garums nedrīkst pārsniegt 16 simbolus.

36.2. maksimālais paroles maiņas periods nedrīkst būt ilgāks par 90 dienām, taču paroli aizliegts pašrocīgi mainīt biežāk nekā divas reizes 24 stundu laikā.

36.3. paroles uzbūvei jābūt komplicētai, izmantojot vismaz vienu lielo latīņu alfabēta burtu, mazo latīņu alfabēta burtu, ciparu un īpašo rakstzīmju kombināciju (kā piemēram, !@#$%^*()_+).

36.4. izveidojot paroli, tā nedrīkst sakrist ar nevienu no 5 iepriekšējām parolēm.

37. Informācijas sistēmas lietotājs nedrīkst izpaust savu paroli jebkurām citām trešajām personām vai citiem lietotājiem, izņemot atsevišķos gadījumos savas prombūtnes laikā, ja atļauju ir devis atbilstošās struktūrvienības vadītājs.

38. Informācijas sistēmas lietotājs nedrīkst savu paroli pierakstīt uz papīra, ja šo dokumentu neglabā seifā vai citā vietā ar ierobežotu citu personu piekļuvi.

39. Ja Informācijas sistēmas lietotājam rodas aizdomas, ka viņa paroli ir uzzinājusi jebkura cita persona, Informācijas sistēmas lietotājam ir pienākums pēc iespējas īsākā laikā šo paroli nomainīt patstāvīgi vai lūgt Datortīklu administratoru to izdarīt savā vietā.

40. Informācijas sistēmas lietotājs ir atbildīgs par informācijas aizsardzību un tā pienākums ir nodrošināt, ka datoriem Informācijas sistēmas lietotāja prombūtnes laikā ir ieslēgts ar paroli aizsargāts ekrānsaudzētājs vai noslēgta datora klaviatūra ar Ctrl-Alt-Del funkcijas palīdzību, izvēloties „Lock Computer" izvēlni.

41. Dienas beigās, beidzot darbu pie datora, tas jāizslēdz izmantojot procedūru: Start =>Shut Dowm =>Ok.

Pielikumā:

1. Krustpils novada pašvaldības Informācijas sistēmu tiesību pieprasījums uz 1 lp.

Domes priekšsēdētājs K.Pabērzs

1. PIELIKUMS
"Krustpils novada pašvaldības
Informācijas sistēmas lietošanas noteikumi"

KRUSTPILS NOVADA PAŠVALDĪBAS
INFORMĀCIJAS RESURSU LIETOTĀJA REĢISTRĀCIJAS ANKETA

Vārds, Uzvārds	
Struktūrvienība	
Amats	
Telefona numurs	

Piešķirt pieeju sekojošiem informācijas resursiem (vajadzīgos atzīmēt ar ☑).

- ☐ **Dokumentu koplietošanas mape (failu serveris)**
- ☐ **E-pasts**
- ☐ **Grāmatvedības uzskaites sistēma**
- ☐ **Personu dzīvesvietas reģistrēšanas sistēma (PERS)**
- ☐ **Personu dzimtsarakstu reģistrācijas informatīvā sistēma (DZIMTS)**
- ☐ **Sociālās palīdzības administrēšanas sistēma (SOPA)**
- ☐ **Nekustamā īpašuma nodokļa administrēšanas sistēma (NINO)**
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____

_____

(Datums, paraksts)

LATVIJAS REPUBLIKA
KRUSTPILS NOVADA PAŠVALDĪBA
Reģ.Nr.90009118116
Rīgas ielā 150a, Jēkabpilī, LV-5202
Tālrunis 65237635, Fakss 65237611, e-pasts: novads@krustpils.lv

Jēkabpilī

15.03.2017.

APSTIPRINĀTI
ar Krustpils novada domes
15.03.2017. sēdes lēmumu
(protokols Nr.5.,17.p.)
Pielikums Nr.11.

Krustpils novada pašvaldība Atašienes pagasta pārvalde Informācijas sistēmas lietošanas noteikumi

I.Vispārīgie jautājumi

1. Informācijas sistēmas lietošanas noteikumi nosaka Krustpils novada pašvaldība, Atašienes pagasta pārvaldes (turpmāk – Pašvaldība) darbinieku pienākumus un prasības pašvaldības izmantotās informācijas sistēmas un interneta lietošanai, kā arī nosaka kārtību, kādā tiek veikta pašvaldības izmantotās informācijas sistēmas lietotāju pieejas tiesību piešķiršana, izmaiņas un anulēšana.

2. Noteikumos lietotie termini:

2.1. **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.

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

2.3. **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.

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

3. Informācijas sistēmas lietošanas noteikumi ir saistoši visiem pašvaldības darbiniekiem (pilna darba laika, nepilnas slodzes un līgumdarbiniekiem), kuri ir nodarbināti pašvaldībā un kam ir piekļuve kādai no pašvaldības informācijas sistēmām.

4. Katra pašvaldības Informācijas sistēmas lietotāja pienākums ir iepazīties ar šiem noteikumiem un ievērot tos ikdienas darbā.

II. Informācijas sistēmas lietotāju administrēšanas kārtība

5. Pašvaldības katras pašvaldības iestādes un struktūrvienības vadītājs ir atbildīgs par sev un to padotībā esošo darbinieku lietotāju pieejas tiesību piešķiršanu, izmaiņu veikšanu un anulēšanu.

6. Lai izveidotu lietotāju pieejas tiesības vai veiktu izmaiņas tajās, Pašvaldības atbilstošās pašvaldības iestādes un struktūrvienības vadītājs raksta pieprasījumu (1.Pielikums), atzīmējot tajā nepieciešamo Informācijas resursu, ko iesniedz Informācijas sistēmas drošības pārvaldniekam.

7. Informācijas sistēmas lietotāju pieejas tiesības tiek piešķirtas Pašvaldības darbiniekiem atbilstoši katra atsevišķā darbinieka noteiktajiem darba pienākumiem un specifikai.

8. Informācijas sistēmas drošības pārvaldnieks izskata lietotāju pieejas tiesību piešķiršanas pieprasījumu un, ja uzskata to par pamatotu, Informācijas sistēmas drošības pārvaldnieks pieprasījumu izveidot atbilstošās informācijas sistēmas lietošanas tiesības nosūta Datortīklu administratoram.

9. Informācijas sistēmas lietotāju pieejas tiesību piešķiršana Pašvaldības informācijas resursiem personām, kuras nav Pašvaldības darbinieki, notiek tikai atsevišķos gadījumos pēc Sistēmas drošības pārvaldnieka pieprasījuma (piemēram, gadījumā ja ir noslēgts līgums starp pašvaldību un atbilstošo personu, kurā ir precīzi noteikti personas pienākumi, pieļaujamie informācijas izmantošanas mērķi, konfidencialitātes prasības un atbildība).

10. Informācijas sistēmas drošības pārvaldnieks ir atbildīgs par Lietotāju pieejas tiesību izveidošanu, administrēšanu un šo pieprasījumu apkopošanu, glabāšanu, kontroli un uzraudzību.

11. Piešķirtās lietotāju pieejas tiesības Pašvaldības informācijas resursiem ir nekavējoties jāanulē šādos gadījumos:

11.1. darbiniekiem, kuri pārtrauc darba (līguma) tiesiskās attiecības ar pašvaldību un / vai tās vairs nav nepieciešamas pienākumu veikšanai.

11.2. personām, kuras ir izpildījušas savstarpēji noslēgto līgumu ar pašvaldību vai šī līguma izbeigšanās (atcelšanas) gadījumā.

12. Iestājoties šo noteikumu 11.punktā minētajam gadījumam, atbilstošās struktūrvienības vadītājam, kura pakļautībā ir augstāk minētais darbinieks (vai koordinējošās struktūrvienības vadītājam gadījumos ar trešajām personām), ir pienākums informēt Datortīklu administratoru, kas veic atbilstošā lietotāja tiesību bloķēšanu.

13. Piešķirtās lietotāju pieejas tiesības var anulēt arī Informācijas sistēmas drošības pārvaldnieks vai Datortīklu administrators, balstoties uz atbilstošā lietotāja Informācijas sistēmas drošības politikas vai to saistošo dokumentu pārkāpumiem, par to rakstiski informējot Pašvaldības izpilddirektoru.

14. Datortīklu administratoram pēc Pašvaldības izpilddirektora vai Informācijas sistēmas drošības pārvaldnieka pieprasījuma, sagatavot Lietotāju pieejas tiesību sarakstu.

15. Datortīklu administratoram sadarbībā ar Informācijas sistēmas drošības pārvaldnieku ir pienākums vismaz reizi gadā veikt Lietotāju pieejas tiesību kontroli, pārbaudot un salīdzinot piešķirto lietotāju pieejas tiesību atbilstību darbinieka (personas, kuras darbojas uz līguma pamata) pienākumiem un specifikai.

III. Informācijas sistēmas lietotāju tiesības, pienākumi un atbildība

16. Informācijas sistēmas lietotājam ir tiesības izmantot viņam lietošanā nodotos datorus un to programmatūru, kā arī Informācijas sistēmas lietotājam ir tiesības pieprasīt atbalstu gadījumā, ja datoram vai tā programmatūrai ir radušies traucējumi.

17. Informācijas sistēmas lietotājs ir atbildīgs par datortehniku, kas nodota viņa rīcībā, kā arī atbild par darbībām, kas tiek veiktas ar viņam nodoto datortehniku.

18. Informācijas sistēmas lietotājs nedrīkst atļaut piekļūt tam nodotai datortehnikai citām personām, ja tas nav nepieciešams tiešo darba pienākumu pildīšanai un to pilnvarojumu nav devis Pašvaldības izpilddirektors, Informācijas sistēmas drošības pārvaldnieks vai Datortīklu administrators.

19. Informācijas sistēmas lietotāja pienākums ir apzināti nepieļaut datorvīrusu iekļūšanu iestādes datorsistēmās un neizmantot nezināmas izcelsmes datu nesējus. Rodoties aizdomām, ka dators ir inficēts ar datorvīrusu, par to nekavējoties jāinformē Informācijas sistēmas drošības pārvaldnieks vai Datortīklu administrators.

20. Informācijas sistēmas lietotājam ir pienākums jebkuru ienākošo elektronisko informāciju (failus) pirms lietošanas obligāti pārbaudīt ar antivīrusa programmatūru, ja tas netiek nodrošināts automātiski.

21. Nelicencētas programmatūras uzstādīšana un lietošana darba stacijās (lietotāja datoros) ir aizliegta. Patvaļīgi uzstādītas programmatūras lietošana, bez Pašvaldības izpilddirektora, Informācijas sistēmas drošības pārvaldnieka vai Datortīklu administratora atļaujas ir aizliegta.

22. Informācijas sistēmas lietotājs nedrīkst izpaust nepilnvarotām personām ziņas par Pašvaldības datoru tīkla uzbūvi un konfigurāciju.

23. Informācijas sistēmas lietotājs nedrīkst no sava darba datora kopēt failus uz ārējiem datu nesējiem (piemēram, CD, DVD, USB kartēm vai citiem datu nesējiem), ja to nevajag tiešo darba pienākumu pildīšanai vai ja tam pilnvarojumu nav devis Pašvaldības izpilddirektors, Informācijas sistēmas drošības pārvaldnieks vai Datortīklu administrators.

24. Ārējo datu nesēju, kurā ir iekopēta ierobežotas pieejamības informācija, no Pašvaldības telpām drīkst iznest tikai ar Pašvaldības izpilddirektora RAKSTISKU atļauju. Šajos gadījumos Informācijas sistēmas lietotājs, kurš no iestādes telpām iznes šādu datu nesēju, uzņemas pilnu atbildību par šo informāciju.

25. Informācijas sistēmas lietotājam ir aizliegts patvarīgi pārvietot, demontēt aparatūru, izjaukt, remontēt iekārtas vai veikt citas darbības, kas varētu traucēt informācijas un tehnisko resursu darbību.

26. Informācijas sistēmas lietotājam ir aizliegts veikt paroļu minēšanu, drošības ievainojamības pārbaudes, kodēto datu atkodēšanu, izmantot noklausīšanās programmas un veikt citas darbības, kas vērstas uz informācijas un tehnisko resursu drošības vājināšanu.

IV. Interneta un e-pasta lietošana

27. Pieeju Internetam darbiniekiem piešķir vienlaicīgi ar Informācijas sistēmas lietotāja pieejas tiesībām Pašvaldības datortīklam (domēnam), kas nepieciešams, lai nodrošinātu iestādes darbību un klientiem sniegtos pakalpojumus.

28. Informācijas sistēmas lietotājam darba vajadzībām ir jāizmanto tikai Pašvaldības piešķirtais e-pasts.

29. Informācijas sistēmas lietotājam ir aizliegts, izmantojot Pašvaldības piešķirto e-pastu, reģistrēties dažādos interneta resursos, kas tiek izmantoti privātām vajadzībām.

30. Informācijas sistēmas lietotājam ir aizliegts atvērt e-pasta pielikumus vai atvērt sūtījumā iekļautās Interneta adreses, kas saņemtas no nenoskaidrotiem sūtītājiem.

31. Lietojot Internetu, darbinieki pārstāv pašvaldību un tie ir atbildīgi, lai Internets tiktu izmantots darba vajadzībām ētiski un atbilstoši likumdošanas prasībām.

32. Darbiniekiem, izmantojot e-pastu, ir jānodrošina, ka visas komunikācijas tiek veiktas profesionālām vajadzībām un netraucē pašu darbinieku darba produktivitāti, kā arī netiek izplatīta vai sūtīta informācija, kas ir aizsargāta ar autortiesībām. Pašvaldība no darbinieka ir tiesīgs piedzīt zaudējumus, kas Pašvaldībai var būt radušies maksājot atlīdzību autortiesību īpašniekam par autortiesību pārkāpumu.

33. Darbinieki ir atbildīgi par visu nosūtīto tekstuālo, audio un vizuālo saturu. Datortīklu administrators bez saskaņošanas ar darbinieku patur sev tiesības pārlūkot darbinieku saņemto un nosūtīto e-pastu saturu, ja uzskata to par nepieciešamu.

34. Informācijas sistēmas drošības pārvaldniekam vai Datortīklu administratoram ir tiesības bloķēt atsevišķu interneta resursu izmantošanu, kā arī ir tiesības piekļūt Informācijas sistēmas lietotāja saglabātajai informācijai, kas atrodas uz Informācijas sistēmas lietotāja datoriem vai serveriem, tikai pildot amata pienākumus vai pildot izpilddirektora rīkojumus.

35. Darbiniekiem ir aizliegts sūtīt tā sauktās "ķēdes vēstules" (t.sk. mēstules, reklāmas, aģitācijas un tml.)– elektroniskus ziņojumus ar lūgumu pārsūtīt tos citiem adresātiem, kā arī ir aizliegts atvērt un darbināt no Interneta tīkla saņemtus aizdomīgus failus. Informācijas sistēmas lietotājam ir jāatceras, ka Interneta tīkls nav drošs datu pārraides mēdijs un nosūtītāja identifikāciju var viegli viltot. Ja par failu rodas šaubas, Informācijas sistēmas lietotājam ir nepieciešams sazināties ar nosūtītāju un noskaidrot, vai šāds dokuments ir ticis nosūtīts.

V. Informācijas sistēmas lietotāja pieejas paroles uzbūve un lietošana

36. Pašvaldības informācijas resursu aizsardzība tiek nodrošināta ar datora paroli datortīkla (domēna) līmenī, kam ir jāatbilst vismaz sekojošām prasībām:

36.1. minimālam paroles garumam ir jābūt vismaz 8 simboli un tās maksimālais garums nedrīkst pārsniegt 16 simbolus.

36.2. maksimālais paroles maiņas periods nedrīkst būt ilgāks par 90 dienām, taču paroli aizliegts pašrocīgi mainīt biežāk nekā divas reizes 24 stundu laikā.

36.3. paroles uzbūvei jābūt komplicētai, izmantojot vismaz vienu lielo latīņu alfabēta burtu, mazo latīņu alfabēta burtu, ciparu un īpašo rakstzīmju kombināciju (kā piemēram, !@#$%^*()_+).

36.4. izveidojot paroli, tā nedrīkst sakrist ar nevienu no 5 iepriekšējām parolēm.

37. Informācijas sistēmas lietotājs nedrīkst izpaust savu paroli jebkurām citām trešajām personām vai citiem lietotājiem, izņemot atsevišķos gadījumos savas prombūtnes laikā, ja atļauju ir devis atbilstošās struktūrvienības vadītājs.

38. Informācijas sistēmas lietotājs nedrīkst savu paroli pierakstīt uz papīra, ja šo dokumentu neglabā seifā vai citā vietā ar ierobežotu citu personu piekļuvi.

39. Ja Informācijas sistēmas lietotājam rodas aizdomas, ka viņa paroli ir uzzinājusi jebkura cita persona, Informācijas sistēmas lietotājam ir pienākums pēc iespējas īsākā laikā šo paroli nomainīt patstāvīgi vai lūgt Datortīklu administratoru to izdarīt savā vietā.

40. Informācijas sistēmas lietotājs ir atbildīgs par informācijas aizsardzību un tā pienākums ir nodrošināt, ka datoriem Informācijas sistēmas lietotāja prombūtnes laikā ir ieslēgts ar paroli aizsargāts ekrānsaudzētājs vai noslēgta datora klaviatūra ar Ctrl-Alt-Del funkcijas palīdzību, izvēloties „Lock Computer" izvēlni.

41. Dienas beigās, beidzot darbu pie datora, tas jāizslēdz izmantojot procedūru: Start =>Shut Dowm =>Ok.

Pielikumā:

1. Krustpils novada pašvaldības Informācijas sistēmu tiesību pieprasījums uz 1 lp.

Domes priekšsēdētājs K.Pabērzs

1. PIELIKUMS
"Krustpils novada pašvaldības
Informācijas sistēmas lietošanas noteikumi"

KRUSTPILS NOVADA PAŠVALDĪBAS
INFORMĀCIJAS RESURSU LIETOTĀJA REĢISTRĀCIJAS ANKETA

Vārds, Uzvārds	
Struktūrvienība	
Amats	
Telefona numurs	

Piešķirt pieeju sekojošiem informācijas resursiem (vajadzīgos atzīmēt ar). ☑

- ☐ **Dokumentu koplietošanas mape (failu serveris)**
- ☐ **E-pasts**
- ☐ **Grāmatvedības uzskaites sistēma**
- ☐ **Personu dzīvesvietas reģistrēšanas sistēma (PERS)**
- ☐ **Personu dzimtsarakstu reģistrācijas informatīvā sistēma (DZIMTS)**
- ☐ **Sociālās palīdzības administrēšanas sistēma (SOPA)**
- ☐ **Nekustamā īpašuma nodokļa administrēšanas sistēma (NINO)**
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____

_____

(Datums, paraksts)