SMILTENES NOVADA PAŠVALDĪBA
Reģ. Nr. 90009067337, Dārza iela 3, Smiltene, Smiltenes novads, LV-4729
tālr. 64774844, e-pasts pasts@smiltenesnovads.lv

NOTEIKUMI
Smiltenē

2026.gada 28. maijā Nr. 8/26

Apstiprināts
ar Smiltenes novada pašvaldības domes
2026. gada 28.maija lēmumu Nr. 185

Smiltenes novada pašvaldības Informācijas sistēmas kiberdrošības politika

Izdoti pamatojoties
uz Pašvaldību likuma 50.panta pirmo daļu,
Ministru kabineta 2025. gada 25. jūnija
noteikumu Nr. 397 "Minimālās kiberdrošības prasības" 28. punktu

1. Vispārīgie jautājumi

1.1. Smiltenes novada pašvaldības Informācijas sistēmas kiberdrošības politika (turpmāk - Politika) nosaka politiku, kādā Smiltenes novada pašvaldība (turpmāk – Pašvaldība) nodrošina pašvaldības izmantotās informācijas sistēmas (turpmāk - SNP IS) aizsardzību pret ārējiem un iekšējiem riskiem, un nodrošina informācijas sistēmas pieejamību, integritāti un konfidencialitāti saskaņā ar spēkā esošajiem normatīvajiem aktiem.

1.2. Politikā lietotie termini:

1.2.1. 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.

1.2.2. Smiltenes novada pašvaldība – institūcija, kas normatīvajos aktos noteiktajā kārtībā organizē un vada informācijas sistēmu darbību.

1.2.3. Pašvaldība - Smiltenes novada pašvaldība, 90009067337, juridiskā adrese Dārza iela 3, Smiltene, Smiltenes nov., LV-4729, kas ir darba devējs ikvienam Darbiniekam.

1.2.4. Sistēmas kiberdrošības pārvaldnieks – persona, kura atbild par Pašvaldības informācijas sistēmas drošības pasākumu izstrādi, ieviešanu un uzturēšanu, kā arī rīkojas ar informācijas resursiem.

1.2.5. Informācijas sistēmas lietotājs – persona, kurai ir pieejamas informācijas sistēmas un tajās glabātā informācija.

1.2.6. Lietotāja ID – Darbiniekam piešķirts unikāls identifikators – piekļuves vārds SNP IS

1.2.7. Politika – Pašvaldības "Informācijas sistēmu kiberdrošības politika".

1.2.6. CERT.LV – informācijas tehnoloģiju drošības incidentu novēršanas institūcija, kas ir Latvijas kompetentā iestāde un kas atbild par informācijas tehnoloģiju drošības incidentu novēršanu un koordinēšanu valsts mērogā;

1.2.7. Autentifikācija – process, kurā elektroniskajā vidē tiek pārbaudīta lietotāja identitāte.

1.2.8. Autorizācija – process, kurā lietotājam pēc veiksmīgas autentifikācijas tiek piešķirtas tiesības veikt konkrētas darbības informācijas sistēmā vai tehniskajā resursā.
1.2.9. Ārpakalpojums – jebkura veida vienošanās starp subjektu un pakalpojuma sniedzēju IKT jomā, saskaņā ar kuru šis pakalpojuma sniedzējs nodrošina procesu, sniedz pakalpojumu, veic tehnisko resursu piegādi vai veic citu darbību subjekta uzdevumā IKT infrastruktūrā.
1.2.10. Drošības pasākumi – tehniski vai organizatoriski pasākumi, kas tiek noteikti risku pārvaldības ietvaros un samazina risku līdz pieņemamam līmenim.
1.2.11. IKT resursi – tehnisko resursu un informācijas resursu kopums.
1.2.12. Informācijas resurss – strukturēta digitālo datu vienība.
1.2.13. Kiberapdraudējums – jebkādi iespējami apstākļi, notikums vai darbība, kas varētu radīt bojājumus vai traucējumus, vai citādi negatīvi ietekmēt tīklu un informācijas sistēmas, to lietotājus un citas personas.
1.2.14. Kiberdrošība – pasākumu kopums, kas tiek veikts, lai aizsargātu informācijas un komunikāciju tehnoloģijas sistēmas, tīklus, ierīces un datus no nesankcionētas piekļuves, izmantošanas, izpaušanas, traucējumiem, modifikācijas vai iznīcināšanas.
1.2.15. Kiberdrošības pārvaldības dokumentācija – šī politika un citi Pašvaldības iekšējie normatīvie akti, kas izstrādāti, lai noteiktu Pašvaldībā ievērojamos kiberdrošības principus Pašvaldības IKT infrastruktūras pārvaldībā, uzturēšanā un lietošanā.
1.2.16. Kiberhigiēna – ikdienas prakse un uzvedības principi, kas samazina kiberincidentu risku (piemēram, drošu paroļu lietošana, programmatūras atjaunināšana).
1.2.17. Kiberincidents – notikums, kas apdraud apstrādātus datus vai tādu pakalpojumu pieejamību, autentiskumu, integritāti vai konfidencialitāti, kurus piedāvā tīklu un informācijas sistēmas, vai kuri pieejami ar tīklu un informācijas sistēmu starpniecību.
1.2.18. Kiberrisks – iespējamība, ka kāds kiberapdraudējums radīs kaitējumu IKT sistēmām, datiem vai procesiem.
1.2.19. Kiberuzbrukums - aktīva uzbrucēja rīcība, kuras mērķis ir ietekmēt datu un informācijas un komunikācijas tehnoloģiju pakalpojumu konfidencialitāti, integritāti vai pieejamību.
1.2.20. Konfidencialitāte – piekļuve informācijas resursam tikai pilnvarotiem IKT procesiem un lietotājiem.
1.2.21. Konts – mehānisms, ar kuru lietotājam tiek piešķirta piekļuve IKT resursam vai informācijas sistēmai. Kontam ir unikāls identifikators, kas nodrošina darbības autora identificēšanu un pieejamo darbību un funkciju apjoma noteikšanu IKT resursā. Konts var būt piesaistīts konkrētai fiziskajai personai (piemēram, standarta lietotāja konts, administratora konts) vai nebūt piesaistāms nevienai fiziskajai personai (piemēram, sistēmkonts).
1.2.22. Lietotāja konts – konts, kas ir piesaistīts konkrētam lietotājam.
1.2.23. Lietotājs – persona, kurai ir piešķirtas tiesības lietot IKT resursu vai informācijas sistēmu.
1.2.24. MFA (daudzfaktoru autentifikācija) – autentifikācijas metode, kurā lietotāja identitāte tiek apstiprināta, izmantojot vismaz divus dažādus faktorus: zināšanas (parole), īpašumā esošs (ierīce) vai biometriskie dati.
1.2.25. Nacionālais kiberdrošības centrs (NKC) – Latvijas kompetentā iestāde kiberdrošības jomā, kas atbild par būtisko un svarīgo pakalpojumu sniedzēju uzraudzību, kā arī koordinē kiberdrošības politikas īstenošanu valstī;
1.2.26. Pieejamība – iespēja lietotājam lietot informācijas sistēmu vai informācijas resursu noteiktā laikā un vietā;
1.2.27. Sistēmkonts – konts, kas nodrošina IKT funkciju vai procesu un nav piesaistāms nevienam lietotājam;
1.2.28. Šifrēšana – process, kurā dati tiek pārveidoti, izmantojot speciālu algoritmu un atslēgu, lai padarītu tos neizprotamus vai neizlasāmus bez atbilstošas atslēgas. Šifrētos datus iespējams atšifrēt atpakaļ oriģinālajā formā, izmantojot pareizu atslēgu un atbilstošo atšifrēšanas algoritmu. Šifrēšanu var izmantot gan datu uzglabāšanā, gan pārraidē.

1.3. Politika ir izstrādāta saskaņā ar Latvijas Republikas Nacionālo kiberdrošības likumu un Ministru kabineta 2025.gada 25.jūnija noteikumiem Nr.397 “Minimālās kiberdrošības prasības”, Fizisko

personu datu apstrādes likumu 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”.

1.4. Pašvaldība ir klasificēta kā būtisko pakalpojumu sniedzējs atbilstoši Nacionālā kiberdrošības likuma prasībām, un tas uzliek pienākumu Pašvaldībai ievērot īpašas kiberdrošības pārvaldības prasības un ziņošanas pienākumus par nozīmīgiem kiberincidentiem kompetentajām institūcijām.

2. Informācijas sistēmas kiberdrošības politikas mērķi un pamatnostādnes

2.1. Pašvaldības pienākums ir nodrošināt, lai tās 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.

2.2. Informācijas sistēmas kiberdrošības politika attiecas uz visiem SNP IS 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.:

2.2.1. pilna darba laika, nepilnas slodzes un līgumdarbiniekiem, kuri ir nodarbināti pašvaldībā;

2.2.2. lietotājiem, kuri ir noslēguši līgumu ar pašvaldību par datu lietošanu vai kuri uz pieprasījuma pamata saņem datus no pašvaldības izmantotām informācijas sistēmām;

2.2.3. ārpakalpojumu sniedzējiem vai konsultantiem, kuri strādā pašvaldības labā;

2.2.4. praksē esošiem izglītības iestāžu skolniekiem/studentiem.

2.3. SNP IS lietotājs par iepazīšanos ar augstāk minētajiem dokumentiem un to ievērošanu DVS Namejs elektroniski paraksta 2.pielikumu “Informācijas sistēmas lietotāja apliecinājums par “Informācijas sistēmas kiberdrošības politikas” prasību ievērošanu”.

2.4. Pašvaldības struktūrvienību vadītāji ir atbildīgi par viņu pakļautībā vai uzraudzībā esošajiem SNP IS lietotājiem. 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.

2.5. SNP IS drošība tiek nodrošināta šādu mērķu realizācijai:

2.5.1. nodrošināt informācijas pieejamību;

2.5.2. nodrošināt informācijas integritāti;

2.5.3. nodrošināt informācijas konfidencialitāti;

2.5.4. aizsargāt sistēmas informācijas resursus;

2.5.5. aizsargāt sistēmas tehniskos resursus;

2.5.6. noteikt sistēmas drošības apdraudējumu;

2.5.7. novērtēt sistēmas drošības risku;

2.5.8. atklāt sistēmas drošības incidentu;

2.5.9. atjaunot sistēmas darbību pēc sistēmas drošības incidenta.

3. Pašvaldības vispārējs raksturojums, darbības joma, sniegtie pakalpojumi

3.1. Pašvaldība ir atvasināta publiska persona — vietējā pārvalde —, kurai ir iedzīvotāju ievēlēta lēmējinstitūcija — dome — un kura patstāvīgi nodrošina tai tiesību aktos noteikto funkciju un uzdevumu izpildi savas administratīvās teritorijas iedzīvotāju interesēs un ir atbildīga par to saskaņā ar ārējiem normatīvie aktiem, tai skaitā Pašvaldības likumu un Pašvaldības nolikumu, un saskaņā ar likumu noslēgtiem publisko tiesību līgumiem. Smiltenes novads izveidots 2021. gada 1. jūlijā, apvienojot Apes, Raunas un Smiltenes novadus (Apes, Bilskas, Blomes, Brantu, Drustu, Gaujienas, Grundzāles, Launkalnes, Palsmanes, Raunas, Smiltenes, Trapenes, Variņu, Virešu), kā arī Smiltenes pilsētu un Smiltenes pagastu. Novada administratīvā teritorija — aptuveni 1 801.32 km², un tajā dzīvo aptuveni 17 697 iedzīvotāji. Pašvaldības lēmējorgāns ir Smiltenes novada pašvaldības dome, turpmāk - dome, kurai pakļautas izpildinstitūcijas, kas īsteno dažādas funkcijas un nodrošina pakalpojumus iedzīvotājiem.

3.2. Pašvaldības darbības joma aptver Pašvaldību likuma 4. pantā un citos normatīvajos aktos noteiktu iedzīvotājiem nozīmīgu funkciju (pakalpojumu) loku, tajā skaitā, bet neaprobežojoties:

3.2.1. organizēt Pašvaldības iedzīvotājiem ūdenssaimniecības, siltumapgādes un sadzīves atkritumu apsaimniekošanas pakalpojumus;

3.2.2. gādāt par Pašvaldības administratīvās teritorijas labiekārtošanu un sanitāro tīrību;

3.2.3. Pašvaldības īpašumā esošo ceļu būvniecību, uzturēšanu un pārvaldību;

3.2.4. gādāt par iedzīvotāju izglītību, tostarp nodrošināt iespēju iegūt obligāto izglītību un gādāt par pirmsskolas izglītības, vidējās izglītības, profesionālās ievirzes izglītības, interešu izglītības un pieaugušo izglītības pieejamību;

3.2.5. sniegt iedzīvotājiem daudzveidīgu kultūras piedāvājumu un iespēju piedalīties kultūras dzīvē, sekmēt pašvaldības teritorijā esošā kultūras mantojuma saglabāšanu un sniegt atbalstu kultūras norisēm;

3.2.6. gādāt par iedzīvotāju veselību — īstenot veselīga dzīvesveida veicināšanas pasākumus un organizēt veselības aprūpes pakalpojumu pieejamību;

3.2.7. veicināt sporta attīstību, tostarp uzturēt un attīstīt pašvaldības sporta bāzes, atbalstīt sportistu un sporta klubu, arī profesionālo sporta klubu, darbību un sniegt atbalstu sporta pasākumu organizēšanai;

3.2.8. nodrošināt iedzīvotājiem atbalstu sociālo problēmu risināšanā, kā arī iespēju saņemt sociālo palīdzību un sociālos pakalpojumus, un citus.

3.2.9. piedalīties sabiedriskās kārtības un drošības nodrošināšanā Pašvaldības administratīvajā teritorijā, un , un citus, normatīvajos aktos Pašvaldībai deleģētos pakalpojumus.

3.3. Kritiskie procesi, kurus var ietekmēt kiberapdraudējumi:

3.3.1. Finanšu un norēķinu sistēmu darbība - Banku maksājumi, rēķinu apstrāde un grāmatvedības uzskaite var tikt paralizēta kiberincidentu gadījumā;

3.3.2. Datu uzglabāšana un pieejamība - Sensitīvi pašvaldības vai iedzīvotāju dati (klientu, darbinieku, nodokļu, sociālie dati) var tikt bojāti, nopludināti vai padarīti nepieejami;

3.3.3. IKT infrastruktūras un serveru darbība- Serveru, tīklu un datu centru pieejamība ir kritiska visiem pārējiem procesiem;

3.3.4. Pakalpojumu nepārtrauktība- Komunālo, sociālo, izglītības un citu pašvaldības pakalpojumu nodrošināšana var apstāties vai būtiski ierobežoties;

3.3.5. Komunikācija un iekšējā sadarbība- E-pasta sistēmas, dokumentu vadība un saziņas kanāli var tikt bloķēti vai kompromitēti;

3.3.6. Sabiedrības informēšana un reputācijas aizsardzība-Dezinformācija vai datu noplūde var negatīvi ietekmēt uzticību organizācijai un tās pakalpojumiem.

4. Nozīmīgākie kiberapdraudējuma veidi

4.1. Lai nodrošinātu efektīvu kiberdrošības pārvaldību un savlaicīgi novērstu kiberincidentu riskus, Pašvaldība regulāri identificē un novērtē nozīmīgākos kiberapdraudējumu veidus, kam var būt pakļauti Pašvaldības īpašumā un valdījumā esošie IKT resursi un informācijas sistēmas

4.2. Pašvaldības īpašumā un valdījumā esošie IKT resursi un informācijas sistēmas, kas nodrošina sabiedrībai svarīgu pakalpojumu nepārtrauktību, ir pakļauti vairākiem nozīmīgiem kiberapdraudējumu veidiem:

4.2.1. Ļaunatūras (malware) un izspiedējvīrusu uzbrukumi – var bloķēt piekļuvi lietotāju datiem un sistēmām, paralizējot pašvaldība ikdienas darbu;

4.2.2. Pikšķerēšanas (phishing) uzbrukumi – darbiniekiem nosūtītas maldinošas vēstules vai saites var radīt nesankcionētu piekļuvi sensitīviem datiem vai sistēmām;

4.2.3. Neatļauta piekļuve informācijas sistēmām (hakeru uzbrukumi) – mēģinājumi iegūt piekļuvi lietotāju datiem, finanšu sistēmām vai iekšējiem tīkliem, izmantojot vājās paroles, neaizsargātus serverus vai ievainojamības;

4.2.4. Pakalpojuma atteices (DoS/DDoS) uzbrukumi – mērķtiecīga sistēmu pārslodze var padarīt nepieejamus klientu, komunikācijas vai pamat ierīču vadības rīkus;

4.2.5. Sociālās inženierijas uzbrukumi (Social Engineering) - cilvēka psiholoģisku manipulēšanu, lai panāktu noteiktu darbību veikšanu vai konfidenciālas informācijas izpaušanu;
4.2.6. Iekšējie apdraudējumi – datu noplūde vai sistēmu bojājumi darbinieku kļūdu vai apzinātas rīcības rezultātā, piemēram, neatbilstoša piekļuves tiesību izmantošana vai datu kopēšana;
4.2.7. Programmatūras un sistēmu ievainojamības – novecojušas vai neatjauninātas sistēmas var kļūt par ieejas punktu uzbrukumiem, kas apdraud gan klientu datu aizsardzību, gan IT infrastruktūras stabilitāti.

4.3. Kiberdrošības pārvaldnieks nodrošina informācijas apriti un reaģēšanu uz potenciālajiem un aktuālajiem kiberapdraudējumiem, informējot darbiniekus par nepieciešamajiem drošības pasākumiem.

5. Informācijas sistēmas drošības politikas administrēšana un pārvaldība

5.1. Informācijas tehnoloģiju kiberdrošības pārvaldību un Informācijas sistēmas drošības politikas koordināciju pašvaldībā veic IT nodaļa sadarbojoties ar kiberdrošības pārvaldnieku.

5.2. IT nodaļas pienākums ir aktualizēt SNP IS kiberdrošības politikas dokumentus vismaz vienu reizi gadā, kā arī šādos gadījumos:
5.2.1 ja izmaiņas sistēmā var ietekmēt sistēmas drošību;
5.2.2. ja mainījušies vai ir atklāti jauni sistēmas drošības apdraudējumi;
5.2.3. ja pēkšņi pieaug sistēmas drošības incidentu skaits, vai ir noticis nozīmīgs sistēmas drošības incidents;
5.2.4. ja izmaiņas Pašvaldības organizatoriskajā struktūrā skar sistēmas drošības vadības organizāciju;
5.2.5. ja izdarīti grozījumi normatīvajos aktos, kas regulē sistēmas darbību.
5.2.6. atbilstoši izmaiņām normatīvajos aktos, izmaiņām Pašvaldības darbībā un izmaiņām Informācijas sistēmas izmantošanā.

6. Informācijas sistēmas kiberdrošības organizācijas struktūra

6.1. SNP IS drošības organizatoriskās struktūras pamatu veido Pašvaldības amatpersonas un struktūrvienības - Pašvaldības izpilddirektors, informācijas sistēmas kiberdrošības pārvaldnieks, IT nodaļa un Informācijas sistēmas lietotāji.

6.2. Informācijas sistēmas drošībai organizācijā Pašvaldības izpilddirektors veic šādas darbības:
6.2.1. organizē informācijas sistēmas drošības izveidi un ieviešanu;
6.2.2. nosaka un apstiprina Sistēmas kiberdrošības politiku;
6.2.3. nosaka SNP IS kiberdrošības pārvaldnieku (3.pielikums "Informācijas sistēmu un informācijas sistēmas kiberdrošības pārvaldnieks");
6.2.4. Informācijas sistēmas kiberdrošības pārvaldnieka prombūtnē pašvaldības izpilddirektors var iecelt tā pienākumu aizvietotāju;
6.2.5. veic citus nepieciešamos pasākumus, lai nodrošinātu informācijas sistēmas drošības organizācijas pilnvērtīgu funkcionēšanu;
6.2.6. nodrošina nepieciešamo organizatorisko struktūru darbības atjaunošanas kārtības realizācijai.

6.3. Informācijas sistēmas kiberdrošības pārvaldnieks nodrošina informācijas sistēmas drošības politikas realizāciju, kā arī veic šādas darbības:
6.3.1. kopā ar IT nodaļas vecāko datortīklu administratoru aktualizē drošības politiku, izstrādā ar informācijas sistēmas drošības saistīto iekšējo normatīvo aktu projektus un veic tās koordināciju;
6.3.2. nodrošina informācijas sistēmās izmantojamās informācijas racionālu un pareizu izmantošanu;
6.3.3. Sadarboties ar ārējām kiberdrošības institūcijām (CERT.LV, NKC).
6.3.4. Organizēt un koordinēt Pašvaldības darbinieku kiberdrošības apmācības un informēšanas pasākumus;

6.3.5. apstiprina informācijas sistēmas lietotāju tiesību piešķiršanu, izmaiņu veikšanu un anulēšanu;

6.4. IT nodaļas pienākums ir:

6.4.1. nodrošināt tehnisko resursu racionālu un pareizu izmantošanu;

6.4.2. nodrošināt tehnisko resursu fiziskās un loģiskās aizsardzības pasākumus;

6.4.3. sadarboties ar informācijas sistēmas kiberdrošības pārvaldnieku, nodrošinot nepieciešamo tehnisko risinājumu attiecīgajam informācijas resursam;

6.4.4. organizēt Sistēmas risku analīzes veikšanu;

6.4.5. nodrošināt Sistēmas tehnisko resursu iegādi, izstrādi, darbību un uzturēšanu;

6.4.6. izmeklēt informācijas drošības incidentus;

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

6.4.8. nodrošināt informācijas sistēmas atjaunošanas procedūras, ja tehnoloģiskie resursi ir bojāti un informācijas sistēmas funkcionēšana traucēta, vai neiespējama saskaņā ar Informācijas sistēmas kiberdrošības politiku.

6.5. IT nodaļai ir pienākums nodrošināt atbilstošu atbalstu, palīdzību un konsultāciju sniegšanu personālam, lai tas varētu pildīt savus pienākumus atbilstoši Informācijas sistēmas kiberdrošības politikas prasībām. SNP IT sistēmas drošības nodrošināšanai, veicot IT iekārtu, programmatūras (turpmāk šajā punktā - Iekārtas) iepirkumus pašvaldības funkciju izpildei, pasūtītājs, kas ir pašvaldības iestāde, Iekārtu iepirkumos tehniskajās specifikācijās iekļauj noteikumus, ka Iekārtas ražotājs drīkst būt juridiska persona, kas reģistrēta NATO, Eiropas Savienības vai Eiropas Ekonomikas zonas dalībvalstī, vai fiziska persona, kas ir Latvijas Republikas valstspiederīgais, NATO, Eiropas Savienības vai Eiropas Ekonomikas zonas valsts pilsonis.

7. Ārpakalpojumu pārvaldība

7.1. Pašvaldība piesaistot ārpakalpojumu sniedzējus IKT jomā, nodrošina, ka netiek paaugstināts kiberapdraudējumu risks un tiek saglabāts noteiktais drošības līmenis. Jebkura ārpakalpojuma izmantošana tiek rūpīgi pārvaldīta visā tā dzīvesciklā, sākot ar pakalpojuma sniedzēja izvēli un beidzot ar līgumattiecību izbeigšanu.

7.2. Ārpakalpojuma sniedzēja izvērtēšana un risku novērtējums:

7.2.1. pirms līguma noslēgšanas par jebkura IKT ārpakalpojuma saņemšanu, Pašvaldība veic potenciālā pakalpojuma sniedzēja risku novērtējumu;

7.2.2. novērtējuma ietvaros tiek analizēta pakalpojuma sniedzēja spēja nodrošināt atbilstību Pašvaldības Kiberdrošības politikas prasībām, tā vispārējā reputācija, datu aizsardzības prakse, kā arī spēkā esošie sertifikāti kiberdrošības jomā,ja tādi ir;

7.2.3. par risku novērtējuma veikšanu ir atbildīgs Pašvaldības izpilddirektors, apstiprinot ārpakalpojuma piesaisti, sadarbojoties ar Kiberdrošības pārvaldnieku.

7.3. Līgumiskās prasības - katrā līgumā ar IKT ārpakalpojuma sniedzēju obligāti tiek iekļauti skaidri un nepārprotami nosacījumi Kiberdrošības jomā. Šiem nosacījumiem ir jāatrunā vismaz šādi punkti:

7.3.1. apņemšanās ievērot Pašvaldības Kiberdrošības politiku un citus saistītos iekšējos normatīvos aktus;

7.3.2. skaidri definētas prasības informācijas konfidencialitātes, integritātes un pieejamības nodrošināšanai attiecībā uz Pašvaldības datiem un sistēmām;

7.3.3. pienākums nekavējoties, bet ne vēlāk kā Pašvaldības noteiktajā termiņā, ziņot Kiberdrošības pārvaldniekam par jebkādiem kiberincidentiem vai drošības vājībām, kas skar Pašvaldības uzticētos IKT resursus;

7.3.4. atbilstība Vispārīgās datu aizsardzības regulas (GDPR) prasībām, ārpakalpojuma ietvaros apstrādājot fizisku personu datus;

7.3.5. Pašvaldības tiesības veikt vai piesaistīt trešās puses, lai veiktu ārpakalpojuma sniedzēja darbības auditu Kiberdrošības jomā, lai pārliecinātos par līgumā noteikto saistību izpildi;

7.3.6. nosacījumi par drošu Pašvaldības datu atgriešanu un/vai neatsaucamu iznīcināšanu pēc līguma termiņa beigām;

7.3.7. skaidrs atbildības sadalījums starp Pašvaldības un pakalpojuma sniedzēju kiberincidentu pārvaldības un seku novēršanas gadījumā.

7.4. Uzraudzība un atbilstības kontrole:

7.4.1. Pašvaldības Kiberdrošības pārvaldnieks sadarbībā ar atbildīgajām struktūrvienībām nodrošina regulāru ārpakalpojumu sniedzēju darbības uzraudzību;

7.4.2. Pašvaldība ietver periodiskas atbilstības pārbaudes, pakalpojuma sniedzēja drošības ziņojumu analīzi un, nepieciešamības gadījumā, līgumā noteikto audita tiesību izmantošanu.

7.5. Ja tiek konstatētas neatbilstības, Kiberdrošības pārvaldnieks sadarbībā ar ārpakalpojuma sniedzēju izstrādā un kontrolē neatbilstību novēršanas plāna izpildi.

8. Informācijas sistēmas lietotāju administrēšanas kārtība

8.1. Pašvaldības katras struktūrvienības vadītājs ir atbildīgs par sev un savā padotībā esošo darbinieku lietotāju pieejas tiesību piešķiršanu, izmaiņu veikšanu un anulēšanu.

8.2. Lai izveidotu lietotāju pieejas tiesības vai veiktu izmaiņas tajās, Pašvaldības atbilstošās struktūrvienības vadītājs raksta pieprasījumu (4.pielikums "Lietotāju pieejas tiesību piešķiršanas vai izmaiņas pieprasījums"), atzīmējot tajā nepieciešamo Informācijas resursu, ko iesniedz SNP IT nodaļas vadītājam.

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

8.4. IT nodaļas vadītājs izskata lietotāju pieejas tiesību piešķiršanas pieprasījumu un, ja uzskata to par pamatotu, Informācijas sistēmas drošības pārvaldnieks pieprasījumu izveidot atbilstošās informācijas sistēmas lietošanas tiesības nosūta/nogādā IT nodaļas vecākajam datortīklu administratoram.

8.5. Informācijas sistēmas lietotāju pieejas tiesību piešķiršana Pašvaldības informācijas resursiem personām, kuras nav Pašvaldības darbinieki, notiek tikai atsevišķos gadījumos pēc Pašvaldības vadītāja 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).

8.6. IT nodaļas vecākais datortīklu administrators ir atbildīgs par Lietotāju pieejas tiesību izveidošanu, administrēšanu un šo pieprasījumu apkopošanu, glabāšanu, kontroli un uzraudzību.

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

8.7.1. darbiniekiem, kuri pārtrauc darba (līguma) tiesiskās attiecības ar pašvaldību;

8.7.2. darbiniekiem, kuri ilgstoši atrodas prombūtnē (slimības dēļ, atvaļinājumā, komandējumā u.c.), ja tās ilgums pārsniedz trīs mēnešus. Šādā gadījumā pieejas tiesības tiek atjaunotas pēc struktūrvienības vadītāja pieprasījuma, darbiniekam atgriežoties pildīt darba pienākumus;

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

8.8. Iestājoties šo noteikumu 23.punktā minētajam gadījumam, atbilstošās struktūrvienības vadītājam, kura pakļautībā ir augstāk minētais darbinieks (vai koordinējošās struktūrvienības vadītājam gadījumos ar trešajām personām), ir pienākums sagatavot un iesniegt IT nodaļas vecākajam datortīklu administratoram Lietotāju pieejas tiesību anulēšanas pieprasījumu (5.pielikums "Lietotāju pieejas tiesību anulēšanas pieprasījums").

8.9. Sistēmas lietotāji, kas veic Sistēmas administrēšanas darbu, izmanto tam īpašus lietotāju kontus (turpmāk – Sistēmas administratora kontus), kas netiek izmantoti ikdienas darbību veikšanai.

8.10. Katrs lietotāja konts ir saistīts ar konkrētu fizisko personu.

8.11. Sistēmkontus aizsargā tā, lai novērstu iespēju lietotājiem tos izmantot.

9. Informācijas sistēmas lietotāju tiesības, pienākumi un atbildība

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

9.2. SNP IS lietotājs ir atbildīgs par datortehniku, kas nodota viņa rīcībā, kā arī atbild par darbībām, kas tiek veiktas ar viņam nodoto datortehniku.
9.3. SNP IS lietotājs nedrīkst atļaut piekļūt tam nodotai datortehnikai citām personām, ja tas nav nepieciešams tiešo darba pienākumu pildīšanai un to pilnvarojumu nav devis Pašvaldības vadītājs vai IT nodaļas vadītājs.
9.4. SNP IS lietotāja pienākums ir racionāli un lietderīgi izmantot informācijas sistēmas un to datus sava darbu pienākumu veikšanai;
9.5. SNP IS lietotāja pienākums ir ziņot par Sistēmā identificētajiem riskiem, informācijas drošības notikumiem un incidentiem.
9.6. SNP IS 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 IT nodaļa.
9.7. SNP IS lietotājam ir pienākums jebkuru ienākošo elektronisko informāciju (failus) pirms lietošanas obligāti pārbaudīt ar antivīrusa programmatūru, ja tas netiek nodrošināts automātiski.
9.8. Nelicencētas programmatūras uzstādīšana un lietošana darba stacijās (lietotāja datoros) ir aizliegta. Patvaļīgi uzstādītas programmatūras lietošana, bez Pašvaldības vadītāja vai IT nodaļas vadītāja atļaujas ir aizliegta.
9.9. Informācijas sistēmas lietotājs nedrīkst izpaust nepilnvarotām personām ziņas par Pašvaldības datoru tīkla uzbūvi un konfigurāciju.
9.10. SNP IS lietotājiem ir pienākums vismaz vienu reizi divu gadu laikā apmeklēt IT drošības apmācības, kas parāda ar kādiem apdraudējumiem lietotājs saskarās virtuālajā vidē – pikšķerēšana, izspiedējvīrusi, informācijas viltošana u.c. Pēc apmācību nokārtošanas darbinieks spēj atšķirt šos apdraudējumus un izvairīties no tiem. Apmācības organizē IT nodaļa un darbiniekiem ir pienākums tās apmeklēt un veiksmīgi nokārtot apmācību testus. Ja SNP IS lietotājs nav apmeklējis apmācības vai veiksmīgi nokārtojis IT apmācību testus, SNP IT nodaļai ir tiesības šo lietotāja kontu bloķēt, līdz lietotājs nav pabeidzis apmācības.
9.11. SNP IS 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 vadītājs, Informācijas sistēmas drošības pārvaldnieks vai IT nodaļas vadītājs.
9.12. Ārējo datu nesēju, kurā ir iekopēta ierobežotas pieejamības informācija, no Pašvaldības telpām drīkst iznest tikai ar Pašvaldības vadītāja RAKSTISKU atļauju. Šajos gadījumos Informācijas sistēmas lietotājs, kurš no iestādes telpām iznes šādu datu nesēju, uzņemas pilnu atbildību par šo informāciju.

10. Interneta un e-pasta lietošana

10.1. Pieeju Internetam darbiniekiem piešķir vienlaicīgi ar Informācijas sistēmas lietotāja pieejas tiesībām Pašvaldības datortīklam (domēnam), kas nepieciešams, lai nodrošinātu iestādes darbību.
10.2. Informācijas sistēmas lietotājam darba vajadzībām ir jāizmanto tikai Pašvaldības piešķirtais e-pasts.
10.3. E-pasta konts tiek izveidots pēc šablona vards.uzvards@smiltenesnovads.lv, katra konta noklusētais lielums ir 6 GB. Ir iespējams palielināt e-pasta konta lielumu griežoties pie IT nodaļas vadītāja un pamatojot nepieciešamību, kāpēc ir nepieciešams to pielielināt.
10.4. SNP IS lietotājam ir aizliegts, izmantojot Pašvaldības piešķirto e-pastu, reģistrēties dažādos interneta resursos, kas tiek izmantoti privātām vajadzībām.
10.5. Lietojot Internetu, darbinieki pārstāv pašvaldību, un tie ir atbildīgi, lai Internets tiktu izmantots darba vajadzībām ētiski un atbilstoši likumdošanas prasībām.
10.6. Darbiniekiem, izmantojot e-pastu, ir jānodrošina, ka komunikācija tiek veikta profesionālām vajadzībām un netraucē pašu darbinieku darba produktivitāti, kā arī netiek izplatīta vai sūtīta informācija, kas ir aizsargāta ar autortiesībām. Pašvaldība no darbinieka ir tiesīga piedzīt zaudējumus, kas Pašvaldībai var būt radušies, maksājot atlīdzību autortiesību īpašniekam par autortiesību pārkāpumu.

10.7. Darbinieki ir atbildīgi par visu nosūtīto tekstuālo, audio un vizuālo saturu. Pašvaldība bez saskaņošanas ar darbinieku patur sev tiesības pārlūkot darbinieku saņemto un nosūtīto e-pastu saturu, ja uzskata to par nepieciešamu.
10.8. IT nodaļas vadītājam 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.
10.9. Darbiniekiem ir aizliegts automātiski saglabāt lietotāj vārdu un paroli visās pārlūk programmatūrās. IT nodaļai ir tiesības piemērot tehniskus risinājumus, kas aizliedz veikt šīs darbības.
10.10. Darbiniekiem ir aizliegts sūtīt tā sauktās "ķēdes vēstules"– 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 medijs, 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.

11. Informācijas sistēmas lietotāja pieejas paroles uzbūve un lietošana

11.1. Pašvaldības informācijas resursu aizsardzība tiek nodrošināta ar datora paroli datortīkla (domēna) līmenī, kam ir jāatbilst vismaz sekojošām prasībām:
  11.1.1. minimālam paroles garumam ir jābūt vismaz 10 simboli;
  11.1.2. maksimālais paroles maiņas periods nedrīkst būt ilgāks par 90 dienām, taču paroli aizliegts pašrocīgi mainīt biežāk nekā divas reizes 24 stundu laikā;
  11.1.3. paroles uzbūvei jābūt komplicētai, izmantojot vismaz vienu lielo latīņu alfabēta burtu, mazo latīņu alfabēta burtu, ciparu un īpašo rakstzīmju kombināciju (kā piemēram, !@#$%^*()_+);
  11.1.4. izveidojot paroli, tā nedrīkst sakrist ar nevienu no 5 iepriekšējām parolēm.
11.2. SNP IS 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.
11.3. SNP IS lietotājs nedrīkst savu paroli pierakstīt uz papīra, ja šo dokumentu neglabā seifā vai citā vietā ar ierobežotu citu personu piekļuvi.
11.4. Infrastruktūras iekārtām, kas nodrošina Sistēmas funkcionēšanu, netiek izmantotas noklusējuma (ražotāja vai izplatītāja uzstādītas) paroles.
11.5. Ja SNP IS 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 IT nodaļu to izdarīt savā vietā.
11.6. SNP IS 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. Arī pusdienu pārtraukumā vai īslaicīgi atstājot savu darba vietu, kad dators ir ieslēgts, ir jāieslēdz ekrānsaudzētājs (Windows+Lock).
11.7. Dienas beigās, beidzot darbu pie datora, tas jāizslēdz izmantojot procedūru: Start =>Shut Down =>Ok.

12. Sistēmas aizsardzības pasākumi

12.1. Pašvaldības datorsistēmas un tehnika (t.sk. datortīkli, programmatūra, informācijas sistēmas, serveri, datori) tiek aizsargāta ar piemērotu fizisko, tehnisko, organizatorisko un vides kontroļu kopumu.
12.2. SNP IS resursiem (datortīklam, datoriem, serveriem u.tml.) bez Smiltenes novada pašvaldības izpilddirektora vai Smiltenes novada pašvaldības IT nodaļas vadītāja atļaujas aizliegts pieslēgt SNP IS nepiederošus tehniskos resursus, tai skaitā (bet ne tikai) personīgos datorus vai datorus, ar kuriem strādā citu organizāciju (uzņēmumu, iestāžu) pārstāvji.
12.3. Serveri 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 IT nodaļa, savukārt par atbilstošo datoru fizisko drošību atbild attiecīgais Informācijas sistēmas lietotājs.

12.4. Visās Iestādes valdījumā esošajās gala lietotāju iekārtās, kas ikdienā tiek izmantotas, lai pieslēgtos sistēmai, ir iekļauta pretvīrusu funkcionalitāte.

12.5. Sistēmas funkcionalitāte ir izpildāma ar minimāli iespējamo tiesību kopu.

12.6. Tehnisko resursu valdītājs sadarbībā ar Sistēmas kiberdrošības pārvaldnieku veic pieejamo programmatūras atjauninājumu izvērtēšanu un nepieciešamības gadījumā – testēšanu.

12.7. Sistēmai jābūt uzstādītiem visiem pieejamiem nepieciešamajiem programmatūras atjauninājumiem.

12.8. Tiek nodrošināta sistēmas pierakstu veidošana un uzglabāšana vismaz 6 mēnešus pēc ieraksta izdarīšanas, uzglabājot pierakstu kopijas atsevišķi no Sistēmas.

12.9. Sistēmas pieraksti tiek veidoti, nodrošinot, ka ierakstā norādītais laiks sakrīt ar faktiskā notikuma koordinēto universālo laiku.

12.10. Veicot Sistēmas izstrādi un testēšanu, nav pieļaujams radīt apdraudējumu sistēmās glabāto datu integritātei, tādēļ šādiem nolūkiem ir izveidota sistēmas testa vide.

13. Ziņošanas par drošības incidentiem

Par visiem datu/informācijas apstrādes drošības incidentiem vai iespējamiem incidentiem Darbiniekam nekavējoties ir jāziņo savam tiešajai vadītājam, Pašvaldības IT personālam, kuri organizē, veic nepieciešamos pasākumus iespējamā kaitējuma novēršanai, radītā kaitējuma seku likvidēšanai un iepriekšējā drošības stāvokļa atjaunošanai.

14. Darbības nepārtrauktības nodrošināšana

14.1. Pašvaldības informācijas sistēmām un elektroniskā veidā saglabātai informācijai regulāras rezerves kopijas veidošanu nodrošina IT nodaļas vecākais datortīklu administrators.

14.2. 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.

14.3. Par visām avārijas situācijām (t.sk. ugunsgrēku, plūdiem, nelaimes gadījumiem utt.) Informācijas sistēmas lietotājiem, IT nodaļai ir nekavējoši jāpaziņo Pašvaldības izpilddirektoram.

15. Noslēguma jautājums

15.1. Ar šo noteikumu spēkā stāšanos atzīt par spēku zaudējušiem Smiltenes novada pašvaldības domes 2021.gada 25.augusta noteikumus Nr. 3/21 “Smiltenes novada pašvaldības Informācijas sistēmas drošības”.

Domes priekšsēdētājs E. Labanovskis

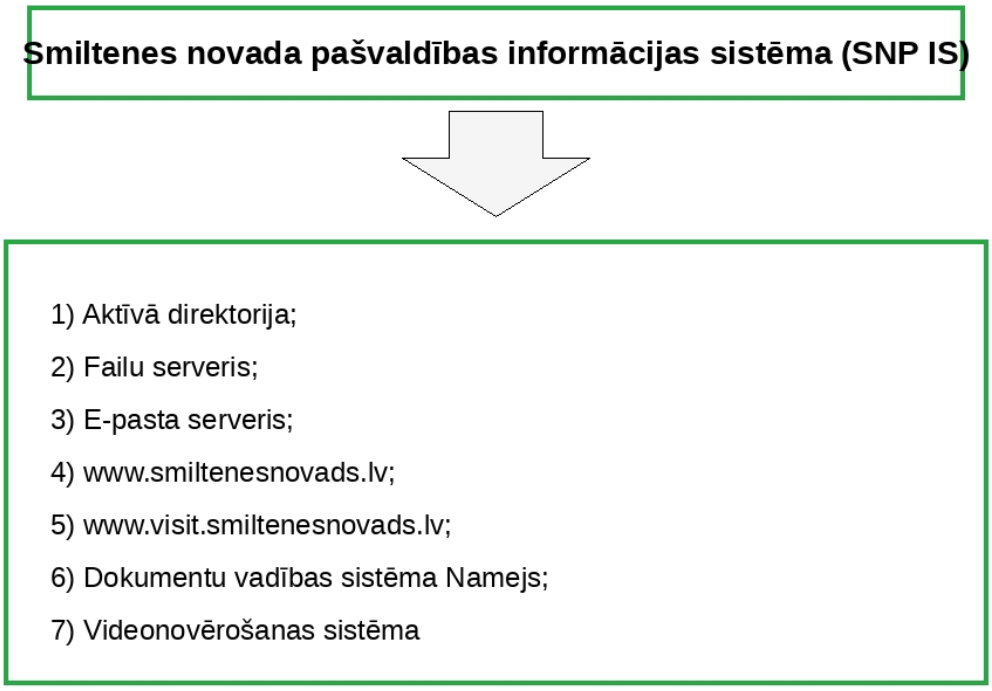
Pielikumā:

1. pielikums - Smiltenes novada pašvaldības informācijas sistēmas shēma;
2.pielikums - Smiltenes novada pašvaldības Informācijas sistēmas lietotāja apliecinājums par “Informācijas sistēmas kiberdrošības politikas” prasību ievērošanu;
3.pielikums - Smiltenes novada pašvaldības Informācijas sistēmas kiberdrošības pārvaldnieka apliecinājums par “Informācijas sistēmas kiberdrošības politikas” prasību ievērošanu;
4.pielikums - Smiltenes novada pašvaldības IS lietotāju pieejas tiesību piešķiršanas vai izmaiņu pieprasījums;
5.pielikums - Smiltenes novada pašvaldības IS lietotāju pieejas tiesību anulēšanas pieprasījums;
6. pielikums - Kiberrisku pārvaldības novērtējums Iestādes informācijas sistēmai (SNP IS) (ierobežota pieejamība);
7. pielikums - Darbības nepārtrauktības plāns (ierobežota pieejamība);
8. pielikums - Smiltenes novada pašvaldības kiberincidentu žurnāls (ierobežota pieejamība);

9. pielikums - Smiltenes novada pašvaldības IKT resursu un informācijas sistēmu katalogs (ierobežota pieejamība);
10. pielikums - Riska reģistrs Smiltenes novada pašvaldības IT infrastruktūrai un sistēmām (ierobežota pieejamība).

1. pielikums
Noteikumiem Nr.8/26 “Smiltenes novada pašvaldības
Informācijas sistēmas kiberdrošības politika”

SMILTENES NOVADA PAŠVALDĪBAS INFORMĀCIJAS SISTĒMAS SHĒMA (SNP IS)



2. PIELIKUMS
"Smiltenes novada pašvaldības
Informācijas sistēmas kiberdrošības politika"

INFORMĀCIJAS SISTĒMAS LIETOTĀJA APLIECINĀJUMS PAR "INFORMĀCIJAS SISTĒMAS KIBERDROŠĪBAS POLITIKAS" PRASĪBU IEVĒROŠANU

Ar šo es, zemāk parakstījies, apliecinu:

1. Esmu iepazinies(usies), izprotu un apņemos ievērot Informācijas kiberdrošības politikas nosacījumu un prasību ievērošanu, kas ir minēti:
    1.1. Informācijas sistēmas kiberdrošības politikā;
2. Apņemos neizmantot konfidenciālu informāciju, kas saņemta no Smiltenes novada pašvaldības, savu vai trešo personu interesēs, kā arī apņemos ievērot Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa regula (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula), Fizisko personu datu apstrādes likuma un Informācijas atklātības likuma prasības.
3. Es piekrītu, ka, pārtraucot darba (līguma) attiecības ar Smiltenes novada pašvaldību jebkādu iemeslu dēļ, es nekavējoties nodošu Smiltenes novada pašvaldībai man 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.

3.PIELIKUMS
"Smiltenes novada pašvaldības
Informācijas sistēmas kiberdrošības politika"

INFORMĀCIJAS SISTĒMAS KIBERDROŠIBAS PĀRVALDNIEKA APLIECINĀJUMS PAR "INFORMĀCIJAS SISTĒMAS KIBERDROŠĪBAS POLITIKAS" PRASĪBU IEVĒROŠANU

Ar šo es, zemāk parakstījies, apliecinu:

1. Esmu iepazinies(usies), izprotu un apņemos ievērot Informācijas kiberdrošības politikas nosacījumu un prasību ievērošanu, kas ir minēti šādos dokumentos:
   1.2. Informācijas sistēmas kiberdrošības politikā;

2. Apņemos neizmantot konfidenciālu informāciju, kas saņemta no Smiltenes novada pašvaldības, savu vai trešo personu interesēs, kā arī apņemos ievērot Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa regula (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula), Fizisko personu datu apstrādes likuma un Informācijas atklātības likuma prasības.

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

4. PIELIKUMS
"Smiltenes novada pašvaldības
Informācijas sistēmas kiberdrošības politika"

SMILTENES NOVADA PAŠVALDĪBAS IS
LIETOTĀJU PIEEJAS TIESĪBU PIEŠĶIRŠANAS VAI IZMAIŅAS PIEPRASĪJUMS

Vārds, uzvārds:	
Personas kods:	
Mob. tālr.:	
E-pasts:	
Deklarētā dzīvesvietas adrese:	
Iestādes / struktūrvienības nosaukums:	
Ieņemamais amats:	
Amatpersonas statuss:	☐ ir jānosaka ☐ nav jānosaka
Lūdzu piešķirt lietotāja pieejas tiesības informācijas resursiem (atzīmēt vajadzīgo) sākot ar 202__.gada ____._____.	

Informācijas resursu nosaukums (atzīmēt ar ☒ vajadzīgo):

☐ E-pasts;

☐ Pieeja pašvaldības iekšējiem datortīkla resursiem (aktīvā direktorija, failu serveris, dokumentu vadības sistēma "Namejs");

☐ Smiltenesnovads.lv tīmekļa vietne;

☐ Visit.smiltene.lv/Visit.smiltenesnovads.lv tīmekļa vietne;

☐ Attālinātā piekļuve koplietošanas resursiem;

☐ Āra interaktīvais stends;

☐ Centrālās administrācijas ēkas (Dārza ielas 3, Smiltene) durvju piekļuves sistēma;

☐ Elektroniskā iepirkumu sistēma;

☐ VISVARIS sistēma (pasvītrot nepieciešamo: NINO un NEKIP, NOMA un LIZ, BRIDZIS, SOPA, PERS, KADRI, BARIS, DZIMTS, GVEDIS, epakalpojumi.lv);

☐ Cits (_____)

Struktūrvienības vadītāja paraksts:	_____
Datums / Datums skatāms laika zīmogā	

5. PIELIKUMS
"Smiltenes novada pašvaldības
Informācijas sistēmas kiberdrošības politika"

SMILTENES NOVADA PAŠVALDĪBAS
LIETOTĀJU PIEEJAS TIESĪBU ANULĒŠANAS PIEPRASĪJUMS

Vārds, uzvārds:	
Personas kods:	
Mob. tālr.:	
E-pasts:	
Deklarētā dzīvesvietas adrese:	
Iestādes / struktūrvienības nosaukums:	
Ieņemamais amats:	
Amatpersonas statuss:	☐ ir jānosaka ☐ nav jānosaka

Lūdzu piešķirt lietotāja pieejas tiesības informācijas resursiem (atzīmēt vajadzīgo) sākot ar 202__.gada ____._____.

Informācijas resursu nosaukums (atzīmēt ar ☒ vajadzīgo):

☐ E-pasts;

☐ Pieeja pašvaldības iekšējiem datortīkla resursiem (aktīvā direktorija, failu serveris, dokumentu vadības sistēma "Namejs");

☐ Smiltenesnovads.lv tīmekļa vietne;

☐ Visit.smiltene.lv/Visit.smiltenesnovads.lv tīmekļa vietne;

☐ Attālinātā piekļuve koplietošanas resursiem;

☐ Āra interaktīvais stends;

☐ Centrālās administrācijas ēkas (Dārza ielas 3, Smiltene) durvju piekļuves sistēma;

☐ Elektroniskā iepirkumu sistēma;

☐ VISVARIS sistēma (pasvītrot nepieciešamo: NINO un NEKIP, NOMA un LIZ, BRIDZIS, SOPA, PERS, KADRI, BARIS, DZIMTS, GVEDIS, epakalpojumi.lv);

☐ Cits (_____)

Struktūrvienības vadītāja paraksts:	_____
Datums / Datums skatāms laika zīmogā	

Domes priekšsēdētājs E. Labanovskis