



LATVIJAS REPUBLIKA  
INČUKALNA NOVADA DOME

Reģ.Nr.9000068337, Atmodas iela 4, Inčukalns, Inčukalna pagasts, Inčukalna novads, LV-2141  
Tālr./fakss 67977310, mob.t. 26181294, e-pasts: dome@incukalns.lv

NOTEIKUMI  
Inčukalnā

2019.gada 22.maijā

Nr.6/2019  
protokols Nr. 8-36.§.

**Inčukalna novada pašvaldības  
Informācijas sistēmas drošības riska pārvaldības plāns**

**I. Vispārīgie jautājumi**

1. Informācijas sistēmas drošības riska pārvaldības plāns nosaka Inčukalna 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. **Inčukalna novada pašvaldība** – institūcija, kas normatīvajos aktos noteiktajā kārtībā organizē un vada informācijas sistēmu darbību.

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

2.4. **Risku pārvaldnieks** – Pašvaldības vai ārpakalpojuma darbinieks, kurš Pašvaldības normatīvajos aktos noteiktā kārtībā veic IT risku pārvaldību. Ārpakalpojuma gadījumā veicamo darbu apjomu un pienākumus nosaka ārpakalpojuma sniedzēja līguma nosacījumi.

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 Risku pārvaldnieks, nepieciešamības gadījumā pieaicinot Pašvaldības vadītāju, Pašvaldības struktūrvienību vadītājus un / vai atsevišķus Informācijas sistēmas lietotājus vai citus konsultantus.

5. Risku vadības procesa koordināciju un metodisko vadību veic Risku pārvaldnieks.

## II. Informācijas resursu risku identificēšana

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

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

8. Lietotājiem ir pienākums ziņot Risku pārvaldniekam par potenciālajiem apdraudējumiem, ievainojamībām, incidentiem, riskiem un to ietekmi.

9. Risku pārvaldnieks risku analīzi veic ikreiz, kad tiek ieviestas būtiskas izmaiņas, kas attiecas uz IS drošību, kā arī uzsākot katru IS informācijas un tehnisko resursu izstrādes, iegādes vai izmaiņu veikšanas projektu.

10. Risku pārvaldnieks katru no identificētajiem riskiem kategorizē, piešķir tam unikālu identifikatoru, kā arī veic tā iestāšanās varbūtības un ietekmes uz Pašvaldības IS drošību novērtējumu.

11. Riska iestāšanās varbūtība ir iespējamais tā iestāšanās biežums viena kalendārā gada laikā, kas tiek noteikts balstoties uz vēsturisko Pašvaldības rīcībā esošo informāciju par notikušajiem drošības incidentiem, ņemot vērā industrijas labās prakses norādes un vadlīnijas attiecībā uz konkrētu risku novērtēšanu, kā arī balstoties uz citu Pašvaldības rīcībā esošo informāciju, kas ļauj iegūt objektīvu novērtējumu attiecībā uz konkrēto risku.

12. Riska iestāšanās **varbūtību un ietekmi** novērtē trīs līmeņos, katram no tiem piešķirot novērtējumu skaitliskā izteiksmē:

13. Riska iestāšanās **varbūtība**:

13.1. Zems līmenis (0-30%);

13.2. Vidējs līmenis (31-70%);

13.3. Augsts līmenis (71-100%).

14. Riska iestāšanās gadījumā tā potenciālo seku **ietekme**:

14.1. Zems līmenis:

14.1.1. Pašvaldībai nodarītie finanšu zaudējumi nepārsniegs EUR 4000.00, vai

14.1.2. īslaicīga ietekme uz Pašvaldības pamata darbības funkciju izpildes nodrošināšanu vai pamata drošības IS funkcionalitāti, vai

14.1.3. tiks apturēta viena vai vairākas Pašvaldības pamata drošības IS uz laiku līdz 8 h.

14.2. Vidējs līmenis:

14.2.1. Pašvaldībai nodarītie finanšu zaudējumi būs robežās no EUR 4000,00 – EUR 10000.00, vai

14.2.2. negatīvi ietekmēta pamata drošības IS datu integritāte;

14.2.3. ierobežotas pieejamības informācija, kas nesatur fizisku personu sensitīvus datus, nonāks citu juridisku vai fizisku personu rīcībā, vai

14.2.4. tiks apturēta viena vai vairākas Pašvaldības pamata drošības IS uz 8-24 h, vai

14.2.5. tiks apturēta viena vai vairākas Pašvaldības paaugstinātas drošības IS uz 1h-8h.

14.3. Augsts līmenis:

14.3.1. Pašvaldībai nodarītie finanšu zaudējumi pārsniegs EUR 10000.00, vai

14.3.2. negatīvi ietekmēta paaugstinātas drošības IS datu integritāte, vai

14.3.3. ierobežotas pieejamības informācija, kas satur fizisku personu sensitīvus datus, nonāks citu juridisku vai fizisku personu rīcībā, vai

14.3.4. tiks apturēta viena vai vairākas Pašvaldības pamata drošības IS uz vairāk kā 24 h, vai

14.3.5. tiks apturēta viena vai vairākas Pašvaldības paaugstinātas drošības IS uz vairāk kā 8 h.

15. Riska iestāšanās varbūtības un atstātās ietekmes līmeņa noteikšanu uz Pašvaldības darbību veic Risku pārvaldnieks, kurš vērtējuma sagatavošanas laikā, lai nodrošinātu iespējami

pilnvērtīgākā vērtējuma veikšanu, var piesaistīt citus Pašvaldībā nodarbinātos, atbilstoši to kompetencē esošajiem darbības jautājumiem, kā arī trešo pušu pārstāvjus atzinumu un ieteikumu sniegšanai attiecībā uz konkrētiem riskiem

16. Riska iestāšanās varbūtības un atstātās ietekmes līmeņa noteikšanas iedalījums:

Ietekme \ Varbūtība	3 – Augsta	2 – Vidēja	1 – Zema
3 – Augsta	9 – Augsta	6 – Augsta	3 – Vidēja
2 – Vidēja	6 – Augsta	4 – Vidēja	2 – Zema
1 – Zema	3 – Vidēja	2 – Zema	1 – Zema

17. Pēc katra riska iestāšanās varbūtības un ietekmes līmeņa noteikšanas, nosaka kopējo riska līmeni, kuru veido iestāšanās **varbūtības un ietekmes kritēriju reizinājums**, ko novērtē šādi:

17.1. augsts riska līmenis (novērtējums ir 6 vai 9) - viens no riska novēršanas kritērijiem ir vērtēts kā augsts, bet otrs kā vidējs vai abi kritēriji ir vērtēti kā augsti;

17.2. vidējs riska līmenis (novērtējums diapazonā no 3 līdz 4) – viens no riska novērtēšanas kritērijiem ir vērtēts kā augsts, bet otrs kā zems vai arī abi kritēriji ir vērtēti kā vidēji;

17.3. zems riska līmenis (novērtējums ir 1 vai 2) – viens no riska novēršanas kritērijiem ir vērtēts kā vidējs, bet otrs kā zems.

18. Ne retāk kā reizi gadā, Risku pārvaldnieks veic visaptverošu IS drošības risku analīzi, kuras ietvaros tiek apskatīti jau iepriekš identificētie riski un veiktie pasākumi risku mazināšanai kā arī apzināti jauni, iepriekš vēl neidentificēti, riski. Risku analīzes rezultātā Risku pārvaldnieks sagatavo ziņojumu, kurā iekļauj vismaz sekojošo informāciju:

18.1. Apkopojumu par gada laikā identificētajiem riskiem (risku reģistru);

18.2. Risku pārvaldības plānu atbilstoši 2.pielikumam.

### III. Risku pārvaldība

19. Rīcību ar riskiem nosaka pamatojoties uz drošības pasākumu izmaksu un iespējamo materiālo un nemateriālo zaudējumu sabalansētību:

19.1. akceptēt risku;

19.2. novērst vai mazināt risku (piemēram, ieviešot atbilstošas kontroles);

19.3. nodot risku trešajām pusēm (piemēram, izmantojot apdrošināšanas pakalpojumus).

20. Riskus, kuru novērtējums atbilst **zemam** līmenim, Risku pārvaldnieks neiekļauj IS drošības risku pārvaldības plānā.

21. Risku pārvaldnieks IS drošības risku pārvaldības plānā iekļauj **augsta** līmeņa riskus.

22. Riskiem, kuru novērtējums atbilst **vidējam** līmenim, veic padziļinātu to izvērtēšanu, apzinot to novēršanai vai ietekmes mazināšanai nepieciešamos veicamos pasākumus un to samērību attiecībā pret attiecīgo risku:

22.1. gadījumā, ja attiecīgā riska novēršanai vai ietekmes mazināšanai nepieciešamo veicamo pasākumu izmaksas ir lielākas nekā iespējamie zaudējumi, Pašvaldības vadība lemj par riska akceptēšanu;

22.2. gadījumā, ja attiecīgā riska novēršanai vai ietekmes mazināšanai nepieciešamo veicamo pasākumu resursu ietilpība ir mazāka nekā riska iestāšanās sekas, risku iekļauj IS drošības risku pārvaldības plānā.

23. Riskiem, kuru kopējais novērtējums atbilst augstam līmenim, kā arī vidējam līmenim, Risku pārvaldnieks sagatavo veicamo pasākumu aprakstus to novēršanai vai riska iestāšanās iespējamības vai atstāto seku līmeņa mazināšanai.

24. Pēc riska novēršanai vai mazināšanai veicamo pasākumu apraksta sagatavošanas, Risku pārvaldnieks nosaka veicamo pasākumu izpildes termiņus, nepieciešamos finanšu līdzekļus,

laika un Pašvaldības nodarbināto resursus, kā arī potenciālo atbildīgo personu par veicamo pasākumu realizāciju.

25. Ja nepieciešami papildus resursi veicamo pasākumu realizācijai, piemēram, citas struktūrvienības nodarbināto resursi, Risku pārvaldnieks iesniedz IS drošības risku pārvaldības plānu apstiprināšanai Pašvaldības vadībai.

26. Ja noteiktu pasākumu veikšanai nepieciešamos finanšu vai cilvēku resursus nepiešķir vai piešķir nepietiekamā apmērā, Risku pārvaldnieks koriģē risku mazināšanas pasākumu aprakstu, nosakot veicamo pasākumu minimumu, kuru realizācija nodrošina identificētā riska iestāšanās varbūtības vai atstāto sekū līmeņa samazināšanu bez papildus finanšu resursu piesaistes vai atbilstoši pieejamajiem finanšu vai cilvēku resursiem un Risku pārvaldnieks iesniedz IS drošības risku pārvaldības plānu apstiprināšanai Pašvaldības vadībai.

#### **IV. Risku uzraudzība**

27. Risku pārvaldnieks, atbilstoši IS drošības risku pārvaldības plānā definēto veicamo pasākumu izpildes termiņiem, veic pārbaudes par risku mazināšanas vai novēršanas pasākumu realizāciju, atzīmējot realizētos pasākumus.

28. Gadījumos, kad nepieciešamie pasākumi nav tikuši realizēti iepriekš noteiktajā termiņā, Risku pārvaldnieks kopā ar personu, kura ir atbildīga par attiecīgā pasākuma realizāciju, apzina apstākļus, kas ir kavējuši attiecīgo pasākumu realizēt sākotnēji paredzētajā termiņā un sagatavo priekšlikumus jauna pasākuma realizācijas termiņa noteikšanai, kā arī nepieciešamības gadījumā nosaka papildus veicamās darbības pasākuma ieviešanas nodrošināšanai.

29. Pēc identificētā riska novēršanas vai mazināšanas veicamā pasākuma izpildes, Risku pārvaldnieks veic atkārtotu riska novērtējumu.

Domes priekšsēdētājs

Aivars Nalivaiko

1.pielikums  
2019.gada 22.maija  
Inčukalna novada domes noteikumiem Nr.6/2019  
„Inčukalna novada pašvaldības  
Informācijas sistēmas drošības riska pārvaldības plāns”

**Inčukalna novada pašvaldības informācijas resursu risku reģistrs**

<b>Nr.</b>	<b>Informācijas resursu risku nosaukums (raksturojums)</b>	<b>Varbūtība</b>	<b>Ietekme</b>	<b>Pārvaldība</b>	<b>Risku rādītājs</b>
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					

2.pielikums  
2019.gada 22.maija  
Inčukalna novada domes noteikumiem Nr.6/2019  
„Inčukalna novada pašvaldības  
Informācijas sistēmas drošības riska pārvaldības plāns”

**Inčukalna novada domes pārskats par pasākumiem risku mazināšanai un novēršanai**

<b>Nr.</b>	<b>Pasākuma apraksts</b>	<b>Termiņš</b>	<b>Atbildīgā amatpersona</b>
1.			
2.			
3.			
4.			
5.			

