

LATVIJAS REPUBLIKA

**PRIEKUĻU NOVADA PAŠVALDĪBA**

Reģistrācijas Nr. 90000057511, Cēsu prospekts 5, Priekuļi, Priekuļu pagasts, Priekuļu novads, LV-4126

www.priekuli.lv, tālr. 64107871, e-pasts: dome@priekulunovads.lv

**APSTIPRINĀTS**

Priekuļu novada domes

2020.gada 28.maija domes sēdē,

protokols Nr.10

**INFORMĀCIJAS SISTĒMAS DROŠĪBAS RISKA PĀRVALDĪBAS PLĀNS**

**I.Vispārīgie jautājumi**

1. Informācijas sistēmas drošības riska pārvaldības plāns nosaka Priekuļu novada pašvaldības (turpmāk – Pašvaldība) 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** **(IS)** – 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. **Priekuļu 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.  **Datorsistēmu un datortīklu administrators** (turpmāk - Datortīklu administrators)– 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.

2**.**5. **Informācijas tehnoloģiju administrators** - Pašvaldības vai ārpakalpojuma darbinieks, kurš Pašvaldības normatīvajos aktos noteiktā kārtībā nodrošina IS atbalsta izveidi, uzturēšanu un koordinēšanu. Ārpakalpojuma gadījumā veicamo darbu apjomu un pienākumus nosaka ārpakalpojuma sniedzēja līguma nosacījumi.

1. 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.

1. Risku vadības procesa ieviešanu un vadību veic Datortīklu administrators, nepieciešamības gadījumā pieaicinot Informāciju tehnoloģiju administratoru un / vai Pašvaldības izpilddirektoru un / vai atsevišķus Informācijas sistēmas lietotājus vai citus konsultantus.
2. Risku vadības procesa koordināciju un metodisko vadību veic Datortīklu administrators.
   * 1. **Informācijas resursu risku identificēšana**
3. 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.
   1. Datortīklu administratoram ir pienākums augstāk minētās sanāksmes laikā apkopot identificētos informāciju resursu riskus, iekļaujot tos Risku reģistrā (1. Pielikums “Informācijas resursu risku reģistrs”).
4. Lietotājiem ir pienākums ziņot Datortīklu administratoram par potenciālajiem apdraudējumiem, ievainojamībām, incidentiem, riskiem un to ietekmi.
5. Datortīklu administrators risku analīzi veic ikreiz, kad tiek ieviestas būtiskas izmaiņas, kas attiecas uz informāciju sistēmu drošību, kā arī uzsākot katru informācijas sistēmas un tehnisko resursu izstrādes, iegādes vai izmaiņu veikšanas projektu.
6. Datortīklu administrators katru no identificētajiem riskiem kategorizē, piešķir tam unikālu identifikatoru, kā arī veic tā iestāšanās varbūtības un ietekmes uz Pašvaldību informācijas sistēmām drošības novērtējumu.
7. 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.
8. Riska iestāšanās **varbūtību un ietekmi** novērtē trīs līmeņos, katram no tiem piešķirot novērtējumu skaitliskā izteiksmē.
9. Riska iestāšanās **varbūtība**:
   1. Zems līmenis - 1 (0-30%);
   2. Vidējs līmenis - 2 (31-70%);
   3. Augsts līmenis - 3 (71-100%).
10. Riska iestāšanās gadījumā tā potenciālo seku **ietekme**:
    1. Zems līmenis:
       1. Pašvaldībai nodarītie finanšu zaudējumi nepārsniegs Euro 4000.00, vai
       2. īslaicīga ietekme uz Pašvaldības pamata darbības funkciju izpildes nodrošināšanu vai pamata drošības IS funkcionalitāti, vai
       3. tiks apturēta viena vai vairākas Pašvaldības pamata drošības IS uz laiku līdz 8 h.
    2. Vidējs līmenis:
       1. Pašvaldībai nodarītie finanšu zaudējumi būs robežās no Euro 4000 - Euro 10000.00, vai
       2. negatīvi ietekmēta pamata drošības IS datu integritāte;
       3. ierobežotas pieejamības informācija, kas nesatur fizisku personu sensitīvus datus, nonāks citu juridisku vai fizisku personu rīcībā, vai
       4. tiks apturēta viena vai vairākas iestādes pamata drošības IS uz 8-24 h, vai
       5. tiks apturēta viena vai vairākas iestādes paaugstinātas drošības IS uz 1h-8h.
    3. Augsts līmenis:
       1. Pašvaldībai nodarītie finanšu zaudējumi pārsniegs Euro 10000.00, vai
       2. negatīvi ietekmēta paaugstinātas drošības IS datu integritāte, vai
       3. ierobežotas pieejamības informācija, kas satur fizisku personu sensitīvus datus, nonāks citu juridisku vai fizisku personu rīcībā, vai
       4. tiks apturēta viena vai vairākas iestādes pamata drošības IS uz vairāk kā 24 h, vai
       5. tiks apturēta viena vai vairākas iestādes paaugstinātas drošības IS uz vairāk kā 8 h.
11. Riska iestāšanās varbūtības un atstātās ietekmes līmeņa noteikšanu uz Pašvaldības darbību veic Datortīklu administrators, kurš vērtējuma sagatavošanas laikā, lai nodrošinātu iespējami pilnvērtīgāka vērtējuma veikšanu, var piesaistīt citus Pašvaldības nodarbinātos, atbilstoši to kompetencē esošajiem darbības jautājumiem, kā arī trešo pušu pārstāvjus atzinumu un ieteikumu sniegšanai attiecībā uz konkrētiem riskiem
12. 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 |

1. Pēc katra riska iestāšanās varbūtības un ietekmes līmeņa noteikšanas, nosaka kopējo riska līmeni, kuru veido iestāšanas **varbūtības un ietekmes kritēriju reizinājums,** ko novērtē šādi:
   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;
   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;
   3. zems riska līmenis (novērtējums ir 1 vai 2) – viens no riska novēršanas kritērijiem ir vērtēts kā vidējs, bet otrs kā zems.
2. Ne retāk kā reizi gadā, Datortīklu administrators 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 Datortīklu administrators sagatavo ziņojumu, kurā iekļauj vismaz sekojošo informāciju:
   1. Apkopojumu par gada laikā identificētajiem riskiem (risku reģistru);
   2. Risku pārvaldības plānu atbilstoši 2.pielikumam.

**III. Risku pārvaldība**

1. Rīcību ar riskiem nosaka pamatojoties uz drošības pasākumu izmaksu un iespējamo materiālo un nemateriālo zaudējumu sabalansētību:
   1. akceptēt risku;
   2. novērst vai mazināt risku (piemēram, ieviešot atbilstošas kontroles);
   3. nodot risku trešajām pusēm (piemēram, izmantojot apdrošināšanas pakalpojumus).
2. Riskus, kuru novērtējums atbilst **zemam** līmenim, Datortīklu administrators neiekļauj IS drošības risku pārvaldības plānā.
3. Datortīklu administrators IS drošības risku pārvaldības plānā iekļauj **augsta** līmeņa riskus.
4. 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:
   1. gadījumā, ja attiecīgā riska novēršanai vai ietekmes mazināšanai nepieciešamo veicamo pasākumu izmaksas ir lielākas nekā iespējamie zaudējumi, Pašvaldības izpilddirektors lemj par riska akceptēšanu;
   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.
5. Riskiem, kuru kopējais novērtējums atbilst augstam līmenim, kā arī vidējam līmenim, Datortīklu administrators sagatavo veicamo pasākumu aprakstus to novēršanai vai riska iestāšanās iespējamības vai atstāto seku līmeņa mazināšanai.
6. Pēc riska novēršanai vai mazināšanai veicamo pasākumu apraksta sagatavošanas, Datortīklu administrators nosaka veicamo pasākumu izpildes termiņus, nepieciešamos finanšu līdzekļus, laika un Iestādes nodarbināto resursus, kā arī potenciālo atbildīgo personu par veicamo pasākumu realizāciju.
7. Ja nepieciešami papildus resursi veicamo pasākumu realizācijai, piemēram, citas struktūrvienības nodarbināto resursi, Datortīklu administrators iesniedz IS drošības risku pārvaldības plānu apstiprināšanai Pašvaldības izpilddirektoram.

**IV. Risku uzraudzība**

1. Datortīklu administrators, atbilstoši IS drošības risku pārvaldības plānā definēto veicamo pasākumu izpildes termiņiem, veic pārbaudes par risku mazināšanas vai novēršanas pasākumu realizāciju, atzīmējot realizētos pasākumus.
2. Gadījumos, kad nepieciešamie pasākumi nav tikuši realizēti iepriekš noteiktajā termiņā, Datortīklu administrators 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.
3. Pēc identificētā riska novēršanas vai mazināšanas veicamā pasākuma izpildes, Datortīklu administrators veic atkārtotu riska novērtējumu.
4. Informācijas sistēmas drošības riska pārvaldības plāns stājas spēkā tā apstiprināšanas dienā.

Pielikumā:

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

Domes priekšsēdētāja (paraksts) Elīna Stapulone

1. PIELIKUMS

**“Priekuļu novada pašvaldības Informācijas sistēmas drošības riska pārvaldības plāns**”

**INFORMĀCIJAS RESURSU RISKU REĢISTRS**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nr. | Informācijas resursu risku | Varbūtība | Ietekme | Pārvaldība | Risku |
| nosaukums (raksturojums) | rādītājs |
|  |  |  |  |
| **1.** |  |  |  |  |  |
| **2.** |  |  |  |  |  |
| **3.** |  |  |  |  |  |
| **4.** |  |  |  |  |  |
| **5.** |  |  |  |  |  |
| **6.** |  |  |  |  |  |
| **7.** |  |  |  |  |  |
| **8.** |  |  |  |  |  |
| **9.** |  |  |  |  |  |
| **10.** |  |  |  |  |  |

2. PIELIKUMS

**“Priekuļu novada pašvaldības Informācijas sistēmas drošības riska pārvaldības plāns”**

**PĀRSKATS PAR PASĀKUMIEM RISKU MAZINĀŠANAI UN NOVĒRŠANAI**

|  |  |  |  |
| --- | --- | --- | --- |
| **Riska Nr.** | **Pasākuma apraksts** | **Termiņš** | **Atbildīgā persona** |
| 1. |  |  |  |
| 2. |  |  |  |
| 3. |  |  |  |
| 4. |  |  |  |
| 5. |  |  |  |