



BEVERĪNAS NOVADA PAŠVALDĪBA

Reģistrācijas Nr.90009115285

“Pagastmāja”, Mūrmuiža, Kauguru pag., Beverīnas nov., LV-4224, tālr. 64281737, fax 64220890, e-pasts: pasvaldiba@beverina.lv,

Beverīnas novada Kauguru pagastā

APSTIPRINĀTS

ar Beverīnas novada pašvaldības
domes 30.05.2019. sēdes lēmumu Nr.85
(protokols Nr.5, 10.§)

Beverīnas novada pašvaldības Informācijas sistēmas drošības riska pārvaldības plāns

*Izdots saskaņā Ministru kabineta 2015. gada 28. jūlija
noteikumu Nr. 442 “Kārtība, kādā tiek nodrošināta informācijas
un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības
prasībām” 8.4. punktu*

I. Vispārīgie jautājumi

1. Informācijas sistēmas drošības riska pārvaldības plāns nosaka Beverīnas 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** – 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. **Beverīnas 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 iespējamus informācijas resursu riskus.
7. Datortīklu administratoram ir pienākums augstāk minētās sanāksmes laikā apkopot identificētos informāciju resursu riskus, iekļaujot tos Risku reģistrā .

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:

10. Ietekme ir novērtējums par iespējamās situācijas (draudu) iestāšanās būtiskumu noteiktā laika periodā.
- | 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 |

iedalījumu skat. tabulā zemāk:

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 .
13. Jo lielāks ir Risku rādītājs, jo informācijas resursu riska prioritāte ir augstāka, tādējādi, 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 sanākumi 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 iespējamajos pasākumos risku mazināšanai un novēršanai.
16. Datortīklu administrators sagatavo sarakstu ar veicamajiem pasākumiem risku mazināšanai un novēršanai, nosakot atbildīgās personas un to ieviešanas terminus.

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 sanākumi pirms augstāk minētā termiņa.

Domes priekšsēdētājs..

M.Zvirbulis