ROPAŽU NOVADA PAŠVALDĪBA
Reģ. Nr. 90000067986
Institūta iela 1A, Ulbroka, Stopiņu pagasts, Ropažu novads, LV-2130
Tālr. 67910518
novada.dome@ropazi.lv
Ulbrokā

IEKŠĒJIE NOTEIKUMI

2022.gada 21.aprīlī Nr. 11

Ropažu novada pašvaldības Informācijas sistēmas drošības riska pārvaldības plāns

Izdoti saskaņā ar
Valsts pārvaldes iekārtas likuma 72.panta pirmās daļas 1.punktu,
Ministru kabineta 2015.gada 28.jūlija noteikumu Nr.442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" 8.4.apakšpunktu

I.Vispārīgie jautājumi

1. Informācijas sistēmas drošības riska pārvaldības plāns nosaka Ropažu novada pašvaldības, tās izveidotās iestādes un pašvaldības aģentūras (turpmāk – institūcija) 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. **Institūcija** - Ropažu novada pašvaldība (Centrālā administrācija), pašvaldību izveidotās iestādes un pašvaldības aģentūras.

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

2.3. **Informācijas sistēma** – strukturizēts informācijas tehnoloģiju un datu bāzu kopums, kuru lietojot tiek nodrošināta pašvaldības funkciju izpildei nepieciešamās informācijas ierosināšana, radīšana, apkopošana, uzkrāšana, apstrādāšana, izmantošana un iznīcināšana.

2.4. **Sistēmas drošības pārvaldnieks** – ar pašvaldības izpilddirektora vai institūcijas vadītāja rīkojumu iecelta persona, kura atbild par institūcijas informācijas sistēmas drošības pasākumu izstrādi, ieviešanu un uzturēšanu, kā arī rīkojas ar informācijas resursiem.

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

3. Institūcijas 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 Sistēmas drošības pārvaldnieks nepieciešamības gadījumā pieaicinot Pašvaldības vadītāju, institūcijas vadītāju, institūcijas struktūrvienību vadītājus un / vai atsevišķus Informācijas sistēmas lietotājus vai citus konsultantus.

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

II. Informācijas resursu risku identificēšana

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

7. Sistēmas drošības pārvaldniekam 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. Sistēmas drošības pārvaldnieks kopā ar pieaicinātiem dalībniekiem veic identificēto 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 institūciju
2	apdraudējumam ir vidēja ietekme uz datu subjektu un / vai institūciju
3	apdraudējumam ir liela ietekme uz datu subjektu un / vai institūciju

11. Pārvaldība ir novērtējums par esošo izveidoto personas datu apstrādes aizsardzības mehānismu, kas ļauj līdz minimumam samazināt tās trūkumu negatīvo ietekmi uz institūciju. 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. Sistēmas drošības pārvaldniekam 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 tuvākā laikā veikt pasākumus risku mazināšanai un novēršanai tā, lai Risku rādītājs nepārsniegtu pieņemamo līmeni.

IV. Informācijas resursu risku vadīšana

15. Sistēmas drošības pārvaldnieks kopā ar pieaicinātiem dalībniekiem atbilstoši Risku reģistrā iekļautajiem riskiem un to risku rādītājiem vienojas un nosaka no institūcijas puses veicamos iespējamos pasākumus risku mazināšanai un novēršanai.

16. Sistēmas drošības pārvaldnieks 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 Sistēmas drošības pārvaldnieks balstoties uz atbildīgo personu par pasākumiem risku mazināšanai un novēršanai sniegto informāciju.

18. Sistēmas drošības pārvaldniekam ir pienākums Risku reģistru un Pārskatu par pasākumiem risku mazināšanai un novēršanai iesniegt institūcijas vadītājam, kā arī regulāri informēt institūcijas vadītāju par risku mazināšanas un novēršanas veikto pasākumu norisi.

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

VI. Noslēguma jautājums

20. Ar šo noteikumu spēkā stāšanos spēku zaudē Stopiņu novada domes 2020.gada 10.februāra iekšējie noteikumi Nr.7 (apstiprināti ar Stopiņu novada domes 2020.gada 5.februāra sēdes lēmumu, prot. Nr.70, p.4.4) "Informācijas sistēmas drošības riska pārvaldības plāns".

Pielikumā:

1. Ropažu novada pašvaldības informācijas resursu risku reģistrs;
2. Ropažu novada pašvaldības pārskats par pasākumiem risku mazināšanai un novēršanai.

Ropažu novada pašvaldības izpilddirektors M.Griščenko

1.pielikums

Ropažu novada pašvaldības iekšējiem noteikumiem
"Ropažu novada pašvaldības
Informācijas sistēmas drošības riska pārvaldības plāns"

ROPAŽU NOVADA PAŠVALDĪBAS
INFORMĀCIJAS RESURSU RISKU REĢISTRS

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

2.pielikums

Ropažu novada pašvaldības iekšējiem noteikumiem
"Ropažu novada pašvaldības
Informācijas sistēmas drošības riska pārvaldības plāns"

ROPAŽU NOVADA PAŠVALDĪBAS
PĀRSKATS PAR PASĀKUMIEM RISKU MAZINĀŠANAI UN NOVĒRŠANAI

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