



BALVU NOVADA PAŠVALDĪBA BALVU NOVADA DOME

Reģ.Nr 90009115622., Bērzpils iela 1A, Balvi, Balvu novads, LV-4501,
tālrunis +371 64522453, e-pasts: dome@balvi.lv

Balvos

APSTIPRINĀTI
ar Balvu novada domes
2026.gada 17.septembra
lēmumu (prot. Nr. 20, 7.§)

NOTEIKUMI

2026.gada 17.septembrī

Nr. 9/2026

Kiberdrošības risku pārvaldības noteikumi

*Izdoti saskaņā ar Valsts pārvaldes iekārtas likuma 72.panta pirmo daļu,
Pašvaldību likuma 50.panta pirmo daļu,
Nacionālās kiberdrošības likumu,
Ministru kabineta 2024. gada 25. jūnija noteikumu Nr. 397
„Minimālās kiberdrošības prasības” 21.punktu*

1. Vispārīgie jautājumi

1.1. Balvu novada pašvaldības Kiberdrošības risku pārvaldības noteikumi (turpmāk – noteikumi) izstrādāti, pamatojoties uz Nacionālās kiberdrošības likumu un citiem Latvijas Republikā spēkā esošajiem normatīvajiem aktiem, saskaņā ar Balvu novada pašvaldības 2022.gada 24.februārī apstiprināto Informācijas drošības politiku (apstiprināta ar Balvu novada domes 2022.gada 24.februāra lēmumu Nr.6., 39.§), lai noteiktu Balvu novada pašvaldības informācijas sistēmas drošības tiesiskās, tehniskās un organizatoriskās pamatprasības, kas jāievēro Balvu novada pašvaldības informācijas sistēmu lietotājiem un citām personām, kuras ir atbildīgas par Balvu novada pašvaldības informācijas sistēmas drošību vai lieto to gan strādājot klātienē, gan attālināti.

1.2. Šo noteikumu mērķis ir noteikt kārtību, kādā Balvu novada pašvaldība īsteno informācijas tehnoloģiju un kiberdrošības risku pārvaldību, nodrošinot savlaicīgu risku identificēšanu, izvērtēšanu, mazināšanu un uzraudzību, lai aizsargātu iestādes būtiskos resursus, nodrošinātu informācijas un informācijas sistēmu konfidencialitāti, integritāti un pieejamību, kā arī veicinātu nepārtrauktu un ilgtspējīgu iestādes darbību.

1.3. Šo noteikumu izpratnē risks ir jebkurš iespējams nākotnes notikums vai apstākļu kopums, kas var negatīvi ietekmēt Balvu novada pašvaldības spēju sasniegt tam noteiktos mērķus, pildīt normatīvajos aktos noteiktās funkcijas vai nodrošināt informācijas tehnoloģiju un

Šis dokuments ir parakstīts ar drošu elektronisko parakstu un satur laika zīmogu

informācijas sistēmu drošu un nepārtrauktu darbību. Risku pārvaldības process ietver risku identificēšanu, analīzi, novērtēšanu, apstrādi un uzraudzību, un tiek piemērots kibernetikas kontekstā, lai identificētu un pārvaldītu riskus, kas saistīti ar informācijas un informācijas sistēmu konfidencialitātes, integritātes un pieejamības apdraudējumu, kā arī ar Balvu novada pašvaldībai piederošo aktīvu aizsardzību.

2. Noteikumu darbības joma

2.1. Šie noteikumi attiecas uz visām Balvu novada pašvaldības struktūrvienībām, darbiniekiem, amatpersonām un ārpakalpojumu sniedzējiem, ciktāl tie ir iesaistīti informācijas tehnoloģiju, informācijas sistēmu vai ar kibernetiku saistītu procesu īstenošanā.

2.2. Noteikumi tiek piemēroti visiem procesiem, resursiem un aktīviem, kas tiek izmantoti Balvu novada pašvaldības darbības nodrošināšanai, tostarp informācijai, informācijas sistēmām, tehnoloģiskajai infrastruktūrai un ar tām saistītajiem pakalpojumiem.

2.3. Noteikumu prasības ir saistošas neatkarīgi no informācijas sistēmu izvietojuma vietas, tehnoloģiskā risinājuma vai pārvaldības modeļa.

3. Atbildība un pienākumi kibernetikas risku pārvaldības procesā

3.1. Katrs Balvu novada pašvaldības darbinieks un amatpersona savas kompetences ietvaros ir atbildīgs par kibernetikas risku un apdraudējumu apzināšanos un šo noteikumu prasību ievērošanu ikdienas darba procesā. Konstatējot vai pamatoti pieņemot iespējamu kibernetikas apdraudējumu, par to nekavējoties tiek informēts tiešais vadītājs vai informācijas tehnoloģiju struktūrvienība turpmākai izvērtēšanai un nepieciešamo pasākumu veikšanai.

3.2. Par informācijas tehnoloģiju un kibernetikas risku pārvaldību Balvu novada pašvaldībā atbildīgais riska īpašnieks ir **datorsistēmu un datortīkla administrators**, kurš nodrošina risku pārvaldības procesa īstenošanu un koordinēšanu.

3.3. **Datorsistēmu un datortīkla administrators** ir atbildīgs par informācijas tehnoloģiju un kibernetikas risku identificēšanu, pastāvīgu uzraudzību un regulāru pārskatīšanu, kā arī par risku novērtēšanas procesa organizēšanu un risku novērtēšanas pārskatu sagatavošanu. **Datorsistēmu un datortīkla administrators** pieņem lēmumus par piemērotākajām risku pārvaldības iespējām, nodrošina efektīvu kontroles pasākumu ieviešanu risku mazināšanai un informē operacionālo direktoru par konstatētajiem riskiem un risku novērtēšanas rezultātiem.

3.4. **Atbildīgā persona** nodrošina risku pārvaldības procesa atbalstu, piešķirot nepieciešamos resursus risku pārvaldības pasākumu īstenošanai. **Atbildīgā persona** pieņem lēmumus par risku pārvaldības iespējām un riska īpašnieka noteikšanu, kā arī uzņemas atbildību par pieņemto risku pārvaldības lēmumu īstenošanu savas kompetences ietvaros.

3.5. **Kibernetikas pārvaldnieks** sniedz atbalstu datorsistēmu un datortīkla administratoram kibernetikas risku identificēšanā un risku novērtēšanas procesā, piedalās risku pārvaldības iespēju izvērtēšanā un sniedz priekšlikumus efektīvu kontroles pasākumu ieviešanai un to efektivitātes mērīšanai. Kibernetikas pārvaldnieks regulāri informē datorsistēmu un datortīkla administratoru par jauniem draudiem vai riskiem, kas var būtiski ietekmēt Balvu novada pašvaldības darbību.

4. Noteikumi par kibedrošības risku pārvaldības procesu

4.1. Balvu novada pašvaldība īsteno risku pārvaldības ietvaru, nodrošinot tā atbilstību spēkā esošajiem normatīvajiem aktiem un efektivitāti, kā arī riska vadības procesa integrāciju iestādes darbībā. Ietvars balstās uz septiņiem galvenajiem riska vadības procesa posmiem, kas definēti starptautiskā standarta ISO/IEC 27005 prasībās, un nodrošina sistemātisku risku identificēšanu, novērtēšanu, apstrādi un uzraudzību.

4.2. Lai veiktu efektīvu riska novērtēšanu, tiek noteikts ar risku saistītais konteksts, kas ļauj veikt visaptverošu novērtējumu. Šis konteksts ietver aktīvu identificēšanu un klasifikāciju, kā arī organizācijas darbības vidi, tostarp fiziskos, loģiskos, administratīvos, publiskos un iekšējos aspektus.

4.3. Riska novērtēšana ietver trīs galvenos posmus: riska identificēšanu, analīzi un kopējo izvērtēšanu. Riska identificēšanā tiek sistemātiski identificēti un kategorizēti visi potenciālie riski, kas var apdraudēt organizācijas mērķus, ņemot vērā gan iekšējos, gan ārējos faktorus. Analīzes posmā tiek izvērtēta katra riska varbūtība un ietekme uz organizāciju, izmantojot kvalitatīvu metodoloģiju un skalas no 1 līdz 5, rezultātā iegūstot riska līmeni no 1 līdz 25, kas tiek klasificēts kā zems, vidēji-zems, vidējs, vidēji-augsts vai augsts risks. Kopējā riska novērtēšanā tiek pieņemti lēmumi par to, kuri riski ir nepieņemami un prasa aktīvu risināšanu, un kuri riski ir pieņemami noteiktajās pieļaujamās robežās.

4.4. Riska apstrādes process ietver pieņemtos lēmumus un darbību plānošanu attiecībā uz identificētajiem riskiem. Katram riskam tiek noteikta apraksta forma, prioritāte, atbildīgā persona un termiņš. Datorsistēmu un datortīkla administrators nodrošina riska apstrādes plāna īstenošanu un izvērtē tā efektivitāti. Organizācija var izmantot vairākus riska apstrādes veidus, tostarp riska novēršanu, samazināšanu, nodošanu trešajai pusei, pieņemšanu vai apzinātu riska palielināšanu, vienlaikus nodrošinot normatīvo aktu un līgumsaistību ievērošanu. Visas riska apstrādes darbības tiek dokumentētas risku reģistrā, kas atrodas datorsistēmu un datortīkla administratora pārziņā, un tiek veikti nepieciešamie pasākumi, lai nepieņemamie riski tiktu mazināti.

4.5. Uzraudzība un pārskatīšana ir nepārtrauktas darbības, kas ietver plānošanu, datu vākšanu, analīzi, rezultātu dokumentēšanu un atgriezeniskās saites sniegšanu. Tās nodrošina, ka riski tiek pienācīgi kontrolēti, riska apstrādes pasākumi ir efektīvi un nepieciešamības gadījumā tiek veikti pielāgojumi, ja mainās organizācijas apstākļi vai informācija. Kiberriski tiek pārskatīti vismaz reizi pusgadā, kā arī pēc būtiskiem kiberincidentiem vai ievērojamām izmaiņām IKT infrastruktūrā.

4.6. Visos riska vadības procesa posmos tiek nodrošināta efektīva komunikācija un konsultēšanās ar iekšējām un ārējām ieinteresētajām pusēm. Šo pasākumu mērķis ir veicināt izpratni par riska vadības procesa būtību, lēmumu pamatotību un darbību nepieciešamību, kā arī iegūt atgriezenisko saiti lēmumu pieņemšanai un riska apstrādes pasākumu uzlabošanai.

5. Noslēguma jautājums

5.1. Atzīt par spēku zaudējušu Balvu novada pašvaldības Informācijas sistēmu drošības riska pārvaldības plānu, kas apstiprināts ar Balvu novada domes 2022. gada 24. februāra lēmumu "Par Informācijas sistēmu drošības riska pārvaldības plāna apstiprināšanu" (sēdes protokols Nr. 6, 41. §).

Domes priekšsēdētājs

Jānis Trupovnieks