



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, 6.§)

NOTEIKUMI

2026.gada 17.septembrī

Nr. 8/2026

Kiberdrošības incidentu 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 incidentu pārvaldības noteikumu (turpmāk – *noteikumi*) ir izdoti, 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.§). Noteikumu mērķis ir noteikt Balvu novada pašvaldības gatavību savlaicīgi atklāt, identificēt, reaģēt uz, ierobežot un atgūties no kiberdrošības incidentiem, kā arī nodrošināt vienotu un sistemātisku pieeju kiberdrošības incidentu pārvaldībai, ievērojot Latvijas Republikā spēkā esošos normatīvos aktus, tostarp Nacionālās Kiberdrošības likumu, kā arī Ministru kabineta noteikumus Nr. 397 “Minimālās kiberdrošības prasības”.

1.2. Šie noteikumi nosaka kiberdrošības incidentu identificēšanas, validācijas un klasifikācijas kārtību, veicot incidentu kategorizāciju atbilstoši to ietekmei uz Balvu novada pašvaldības informācijas sistēmām, informācijas aktīviem un darbības nepārtrauktību, kā arī paredz incidentu risināšanas prioritāšu noteikšanu un koordinētu rīcību incidentu seku un ietekmes efektīvai novēršanai.

1.3. Šo noteikumu mērķis ir reglamentēt kiberdrošības incidentu pārvaldības procesus Balvu novada pašvaldībā, tostarp:

- 1.3.1. reaģēšanu uz iespējamu vai faktisku kiberdrošības incidentu;
- 1.3.2. incidenta identificēšanu un validāciju;
- 1.3.3. kiberdrošības incidentu klasifikāciju;

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

- 1.3.4. incidenta risināšanas un seku novēršanas pasākumu īstenošanu;
- 1.3.5. eskalācijas un ziņošanas kārtību atbilstoši normatīvo aktu prasībām;
- 1.3.6. incidenta seku mazināšanas pasākumus;
- 1.3.7. digitālo pierādījumu saglabāšanu un aizsardzību;
- 1.3.8. incidenta pirmcēloņa analīzi;
- 1.3.9. pēcincidenta analīzi;
- 1.3.10. korigējošo un preventīvo darbību noteikšanu un ieviešanu.

1.4. Šajos noteikumos lietotie termini atbilst Latvijas Republikā spēkā esošajos normatīvajos aktos noteiktajai terminoloģijai, tai skaitā Nacionālās kiberdrošības likumā, Ministru kabineta noteikumos Nr. 397 un citos ar kiberdrošību un personas datu aizsardzību saistītajos normatīvajos aktos, ja šajos noteikumos nav noteikts citādi.

1.5. **Kiberdrošības incidents** – noteikts kiberdrošības notikums vai vairāku kiberdrošības notikumu kopums, kas ir izraisījis vai ar augstu varbūtību var izraisīt negatīvu ietekmi uz informācijas vai informācijas sistēmu konfidencialitāti, integritāti vai pieejamību, kā arī var ietekmēt Balvu novada pašvaldības darbības nepārtrauktību vai personas datu aizsardzību.

1.6. **Kiberdrošības notikums** – identificēts vai konstatēts gadījums, kam ir potenciāls ietekmēt kiberdrošību un kas rada risku informācijas vai informācijas sistēmu konfidencialitātes, integritātes vai pieejamības apdraudējumam, bet nav izraisījis faktisku kaitējumu vai drošības pārkāpumu.

1.7. **Pierādījumu saglabāšana** – organizēts un kontrolēts process, kura ietvaros visi ar kiberdrošības incidentu saistītie dati, žurnālfaili, sistēmu ieraksti, failu kopijas un cita būtiska informācija tiek savlaicīgi identificēta, saglabāta, aizsargāta un apstrādāta konfidenciali, nodrošinot to integritāti, nemainīgumu un pieejamību tikai pilnvarotām personām izmeklēšanas, audita, normatīvo aktu prasību izpildes un iespējamo tiesisko procedūru nodrošināšanai.

2. Noteikumu darbības joma

2.1. Šie noteikumi attiecas uz visiem Balvu novada pašvaldības darbības procesiem, ar tiem saistītajām informācijas un komunikācijas tehnoloģijām, informācijas sistēmām, digitālajiem un fiziskajiem informācijas aktīviem, kā arī uz visiem cilvēkresursiem, kas ir iesaistīti Balvu novada pašvaldības funkciju nodrošināšanā, neatkarīgi no nodarbinātības formas vai darba izpildes vietas.

2.2. Noteikumu darbības joma ir saistoša visiem Balvu novada pašvaldības digitālajiem resursiem, tostarp, bet ne tikai, informācijas sistēmām, datortehnikai, programmatūrai, lietojumprogrammām, datu bāzēm, tīkla infrastruktūrai, mākoņpakalpojumiem un datu glabāšanas risinājumiem, kā arī tiem fiziskajiem un loģiskajiem resursiem, kuru darbība vai traucējumi var būtiski ietekmēt Balvu novada pašvaldības darbības nepārtrauktību, informācijas drošību vai personas datu aizsardzību.

3. Atbildība un pienākumi kiberdrošības incidentu pārvaldības procesā

3.1. Kiberdrošības incidentu pārvaldības procesā iesaistīto personu lomas, pienākumi un atbildība tiek noteikti, lai nodrošinātu savlaicīgu, koordinētu un efektīvu kiberdrošības incidentu atklāšanu, izmeklēšanu, seku mazināšanu un atkārtotās novēršanu, ievērojot Ministru kabineta noteikumu Nr. 397 prasības.

3.2. **Datorsistēmu un datortīklu administrators** ir atbildīgs par:

3.2.1. kiberdrošības incidentu seku novēršanas pasākumu organizēšanu, īstermiņa risinājumu īstenošanu apdraudējumu samazināšanai, incidentu pirmcēloņu analīzes veikšanu un ilgtermiņa pasākumu ieviešanu atkārtotās novēršanai;

3.3. Balvu novada pašvaldības darbinieki ir atbildīgi par:

3.3.1. informācijas konfidencialitātes nodrošināšanu kiberdrošības incidentu laikā un pēc tiem;

3.3.2. ar kiberdrošības incidentiem saistīto pierādījumu saglabāšanu, aizsardzību un neizpaušanu;

3.3.3. nepieciešamā atbalsta sniegšanu kiberdrošības incidentu izmeklēšanas procesā, tai skaitā informācijas sniegšanu un resursu piešķiršanu, ciktāl tas ir attiecināms uz konkrēto darbinieku pienākumiem.

3.4. **Kiberdrošības pārvaldnieks** ir atbildīgs par:

3.4.1. kiberdrošības incidentu metriku regulāru sagatavošanu un iesniegšanu Balvu novada pašvaldības vadībai;

3.4.2. Balvu novada pašvaldības darbinieku informēšanu par kiberdrošības incidentu ziņošanas kārtību un pieejamajiem saziņas kanāliem.

3.4.3. kiberdrošības incidentu pārvaldības procesa vadību, koordinēšanu un nepārtrauktu pilnveidošanu;

3.4.4. noteikumu regulāru pārskatīšanu un aktualizēšanu, nodrošinot atbilstību Ministru kabineta noteikumu Nr. 397 prasībām un procesa efektivitātes uzlabošanu;

3.4.5. kiberdrošības incidentu regulāru analīzi un ar tiem saistīto risku izvērtēšanu atbilstoši Balvu novada pašvaldības risku reģistram;

3.4.6. kiberdrošības incidentu simulāciju organizēšanu ne retāk kā reizi gadā, iesaistot datorsistēmu un datortīkla administratoru, lai nodrošinātu sagatavotību kiberdrošības incidentu gadījumiem;

3.4.7. kiberdrošības incidentu reģistrēšanu Balvu novada pašvaldības kiberdrošības incidentu žurnālā;

3.4.8. kiberdrošības incidentu izmeklēšanu, analīzes veikšanu un kontroles pasākumu īstenošanas koordinēšanu sadarbībā ar atbildīgajām struktūrvienībām risku mazināšanai.

3.5. **Datorsistēmu un datortīklu administrators** ir atbildīgs par:

3.5.1. nepieciešamā tehniskā atbalsta sniegšanu kiberdrošības incidentu izmeklēšanas un seku mazināšanas procesā;

3.5.2. drošības kontroles pasākumu īstenošanu pirms kiberdrošības incidenta, tā laikā un pēc tā, atbilstoši normatīvo aktu un šo noteikumu prasībām.

4. Noteikumi par kiberdrošības incidentu pārvaldību

4.1. Kiberdrošības incidentu pārvaldības process Balvu novada pašvaldībā ir izstrādāts, lai nodrošinātu savlaicīgu, koordinētu un sistemātisku reaģēšanu uz visiem kiberdrošības incidentiem.

4.2. Kiberdrošības incidentu pārvaldības process ietver šādus posmus:

- 4.2.1. kiberdrošības incidenta identificēšanu;
- 4.2.2. incidenta apstiprināšanu un klasifikāciju;
- 4.2.3. eskalāciju un informācijas nodošanu atbildīgajām personām;
- 4.2.4. incidenta risināšanu un ietekmes ierobežošanu;
- 4.2.5. informācijas sistēmu un pakalpojumu atjaunošanu;
- 4.2.6. pēcincidenta analīzi un mācības.

4.3. Kiberdrošības incidenti tiek identificēti, izmantojot tehniskos drošības risinājumus un organizatoriskos pasākumus, tostarp, bet ne tikai, ielaušanās atklāšanas sistēmas, drošības informācijas un notikumu pārvaldības risinājumus, antivīrusu programmatūru, drošības operāciju centru paziņojumus, kā arī darbinieku ziņojumus.

4.4. Balvu novada pašvaldība nodrošina, ka informācijas sistēmas spēj ģenerēt notikumu žurnālus un citus datus, kas ir nepieciešami kiberdrošības incidentu savlaicīgai identificēšanai, analīzei un novēršanai.

4.5. Balvu novada pašvaldības darbiniekiem ir pienākums nekavējoties ziņot par konstatētiem vai aizdomīgiem kiberdrošības notikumiem vai incidentiem, neatkarīgi no darbinieka tehniskajām zināšanām.

4.6. Par kiberdrošības incidentiem vai notikumiem darbinieki ziņo, izmantojot šādus saziņas kanālus:

4.6.1. elektroniskā pasta adresi - dome@balvi.lv un it@balvi.lv.

4.6.2. zvanot atbildīgajai personai, datorsistēmu un datortīkla administratoram – +371-26468947;

4.7. IT vadītājs par konstatētu kiberdrošības incidentu informē Kiberdrošības pārvaldnieku.

4.8. Kiberdrošības pārvaldnieks reģistrē visus kiberdrošības incidentus Balvu novada pašvaldības kiberdrošības incidentu žurnālā.

4.9. Pēc incidenta identificēšanas tiek apkopota un saglabāta ar incidentu saistītā informācija, tostarp:

- 4.9.1. incidenta konstatēšanas datums un laiks;
- 4.9.2. incidenta notikšanas datums un laiks (ja zināms);
- 4.9.3. incidenta veida kods;
- 4.9.4. vispārīgs incidenta apraksts;
- 4.9.5. iespējamie cēloņi un kompromitēšanas indikatori;
- 4.9.6. incidenta ietekmes novērtējums;
- 4.9.7. incidenta nozīmīguma atzīme;
- 4.9.8. ziņošanas statuss kompetentajām institūcijām;
- 4.9.9. incidenta risināšanas statuss.

4.10. Kiberdrošības incidenti tiek klasificēti pēc veida, izmantojot incidentu kodus saskaņā ar šo noteikumu pielikumu.

4.11. Kiberdrošības incidenta ietekme tiek novērtēta pēc ietekmes pakāpes un nodoma.

4.12. Pēc ietekmes smaguma pakāpes incidenti tiek klasificēti kā:

- 4.12.1. kritiski;
- 4.12.2. augsti;

4.12.3. vidēji;

4.12.4. zemi.

4.13. Pēc nodoma kiberdrošības incidenti tiek iedalīti ļaunprātīgos, nejaušos vai dabiskas izcelsmes incidentos.

4.14. Datorsistēmu un datortīkla administrators un Kiberdrošības pārvaldnieks kopīgi novērtē incidenta nozīmīgumu saskaņā ar Ministru kabineta noteikumu Nr. 397 prasībām.

4.15. Visi kiberdrošības incidenti tiek apstrādāti konfidenciali, nodrošinot informācijas pieejamību tikai pilnvarotām personām.

4.16. Incidentu eskalācija tiek veikta atbilstoši incidenta ietekmes līmenim un noteiktajiem reakcijas termiņiem.

4.17. Nozīmīgu kiberdrošības incidentu gadījumā Kiberdrošības pārvaldnieks nodrošina ziņošanu CERT.LV normatīvajos aktos noteiktajos termiņos un formā, izmantojot drošu elektronisko parakstu.

4.18. Kiberdrošības pārvaldnieks koordinē pasākumus kiberdrošības incidenta novērtēšanai, izolēšanai un seku mazināšanai.

4.19. Incidenta risināšanas ietvaros var tikt ierobežota piekļuve sistēmām, atvienotas iekārtas vai apturēta datu plūsma, lai novērstu incidenta izplatīšanos.

4.20. Ar incidentu saistītie pierādījumi tiek savākti, saglabāti un aizsargāti, nodrošinot to integritāti un pieejamību izmeklēšanas vajadzībām.

4.21. Pēc incidenta ietekmes ierobežošanas tiek veikti pasākumi ietekmēto sistēmu, pakalpojumu un datu atjaunošanai.

4.22. Atjaunošanas pasākumi ietver ievainojamību novēršanu, sistēmu testēšanu, piekļuves atjaunošanu un datu atjaunošanu no rezerves kopijām.

4.23. Pēc katra kiberdrošības incidenta tiek veikta pēcincidenta analīze ne vēlāk kā piecu darbdienu laikā pēc incidenta atrisināšanas.

4.24. Analīzes rezultāti tiek dokumentēti kiberdrošības incidentu žurnālā un izmantoti preventīvo pasākumu, kontroles uzlabojumu un darbinieku apmācību plānošanai.

Domes priekšsēdētājs

Jānis Trupovnieks