



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, 5.§)

NOTEIKUMI

2026.gada 17.septembrī

Nr. 7/2026

Šifrēšanas un atslēgu 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 Šifrēšanas un atslēgu 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 šifrēšanas un šifrēšanas atslēgu pārvaldības kārtību Balvu novada pašvaldībā, nodrošinot šifrēšanas atslēgu drošību un integritāti, lai aizsargātu konfidencialus datus un informāciju pret nesankcionētu piekļuvi, izpaušanu, modificēšanu vai ļaunprātīgu izmantošanu.

2. Noteikumu darbības joma

2.1. Šie noteikumi attiecas uz visām Balvu novada pašvaldības informācijas sistēmām un tehnoloģiskajiem risinājumiem, tostarp informācijas tehnoloģiju infrastruktūru,

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

lietojumprogrammām, informācijas sistēmām, datu apstrādes un glabāšanas risinājumiem, kā arī citiem tehniskajiem līdzekļiem, kuros tiek izmantota šifrēšana vai veikta šifrēšanas atslēgu pārvaldība.

2.2. Šie noteikumi apkopo ieteicamās un labākās prakses šifrēšanas un šifrēšanas atslēgu drošai un efektīvai pārvaldībai, aptverot tehniskos, operatīvos, administratīvos un vadības procesus, un nodrošina vienotu pieeju šifrēšanas atslēgu pārvaldībai Balvu novada pašvaldībā atbilstoši iestādes darbības vajadzībām un normatīvo aktu prasībām.

3. Atbildība un pienākumi šifrēšanas un šifrēšanas atslēgu pārvaldības procesā

3.1. Šifrēšanas un šifrēšanas atslēgu pārvaldības procesā iesaistīto personu lomas un pienākumi tiek noteikti, lai nodrošinātu šifrēšanas risinājumu un atslēgu pārvaldības prasību savlaicīgu, nepārtrauktu un efektīvu ieviešanu, uzturēšanu un uzraudzību Balvu novada pašvaldībā.

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

3.2.1. šifrēšanas un šifrēšanas atslēgu pārvaldības prasību ieviešanu Balvu novada pašvaldībā;

3.2.2. šifrēšanas atslēgu izveidi, glabāšanu, izplatīšanu, atjaunošanu un drošu iznīcināšanu atbilstoši šiem noteikumiem un informācijas drošības prasībām.

3.3. **Atbildīgā persona** ir atbildīga par:

3.3.1. šifrēšanas noteikumu ievērošanas nodrošināšanu Balvu novada pašvaldībā;

3.3.2. šifrēšanas un šifrēšanas atslēgu pārvaldības procesu apstiprināšanu un to atbilstības nodrošināšanu informācijas drošības prasībām;

3.3.3. **Datorsistēmu un datortīkla administratora** darba koordinēšanu šifrēšanas risinājumu ieviešanā, uzturēšanā un uzraudzībā;

3.3.4. lēmumu par resursu piešķiršanu šifrēšanas risinājumu ieviešanai un uzturēšanai saskaņošanu ar Balvu novada pašvaldības vadību.

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

3.4.1. konsultāciju sniegšanu informācijas tehnoloģiju vadītājam par izmantojamajām kriptogrāfijas metodēm, algoritmiem un šifrēšanas risinājumiem;

3.4.2. šifrēšanas un šifrēšanas atslēgu pārvaldības procesā konstatēto trūkumu un drošības rādītāju izvērtēšanu, kā arī koriģējošo un preventīvo pasākumu izstrādi un ierosināšanu, ja tas nepieciešams.

4. Noteikumi par šifrēšanu un šifrēšanas atslēgu pārvaldību

4.1. Balvu novada pašvaldība nodrošina datu aizsardzību, izmantojot šifrēšanu datu glabāšanas un apstrādes laikā, kā arī datu pārraides procesā, lai novērstu nesankcionētu piekļuvi, datu izpaušanu vai ļaunprātīgu izmantošanu.

4.2. Datu šifrēšanas noteikumi datu miera stāvoklī ir sekojoši:

4.2.1. Darbstacijām, serveriem un pārnēsājamiem datu nesējiem, kuros tiek glabāti vai apstrādāti Balvu novada pašvaldības dati, ir jābūt aizsargātiem ar šifrēšanas risinājumiem;

4.2.2. Windows operētājsistēmas ierīcēs pēc iespējas tiek izmantota pilna diska šifrēšana, izmantojot BitLocker, visiem iekšējiem cietajiem diskkiem (HDD/SSD);

4.2.3. MacOS operētājsistēmas ierīcēs pēc iespējas tiek izmantota FileVault pilna diska šifrēšana visiem iekšējiem cietajiem diskem (HDD/SSD);

4.2.4. Ārējie datu nesēji (tostarp USB zibatmiņas, ārējie HDD un SSD diskī), kuros tiek glabāti Balvu novada pašvaldības dati, tiek šifrēti, izmantojot iestādes apstiprinātus šifrēšanas rīkus;

4.2.5. Nešifrētu ārējo datu nesēju izmantošana Balvu novada pašvaldības darbībā ir aizliegta;

4.2.6. Pārvadājot vai nododot ārējās atmiņas ierīces, ir jānodrošina, ka tās ir pilnībā šifrētas, un, ja iespējams, papildus jāizmanto paroles aizsardzība vai citi drošības risinājumi, tostarp šifrēti konteineri vai arhīvi;

4.2.7. Šifrēšanas risinājumi tiek pārvaldīti centralizēti, un lietotājiem nav tiesību patvaļīgi deaktivizēt, apiet vai mainīt šifrēšanas iestatījumus.

4.3. Datu šifrēšanas noteikumi datu pārraides laikā ir sekojoši:

4.3.1. Visām informācijas sistēmām, lietojumprogrammām un pakalpojumiem, kas nodrošina datu pārraidi tīklā, ir jāizmanto droša šifrēšana, balstoties uz atbalstītām un drošām tehnoloģijām;

4.3.2. Tīkla savienojumos pēc iespējas tiek izmantota vismaz TLS 1.2 vai jaunāka protokola versija; nedrošu vai novecojušu protokolu (tostarp SSL, TLS 1.0 un TLS 1.1) izmantošana nav pieļaujama, izņemot gadījumus, kad ir saņemta informācijas tehnoloģiju vadītāja rakstiska atļauja;

4.3.3. Virtuālo privāto tīklu (VPN) risinājumi tiek konfigurēti atbilstoši atzītajām kriptogrāfijas labās prakses rekomendācijām, nodrošinot drošu šifrēšanu, drošus atslēgu apmaiņas algoritmus un stipru autentifikāciju;

4.3.4. Konfidencialas vai sensitīvas informācijas apmaiņa elektroniskā pasta saziņā tiek veikta, izmantojot šifrēšanu, lai nodrošinātu informācijas konfidencialitāti, integritāti un autentiskumu;

4.3.5. Savienojumos ar trešo pušu pakalpojumiem un integrācijām, tostarp API un datu apmaiņas kanāliem, ir jāizmanto tikai droši protokoli ar atbilstošu šifrēšanu;

4.3.6. Nešifrētu vai nedrošu protokolu, tostarp HTTP, FTP un Telnet, izmantošana ir aizliegta;

4.3.7. Visi izmantotie šifrēšanas mehānismi tiek regulāri pārskatīti un, ja nepieciešams, atjaunināti, lai nodrošinātu atbilstību aktuālajām informācijas drošības prasībām un labākajai praksei.

4.4. Šifrēšanas atslēgu pārvaldības noteikumi ir sekojoši:

4.4.1. Balvu novada pašvaldībā tiek nodrošināta droša autentifikācijas un šifrēšanas atslēgu pārvaldība visā to dzīves ciklā;

4.4.2. Visi piekļuves marķieri, kriptogrāfijas atslēgas, API atslēgas un paroles tiek glabātas tikai iestādes apstiprinātā paroļu un atslēgu glabātuvē;

4.4.3. Piekļuves datu un šifrēšanas atslēgu iekļaušana lietojumprogrammu pirmkodos, konfigurācijas failos vai skriptos kā brīvi pieejamas vērtības ir aizliegta;

4.4.4. Šifrēšanas atslēgas lietojumprogrammās tiek nodrošinātas, izmantojot vides mainīgos vai līdzvērtīgus drošus mehānismus, un nepieciešamības gadījumā tiek izmantoti droši pieprasījumi atslēgu iegūšanai;

4.4.5. Piekļuves datu izmantošana lietojumprogrammās vai skriptos ir pieļaujama tikai ar drošu mehānismu palīdzību, kas nodrošina datu aizsardzību pret nesankcionētu piekļuvi;

4.4.6. Piekļuve šifrēšanas atslēgām un piekļuves marķieriem tiek piešķirta tikai autorizētiem lietotājiem vai sistēmu procesiem, ievērojot nepieciešamības zināt principu;

4.4.7. Šifrēšanas atslēgas un piekļuves marķieri tiek regulāri pārskatīti un nekavējoties mainīti gadījumos, kad pastāv aizdomas par to kompromitāciju vai ir konstatēts drošības incidents.

Domes priekšsēdētājs

Jānis Trupovnieks