ROPAŽU NOVADA PAŠVALDĪBA
Reģ. Nr. 90000067986
Institūta iela 1A, Ulbroka, Stopiņu pagasts, Ropažu novads, LV-2130
Tālr. 27885518
novada.dome@ropazi.lv
Ulbrokā

IEKŠĒJIE NOTEIKUMI

15.10.2026. Nr. 1.1-3/26/84

Kiberdrošības politika

Izdota saskaņā ar
Valsts pārvaldes iekārtas likuma 72. panta pirmās daļas 1. punktu,
Ministru kabineta 2025. gada 25. jūnija noteikumu Nr. 397 "Minimālās kiberdrošības prasības"
28. punktu

1.Vispārīgie jautājumi

1.1. Organizācijas raksturojums:

1.1.1. Ropažu novada pašvaldība (turpmāk - Pašvaldība) izveidota 2021. gada 1. jūlijā administratīvi teritoriālās reformas rezultātā. Ropažu novadā atrodas Stopiņu pagasts, kurā ir novada administratīvais centrs - Ulbroka, Ropažu pagasts, Garkalnes pagasts un Vangažu pilsēta.

1.1.2. Pašvaldība ir atvasināta publiska persona, kurai ir iedzīvotāju ievēlēta lēmējinstitūcija – dome. Tā darbojas savas administratīvās teritorijas iedzīvotāju interesēs un patstāvīgi nodrošina likumos noteiktās funkcijas un pakalpojumus. Pašvaldība atbild par domes un pašvaldības administrācijas darbību.

1.2. Politikas mērķis:

1.2.1. Kiberdrošības politika (turpmāk - Politika) nosaka vienotas prasības un pārvaldības principus, kādos Pašvaldība, Pašvaldības izveidotās iestādes, t.sk., Pašvaldības policija (turpmāk - Policija) nodrošina izmantoto aktīvu aizsardzību pret ārējiem un iekšējiem kiberriskiem. Politika nosaka veidus, kādos tiek nodrošināta aktīvu pieejamība, integritāte un konfidencialitāte, kā arī pašvaldības funkciju un sniegto pakalpojumu nepārtrauktību.

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

1.3. Politikas piemērojamība un mērķauditorija:

1.3.1. Politika attiecas uz Pašvaldības struktūrvienībām, tostarp Policiju, darbiniekiem, citām personām un ārpakalpojumiem, kā arī pašvaldības izveidotām iestādēm, kuras izmanto pašvaldības valdījumā un/vai īpašumā esošos Informācijas, Informācijas un komunikācijas tehnoloģiju (turpmāk - IKT) un atbalsta aktīvus.

1.3.2. Šīs Politikas izpratnē termins "Pašvaldība" ietver pašvaldības domi, pašvaldības administrāciju, Centrālo administrāciju, pašvaldības iestādes, tostarp Policiju, kā arī citas pašvaldības pakļautībā esošās iestādes. Gadījumos, kad normatīvie akti Pašvaldību un Pašvaldības policiju nosaka kā atsevišķus kiberdrošības subjektus, šajā Politikā noteiktās prasības piemērojamas katram no tiem atsevišķi, ciktāl normatīvie akti nenosaka citādi.

1.4. Ieinteresētās puses:

1.4.1. Ieinteresētās puses ir visas personas, institūcijas vai organizācijas, kuras ietekmē vai kuras tiek ietekmētas no pašvaldības darbības, pakalpojumiem un lēmumiem.

1.4.2. Iekšējās ieinteresētās puses:

1.4.2.1. Pašvaldības deputāti – pieņem politiskos un stratēģiskos lēmumus;

1.4.2.2. Pašvaldības administrācija un darbinieki – īsteno pakalpojumu sniegšanu un pārvaldi;

1.4.2.3. Izglītības, kultūras un sporta iestādes – skolas, bibliotēkas, muzeji, sporta zāles;

1.4.3. Ārējās ieinteresētās puses:

1.4.3.1. Pašvaldības iedzīvotāji;

1.4.3.2. Uzņēmēji un investori;

1.4.3.3. Sabiedriskās organizācijas un biedrības;

1.4.3.4. Valsts institūcijas;

1.4.3.5. Citas pašvaldības un pilsētas.

2.Normatīvais un metodiskais ietvars

2.1. Nacionālais kiberdrošības likums:

2.1.1. Šī Politika ir izstrādāta saskaņā ar Nacionālās kiberdrošības likumu (turpmāk - NKL), ņemot vērā Pašvaldības un pašvaldības Policijas statusus kā Būtisko pakalpojumu sniedzējiem. NKL nosaka pienākumus kiberdrošības pārvaldības, risku vadības un incidentu ziņošanas jomā, kurus pašvaldība īsteno, ievērojot šo politiku.

2.2. Ministru kabineta noteikumi Nr. 397 "Minimālās kiberdrošības prasības":

2.2.1. Šī politika ir izstrādāta, ievērojot Ministru kabineta noteikumos Nr. 397 "Minimālās kiberdrošības prasības" (turpmāk - MK397) noteiktās IKT drošības prasības.

2.3. Citi piemērojamie normatīvie akti un standarti:

2.3.1. Politika ir izstrādāta, ievērojot arī citus piemērojamos normatīvos aktus, kas regulē informācijas drošību, personas datu aizsardzību un IKT izmantošanu. Personas datu apstrādes drošība tiek nodrošināta atbilstoši Vispārīgā datu aizsardzības regulas (Eiropas Parlamenta un Padomes regulai Nr. 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko

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

atceļ Direktīvu 95/46/EK) un Fizisko personu datu apstrādes likuma prasībām. Kiberdrošības pārvaldības sistēma tiek veidota, balstoties uz standarta ISO/IEC 27001 "Informācijas drošības pārvaldības sistēmas" principiem, nodrošinot sistemātisku pieeju drošības risku identificēšanai, novērtēšanai, apstrādei un uzraudzībai. Pašvaldības darbības nepārtrauktības plānošana un kritisko pakalpojumu atjaunošana tiek organizēta saskaņā ar standarta ISO 22301:2019 „Drošība un noturība. Darbības nepārtrauktības pārvaldības sistēmas principiem. Savukārt kiberdrošības incidentu pārvaldība un dokumentēšana balstās uz standarta ISO/IEC 27001 „Informācijas drošības pārvaldības sistēmas" prasībām. Gadījumos, kad pašvaldībā tiek izstrādātas vai izmantotas mākslīgā intelekta sistēmas (turpmāk - MI), to ieviešana un izmantošana tiek organizēta atbilstoši Eiropas Savienības Mākslīgā intelekta akta prasībām.

2.4. Kiberdrošības pārvaldības dokumentācijas arhitektūra:

2.4.1. Šī Politika kalpo par pamatu šī punkta apakšpunktos minētajiem noteikumiem un procedūrām, kas detalizē kiberdrošības prasību praktisko ieviešanu:

2.4.1.1. Informācijas, IKT un atbalsta aktīvu pārvaldības noteikumi – nosaka kārtību, kādā tiek identificēti, uzskaitīti un pārvaldīti uz IKT attiecināmie aktīvi;

2.4.1.2. IKT drošības riska vadības noteikumi – nosaka kārtību, pēc kuras tiek identificēti un novērtēti kiberdrošības riski;

2.4.1.3. Piekļuves tiesību un lietotāju identitātes pārvaldības noteikumi – nosaka kārtību lietotāju kontu izveidei, tiesību piešķiršanai un uzraudzībai;

2.4.1.4. IKT lietotāju kiberdrošības noteikumi – praktiska instrukcija katram darbiniekam par drošu darba vides, e-pasta un interneta lietošanu;

2.4.1.5. IKT resursu un informācijas sistēmu drošības pārvaldības noteikumi – nosaka obligātās kiberdrošības prasības attiecībā uz sistēmu un IKT resursu pārvaldību;

2.4.1.6. Kiberdrošības incidentu pārvaldības noteikumi – nosaka, kā tiek atklāti un apstrādāti kiberincidenti;

2.4.1.7. IKT darbības nepārtrauktības un atjaunošanas plāna vadlīnijas – nosaka vienotu pieeju darbības nepārtrauktības plānu izstrādei;

2.4.1.8. Ārpakalpojumu sniedzēju kiberdrošības prasību noteikumi – definē minimālos drošības prasības ārpakalpojumiem.

2.4.2. Kiberdrošības pārvaldības ietvaros tiek uzturēti un regulāri aktualizēti šī punkta apakšpunktos minētie operatīvie dokumenti:

2.4.2.1. Kiberdrošības lomu un atbildības matrica – vienots pārskats par katras puses atbildību kiberdrošības procesos;

2.4.2.2. Informācijas sistēmu un IKT resursu katalogs - satur detalizētu informāciju par visām informācijas sistēmām un resursiem, to klasēm, īpašniekiem, turētājiem un administratoriem;

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

2.4.2.3. Iekšējo IKT resursu un atbalsta aktīvu katalogs – ietver pašvaldības īpašumā un valdījumā esošos Informācijas, IKT un IKT atbalsta aktīvus, to tehniskos parametrus, atrašanās vietas un dzīves cikla informāciju;

2.4.2.4. Kiberdrošības risku reģistrs – dokumentē visus identificētos riskus, to līmeņus, izvēlētos apstrādes veidus un atbildīgās personas;

2.4.2.5. Apmācību reģistrs – nodrošina visu nodarbināto un IKT personāla veikto instruktāžu, apmācību un novērtējuma rezultātu uzskaiti;

2.4.2.6. Darbības ietekmes analīze (turpmāk - BIA) – apkopo informāciju par pakalpojumu kritiskumu, maksimāli pieļaujamajiem pārtraukuma laikiem un atjaunošanas prioritātēm;

2.4.2.7. Kiberincidentu reģistrs – nodrošina visu notikušo incidentu uzskaiti, to analīzi un novēršanas gaitu;

2.4.2.8. IKT darbības nepārtrauktības plāni ar pielikumiem;

2.4.2.9. Informācijas sistēmas lietošanas noteikumi;

2.4.2.10. Ārpakalpojumu sniedzēju kiberdrošības prasību matrica.

3. Kiberdrošības pārvaldības principi

3.1. Riskos balstīta pieeja:

3.1.1. Kiberdrošības pasākumi tiek plānoti un īstenoti, balstoties uz kiberdrošības risku izvērtējumu. Riska līmenis tiek noteikts, ņemot vērā apdraudējumu iespējamību, iespējamo ietekmi uz pašvaldības informācijas sistēmām un pakalpojumu nepārtrauktību.

3.1.2. Drošības pasākumi tiek izvēlēti proporcionāli identificētajam riskam un regulāri pārskatīti.

3.1.3. Kiberdrošības lēmumi tiek pieņemti, nodrošinot, ka drošības pasākumi ir samērīgi ar identificētajiem kiberdraudiem un pašvaldības sniegto pakalpojumu kritiskumu.

3.2. Atbildības un pilnvaru sadalījums:

3.2.1. Kiberdrošības pārvaldībā ir nodalītas lomas, atbildības un pilnvaras starp Domi, Izpilddirektoru, Kiberdrošības pārvaldnieku, IT atbalsta nodaļu, Pašvaldības Iestāžu, Pašvaldības pārvalžu un nodaļu vadītājiem, Pašvaldības darbiniekiem un ārējiem pakalpojumu sniedzējiem un sadarbības partneriem. Katra iesaistītā puse ir atbildīga par tai noteikto pienākumu izpildi atbilstoši šai Politikai un saistītajiem iekšējiem dokumentiem. Lai nodrošinātu nepārprotamu un skaidru pienākumu sadali galvenajos kiberdrošības pārvaldības procesos, tiek piemērota Kiberdrošības lomu un atbildības matrica (RACI matrica).

3.3. Mākslīgā intelekta pārvaldības princips:

3.3.1. Mākslīgā intelekta (turpmāk – MI) sistēmas tiek ieviestas un lietotas nodrošinot atbilstību Eiropas Savienības Mākslīgā Intelekta aktam. MI izmantošanā prioritāte ir datu drošībai, caurskatāmībai un cilvēka veiktai uzraudzībai.

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

4. Lomas un atbildības

4.1. Dome iezīmē kiberdrošības attīstības virzienu un piešķir stratēģisko finansējumu.

4.2. Izpilddirektors nodrošina kiberdrošības pārvaldības ieviešanu, apstiprina politikas un noteikumus. Nodrošina nepieciešamos resursus kiberdrošības pasākumu īstenošanai.

4.3. Lietotāji ievēro šajā Politikā un saistītajos iekšējos dokumentos noteiktās kiberdrošības prasības un nekavējoties ziņo par aizdomīgiem notikumiem vai incidentiem.

4.4. Ārpakalpojumu sniedzēji ievēro pašvaldības noteiktās kiberdrošības prasības un līgumā noteiktos pienākumus.

5. Kiberdrošības pārvaldības cikls

5.1. Kiberdrošības pasākumi tiek plānoti, balstoties uz risku izvērtējumu, normatīvo aktu prasībām un pašvaldības pakalpojumu nepārtrauktības nodrošināšanu.

5.2. Plānotie kiberdrošības pasākumi tiek ieviesti atbilstoši noteiktajām atbildībām un apstiprinātajiem iekšējiem dokumentiem. Ieviešana un izpilde tiek uzraudzīta.

5.3. Kiberdrošības pārvaldība tiek regulāri pārskatīta un uzlabota, ņemot vērā uzraudzības rezultātus, incidentu analīzi un izmaiņas risku vidē.

6. Darbības ietekmes analīze

6.1. Darbības ietekmes analīzes mērķis ir noteikt pašvaldības sniegto pakalpojumu kritiskumu, izvērtējot to pārtraukuma iespējamo ietekmi uz sabiedrību, normatīvo prasību izpildi, finanšu stabilitāti, reputāciju un pašvaldības darbības nepārtrauktību.

6.2. BIA rezultāti tiek izmantoti:

6.2.1. IKT resursu un informācijas sistēmu kritiskuma noteikšanai;

6.2.2. kiberdrošības risku izvērtēšanai;

6.2.3. darbības nepārtrauktības un atjaunošanas plānošanai.

6.3. BIA tiek veikta visiem pašvaldības sniegtajiem pakalpojumiem, kā arī iekšējām funkcijām, kuru darbības pārtraukums var ietekmēt pakalpojumu sniegšanu.

7. Risku izvērtējums

7.1. Kiberdrošības risku izvērtējums tiek veikts, lai identificētu, analizētu un novērtētu riskus, kas var ietekmēt Pašvaldības informācijas, IKT un atbalsta aktīvu konfidencialitāti, integritāti, pieejamību, kā arī Pašvaldības sniegto pakalpojumu nepārtrauktību.

7.2. Risku izvērtēšana tiek īstenota, ņemot vērā pakalpojumu kritiskumu, BIA rezultātus, informācijas sistēmu un IKT resursu kritiskumu, identificētos draudus un ievainojamības.

8. Politikas ieviešana un uzraudzība

8.1. Šī Politika stājas spēkā pēc tās apstiprināšanas un ir saistoša visām iesaistītajām pusēm. Politikas ieviešanu nodrošina pašvaldības izpilddirektors, atbildīgās struktūrvienības un darbinieki. Politikas ievērošana tiek regulāri uzraudzīta un kontrolēta.

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

9. Atbildība par Politikas neievērošanu

9.1. Par Politikas neievērošanu personas tiek sauktas pie atbildības atbilstoši spēkā esošajiem Pašvaldības un Latvijas Republikas normatīvajiem aktiem.

10. Politikas pārskatīšana un aktualizēšana

10.1. Politika tiek regulāri pārskatīta un, ja nepieciešams, aktualizēta, ņemot vērā normatīvo aktu izmaiņas, risku izvērtējuma rezultātus un kiberdrošības incidentus.

11. Noslēguma jautājums

11.1. Ar šīs Politikas spēkā stāšanos spēku zaudē Ropažu novada pašvaldības iekšējie normatīvie akti: Nr. 8 "Informācijas sistēmas drošības politika" (Reģ. 26.04.2022., Nr. 1.3/22/8), Nr. 9 "Informācijas sistēmas drošības noteikumi" (Reģ. 26.04.2022., Nr. 1.3/22/9), Nr. 10 "Informācijas sistēmas lietošanas noteikumi" (Reģ. 26.04.2022., Nr. 1.3/22/10), Nr. 11 "Informācijas sistēmas drošības riska pārvaldības plāns" (Reģ. 26.04.2022., Nr. 1.3/22/11), Nr. 12 "Informācijas sistēmas darbības atjaunošanas plāns" (Reģ. 26.04.2022., Nr. 1.3/22/12).

Pašvaldības izpilddirektors Jānis Belkovskis

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