

Projekts uz 03.03.2023.

Vēlamais izskatīšanas laiks:

Finanšu komitejā 15.03.2023.

domē 22.03.2023.

Ziņotājs: Māris Lazdiņš

APSTIPRINĀTI

Ādažu novada pašvaldības domē

2023. gada 22. martā (protokols Nr. \_\_ § \_\_)

NOTEIKUMI

Ādažos, Ādažu novadā

2023. gada 22. martā  **Nr. X/2023**

**Ādažu novada pašvaldības informācijas sistēmu darbības atjaunošanas plāns**

*Izdoti saskaņā ar Ministru kabineta 20.07.2015.*

*noteikumu Nr. 442 „Kārtība, kādā tiek nodrošināta*

*informācijas un komunikācijas tehnoloģiju sistēmu*

*atbilstība minimālajām drošības prasībām”*

*8. un 11. un 33. punktu*

**I. Vispārīgi jautājumi**

1. Šie noteikumi ietver kārtību, kādā Ādažu novada pašvaldība (turpmāk – Pārzinis), kā arī tās struktūrvienības un iestādes (turpmāk – institūcijas) nodrošina izmantoto informācijas sistēmu atjaunošanu darbības traucējumu gadījumā uz institūciju serveriem.
2. Noteikumos lietotie termini:
   1. **par tehniskajiem resursiem atbildīgā persona** – Pārziņa atbildīgā persona, kurai ar amata aprakstu uzticēta atbildība par informācijas tehnoloģiju resursiem un to drošību (Informācijas tehnoloģijuadministrators);
   2. **informācijas sistēma** (turpmāk - IS) – strukturizēts informācijas tehnoloģiju un datu bāzu kopums, kas nodrošina Pārziņa funkciju izpildei nepieciešamās informācijas ierosināšanu, radīšanu, apkopošanu, uzkrāšanu, apstrādāšanu, izmantošanu un iznīcināšanu;
   3. **IS tehniskie resursi –** serveri, tīkla aparatūra, komunikāciju līnijas un citi tehniskie līdzekļi, ko izmanto informācijas uzglabāšanai un apritei;
   4. **IS informācijas resursi** – datu faili, datu bāzes, arhīvi, u.c. informācija;
   5. **IS lietotājs** **–** persona, kurai darba pienākumu veikšanai piešķirta datortehnika un piekļuves tiesības darbam Pārziņa IS;
   6. **IS ārējie lietotāji** – personas, kurām ir tiesisks pamats un nodrošinātas tehniskas iespējas piekļūt Pārziņa IS;
   7. **drošības incidents** - jebkāds kaitīgs notikums vai nodarījums, kura rezultātā tiek vai var tikt ietekmēta IS integritāte, konfidencialitāte un pieejamība;
   8. **risks** - varbūtība, ka īstenojoties drošības apdraudējumam, Pārziņa informācijas vai tehniskie resursi varētu mainīties, sabojāties, tikt iznīcināti vai nonākt tādu personu rīcībā, kuras nav tam pilnvarotas, vai piekļūšana informācijas resursiem varētu būt traucēta, vai neiespējama;
   9. **integritāte** - nesankcionēta lietotāja veiktās informācijas izmaiņas nav iespējamas (vai vismaz ir atklātas), un autorizēto lietotāju veiktās izmaiņas tiek izsekotas;
   10. **konfidencialitāte** - informāciju redz un izmanto tikai personas, kurām tas atļauts;
   11. **auditācijas pieraksti** – analīzei pieejami pieraksti, kuros reģistrēti dati par konkrētiem IS notikumiem (piekļuve, datu ievade, maiņa, dzēšana, izvade, u.c.);
3. Šo noteikumu mērķis ir nodrošināt Pārziņa darbības turpināšanu, iespējamo zaudējumu minimizēšanu un saistību izpildi gadījumos, ja IS darbība ir traucēta ārēju vai iekšēju faktoru gadījumā (piemēram, IS tehniskie bojājumi, personāla kļūdas, ļaunprātīga rīcība, datu pārraides sistēmu bojājumi, elektrības padeves traucējumi, ugunsgrēks, plūdi, daļēji vai pilnīgi telpu postījumi, u.tml.).
4. Pārziņa vadība veic pārraudzību par darbības atjaunošanas plānošanu, piešķirot nepieciešamos personāla, tehnoloģiskos un finanšu resursus.
5. IS darbības atjaunošanas plāns ir saistošs par tehniskajiem resursiem atbildīgai personai**,**  ITN un datu aizsardzības speciālistam.

# II. Darbības traucējuma identificēšana

1. Īslaicīgs IS darbības traucējums ir situācija, ja tiek pārtraukta vai daļēji pārtraukta IS darbība līdz 2 stundām. Identificējot šo traucējumu, ITN ir saprotami traucējuma iemesli, un ir pamatota pārliecība, ka traucējums tiks novērsts 2 stundu laikā.
2. Ilglaicīgs darbības traucējums ir situācija, ja tiek pārtraukta vai daļēji pārtraukta IS darbība vairāk par 2 stundām. Identificējot šo traucējumu, ITN ir saprotami darbības traucējumu iemesli, apzinoties, ka novēršanai būs nepieciešams ilgāks laiks par 2 stundām.
3. IS darbības traucējums var pilnīgi vai daļēji pārtraukt Pārziņa un institūciju funkciju veikšana, un to var nebūt iespējams atjaunot nepieciešamajā apjomā un kvalitātē.

# III. Veicamie pasākumi pēc IS fiziska apdraudējuma drošības incidenta

1. Vispirms jānosaka, vai situācijas bīstamība prasa arī personāla evakuāciju un nekavējoties jāinformē Pārziņa vadība.
2. ITN pēc darbības traucējuma identificēšanas informē par darbības traucējumu iesaistītos Pārziņa un piekritīgo institūciju darbiniekus.
3. Rīcība atsevišķos ārkārtas situāciju gadījumos:
   1. ugunsgrēka trauksmes, atklātas uguns vai piedūmojuma gadījumā jārīkojas atbilstoši noteikumiem „Rīcības plāns ugunsgrēka gadījumā”;
   2. serveri elektroapgādes traucējumu gadījumiem ir pieslēgti pie nepārtrauktās barošanas avotiem (turpmāk - UPS);
   3. ilgstošu elektroapgādes pārtraukumu gadījumā ITN dod nepieciešamos norādījumus turpmākajām darbībām ar IS resursiem.

# IV. Sistēmas darbības atjaunošanas pasākumi

1. Ja pēc drošības incidenta ir pieejamas minimālās un daļa no pārējām funkcijām:
   1. tiek veikta IS incidenta analīze;
   2. tiek noteikti, izvērtēti un iesviesti nepieciešamie uzlabojumi.
2. Ja pēc drošības incidenta pieejamas tikai minimālās funkcijas:
   1. tiek veikta IS incidenta analīze;
   2. tiek veikti pasākumi pārējo funkciju darbības atjaunošanai;
   3. tiek noteikti, izvērtēti un ieviesti nepieciešamie uzlabojumi.
3. Ja pēc drošības incidenta IS funkcijas nav pieejamas:
   1. tiek veikti pasākumi minimālo funkciju darbības atjaunošanai;
   2. tiek veikta IS incidenta analīze;
   3. tiek veikti pasākumi pārējo funkciju darbības atjaunošanai;
   4. tiek noteikti, izvērtēti un ieviesti nepieciešamie uzlabojumi.
4. IS bojājumu novērtējumu veic informācijas resursu un tehnisko resursu  
   valdītāji.
5. Lēmumu par IS atjaunošanu var pieņemt:
   1. pašvaldības izpilddirektors;
   2. par tehniskajiem resursiem atbildīgā persona;
   3. tehnisko resursu valdītājs (IS īpašnieks).
6. Par tehniskajiem resursiem atbildīgā persona nodrošina:
   1. atjaunošanas vietas noteikšanu;
   2. nepieciešamo resursu identificēšanu;
   3. rezerves kopiju un sistēmas instalēšanas datu iegūšanu;
   4. tehnisko resursu atjaunošanu;
   5. tehnisko resursus darbības pārbaudi;
   6. IS informācijas resursu atjaunošanu;
   7. IS informācijas resursu integritātes pārbaudi.

# V. IS darbības atjaunošanas pasākumi

1. Ja nepieciešams, par tehniskajiem resursiem atbildīgā persona izveido Negadījumu seku novēršanas un atjaunošanas grupu.
2. Negadījumu seku novēršanas un atjaunošanas grupa:
   1. pieņem lēmumu par konkrētām reaģējošām darbībām negadījumu seku novēršanai;
   2. novērtē telpu un iekārtu bojājumu pakāpi un stāvokli;
   3. novērtēt bojātās IS nozīmīgumu Pārziņa vai institūciju darbībai, nosaka apdraudējuma vai darbības pārtraukuma iemeslus;
   4. novērtē Pārzinim un iestādēm radītos zaudējumus infrastruktūras un IS atjaunošanai;
   5. pieņem lēmumu par IS darbības atjaunošanu esošajās telpās vai pārvietošanu uz citām telpām;
   6. nosaka turpmākās darbības IS atjaunošanai, to prioritāro kārtību, nepieciešamās darbības datu bāžu vai atsevišķu failu atjaunošanai, kā arī paredzamo darbības atjaunošanai nepieciešamo laiku;
   7. sadarbībā ar par tehniskajiem resursiem atbildīgo personu sastāda aizvietošanai nepieciešamā aprīkojuma sarakstu (aparatūra, programmatūra, palīgmateriāli).

# VI. Atbildīgo personu apmācības, nodarbību un sagatavotības pārbaužu plāns

1. Par tehniskajiem resursiem atbildīgā persona nodrošina iesaistīto darbinieku atbilstošas apmācības IS darbības nepārtrauktības nodrošināšanai.
2. Pārziņa darbinieki, kas iesaistīti IS darbības atjaunošanā, parakstās par iepazīšanos ar plānu un nodrošina aktuālas kontaktinformācijas uzturēšanu plānā.
3. Reizi gadā tiek veikta atjaunošanas procedūru dokumentāla pārbaude.
4. Reizi piecos gados tiek veikta pilna atjaunošanas procedūru praktiskā pārbaude.

VII. Noslēguma jautājumi

1. Šos noteikumus pārskata reizi gadā, kā arī:
   1. ja izmaiņas IS var ietekmēt IS drošību;
   2. ja mainījušies vai atklāti jauni IS drošības apdraudējumi;
   3. ja pieaug IS drošības incidentu skaits vai noticis nozīmīgs incidents;
   4. ja izmaiņas iestādes struktūrā skar IS drošības vadības organizāciju;
   5. ja izdarīti grozījumi normatīvajos aktos, kas regulē IS darbību.

Pašvaldības domes priekšsēdētāja K.Miķelsone

*@ ITN, IZD, PN, Informācijas tehnoloģiju administratoram*