APSTIPRINĀTS
SIA “Daugavpils ūdens” padomes
2026.gada 22.maija sēdē
prot. Nr.2026/4

KIBERDROŠĪBAS POLITIKA

Daugavpils, 2026

SATURS

1. VISPĀRĪGIE JAUTĀJUMI

1.1. Kiberdrošības politika nosaka sabiedrības ar ierobežotu atbildību "Daugavpils ūdens" (turpmāk – Sabiedrība) vispārējo pieeju kiberdrošības pārvaldībai un kalpo kā pamats iekšējai drošības kontrolei, riska pārvaldībai un atbilstības nodrošināšanai attiecībā uz Sabiedrības esošo informācijas un komunikācijas tehnoloģiju kiberdrošību, informācijas un informācijas sistēmu pieejamību, integritāti un konfidencialitāti.

1.2. Kiberdrošības politika ir izstrādāta saskaņā ar Nacionālās kiberdrošības likumu un uz šī likuma pamata izdotiem Ministru kabineta noteikumiem, tai skaitā Ministru kabineta 2025.gada 25.jūnija noteikumiem Nr.397 "Minimālās kiberdrošības prasības", ievērojot Sabiedrības Korporatīvas pārvaldības politikas pamatnostādnes.

1.3. Sabiedrība ir subjekts, kas, ievērojot Nacionālās kiberdrošības likuma nosacījumus, atbilst būtisko pakalpojuma sniedzēja statusam.

1.4. Kiberdrošības politikā lietotie termini:

1.4.1. Informācijas resurss – strukturēta digitālo datu vienība.

1.4.2. Informācijas sistēma – organizēta sistēma, kas paredzēta informācijas resursu pārvaldībai, elektroniskajai apstrādei un uzglabāšanai, izmantojot tehniskos resursus.

1.4.3. Informācijas un komunikācijas tehnoloģijas (turpmāk – IKT) – tehnoloģijas, kuras tām paredzēto uzdevumu izpildei ar tehnisko līdzekļu palīdzību veic informācijas elektronisko apstrādi, tai skaitā izveidošanu, izmainīšanu, dzēšanu, glabāšanu, attēlošanu, pārsūtīšanu vai pārraidīšanu, un nodrošina tehnoloģijas izmantotāju savstarpējo komunikāciju.

1.4.4. IKT resursi – tehnisko resursu un informācijas resursu kopums.

1.4.5. Integritāte – informācijas resursa un tā elektroniskās apstrādes metožu precizitāte, pareizība un pilnīgums.

1.4.6. Konfidencialitāte – piekļuve informācijas resursam tikai autorizētiem IKT procesiem un lietotājiem.

1.4.7. Pieejamība – iespēja lietotājam lietot informācijas sistēmu vai informācijas resursu noteiktā laikā un vietā.

1.4.8. Kiberdrošības pārvaldnieks – ar Sabiedrības Valdes rīkojumu iecelts darbinieks vai ārpakalpojuma sniedzējs, kas atbild par Sabiedrības kiberdrošības pasākumu izstrādi, ieviešanu, uzturēšanu un uzraudzību.

1.4.9. Kiberapdraudējums – jebkādi iespējami apstākļi, notikums vai darbība, kas var radīt bojājumus vai traucējumus vai citādi negatīvi ietekmēt tīklu un informācijas sistēmas.

1.4.10. Kiberdrošības incidents (kiberincidents) – notikums, kas apdraud apstrādātus datus vai pakalpojumu pieejamību, autentiskumu, integritāti vai konfidencialitāti.

1.4.11. Kiberrisks – kiberincidenta izraisītu zaudējumu vai pakalpojumu traucējumu iespējamība.

1.4.12. IKT resursu īpašnieks – Sabiedrības darbinieks, kura kompetencē atrodas konkrētas informācijas sistēmas darbības procesa organizēšana.

1.4.13. IKT tehnisko resursu turētājs – Sabiedrības datorsistēmu un datortīklu administrators vai datorsistēmu tehniķis vai ārpakalpojuma sniedzējs, kas veic datortīklu, serveru un to saistīto iekārtu uzturēšanu un administrēšanu.

1.4.14. Informācijas sistēmas lietotājs – persona, kurai ir piešķirtas piekļuves tiesības Sabiedrības IKT resursiem.

1.4.15. Fiziskā aizsardzība – IKT aizsardzība pret fiziskas iedarbības radītiem bojājumiem.

1.4.16. Loģiskā aizsardzība – IKT aizsardzība, kuru realizē ar programmatūras līdzekļiem.

1.4.17. Risku pārvaldības grupa – ar valdes rīkojumu nozīmēta darbinieku grupa, kas uzrauga risku pārvaldību Sabiedrībā, pieņem lēmumu par risku iekļaušanu risku reģistrā, veic risku pārvērtēšanu, izstrādā risku mazināšanas pasākumu plānus.

1.5. Detalizētu kiberdrošības pārvaldības procesu norisi nosaka Sabiedrības iekšējie normatīvie akti, t.sk. kiberdrošības pārvaldības dokumentācija, kas izstrādāta atbilstoši Ministru kabineta 2025.gada 25.jūnija noteikumu Nr.397 "Minimālās kiberdrošības prasības" nosacījumiem.

1.6. Politika ir saistoša visiem Sabiedrības darbiniekiem, tajā skaitā Padomei un Valdei.

1.7. Padome un Valde nodrošina šīs politikas izpildes kontroli.

2. VISPĀRĪGA INFORMĀCIJA PAR SABIEDRĪBAS DARBĪBAS JOMU

2.1. Sabiedrība ir kapitālsabiedrība, kuras pamatdarbība ir sabiedrisko ūdensapgādes un kanalizācijas pakalpojumu nodrošināšana Daugavpils valstspilsētas administratīvajā teritorijā.

2.2. Sabiedrības sniegtie pakalpojumi ir cieši saistīti ar IKT resursu un informācijas sistēmu izmantošanu, kas ir pakļauti kiberriskiem un kurus var ietekmēt iespējams kiberapdraudējums.

3. KIBERDROŠĪBAS POLITIKAS PRINCIPI UN PAMATNOSTĀDNES

3.1. Sabiedrības pienākums ir nodrošināt, lai tās rīcībā esošā informācija tiktu apstrādāta, glabāta un pārvaldīta droši un pārbaudāmi, sniedzot tās darbiniekiem un lietotājiem skaidri noteiktas prasības IKT resursu izmantošanā, un nodrošinot informācijas sistēmu aizsardzību no ārējiem un iekšējiem, apzinātiem un nejaušiem kiberapdraudējumiem.

3.2. Kiberdrošības politika attiecas uz visiem Sabiedrības informācijas sistēmu lietotājiem, kuri veic darbības ar IKT resursiem, tai skaitā:

3.2.1. Sabiedrības darbiniekiem neatkarīgi no to ieņemamā amata;

3.2.2. lietotājiem, kuri ir noslēguši līgumu ar Sabiedrību par datu lietošanu.

3.3. Informācijas sistēmu lietotājs atbild par Kiberdrošības politikas nosacījumu ievērošanu, kas noteikti:

3.3.1. Kiberdrošības politikā;

3.3.2. Sabiedrības iekšējos normatīvajos aktos, kas nosaka informācijas sistēmu lietošanas prasības.

3.4. Kiberdrošības pārvaldnieks sadarbībā ar atbilstošo IKT resursu īpašnieku un IKT tehnisko resursu turētāju atbild par Kiberdrošības politikas nosacījumu ievērošanu, kas noteikti:

3.4.1. Kiberdrošības politikā;

3.4.2. Sabiedrības iekšējos normatīvajos aktos, kas nosaka informācijas sistēmu lietošanas prasības;

3.4.3. pārējos iekšējos normatīvajos aktos, kas nosaka kiberdrošības pārvaldības procesu Sabiedrībā.

3.5. Kiberdrošības pārvaldība tiek nodrošināta šādu uzdevumu īstenošanai:

3.5.1. nodrošinātu IKT informācijas sistēmu un resursu pieejamību;

3.5.2. nodrošinātu IKT informācijas sistēmu un resursu integritāti;

3.5.3. nodrošinātu IKT informācijas sistēmu un resursu konfidencialitāti;

3.5.4. aizsargātu IKT informācijas sistēmas un resursus un nodrošinātu informācijas sistēmu un resursu darbības nepārtrauktību;

3.5.5. identificētu IKT informācijas sistēmu un resursu kiberdrošības apdraudējumus;

3.5.6. novērtētu IKT informācijas sistēmu un resursu kiberriskus;

3.5.7. atklātu kiberincidentus;

3.5.8. atjaunotu IKT informācijas sistēmu un resursu darbību pēc kiberincidenta.

3.6. Sabiedrība nodrošina kiberdrošības pārvaldības dokumentu kopuma izveidošanu un uzturēšanu atbilstoši Ministru kabineta 2025.gada 25.jūnija noteikumu Nr.397 "Minimālās kiberdrošības prasības" nosacījumiem.

3.7. Sabiedrība nodrošina, ka kiberdrošības pārvaldības dokumentu kopuma daļas ir pieejamas tikai personām, kurām tās nepieciešamas darba pienākumu vai ārpakalpojuma izpildei.

4. KIBERDROŠĪBAS PĀRVALDĪBAS STRUKTŪRA

4.1. Padome:

4.1.1. apstiprina Kiberdrošības politiku;

4.1.2. uzrauga Sabiedrības kiberdrošības pārvaldības pasākumu īstenošanu;

4.1.3. sniedz priekšlikumus Kiberdrošības politikas pilnveidošanai;

4.1.4. nodrošina savu pienākumu izpildi atbilstoši ārējiem un Sabiedrības iekšējiem normatīvajiem aktiem.

4.2. Valde:

4.2.1. nodrošina Kiberdrošības politikas un iekšējo normatīvo dokumentu izstrādi, kas reglamentē kiberdrošības pārvaldības procesus Sabiedrībā;

4.2.2. apstiprina kiberdrošības pārvaldības procesus Sabiedrībā reglamentējošo iekšējo normatīvo dokumentāciju, kas izstrādāta Kiberdrošības politikas īstenošanai;

4.2.3. nozīmē Sabiedrības kiberdrošības pārvaldnieku;

4.2.4. uzrauga un atbild par Sabiedrības kiberdrošības pārvaldības pasākumu īstenošanu;

4.2.5. nodrošina savu pienākumu izpildi atbilstoši ārējiem un Sabiedrības iekšējiem normatīvajiem aktiem.

4.3. Kiberdrošības pārvaldnieks:

4.3.1. organizē Sabiedrības informācijas un komunikācijas tehnoloģiju infrastruktūras drošības pasākumus;

4.3.2. veic informācijas un komunikācijas tehnoloģiju drošības pārbaudi un atbilstoši tās rezultātiem organizē konstatēto trūkumu novēršanu;

4.3.3. nodrošina kiberdrošības politikas un ar to saistīto iekšējo normatīvo aktu izstrādi, ieviešanas koordinēšanu un aktualizāciju;

4.3.4. nodrošina kiberdrošības prasību ievērošanas uzraudzību;

4.3.5. organizē kiberrisku identificēšanas un pārvaldības procesus;

4.3.6. organizē kiberincidentu identificēšanu, analīzi un dokumentēšanu, kā arī koordinē nepieciešamos pasākumus incidentu novēršanai un seku mazināšanai;

4.3.7. normatīvajos aktos noteiktajos gadījumos nodrošina informācijas sniegšanu par kiberincidentiem Sabiedrības vadībai un ziņošanu uzraugošajām institūcijām, tai skaitā Nacionālajam kiberdrošības centram.

4.4. IKT resursu īpašnieks:

4.4.1. nodrošina informācijas sistēmu un informācijas resursu lietošanas procesu organizēšanu atbilstoši Sabiedrības darbības mērķiem un normatīvo aktu prasībām;

4.4.2. sadarbībā ar kiberdrošības pārvaldnieku un IKT tehnisko resursu turētāju nodrošina informācijas sistēmu un resursu lietotāju piekļuves tiesību piešķiršanas, izmaiņu veikšanas vai anulēšanas procesu īstenošanu;

4.4.3. sadarbībā ar kiberdrošības pārvaldnieku un IKT tehnisko resursu turētāju identificē drošības riskus un nodrošina nepieciešamo drošības pasākumu ieviešanu attiecīgajā informācijas sistēmā.

4.5. IKT tehnisko resursu turētājs:

4.5.1. veic datortīklu, serveru, datu glabāšanas sistēmu, lietotāju darba staciju un citu tehnoloģisko resursu uzturēšanu un administrēšanu, kā arī piekļuves tiesību tehnisko pārvaldību;

4.5.2. nodrošina tehnisko resursu fiziskās un loģiskās aizsardzības pasākumus;

4.5.3. nodrošina informācijas sistēmu un to darbību nodrošinošo operētājsistēmu žurnālfailu, kā arī tīkla plūsmas žurnālfailu veidošanas un uzglabāšanas procesu pārvaldību;

4.5.4. sadarbībā ar kiberdrošības pārvaldnieku nodrošina IKT sistēmu darbības uzraudzību;

4.5.5. nodrošina informācijas sistēmu rezerves kopiju veidošanas un uzglabāšanas procesu pārvaldību un informācijas sistēmu darbības atjaunošanu gadījumos, kad to darbība tiek traucēta kiberincidentu vai tehnisku bojājumu rezultātā;

4.5.6. nodrošina atbilstošu atbalstu un konsultāciju sniegšanu IKT resursu īpašniekiem, informācijas sistēmu lietotājiem un IKT ārpakalpojumu sniedzējiem Sabiedrības informācijas sistēmu, informācijas resursu un IKT tehnisko resursu lietošanas jautājumos.

4.6. Informācijas sistēmas lietotājs:

4.6.1. ievēro Sabiedrības Kiberdrošības politikas un ar to saistīto iekšējo normatīvo aktu prasības, kā arī nodrošina piešķirto informācijas sistēmu, informācijas resursu un IKT tehnisko resursu piekļuves datu drošu izmantošanu;

4.6.2. racionāli un lietderīgi izmanto informācijas sistēmas un to datus savu darbu pienākumu veikšanai, rūpējoties par informācijas konfidencialitātes, pieejamības un integritātes saglabāšanu Sabiedrībā;

4.6.3. ir atbildīgs par visām savām darbībām, kas veiktas ar viņam piešķirtajiem piekļuves līdzekļiem un Sabiedrības informāciju, informācijas sistēmām un tehniskiem resursiem;

4.6.4. nekavējoties informē savu tiešo vadītāju vai Kiberdrošības pārvaldnieku, ja tiek konstatēti drošības incidenti, aizdomīgas darbības vai iespējami kiberdrošības apdraudējumi.

4.7. Sabiedrība nodrošina IKT tehnisko resursu turētāju atbilstošo pienākumu sadali, lai novērstu iespējamu interešu konfliktu.

5. IKT RESURSU UN INFORMĀCIJAS SISTĒMU KLASIFIKĀCIJA

5.1. Sabiedrības īpašumā un valdījumā esošie IKT resursi un informācijas sistēmas tiek iedalītas drošības klasēs, ievērojot Ministru kabineta 2025.gada 25.jūnija noteikumu Nr.397 "Minimālās kiberdrošības prasības" nosacījumus.

5.2. Sabiedrības īpašumā un valdījumā esošo IKT resursu un informācijas sistēmu klasifikācijas sarakstu apstiprina Sabiedrības Valde.

5.3. Kiberdrošības pārvaldnieks sadarbībā ar IKT resursu īpašniekiem un IKT tehnisko resursu turētājiem vismaz reizi gadā pārskata Sabiedrības īpašumā un valdījumā esošo IKT resursu un informācijas sistēmu klasifikācijas sarakstu, nepieciešamības gadījumā to aktualizējot un iesniedzot to Sabiedrības Valdei apstiprināšanai.

6. IKT RESURSU UN INFORMĀCIJAS SISTĒMU KATALOGS

6.1. Sabiedrības īpašumā un valdījumā esošie IKT resursi un informācijas sistēmas, kas ir pakļautas kiberriskiem, tiek uzskaitītas IKT resursu un informācijas sistēmu katalogā.

6.2. IKT resursu un informācijas sistēmu katalogā tiek iekļauta informācija par Sabiedrības īpašumā un valdījumā esošajiem IKT resursu un informāciju sistēmām, šo resursu un informācijas sistēmu atbalstošām sistēmām, servisiem, programmatūru, izmantoto aparatūru, fizisko infrastruktūru, datu nesējiem, kā arī izveidoto tīklu shēmu.

6.3. Kiberdrošības pārvaldnieks sadarbībā ar IKT resursu īpašniekiem un IKT tehnisko resursu turētājiem nodrošina Sabiedrības IKT resursu un informācijas sistēmu kataloga uzturēšanu un izmaiņu gadījumā nekavējoties, bet ne vēlāk kā viena mēneša laikā aktualizē to.

7. KIBERINCIDENTU PĀRVALDĪBA

7.1. Sabiedrība nodrošina kiberincidentu pārvaldību, kas ietver:

7.1.1. Sabiedrības īpašumā un valdījumā esošajos tīklos un informācijas sistēmās konstatēto kiberincidentu identificēšanu un reģistrēšanu kiberincidentu žurnālā, nodrošinot ziņu reģistrēšanu ne vēlāk kā 24 stundu laikā no kiberincidenta konstatēšanas brīža vai pēc jebkādām izmaiņām iepriekš žurnālā norādītajās ziņās;

7.1.2. kiberincidentu ietekmes novērtēšanu uz Sabiedrības IKT infrastruktūras kiberdrošību, informācijas un informācijas sistēmu pieejamību, integritāti un konfidencialitāti;

7.1.3. pasākumu un procedūru ieviešanu kiberincidentu risināšanai, ietekmes mazināšanai, un seku likvidēšanai;

7.1.4. pasākumu un procedūru ieviešanu kiberincidentu pirmcēloņu atklāšanai, analīzei un novēršanai, pierādījumu saglabāšanai un drošības pasākumu uzlabošanai pēc kiberincidenta;

7.1.5. iekšējās un ārējas komunikācijas plānu kiberincidenta gadījumā noteikšanu;

7.1.6. informācijas sniegšanu par kiberincidentu Nacionālajam kiberdrošības centram Nacionālās kiberdrošības likuma noteiktajā kārtībā.

7.2. Sabiedrība uztur kiberincidentu žurnālu, kurā iekļauj vismaz šādu informāciju par kiberincidentiem:

7.2.1. kiberincidenta konstatēšanas datumu un laiku, kā arī kiberincidenta datumu un laiku, ja tāds ir zināms;

7.2.2. kiberincidenta veida kodu(-us) atbilstoši Ministru kabineta 2025.gada 25.jūnija noteikumu Nr.397 "Minimālās kiberdrošības prasības" 7. pielikumā ietvertajai tipoloģijai;

7.2.3. kiberincidenta vispārīgo aprakstu;

7.2.4. kiberincidenta cēloņus un kompromitēšanas indikatorus, ja tādi ir zināmi;

7.2.5. kiberincidenta ietekmes novērtējumu;

7.2.6. atzīmi par to, vai kiberincidents uzskatāms par nozīmīgu kiberincidentu;

7.2.7. atzīmi par kiberincidenta paziņošanu kiberincidentu novēršanas institūcijai (nozīmīga kiberincidenta gadījumā – arī par agrīnā brīdinājuma, sākotnējā ziņojuma, starpposma/progresa ziņojuma un galaziņojuma iesniegšanu);

7.2.8. aktuālo kiberincidenta risināšanas statusu (piemēram, "neiesākts", "procesā", "atrisināts").

8. KIBERRISKU PĀRVALDĪBA

8.1. Sabiedrības kiberdrošības risku pārvaldība tiek īstenota, ievērojot Sabiedrības Risku pārvaldības politikas pamatnostādnes.

8.2. Kiberrisku pārvaldības procesā tiek identificēti, analizēti, novērtēti un uzraudzīti kiberdrošības riski, izvērtējot draudu avotus, sistēmu ievainojamības, iespējamo ietekmi un kiberincidentu varbūtību.

8.3. Kiberrisku pārvaldības procesu nodrošina kiberdrošības pārvaldnieks sadarbībā ar IKT resursu īpašniekiem un IKT tehnisko resursu turētājiem.

8.4. Kiberrisku novērtēšana tiek veikta vismaz reizi gadā vai pēc būtiskām izmaiņām Sabiedrības īpašumā un valdījumā esošo IKT resursu un informācijas sistēmu konfigurācijā, kā arī pēc nozīmīgu kiberincidentu iestāšanās.

8.5. Kiberrisku novērtēšanu un uzraudzību nodrošina Sabiedrības Risku pārvaldības grupa saskaņā ar Sabiedrības Risku pārvaldības politiku, Sabiedrības Risku pārvaldības procedūru un citiem iekšējiem normatīvajiem aktiem (turpmāk – Risku pārvaldības dokumentācija).

8.6. Pamatojoties uz kiberrisku novērtēšanas rezultātiem, tiek plānoti un ieviesti konkrēti kiberrisku mazināšanas pasākumi, kuru mērķis ir samazināt risku iestāšanās varbūtību vai negatīvās sekas.

8.7. Kiberdrošības pārvaldnieks nodrošina kiberrisku mazināšanas plāna izpildes kontroli un ziņo par plāna izpildes gaitu Sabiedrības Risku pārvaldības grupai Risku pārvaldības dokumentācijā noteiktajā kārtībā.

8.8. Sabiedrība uztur centralizētu kiberrisku reģistru, kurā tiek uzskaitīti visi identificētie kiberriski, to novērtējums, potenciālā ietekme, mazināšanas pasākumi.

8.9. Kiberrisku reģistrs tiek aktualizēts vismaz reizi gadā vai pēc būtiskām izmaiņām Sabiedrības īpašumā un valdījumā esošo IKT resursu un informācijas sistēmu infrastruktūrā, kā arī pēc kiberincidentiem, kas var ietekmēt risku līmeni.

8.10. Kiberdrošības pārvaldnieks sadarbībā ar IKT resursu īpašniekiem un IKT tehnisko resursu turētājiem regulāri pārskata kiberrisku reģistru, un nepieciešamības gadījumā ierosina veikt izmaiņas, par ko informē Sabiedrības Risku pārvaldības grupu un vadību Risku pārvaldības dokumentācijā noteiktajā kārtībā.

9. NOZĪMĪGĀKIE KIBERAPDRAUDĒJUMU VEIDI

9.1. Lai nodrošinātu efektīvu kiberdrošības pārvaldību un savlaicīgi novērstu kiberincidentu riskus, Sabiedrība regulāri identificē un novērtē nozīmīgākos kiberapdraudējumu veidus, kam var būt pakļauti Sabiedrības īpašumā un valdījumā esošie IKT resursi un informācijas sistēmas.

9.2. Sabiedrības kiberdrošības pārvaldnieks sadarbībā ar IKT resursu īpašniekiem un IKT tehnisko resursu turētājiem regulāri aktualizē šo apdraudējumu sarakstu, izvērtējot incidentu statistiku, tehnoloģiju attīstību un ārējo institūciju sniegto informāciju par aktuāliem draudiem:

9.2.1. sociālās inženierijas uzbrukumi (Social Engineering);

9.2.2. pikšķerēšanas uzbrukumi (Phishing);

9.2.3. izspiedējvīrusi (Ransomware);

9.2.4. ļaunprogrammatūra (Malware);

9.2.5. pakalpojumu atteices uzbrukumi (DDoS - Distributed Denial of Service);

9.2.6. iekšējie draudi un neatļauta piekļuve;

9.2.7. sabotāža un mērķtiecīgi uzbrukumi;

9.2.8. citu apdraudējumu veidu izvērtējums.

9.3. Kiberdrošības pārvaldnieks nodrošina informācijas apriti un reaģēšanu uz potenciālajiem un aktuālajiem kiberapdraudējumiem, informējot IKT resursu īpašniekus, IKT tehnisko resursu turētājus un informācijas sistēmu lietotājus par nepieciešamajiem drošības pasākumiem.

10. IKT DARBĪBAS NEPĀRTRAUKTĪBAS NODROŠINĀŠANA

10.1. Sabiedrība īsteno sistemātisku pieeju IKT infrastruktūras darbības nepārtrauktības plānošanā, lai nodrošinātu kritisko pakalpojumu un funkciju atjaunošanu pēc iespējamiem incidentiem vai ārkārtas situācijām, un uztur kiberrisku pārvaldības un IKT darbības nepārtrauktības plānu (plāns var sastāvēt no vairākiem dokumentiem).

10.2. IKT infrastruktūras darbības nepārtrauktības plānošana tiek balstīta uz risku novērtējumu un Sabiedrības īpašumā un valdījumā esošo IKT resursu un informācijas sistēmu klasifikācijas rezultātiem, definējot pieļaujamos atjaunošanas laika mērķus (Recovery Time Objective - RTO), atjaunošanas punkta mērķus (Recovery Point Objective - RPO), kā arī maksimāli pieļaujamo dīkstāves laiku (Maximum Tolerable Downtime - MTD) katram kritiskajam resursam vai informācijas sistēmai.

10.3. Kiberrisku pārvaldības un IKT darbības nepārtrauktības plānā iekļauj vismaz:

10.3.1. kiberrisku novērtēšanas metodiku (piem., pieņemamās vērtības, novērtēšanas matrica, pārskatīšanas periodiskums);

10.3.2. kiberrisku novērtējumu (tostarp ar piegādes ķēdēm saistīto risku analīzi) un, ja attiecināms, salīdzinājumu ar iepriekšējo periodu;

10.3.3. kiberrisku pārvaldības pasākumu plānu ar konkrētiem pasākumiem, atbildīgajiem un termiņiem/periodiskumu.

10.4. IKT infrastruktūras darbības nepārtrauktības plāna izstrādi, izpildes uzraudzību un kontroli nodrošina kiberdrošības pārvaldnieks sadarbībā ar IKT resursu īpašniekiem un IKT tehnisko resursu turētājiem.

10.5. IKT infrastruktūras darbības nepārtrauktības plānu apstiprina Sabiedrības Valde.

10.6. Nepārtrauktības plānā ietvertie pasākumi tiek savlaicīgi ieviesti, nosakot konkrētas atbildības, uzdevumus, termiņus un nepieciešamos resursus šo pasākumu īstenošanai.

10.7. Kiberdrošības pārvaldnieks regulāri pārskata un aktualizē kiberrisku pārvaldības un IKT darbības nepārtrauktības plānu atbilstoši Ministru kabineta 2025.gada 25.jūnija noteikumu Nr.397 "Minimālās kiberdrošības prasības" prasībām (t. sk. atbilstoši Sabiedrības īpašumā/valdījumā esošo informācijas sistēmu drošības klasēm).

10.8. Sabiedrība nodrošina rezerves IKT resursus darbības nepārtrauktības nodrošināšanai nozīmīgā kiberincidenta vai krīzes gadījumā (informācijas sistēmu rezerves kopijas, rezerves serveri un datu glabātuves, galvenā ugunsmūra un iekšējā tīkla galveno elementu rezerves risinājumi, rezerves interneta pieslēgums).

10.9. Rezerves resursu konfigurācija tiek regulāri pārbaudīta un testēta, lai pārliecinātos par to efektivitāti un gatavību nodrošināt nepārtrauktu IKT infrastruktūras darbību ārkārtas situācijās.

10.10. Sabiedrība nodrošina, ka kiberdrošības pārvaldniekam un, ja attiecināms, citām par darbības nepārtrauktības pasākumu īstenošanu atbildīgajām personām ir nepieciešamās zināšanas un pilnvaras, lai nekavējoties veiktu tūlītējās nepieciešamās darbības kiberapdraudējuma novēršanai, kiberincidentu risināšanai vai kiberuzbrukuma seku novēršanai.

11. ĀRPAKALPOJUMU PRASĪBAS

11.1. Slēdzot ārpakalpojuma līgumu par IKT resursa vai pakalpojuma iegādi, Sabiedrība nodrošina, ka:

11.1.1. ārpakalpojuma sniedzējs atbilst Nacionālā kiberdrošības likuma un Ministru kabineta 2025.gada 25.jūnija noteikumu Nr.397 "Minimālās kiberdrošības prasības" 4. nodaļā iekļautajām prasībām;

11.1.2. ārpakalpojuma sniedzējam tiek piemērotas IKT resursu, informācijas sistēmu un pakalpojumu prasības, kas nav zemākas par Sabiedrības Kiberdrošības politikā, uz šīs politikas izstrādātajos iekšējos normatīvajos aktos un citos spēkā esošajos normatīvajos aktos iekļautajām prasībām.

11.2. Papildus Sabiedrība nodrošina, ka ārpakalpojuma līgumos un ārpakalpojuma iegādes procesā tiek izpildītas šādas prasības:

11.2.1. ja ārpakalpojums ietver jaunas informācijas sistēmas izstrādi vai esošas informācijas sistēmas izmaiņas, līgumā nosaka uzturēšanas un atbalsta nodrošināšanas laikposmu (t. sk. drošības nepilnību novēršanu) un paredz iespēju minētajā laikposmā turpināt ekspluatāciju ar obligāti nepieciešamā programmnodrošinājuma jaunākām versijām;

11.2.2. A un B konfidencialitātes klases informācijas sistēmām testa vidē izmanto tikai sintētiskus datus, un ārpakalpojuma līguma izpilde netiek veikta attiecīgās informācijas sistēmas produkcijas vidē;

11.2.3. pirms ārpakalpojuma iegādes tiek apzināti un novērtēti ar ārpakalpojumu saistītie riski, tostarp piegādes ķēdes drošības riski, noteiktas ārpakalpojuma kvalitātes/drošības/pieejamības prasības šo risku mazināšanai, kā arī noteikta ārpakalpojuma izbeigšanas stratēģija;

11.2.4. ārpakalpojuma sniedzējs nodrošina, ka apakšuzņēmēji atbilst visām ārpakalpojuma sniedzējam noteiktajām prasībām; Sabiedrība un ārpakalpojuma sniedzējs nodrošina apakšuzņēmējiem deleģēto pakalpojumu uzraudzību un atbilstību;

11.2.5. ārpakalpojuma sniedzējs ne vēlāk kā līdz līguma noslēgšanai iesniedz Sabiedrībai ārpakalpojuma izpildē iesaistīto fizisko personu sarakstu ar skaidrojumu par katras personas iesaisti un informē par izmaiņām līguma izpildes laikā;

11.2.6. pirms ārpakalpojuma līguma slēgšanas līgums tiek saskaņots ar Sabiedrības kiberdrošības pārvaldnieku, un Sabiedrība nosaka atbildīgo personu par līguma izpildes uzraudzību kiberdrošības jomā.

12. KIBERHIGIĒNAS PASĀKUMI

12.1. Sabiedrība nodrošina, ka IKT resursu un informācijas sistēmu izmantošanā un uzturēšanā iesaistītām personām tiek nodrošinātas vismaz šādas apmācības kiberdrošības jautājumos:

12.1.1. Informācijas sistēmu lietotājiem un IKT resursu īpašniekiem:

12.1.1.1. sākotnējās kiberdrošības apmācības ne vēlāk kā viena mēneša laikā no šai personai izveidotā lietotāja konta;

12.1.1.2. kārtējās kiberdrošības apmācības vismaz reizi gadā;

12.1.1.3. ārkārtas kiberdrošības instruktāžas identificējot jaunu risku, ievainojamību vai kiberapdraudējumu, paredzot normatīvo aktu prasību izmaiņas, plānojot vai veicot nozīmīgas izmaiņas IKT infrastruktūrā, programmatūrā vai Sabiedrības darbības procesos.

12.1.2. IKT tehnisko resursu turētājiem:

12.1.2.1. sākotnējās kiberdrošības apmācības ne vēlāk kā viena mēneša laikā no šai personai izveidotā lietotāja (resursa administratora) konta;

12.1.2.2. kārtējās apmācības kiberdrošības jomā kiberrisku pārvaldības un IKT darbības nepārtrauktības pasākumu efektīvai īstenošanai vismaz reizi gadā;

12.1.2.3. papildu apmācības identificējot jaunu risku, ievainojamību vai kiberapdraudējumu, paredzot normatīvo aktu prasību izmaiņas, plānojot vai veicot nozīmīgas izmaiņas IKT infrastruktūrā, programmatūrā vai Sabiedrības darbības procesos.

12.2. Kiberdrošības apmācības tiek organizētas, izvēloties tādu apmācības veidu un saturu, kas atbilst IKT resursu un informācijas sistēmu izmantošanā un uzturēšanā iesaistīto personu darba pienākumiem IKT resursu un informācijas sistēmu lietošanas un uzturēšanas jomā, kā arī Sabiedrības darbības specifikai ūdensapgādes un kanalizācijas pakalpojumu nodrošināšanā.

12.3. Kiberdrošības apmācību un instruktāžu saturs tiek pārskatīts un, ja nepieciešams, aktualizēts vismaz reizi gadā vai identificējot jaunu risku, ievainojamību vai kiberapdraudējumu, paredzot normatīvo aktu prasību izmaiņas, plānojot vai veicot nozīmīgas izmaiņas IKT infrastruktūrā, programmatūrā vai Sabiedrības darbības procesos.

12.4. Sabiedrība nodrošina, ka IKT resursu un informācijas sistēmu izmantošanā un uzturēšanā iesaistītām personām ir pieejami aktuālie kiberdrošības apmācību materiāli.

12.5. Sabiedrība uzskaita organizētās kiberdrošības apmācības un vismaz reizi gadā novērtē IKT resursu un informācijas sistēmu izmantošanā un uzturēšanā iesaistīto personu zināšanas kiberdrošības jautājumos, kā arī īstenoto kiberdrošības apmācību efektivitāti.

12.6. Kiberdrošības pārvaldniekam ir pienākums vismaz reizi gadā piedalīties kiberincidentu novēršanas institūcijas - Nacionālā kiberdrošības centra organizētajās apmācībās kiberdrošības jomā.

13. NOSLĒGUMA JAUTĀJUMI

13.1. Kiberdrošības politika tiek pārskatīta un aktualizēta pēc nepieciešamības, bet ne retāk kā reizi trijos gados.

13.2. Sabiedrība nodrošina darbinieku iepazīstināšanu ar kiberdrošības politiku.

13.3. Kiberdrošības politika ir pieejama Sabiedrības tīmekļa vietnē.

13.4. Kiberdrošības politika stājās spēkā ar 22.05.2026.