

APSTIPRINĀTA
ar AS "RĪGAS SILTUMS" padomes
2026 gada 27.augusta
lēmumu Nr.6 (protokols Nr. 14)

**AS „RĪGAS SILTUMS”
KIBERDROŠĪBAS POLITIKA**

Rīga, 2026

IEVADS

AS “RĪGAS SILTUMS” (turpmāk – RS) kiberdrošība tiek uzskatīta par būtisku priekšnoteikumu uzņēmuma stratēģisko mērķu sasniegšanai, pakalpojumu nepārtrauktībai un sabiedrības interesēm informācijas un komunikācijas tehnoloģiju (turpmāk - IKT) kritiskās infrastruktūras kontekstā.

RS padome un valde, apzinoties IKT nozīmi RS pamatdarbības nodrošināšanā, kā arī pieaugošos kiberriskus un kiberapdraudējumus, ar šo kiberdrošības politiku (turpmāk – Politika) apliecina savu apņemšanos nodrošināt augstu kiberdrošības līmeni RS, kas atbilst attiecināmo normatīvo aktu prasībām un labai praksei kiberdrošības jomā.

RS padome un valde apstiprina, ka kiberdrošība ir neatņemama uzņēmuma pārvaldības, korporatīvo risku vadības un uzņēmuma darbības nepārtrauktības sastāvdaļa, un uzņemas nodrošināt nepieciešamos organizatoriskos, tehniskos un cilvēkresursu nodrošināšanas pasākumus, kas ir nepieciešami šīs Politikas ieviešanai, uzturēšanai un regulārai pārskatīšanai.

1. Terminu skaidrojums

- 1.1. **Autentifikācija** – process, kurā elektroniskajā vidē tiek pārbaudīta Lietotāja identitāte.
- 1.2. **Autorizācija** – process, kurā Lietotājam tiek piešķirtas tiesības veikt konkrētas darbības Informācijas sistēmā vai Tehniskajā resursā.
- 1.3. **Ievainojamība** – IKT vai to pakalpojumu vājums, uzņēmība pret tehniskām problēmām vai nepilnību, kas var tikt izmantota kiberapdraudējumam.
- 1.4. **Informācijas resurss** – strukturēta digitālo datu vienība (datne), kas tiek elektroniski apstrādāta, izmantojot Tehniskos resursus.
- 1.5. **Informācijas sistēma (IS)** – datu ievades, uzglabāšanas un apstrādes sistēma, kas nodrošina noteikto funkciju izpildi un paredz Lietotāju pieeju tajā glabātajiem datiem vai informācijai.
- 1.6. **Informācijas un komunikācijas tehnoloģijas (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 (turpmāk – elektroniskā apstrāde), un nodrošina tehnoloģijas izmantotāju savstarpējo komunikāciju.
- 1.7. **IKT resursi** – tehnisko resursu un Informācijas resursu kopums.
- 1.8. **Integritāte** – informācijas un tās elektroniskās apstrādes metožu precizitāte, pareizība un pilnīgums.

- 1.9. **Kiberapdraudējums (kiberdraudi)** – jebkādi iespējami apstākļi, notikums vai darbība, kas varētu radīt bojājumus vai traucējumus vai citādi negatīvi ietekmēt IKT resursus vai Informācijas sistēmas, to Lietotājus un citas personas.
- 1.10. **Kiberdrošība** – darbības, kas jāveic, lai aizsargātu datu pārraides tīklu un Informācijas sistēmas, to Lietotājus un citas personas, kuras skar kiberdraudi.
- 1.11. **Kiberdrošības incidents (kiberincidents)** – notikums, kas apdraud apstrādātus datus vai tādu pakalpojumu Pieejamību, autentiskumu, Integritāti vai Konfidencialitāti, kurus piedāvā datu pārraides tīklu un Informācijas sistēmas vai kuri pieejami ar to starpniecību.
- 1.12. **Kiberrisks** - kiberincidenta izraisītu zaudējumu vai pakalpojumu traucējumu iespējamība, ko izsaka kā šādu zaudējumu vai traucējumu ietekmes un minētā incidenta varbūtības apvienojumu.
- 1.13. **Konfidencialitāte** – piekļuves nodrošināšana informācijai tikai pilnvarotiem procesiem un lietotājiem.
- 1.14. **Lietotājs** – persona, kurai ir piešķirtas tiesības lietot Informācijas sistēmu.
- 1.15. **Pieejamība** – iespēja pilnvarotām personām lietot informāciju noteiktā laikā un vietā.
- 1.16. **Politika** – šī AS “RĪGAS SILTUMS” Kiberdrošības politika.
- 1.17. **RS** – akciju sabiedrība “RĪGAS SILTUMS”.
- 1.18. **Tehniskais resurss** – aparatūra, tostarp tīkla darbību nodrošinošās iekārtas, darbstacijas, serveri, datu nesēji un citas saistītas iekārtas, programmatūra, tostarp sistēmfaili, sistēmprogrammas, lietojumprogrammas un palīgprogrammas.

2. Politikas mērķis

Šīs Politikas mērķis ir izveidot, ieviest, uzturēt un nepārtraukti pilnveidot efektīvu un informācijā par aktuālajiem Kiberriskiem balstītu Kiberdrošības pārvaldības sistēmu, kas aizsargā ar RS darbību saistītās informācijas (neatkarīgi no datu nesēja veida), Informācijas sistēmu un saistīto Informācijas resursu Konfidencialitāti, Pieejamību un Integritāti.

3. Politikas darbības mērogs

- 3.1. Politika attiecināma uz visu RS IKT resursu un Informācijas sistēmu aizsardzību, kas ir RS īpašumā, valdījumā vai pārvaldīšanā.

- 3.2. Politika attiecas uz visiem RS darbiniekiem un amatpersonām, darbuņēmējiem un sadarbības partneriem, kuriem ir piekļuve pie RS tīkla, Informācijas sistēmām, Informācijas resursiem un Tehniskiem resursiem.
- 3.3. Politikas izpilde ir obligāta visās RS struktūrvienībās un visos procesos, kas saistīti ar RS IKT resursu izmantošanu, attīstību un uzturēšanu.

4. Kiberdrošības pārvaldības sistēmas darbības konteksts

- 4.1. RS ir vadošais centralizētās siltumapgādes uzņēmums Rīgā, kas nodarbojas ar siltumenerģijas ražošanu un pārvadi.
- 4.2. RS darbība balstās uz nepārtrauktu, drošu un uzticamu tehnoloģisko procesu norisi, kā arī ar tiem saistītās Informācijas un Tehnisko resursu pieejamību, Integritāti un Konfidencialitāti. RS IKT resursi ietver gan administratīvās Informācijas sistēmas, gan industriālās vadības un automatizācijas sistēmas, kuru drošība ir īpaši nozīmīga IKT kritiskās infrastruktūras kontekstā.
- 4.3. Kiberdrošība ir būtiska RS darbības nepārtrauktības un pakalpojumu kvalitātes nodrošināšanas sastāvdaļa, tāpēc RS regulāri pārskata un pielāgo savas stratēģijas un taktikas, lai reaģētu uz mainīgajiem draudiem un tehnoloģiskajām izmaiņām.
- 4.4. Kiberdrošības pārvaldība RS tiek nodrošināta, ņemot vērā šādu RS identificēto galveno ieinteresēto pušu vajadzības un prasības attiecībā uz kiberdrošību:
 - 4.4.1. **klienti**, kuri sagaida nepārtrauktu, drošu un kvalitatīvu siltumapgādes pakalpojumu;
 - 4.4.2. **akcionāri un RS vadība**, kas ir atbildīga par RS ilgtspējīgu attīstību, risku vadību un reputācijas saglabāšanu;
 - 4.4.3. **darbinieki un sadarbības partneri**, kuri ikdienā izmanto RS Informācijas sistēmas un ir iesaistīti tehnoloģisko procesu nodrošināšanā;
 - 4.4.4. **pakalpojumu sniedzēji un piegādātāji**, tostarp informācijas tehnoloģiju, industriālās vadības un automatizācijas sistēmu uzturētāji, kuriem var būt piekļuve RS Informācijas resursiem;
 - 4.4.5. **valsts un pašvaldību institūcijas**, tai skaitā **uzraugošās un drošības iestādes**.
- 4.5. RS Kiberdrošības pārvaldības sistēmai ir jāspēj efektīvi pārvaldīt Kiberriskus, ņemot vērā RS Kiberdrošības incidentu statistiku, tehnoloģiju attīstības

tendences un ārējos informācijas avotos pieejamo informāciju par aktuāliem kiberdraudiem.

- 4.6. Atbilstoši 2024. gada 20. jūnijā pieņemtajam Latvijas Republikas likumam “Nacionālais kiberdrošības likums” un Ministru kabineta 2025. gada 25. jūnija noteikumu Nr.397 “Minimālās kiberdrošības prasības” noteiktajam, RS klasificējas kā IKT būtisko pakalpojumu sniedzējs, kas uzliek pienākumu ievērot šajā likumā un uz tā pamata izstrādātajos Ministru kabineta noteikumos noteiktās minimālās kiberdrošības prasības. RS savā darbībā ievēro arī prasības, kas izriet citiem Latvijas Republikas un Eiropas Savienībā spēkā esošajiem normatīvajiem aktiem informācijas drošības, kiberdrošības un personas datu aizsardzības jomā, tostarp (bet ne tikai) Vispārīgā datu aizsardzības regula (ES) 2016/679 (VDAR) un Fizisko personu datu apstrādes likums.
- 4.7. RS nodrošina, ka Kiberdrošības prasības tiek regulāri pārskatītas un aktualizētas atbilstoši normatīvā regulējuma izmaiņām un kompetento iestāžu izstrādātajām vadlīnijām.
- 4.8. Ņemot vērā RS darbību enerģētikas nozarē, kā arī to, ka RS Nacionālā kiberdrošības likuma izpratnē ir IKT kritiskās infrastruktūras turētājs, RS īpašu uzmanību pievērš normatīvo aktu prasībām, starptautiskajiem standartiem un vadlīnijām (piemēram, ISO/ IEC 27001, 27002), kā arī labai praksei, kas attiecināmas uz šādiem informācijas un kiberdrošības aspektiem:
- 4.8.1. industriālo vadības un automatizācijas sistēmu aizsardzība;
 - 4.8.2. tehnoloģisko procesu nepārtrauktības un drošas vadības nodrošināšana;
 - 4.8.3. kiberincidentu savlaicīga atklāšana, novēršana un ietekmes mazināšana;
 - 4.8.4. Lietotāju piekļuves tiesību pārvaldība un Lietotāju atbildība;
 - 4.8.5. sadarbība ar valsts kiberdrošības uzraudzības institūcijām un nozares partneriem.

5. Vadības apņemšanās un Kiberdrošības mērķi

- 5.1. Lai uzraudzītu un spētu novērtēt RS Kiberdrošības pārvaldības sistēmas rezultātus, tai skaitā – šīs Politikas darbības efektivitāti, kā arī nodrošinātu šīs sistēmas nepārtrauktu attīstību un atbilstību RS stratēģiskajiem mērķiem un normatīvo aktu prasībām, RS valde apstiprina konkrētus, izmēramus sasniedzamos mērķus attiecībā uz Kiberdrošību un nosaka atbildīgos par šo mērķu izpildi:

- 5.1.1. Kiberdrošības mērķi tiek pārskatīti reizi gadā;
 - 5.1.2. mērķi ir balstīti risku novērtējumā un ietver Konfidencialitātes, Integritātes, Pieejamības, kiberincidentu skaita, auditu rezultātu u.c. rādītājus;
 - 5.1.3. priekšlikumu par Kiberdrošības mērķiem, kā arī par to izmaiņām, sagatavo un valdei iesniedz RS kiberdrošības pārvaldnieks;
 - 5.1.4. RS kiberdrošības pārvaldnieks vismaz reizi pusgadā informē RS valdi un padomi par kiberdrošības mērķu izpildes rezultātiem.
- 5.2. RS valde apņemas nodrošināt Politikas prasību izpildei un Kiberdrošības mērķu sasniegšanai nepieciešamos finanšu, cilvēku un tehniskos resursus, kā arī Kiberdrošības procesu integrāciju RS procesos.

6. Kiberdrošības pārvaldības organizatoriskā struktūra, atbildību sadalījums

- 6.1. RS kiberdrošības pārvaldības organizatoriskā struktūra ir izveidota, iekšējos normatīvajos aktos (valdes rīkojumos, amata aprakstos, procedūrās un instrukcijās u.c.) nosakot ar kiberdrošības pārvaldību saistītās lomas un to atbildības, kā arī ievērojot nosacījumu, ka šai struktūrai ir jābūt atbilstošai RS kiberdrošības pārvaldības sistēmas darbības kontekstam, jānodrošina kiberdrošības integrācija RS ikdienas darbības procesos, kā arī jāveicina efektīva iekšējā un ārējā komunikācija un sadarbība kiberdrošības jautājumos arī ar visām ieinteresētajām pusēm.
- 6.2. RS **padome** nodrošina RS kiberdrošības pārvaldības stratēģisko uzraudzību. Padome apstiprina Politiku, uzrauga RS kiberdrošības pārvaldības sistēmas atbilstību RS stratēģijai un organizācijas risku pārvaldības principiem.
- 6.3. RS **valde** atbild par RS kiberdrošības pārvaldību organizācijas operatīvajā līmenī. Valde akceptē Politiku, nodrošina tās ieviešanu RS, t.sk. nodrošina kiberdrošības pārvaldības organizācijas izveidi un resursu piešķiršanu tās pilnvērtīgai funkcionēšanai.
- 6.4. RS valde, ievērojot ārējos normatīvajos aktos šai lomai noteiktās prasības, ieceļ **kiberdrošības pārvaldnieku**, kas organizē un koordinē Politikā noteikto Kiberdrošības prasību ieviešanu, uzrauga Kiberdrošības pasākumu izpildi, informē valdi par Kiberdrošības riskiem un incidentiem, kā arī nodrošina Politikas un saistīto iekšējo normatīvo aktu uzturēšanu.
- 6.5. Visām RS Informācijas sistēmām ir noteikti **sistēmu īpašnieki**, kuri nodrošina konkrētu Informācijas un/ vai Tehnisko resursu vai to daļu pārvaldību.

- 6.6. Sistēmu īpašnieku pārvaldībā esošo Informācijas un/ vai Tehnisko resursu funkcionēšanu un tehnisko apkalpošanu nodrošina **sistēmu tehnisko resursu turētāji**. Sistēmu Tehnisko resursu turētāji atbilstoši iekšējos normatīvajos aktos noteiktajai kārtībai ir atbildīgi par attiecīgo Informācijas un vai Tehnisko resursu ekspluatēšanu saskaņā ar to izstrādātāju uz sistēmas īpašnieku norādēm.
- 6.7. RS **struktūrvienību vadītāji** ir atbildīgi par Politikas un uz tās pamata izstrādātajos iekšējos normatīvajos aktos noteikto prasību izpildes nodrošināšanu savu struktūrvienību darbībā.
- 6.8. Visi RS **darbinieki** un RS **IS lietotāji** ikdienas darbā ievēro prasības, kas noteiktas Politikā un uz tās pamata izstrādātajos iekšējos normatīvajos aktos. Par šo prasību neievērošanu var tikt piemērota atbildība vai disciplinārsodi saskaņā ar RS iekšējos noteikumus noteikto kārtību.

7. Kiberdrošības pamatprincipi

- 7.1. Ar RS darbību saistītās informācijas Konfidencialitāte, Integritāte un Pieejamība tiek nodrošināta, identificējot un uzskaitot visus RS īpašumā un valdījumā esošos IKT resursus un IS, nosakot un piemērojot Informācijas resursu drošības prasībām atbilstošas organizatoriskās, cilvēku, fiziskās un tehnoloģiskās drošības procedūras (kontroles), kas attiecīgi aizsargā informāciju pret nesankcionētu piekļuvi, izmaiņām, iznīcināšanu vai nepieejamību.
- 7.2. Atbilstoši RS Kiberdrošības pārvaldības sistēmas darbības kontekstam, kā arī Kiberdrošības mērķiem tiek veikta pastāvīga Kiberrisku identificēšana, analīze un novērtēšana. Balstoties uz Kiberrisku novērtējuma rezultātiem, tiek plānotas un ieviestas atbilstošas Kiberdrošības procedūras (kontroles), tai skaitā. pasākumi RS Kiberdrošības pārvaldības sistēmas nepārtrauktai attīstībai un Kiberrisku pārvaldībai.
- 7.3. Saskaņā ar RS Risku pārvaldības politikā noteiktajām pamatnostādnēm RS izstrādā, uztur, kā arī vismaz reizi gadā pārskata un aktualizē Kiberrisku pārvaldības plānu. Kiberrisku pārvaldības plānu apstiprina RS valde.
- 7.4. Plānojot pasākumus RS Kiberdrošības pārvaldības sistēmas nepārtrauktai attīstībai un Kiberrisku pārvaldībai, RS ievēro ārējos normatīvajos aktos un industrijas standartos noteiktās prasības, tai skaitā (bet ne tikai) prasības attiecībā uz IKT resursu un IS uzskaiti, Lietotāju un piekļuves tiesību pārvaldību,

- datu pārraides tīklu drošību, žurnālfailu un rezerves kopiju pārvaldību, šifrēšanu, kiberhigēnu.
- 7.5. RS ir izstrādāta un tiek uzturēta vienota Kiberdrošības incidentu pārvaldības kārtība, saskaņā ar kuru tiek nodrošināta kiberincidentu savlaicīga atklāšana, reģistrēšana, analīze un vadība, tostarp kiberincidentu eskalācija un ziņošana atbildīgajām institūcijām normatīvajos aktos noteiktajā kārtībā un termiņos.
- 7.6. RS IKT darbības nepārtrauktība un atjaunošanās spējas darbības traucējumu gadījumā tiek nodrošinātas, atbilstoši normatīvo aktu prasībām ieviešot un uzturot IKT darbības nepārtrauktības plānu. Tā izstrādes ietvaros tiek veikta krīzes un katastrofu ietekmes analīze, tiek noteikti IKT darbības nepārtrauktības mērķi un kritēriji IKT darbības nepārtrauktības plānu aktivizēšanai, veikts ar krīzes situācijām un katastrofām saistīto Kiberrisku novērtējums un izstrādāts to mazināšanas pasākumu plāns, izstrādāti atbilstoši IKT darbības atjaunošanas un komunikācijas plāni.
- 7.7. Lai veicinātu RS darbinieku un sadarbības partneru informētību un izpratni Kiberdrošības jautājumos, RS nodrošina regulāras apmācības, informēšanas pasākumus, kā arī skaidru pienākumu un atbildības sadalījumu Kiberdrošības pārvaldībā. Apmācības aptver gan vispārējos drošības jautājumus, gan specifiskas prasības konkrētām Kiberdrošības pārvaldībā iesaistītām lomām.
- 7.8. RS nodrošina fizisko aizsardzību telpām, iekārtām un IKT infrastruktūrai, tostarp katlumājām, siltumtīkliem, datu centriem un vadības telpām. Fiziskās drošības pasākumi ierobežo nesankcionētu piekļuvi un mazina riskus, kas var ietekmēt tehnoloģisko procesu drošu darbību.
- 7.9. RS nodrošina Lietotāju un piekļuves tiesību pārvaldību, piemērojot organizatoriskus un tehniskus pasākumus (kontroles), kas nodrošina piekļuvi Informācijas sistēmām un “Tehniskajiem resursiem tikai autentificētām un atbilstoši autorizētām personām. Piešķirot piekļuves tiesības RS Informācijas resursiem, tiek ievēroti “nepieciešamības zināt” un minimālo piekļuves tiesību principi, kā arī tiek nodrošināta regulāra piekļuves tiesību pārskatīšana.
- 7.10. RS nodrošina Informācijas sistēmu izstrādes, ieviešanas un izmaiņu pārvaldību visā to dzīves ciklā, piemērojot uz Kiberrisku novērtējuma balstītus organizatoriskos un tehniskos pasākumus, lai attiecīgi novērstu vai pēc iespējas mazinātu potenciālos Kiberriskus gan izstrādājamajām, gan ar tām saistītajām Informācijas sistēmām un Informācijas resursiem.

- 7.11. Pirms IKT ārpakalpojuma iegādes RS apzina un novērtē ar to saistītos Kiberriskus, tostarp piegādes ķēdes drošības riskus, un nosaka ārpakalpojuma kvalitātes, drošības un pieejamības prasības, kā arī ārpakalpojuma izbeigšanas nosacījumus. Attiecības ar ārpakalpojumu sniedzējiem tiek regulētas ar rakstveida līgumiem, kuros noteiktas pušu tiesības, pienākumi, atbildība un drošības prasības, kas attiecināmas arī uz apakšuzņēmējiem.
- 7.12. RS, ievērojot normatīvo aktu prasības, nodrošina efektīvu iekšējo un ārējo komunikāciju Kiberdrošības jautājumos, ieskaitot sadarbību ar Aizsardzības ministriju, Satversmes aizsardzības biroju un Nacionālo kiberdrošības centru. RS sistemātiski apkopo un uztur informāciju par Kiberdrošību uzraugošo iestāžu lēmumiem, pieprasījumiem un tiesiskajiem pienākumiem, kas attiecas uz RS, kā arī nodrošina šo lēmumu izpildi un dokumentē izpildes statusu.
- 7.13. RS ievieš Kiberdrošības pasākumu nepārtraukta uzlabošana tiek nodrošināta, uzraugot Kiberdrošības pārvaldības sistēmas darbības efektivitāti, analizējot kiberincidentus un to cēloņus, organizējot iekšējos un ārējos Kiberdrošības pārvaldības sistēmas auditus, t.sk. regulārus Informācijas sistēmu un Tehnisko resursu ievainojamību drošības testus, kā arī ieviešot uzraudzības rezultātā izstrādātos korektīvos un preventīvos pasākumus.

8. Politikas īstenošana un izpildes uzraudzība

- 8.1. Politikas prasību ieviešanai un izpildes nodrošināšanai kiberdrošības pārvaldnieks izstrādā attiecīgus RS iekšējos normatīvos aktus (procedūras, instrukcijas, rokasgrāmatas u.tml.) un uzrauga to izpildi.
- 8.2. Politikas un uz tās pamata izstrādāto RS iekšējo normatīvo aktu prasību izpildes uzraudzības ietvaros RS nodrošina vismaz šādus pasākumus:
- 8.2.1. atbilstības auditi, t.sk. Kiberdrošības atbilstības pārbaudes, kas tiek nodrošinātas ne retāk kā reizi trijos gados;
 - 8.2.2. ielaušanās testi un drošības skenēšana, t.sk. ielaušanās testi RS A Drošības klases IS pirms to nodošanas ekspluatācijā un vismaz reizi trijos gados IS ekspluatācijas laikā;
 - 8.2.3. pašvērtējuma ziņojumu sagatavošana un iesniegšana uzraugošajām iestādēm atbilstoši normatīvo aktu prasībām.
- 8.3. Kiberdrošības pārvaldnieks nodrošina RS valdes informēšanu par Politikas izpildes uzraudzības ietvaros īstenoto pasākumu rezultātiem, nodrošina šo

pasākumu rezultātā konstatēto neatbilstību vai levainojamību novēršanas pasākumu plānošanu, to izpildes uzraudzību.

- 8.4. Nepieciešamības gadījumā, pamatojoties uz normatīvajiem aktiem RS ir tiesības ziņot par Kiberdrošības pārkāpumiem tiesībsargājošajām iestādēm.

9. Noslēguma noteikumi

- 9.1. Politika tiek pārskatīta un aktualizēta ne retāk kā reizi trijos gados, kā arī gadījumos, ja tiek pārskatīts Politikas darbības ietvars, veiktas izmaiņas saistošajos normatīvajos aktos, reaģējot uz ar tehnoloģiju attīstību saistītām izmaiņām drošības apdraudējumu tendencēs, kā arī ņemot vērā mācības, kas gūtas no notikušiem vai gandrīz notikušiem Incidentiem, iekšējo un ārējo pārbažu un riska analīzes rezultātiem.
- 9.2. Politikas pārskatīšanu un aktualizāciju veic kiberdrošības pārvaldnieks.

Kiberdrošības pārvaldnieks

J.Maskalons