

Latvenergo koncerna Kiberdrošības politika

1. Politikas mērķis

- 1.1. Latvenergo koncerna (turpmāk – Koncerna) kiberdrošības politika (turpmāk – Politika) nosaka vienotus principus koncerna resursu aizsardzībai pret kiberriskiem.
- 1.2. Politikas galvenais mērķis ir īstenot kiberdrošības pārvaldības efektīvu darbību, lai:
 - 1.2.1. Nodrošinātu atbilstību Eiropas Savienības un nacionālajiem normatīviem aktiem;
 - 1.2.2. Organizētu ekonomiski pamatotu resursu aizsardzību, ievērojot konfidencialitātes, integritātes, pieejamības prasības informācijas sistēmām (turpmāk – IS), kritiskajiem procesiem, kritiskajiem pakalpojumiem un kritiskās infrastruktūras kopumam;
 - 1.2.3. Sniegtu atbalstu darbības nepārtrauktības plānošanas, uzturēšanas un testēšanas procesos.

2. Terminu skaidrojums

- 2.1. **Gandrīz noticis kiberincidents** – notikums, kurš būtu varējis apdraudēt apstrādātus datus vai tīklu un IS piedāvāto vai ar tīklu un IS starpniecību pieejamo pakalpojumu pieejamību, autentiskumu, integritāti vai konfidencialitāti, bet kura pilnīga īstenošanās tika sekmīgi novērsta vai kurš neīstenojās.
- 2.2. **Ievainojamība** – informācijas un komunikācijas tehnoloģiju vai to pakalpojumu vājums, uzņēmība pret tehniskām problēmām vai nepilnība, kas var tikt izmantota kiberapdraudējumam. Ievainojamība tiek uzskatīta par kiberincidenta paveidu.
- 2.3. **Kiberdrošības incidents** (turpmāk – kiberincidents) – notikums, kas apdraud apstrādātus datus vai tādu pakalpojumu pieejamību, autentiskumu, integritāti vai konfidencialitāti, kurus piedāvā tīklu un IS vai kuri pieejami ar tīklu un IS starpniecību.
- 2.4. **Kiberhigiēna** – ikdienas prakšu un paradumu kopums, kura mērķis ir mazināt kiberapdraudējumus, nodrošināt datu aizsardzību un saglabāt informācijas un komunikācijas tehnoloģiju resursu pieejamību, integritāti un konfidencialitāti.
- 2.5. **Kiberrisks** – kiberincidenta izraisītu zaudējumu vai pakalpojumu traucējumu iespējamība, ko izsaka kā šādu zaudējumu vai traucējumu ietekmes un minētā incidenta varbūtības apvienojumu.
- 2.6. **Kiberdrošība** ir darbības, kas jāveic, lai aizsargātu tīklu un IS, to lietotājus un citas personas, kuras skar kiberdraudi.
- 2.7. **Kiberdraudi** ir jebkādi iespējami apstākļi, notikums vai darbība, kas varētu radīt bojājumus vai traucējumus vai citādi negatīvi ietekmēt tīklu un IS, to lietotājus un citas personas.
- 2.8. **Kiberdrošības aizsardzības pasākumi** jeb drošības kontroles – tehniski vai organizatoriski pasākumi, kas tiek noteikti kiberrisku pārvaldības ietvaros un samazina kiberrisku līdz pieņemamam līmenim.

3. Politikas nostādnes un pamatprincipi

- 3.1. Koncernā un Latvenergo kapitālsabiedrībās ir noteikts un patstāvīgi tiek pilnveidots kiberdrošības pārvaldības dokumentu un pasākumu kopums, kura īstenošana nodrošina Politikas mērķa sasniegšanu un atbilstību Nacionālās kiberdrošības likumam.
- 3.2. Politika izstrādāta vadoties pēc labās prakses kiberdrošības principiem, kā arī ņemot vērā aktuālos kiberriskus industrijā.
- 3.3. Koncerna un Latvenergo kapitālsabiedrību kiberdrošības pārvaldības sistēma organizēta vadoties pēc ISO 27002¹ pamatprincipiem.

¹ ISO 27002:2024 Informācijas drošība, kiberdrošība un privātuma aizsardzība. Informācijas drošības kontroles.

Numurs: P069 Redakcija: 01	Politika Latvenergo koncerna Kiberdrošības politika	Lapa 2 (5)
-------------------------------	--	------------

- 3.4. **Zina tikai tas, kuram jāzina** – princips, ko izmanto informācijas aprites drošībai – gūstot pārliecību, ka informācija ir pieejama vienīgi tām personām, kurām tā nepieciešama darba pienākumu veikšanai.
- 3.5. **Viss, kas nav atļauts, ir aizliegts** – ja atļauja darbībai ar konkrēto informāciju, IS resursu vai tā daļu nav skaidri un nepārprotami noteikta, tad šāda darbība ir aizliegta.
- 3.6. **"Tīra" galda un "tīra" ekrāna politika** – darbinieks ikdienas darbības uztur tīru un sakārtotu vidi, gan darba galda virsmu, gan datora ekrāna virsmu. Īpašu izmanību pievēršot ierobežotas pieejamības informācijas apstrādei.
- 3.7. **Četru acu princips** – par konfliktējošām aktivitātēm (piemēram, izstrāde un uzturēšana, uzturēšana un uzraudzība, resursu pieprasījumi) lēmumu pieņem vismaz divi koncerna darbinieki.
- 3.8. **Kiberdrošība ir kopīga atbildība** – ikviens darbinieks ikdienā veic pienākumus kiberdrošības nodrošināšanā, izmantojot atļautos rīkus un risinājumus, kā arī saprātīgi analizē un lieto publiski pieejamo informāciju. Arī darbinieka bezdarbība var apdraudēt visu darbinieku ikdienu, kā arī Koncerna vai Latvenergo kapitālsabiedrības resursus.
- 3.9. **"Mazākais ļaunums"** – izvēlēties tādu aizsardzības pasākumu kopumu, kas rada vismazāko kaitējumu koncerna resursiem, piemēram, ierobežot, bloķēt noteiktas tīmekļa vietnes, lai novērstu urķēšanas iespējamību.

4. Kiberdrošības kontroles

- 4.1. Informācijas un komunikācijas tehnoloģiju resursi un to daļas tiek identificētas, klasificētas un novērtētas saskaņā ar Nacionālās kiberdrošības likuma un Koncerna iekšējiem normatīviem aktiem, ievērojot IS drošības klases noteikšanas metodiku.
- 4.2. Kiberrisku novērtējums tiek veikts vismaz reizi gadā, saskaņā ar Koncerna iekšējiem normatīviem aktiem.
- 4.3. Visiem Koncerna un Latvenergo kapitālsabiedrību resursiem tiek nodrošināti samērīgi aizsardzības pasākumi, kas attiecināmi uz kritiskās infrastruktūras īpašniekiem un būtisko pakalpojumu sniedzējiem.
- 4.4. Iepirkuma procesā, iegādājoties komponentes vai IS resursu daļas kritiskās infrastruktūras vajadzībām, pirms līguma slēgšanas tiek veikti, gan pakalpojuma sniedzēja, gan paša pakalpojuma kiberrisku novērtējumi, lai pārliecinātos, ka pakalpojuma sniedzēja kopējais kiberdrošības līmenis nav zemāks par Koncernā vai Latvenergo kapitālsabiedrībās uzturēto.
- 4.5. Slēdzot līgumu ar iepirkuma procedūrā izvēlētu pakalpojuma sniedzēju par IS resursu piegādi vai pakalpojumu sniegšanu Koncernam vai Latvenergo kapitālsabiedrībai, ārpalpojuma sniedzējs, tā piesaistītais apakšuzņēmējs un tehniskā resursa ražotājs (ja attiecināms) atbilst Nacionālās kiberdrošības likuma un Ministru kabineta noteikumu Nr. 397 "Minimālās kiberdrošības prasības" prasībām.
- 4.6. Koncernā un Latvenergo kapitālsabiedrībās tiek izveidoti un uzturēti kiberdrošības prasību dokumenti IS un tās komponentēm, ņemot vērā normatīvo aktu un industrijas prasības.

5. Kiberdrošības pārvaldības organizatoriskā struktūra

- 5.1. Kiberdrošības pārvaldību Koncernā un Latvenergo kapitālsabiedrībās īsteno kiberdrošības pārvaldnieks, kurš tiek nozīmēts uz trīs gadu termiņu.
- 5.2. Kiberdrošības pārvaldniekam ir šādi pienākumi:
 - 5.2.1. Nodrošināt kiberdrošības kontroli pilnveidi;

Numurs: P069 Redakcija: 01	Politika Latvenergo koncerna Kiberdrošības politika	Lapa 3 (5)
-------------------------------	--	------------

- 5.2.2. Nodrošināt kiberdrošības pārbaudes un atbilstoši rezultātiem organizēt konstatēto trūkumu novēršanu;
- 5.2.3. Apmeklēt apmācības kiberdrošības jautājumos;
- 5.2.4. Nodrošināt darbinieku sākotnējo, kārtējo un ārkārtas instruktāžu par aktuālajiem kiberriskiem, kiberdrošību un citām nepieciešamām tēmām;
- 5.2.5. Vismaz reizi gadā vai mainoties apstākļiem (jauni apdraudējumi, kiberriska līmenis, kiberincidents) nodrošināt sākotnējo, kārtējo un ārkārtas instruktāžu satura pārskatīšanu;
- 5.2.6. Veikt saziņu ar kompetento kiberincidentu novēršanas institūciju, citām kompetentajām institūcijām, citiem subjektiem un pakalpojumu saņēmējiem kiberincidenta konstatēšanas gadījumos;
- 5.2.7. Iepirkuma un līguma slēgšanas procesa ietvaros, izvērtēt kiberdrošības prasības risinājumiem, projektiem, IS, to atbilstību gan iekšējiem, gan ārējiem normatīviem aktiem.
- 5.3. Kiberdrošības pārvaldniekam ir šādas tiesības:
 - 5.3.1. Pārbaudīt lietotāju kontu sarakstu, tiem piešķirtās piekļuves tiesības un to veiktās darbības IS, tostarp lietotāju veiktās informācijas resursu izmaiņas un tehnisko resursu konfigurāciju izmaiņas;
 - 5.3.2. Nodrošināt auditācijas pierakstu analīzi par lietotāju veiktajām darbībām;
 - 5.3.3. Kiberincidenta, pamatotu aizdomu par kiberincidentu vai nesekmīgi nokārtotu kiberdrošības apmācību gadījumā pieprasīt bloķēt ar kiberincidentu saistītos lietotāju kontus;
 - 5.3.4. Pārbaudīt reģistrēto lietotāju zināšanas par kiberhigiēnu, IS lietošanas noteikumiem un nepieciešamības gadījumā organizēt papildu apmācības, lai šīs zināšanas pilnveidotu;
 - 5.3.5. Pieprasīt no IS uzturētāja IS auditācijas pierakstus, ja IS vai tās daļu uzturēšana notiek ārpakalpojuma ietvaros.
- 5.4. Koncerna IT un T virziena pārstāvjiem un Latvenergo kapitālsabiedrību funkciju vai struktūrvienību pārstāvjiem tiek noteiktas papildu kiberdrošības lomas, kuras tiek pārskatītas reizi trijos gados:
 - 5.4.1. Atbildīgais par IS rezerves kopiju pārvaldības procesu nodrošināšanu;
 - 5.4.2. Atbildīgais par IS auditācijas pierakstu pārvaldības procesu nodrošināšanu;
 - 5.4.3. Atbildīgais par kiberrisku pārvaldību;
 - 5.4.4. Atbildīgais par informācijas un komunikācijas tehnoloģiju darbības nepārtrauktības plāna izstrādi, pārskatīšanu un aktualizēšanu, kā arī par plānā ietverto pasākumu īstenošanu.
- 5.5. Koncerna un Latvenergo kapitālsabiedrību pamatdarbības un atbalsta funkciju pārstāvjiem tiek noteiktas papildu atbildības IS resursu administratīvajai pārvaldībai: IS turētājs, IS resursa turētājs, IS galvenais lietotājs.
- 5.6. IS resursa tehnisko pārvaldību veic Koncerna un Latvenergo kapitālsabiedrību IT un T virziena un IT funkcijas noteikti darbinieki.
- 5.7. IS administratīvās pārvaldības atbildības kategorijas tiek noteiktas saskaņā ar koncerna sabiedrībā noteikto kārtību.
- 5.8. IS turētājs ir atbilstošas Koncerna un Latvenergo kapitālsabiedrību pamatdarbības vai atbalsta funkcijas noteikts darbinieks.
- 5.9. IS turētāja pienākumi un atbildība:
 - 5.9.1. Nosaka IS attīstību;
 - 5.9.2. Izvērtē būtiskos kiberriskus;
 - 5.9.3. Nodrošina IS atbilstību Politikai un regulējošās vides prasībām.
- 5.10. IS resursa turētājs ir IS turētāja noteikts darbinieks.

Numurs: P069 Redakcija: 01	Politika Latvenergo koncerna Kiberdrošības politika	Lapa 4 (5)
-------------------------------	--	------------

- 5.11. IS resursa turētāja pienākumi un atbildība:
 - 5.11.1. Saskaņo ar IS attīstību saistītos funkcionālos izmaiņu pieprasījumus;
 - 5.11.2. Nodrošina Lietotāju piekļuves tiesību pārvaldību, aktualizē piekļuves tiesību reģistru;
 - 5.11.3. Veic IS informācijas resursu klasificēšanu;
 - 5.11.4. Veic kiberrisku pārvaldību;
 - 5.11.5. Nosaka IS resursa SLA (*Service Level Agreement*) kritērijus;
 - 5.11.6. Nodrošina pamatdarbības vai atbalsta funkciju IS prasību definēšanu.
- 5.12. IS galvenais lietotājs ir IS resursa turētāja noteikts darbinieks.
- 5.13. IS galvenā lietotāja pienākumi un atbildība:
 - 5.13.1. Izvērtē un analizē ar IS saistītos pieprasījumus (t. sk. pieteikumu apstrādes sistēmas BURA pieteikumus, izmaiņu pieprasījumus, incidentus, problēmas);
 - 5.13.2. Veic akcepttestēšanu;
 - 5.13.3. Nodrošina datu integritātes pārbaudes;
 - 5.13.4. Nodrošina IS lietotāju (turpmāk – Lietotājs) apmācību un atbalstu;
 - 5.13.5. Piedalās kiberrisku pārvaldībā.
- 5.14. Koncerna un Latvenergo kapitālsabiedrību Lietotājs ir persona, kura stājusies darba tiesiskajās attiecībās ar Koncerna un Latvenergo kapitālsabiedrību.
- 5.15. Lietotāja pienākumi un atbildība:
 - 5.15.1. Ievēro Politikā un saistītajos normatīvos aktos noteiktās kiberdrošības prasības;
 - 5.15.2. Ievēro noteikumus, vadlīnijas un procedūras, kas attiecas uz IS un to komponentu aizsardzību, atbilstošu lietošanu;
 - 5.15.3. Rūpējas par IS kiberdrošību un rīkojas, lai aizsargātu sevi un koncerna resursus ikdienā;
 - 5.15.4. Pieprasa un pēc kiberdrošības apmācību sekmīgas apguves saņem piekļuves tiesības darbam ar nepieciešamajiem IS resursiem;
 - 5.15.5. Izmanto IS resursus atbilstoši piešķirtajām piekļuves tiesībām;
 - 5.15.6. Pret IS resursiem izturas godprātīgi un ievēro konfidencialitāti;
 - 5.15.7. Nekavējoties ziņo AS "Latvenergo" Operatīvās vadības centram (palīdzības dienestam), ja ir aizdomas par kiberdrošības incidentu, gandrīz notikušu kiberincidentu, aizdomām par kiberincidentu vai Politikas vai citos kiberdrošības dokumentos minēto nosacījumu pārkāpumu, kā rezultātā var būt apdraudēta IS konfidencialitāte, integritāte vai pieejamība;
 - 5.15.8. Apmeklē koncerna sabiedrības sākotnējās, ikgadējās un ārkārtas kiberdrošības apmācības.

6. Sadarbība un Politikas uzraudzība

- 6.1. AS "Latvenergo" IT un T Drošības analīzes funkcija koordinē Politikas ieviešanu Koncernā un Latvenergo kapitālsabiedrībās, sadarbojoties ar kiberdrošības pārvaldnieku un Koncerna un Latvenergo kapitālsabiedrību sabiedrību struktūrvienībām.
- 6.2. Kiberdrošības pārvaldnieks sadarbojas ar valsts institūcijām ārējos normatīvos aktos noteiktajos gadījumos.
- 6.3. Par Politikas uzturēšanu un kontroli ir atbildīgs kiberdrošības pārvaldnieks.
- 6.4. Politika tiek aktualizēta, ņemot vērā izmaiņas normatīvajos aktos, dokumentētu kiberdrošības incidentu, kiberdrošības pārbaužu un kiberrisku novērtējumus, bet ne retāk kā reizi trijos gados.
- 6.5. Koncerna un Latvenergo kapitālsabiedrību IS resursu izmantošanu un piekļuvi kontrolē AS "Latvenergo" IT un T Drošības analīzes funkcija, organizējot kiberdrošības notikumu novērošanu, analīzi, lai noteiktu izmantoto kiberdrošības līdzekļu pietiekamību, atbilstību,

Numurs: P069 Redakcija: 01	Politika Latvenergo koncerna Kiberdrošības politika	Lapa 5 (5)
-------------------------------	--	------------

lietderību, konstatētu kiberdrošības pārkāpumus, izstrādātu ieteikumus kiberdrošības pārbaudes līdzekļu un kiberdrošības procedūru uzlabošanai.

- 6.6. Koncerna un Latvenergo kapitālsabiedrību kiberdrošības pārvaldības ārējās atbilstības pārbaudes var veikt tikai Kiberdrošības auditoru sarakstā iekļauts auditors (saskaņā ar Nacionālās kiberdrošības likuma 44.pantu), sniedzot ziņojumu par aktuālo kiberdrošības kontroļu efektivitāti, kopējo kiberdrošības līmeni. Šiem ziņojumiem tiek noteikts ierobežotas pieejamība statuss.