



Energiaviraston ohjeistus sähköverkonhaltijoiden varautumis- ja valmiussuunnittelusta 2025

1.1 Asiaan liittyvä lainsäädäntö

Sähkömarkkinalain (588/2013) 28 §:n mukaan

Verkonhaltijan on asianmukaisella suunnittelulla varauduttava sähköverkkoonsa kohdistuviin normaaliolojen häiriötilanteisiin, sähköjärjestelmässä ilmenevien sähkönsaannin häiriöiden edellyttämien säännöstelytoimenpiteiden täytäntöönpanoon ja valmiuslaissa tarkoitettuihin poikkeusoloihin. Verkonhaltijan on laadittava varautumissuunnitelma sekä osallistuttava tarpeellisessa laajuudessa huoltovarmuuden turvaamiseen tähtäävään valmiussuunnitteluun. Varautumissuunnitelma on päivitettävä vähintään kerran kolmessa vuodessa ja silloin, kun olosuhteissa tapahtuu merkittäviä muutoksia.

Tarkempia säännöksiä varautumissuunnitelman sisällöstä voidaan antaa valtioneuvoston asetuksella. Säännökset voivat koskea yhteiskunnan johtamisen ja turvallisuuden, väestön toimeentulon sekä elinkeinoelämän toimintakyvyn varmistamiseksi tarpeellista sähköverkkojen toiminnan sekä sähkönsiirron ja -jakelun järjestelyä.

Varautumissuunnitelma ja siihen tehtävät muutokset on toimitettava Energiavirastolle. Energiavirastolla on oikeus kuuden kuukauden kuluessa varautumissuunnitelman vastaanottamisesta vaatia verkonhaltijaa tekemään siihen muutoksia, jos se ei täytä säädettyjä vaatimuksia.

1.1.1 Muuttuva varautumislainsäädäntö

Kriittisten toimijoiden häiriönsietokykyä koskevan Euroopan parlamentin ja neuvoston direktiivin (EU) 2022/2557 (CER direktiivi) kansallinen täytäntöönpano on tämän ohjeistuksen antohetkellä vielä kesken, joten on siten toistaiseksi epäselvää, miten direktiivi tulee vaikuttamaan sähköverkonhaltijoiden riskienhallintavoitteisiin. Sisäministeriö on 19.12.2024 antanut eduskunnalle hallituksen esityksen HE 205/2024 vp, jonka tarkoituksena on panna täytäntöön kriittisten toimijoiden häiriönsietokykyä koskeva CER-direktiivi. Hallituksen esityksessä ehdotetun lain yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta 30 §:n mukaan päätös kriittisen toimijan määrittämisestä tehdään ensimmäisen kerran viimeistään 17.7.2026 ja edelleen näiden toimijoiden on laadittava häiriönsietokykyä koskeva suunnitelma ensimmäisen kerran loppukeväästä 2028. Näin ollen sähköverkonhaltijat, joiden katsotaan olevan lain tarkoittamia kriittisiä toimijoita, on huomioitava kyseisessä laissa esitetyt uudet vaatimukset 30.6.2028 toimitettavissa varautumissuunnitelmissa.

Eduskunnalle annetussa hallituksen esityksessä sähkömarkkinalain 28 §:ää ei kuitenkaan olla kumoamassa direktiivin täytäntöönpanon yhteydessä, joten sähköverkonhaltijoiden on todennäköisesti jatkossakin toimitettava varautumis- ja valmiussuunnitelmansa Energiavirastolle kolmen vuoden välein.



Edellä mainitun perusteella sähköverkonhaltijoiden on laadittava sähkömarkkinalain 28 §:n mukaiset varautumissuunnitelmat ja toimittavat ne Energiavirastolle 30.6.2025 mennessä, jollei toisin ohjeisteta.

1.1.2 Muuttuva kyberturvallisuuslainsäädäntö

Sähkömarkkinalain 29 a §:n mukaan

Verkonhaltijan on huolehdittava käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta.

Sähkömarkkinalain 29 a §:n esitöiden mukaisesti tietoturvariskienhallinta on tehtävä dokumentoidusti ja dokumentointi voidaan ottaa osaksi 28 §:ssä tarkoitettua varautumissuunnitelmaa. Energiaviraston valvonta on 29 a §:n osalta sinänsä jälkivalvontaa. Tietoturvariskien hallinta liittyy kuitenkin olennaisesti verkonhaltijan varautumissuunnitteluun ja siksi varautumissuunnitelmassa on tuotava esille tietoturvariskienhallinnan peruseräpäätteet ja toimintamallit.

Edellä mainittu sähkömarkkinalain 29 a § on ehdotettu kumottavaksi NIS2-direktiivin täytäntöönpanon yhteydessä. NIS2-direktiivin velvoitteet on tarkoitus panna täytäntöön Kyberturvallisuuslailla (XXX/2024). Lailla on ehdotettu kumottavaksi myös sähköverkonhaltijoita koskeva sähkömarkkinalain 29 a § velvoite viestintäverkkojen ja tietojärjestelmien riskienhallinnasta, josta säädettiin alkupe-
räisen NIS-direktiivin täytäntöönpanossa.

Energiavirasto toteaa, että **viestintäverkkojen ja tietojärjestelmien toiminnan häiriöttömyyden ja toiminnan jatkuvuuden turvaaminen ovat edelleen keskeinen osa sähkömarkkinalain 28 §:n mukaista varautumissuunnittelua**, jolla verkonhaltijan on varauduttava sähköverkkoonsa kohdistuviin normaaliolojen häiriötilanteisiin, sähköjärjestelmässä ilmenevien sähkönsaannin häiriöiden edellyttämien säännöstelytoimenpiteiden täytäntöönpanoon ja valmiuslaissa tarkoitettuihin poikkeusoloihin. **Tästä syystä verkonhaltijoiden on jatkossakin kuvattava varautumissuunnitelmassaan mallipohjan 9 luvussa esitettyjä asioita.**

Tämän ohjeistuksen antohetkellä on vielä epäselvää, sovelletaanko tulevaa kyberturvallisuuslakia kaikkiin sähköverkonhaltijoihin. Ehdotetun kyberturvallisuuslain mukaan toimijoiden on ilmoitauduttava valvoville viranomaisille viimeistään 31.12.2024 mennessä, mikäli toimija täyttää lain soveltamisalaan kuulumisen edellytykset. Lain täytäntöönpano on kuitenkin viivästynyt ja todennäköisesti ilmoittautumisaikataulua jatketaan ensi vuoden puolelle.

Energiavirasto tulee ehdotetun kyberturvallisuuslain mukaan toimimaan valvovana viranomaisena sähkötoimialalla. Energiavirasto antaa kyberturvallisuuslaista ml. toimijaluetteloon ilmoittautumisesta tarkemman ohjeistuksen lain tultua voimaan.

Ehdotetun kyberturvallisuuslain 3 §:n mukaisesti sähköverkonhaltijat voivat kuulua lain soveltamisalaan, mikäli:

(toimija) täyttää tai ylittää mikroyritysten sekä pienten ja keskisuurten yritysten määritelmästä annetun komission suosituksen 2003/361/EY liit-



teen 2 artiklan mukaiset keskisuuria yrityksiä koskevat edellytykset ja tarjoaa palvelujaan tai harjoittaa toimintaansa jossakin Euroopan unionin jäsenvaltiossa;

Lisäksi lakia sovelletaan sähköverkonhaltijaan sen koosta riippumatta, jos:

- 1) se tarjoaa palvelua, joka on yhteiskunnan tai talouden kriittisten toimintojen ylläpitämisen kannalta keskeinen ja jota muut toimijat eivät tarjoa;*
- 2) häiriö sen tarjoamassa palvelussa vaikuttaisi merkittävästi yleiseen järjestykseen, yleiseen turvallisuuteen tai kansanterveyteen;*
- 3) häiriö sen tarjoamassa palvelussa voisi aiheuttaa merkittävän systemisen riskin erityisesti aloilla, joilla tällaisella häiriöllä voisi olla rajat ylittäviä vaikutuksia; tai*
- 4) se on kriittinen, koska sillä on erityisen suuri merkitys kansallisella tai alueellisella tasolla kyseisen toimialan tai palvelutyypin tai jonkin Euroopan unionin jäsenvaltion muiden keskinäisriippuvaisten toimialojen kannalta.*

Ehdotetun lain mukaan edellä tarkoitetuista kriteereistä voidaan antaa tarkempia säännöksiä valtioneuvoston asetuksella.

NIS2-direktiivin mukaisesti myös sähköverkonhaltijat, jotka määritetään määritetty kriittisiksi toimijoiksi CER-direktiivin (EU) 2022/2557 nojalla kuuluu tulkita NIS2-direktiivin ja siten myös Kyberturvallisuuslain soveltamisalaan. Asiasta säädetään CER-direktiivin kansallisen täytäntöönpanon yhteydessä.

Ehdotetun kyberturvallisuuslain riskienhallintaa koskevat pykälät:

7 § Riskienhallinta

Toimijan on tunnistettava, arvioitava ja hallittava riskejä, joita kohdistuu sen toiminnoissa tai palveluntarjonnassa käytettävien viestintäverkkojen ja tietojärjestelmien turvallisuuteen. Kyberturvallisuutta koskevalla riskienhallinnalla tulee estää tai minimoida poikkeamien vaikutus toimintaan, toiminnan jatkuvuuteen, palvelujen vastaanottajiin ja muihin palveluihin.

Toimijan on toteutettava riskienhallintatoimenpiteet, jotka ovat ajantasaisia, oikeasuhtaisia ja riittäviä suhteessa toiminnassa käytettäville viestintäverkoille ja tietojärjestelmille aiheutuviin riskeihin ja viestintäverkon tai tietojärjestelmän merkitykseen toimijan toiminnan ja palveluntarjonnan kannalta.

8 § Kyberturvallisuutta koskeva riskienhallinnan toimintamalli

Toimijalla on oltava käytössä ajantasainen kyberturvallisuutta koskeva riskienhallinnan toimintamalli viestintäverkkojen ja tietojärjestelmien ja



niiden fyysisen ympäristön suojaamiseksi poikkeamilta ja niiden vaikutuksilta.

Kyberturvallisuutta koskevassa riskienhallinnan toimintamallissa on tunnistettava viestintäverkkoihin ja tietojärjestelmiin ja niiden fyysiseen ympäristöön kohdistuvat riskit ottaen huomioon kaikki vaaratekijät huomioitava lähestymistapa. Toimintamallissa on määritettävä ja kuvattava kyberturvallisuutta koskevan riskienhallinnan tavoitteet, menettelyt ja vastuut sekä 9 §:n mukaiset toimenpiteet, joilla viestintäverkkoja ja tietojärjestelmiä ja niiden fyysistä ympäristöä suojataan kyberuhkilta ja poikkeamilta (hallintatoimenpiteet).

9 § Toimenpiteet kyberturvallisuutta koskevien riskien hallinnassa

Toimijoiden on toteutettava kyberturvallisuutta koskevan riskienhallinnan toimintamallin mukaiset oikeasuhtaiset tekniset, operatiiviset tai organisatoriset hallintatoimenpiteet viestintäverkkojen ja tietojärjestelmien turvallisuuteen kohdistuvien riskien hallitsemiseksi ja haitallisten vaikutusten estämiseksi tai minimoimiseksi.

Toimintamallissa ja siihen perustuvissa hallintatoimenpiteissä on otettava huomioon ja pidettävä yllä ajantasaisesti ainakin:

- 1) kyberturvallisuutta koskevan riskienhallinnan toimintaperiaatteet ja hallintatoimenpiteiden vaikuttavuuden arviointi;*
- 2) viestintäverkkojen ja tietojärjestelmien turvallisuutta koskevat toimintaperiaatteet;*
- 3) viestintäverkkojen ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus sekä tarvittavat menettelyt haavoittuvuuksien käsittelemiseksi ja julkistamiseksi;*
- 4) toimitusketjun välittömien toimittajien tuotteiden ja palveluntarjoajien palvelujen yleinen laatu ja häiriönsietokyky, niihin sisällytetyt hallintatoimenpiteet sekä välittömien toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt;*
- 5) omaisuudenhallinta ja sen turvallisuuden kannalta tärkeiden toimintojen tunnistaminen;*
- 6) henkilöstöturvallisuus ja kyberturvallisuuskoulutus;*
- 7) pääsynhallinnan ja todentamisen menettelyt;*
- 8) salausten menetelmien käyttämistä koskevat toimintaperiaatteet ja menettelyt sekä tarvittaessa toimenpiteet suojatun sähköisen viestinnän käyttämiseksi;*
- 9) poikkeamien havainnointi ja käsittely turvallisuuden ja toimintavarmuuden palauttamiseksi ja ylläpitämiseksi;*



10) varmuuskopiointi, palautumissuunnittelu, kriisinhallinta ja muu toiminnan jatkuvuuden hallinta ja tarvittaessa suojattujen varaviestintäjärjestelmien käyttö;

11) perustason tietoturvakäytännöt toiminnan, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden ja tietoaineistoturvallisuuden varmistamiseksi; sekä

12) toimenpiteet viestintäverkkojen ja tietojärjestelmien fyysisen ympäristön ja tilaturvallisuuden sekä välttämättömien resurssien varmistamiseksi.

Toimenpiteet on suhteutettava toiminnan laatuun ja laajuuteen, poikkeamasta kohtuudella ennakoitavissa oleviin välittömiin vaikutuksiin, toimijan viestintäverkkojen ja tietojärjestelmien riskialttiuteen, poikkeamien todennäköisyyteen ja vakavuuteen, toimenpiteistä aiheutuviin kustannuksiin sekä ajantasainen kehitys huomioon ottaen käytettävissä oleviin teknisiin mahdollisuuksiin torjua uhka.

Valvova viranomainen voi toimialallaan antaa riskienhallintavelvollisuuksia tarkentavia teknisiä määräyksiä:

1) toimialakohtaisista erityispiirteistä, jotka on otettava huomioon kyberturvallisuutta koskevassa riskienhallinnan toimintamallissa ja 2 momentissa tarkoitetuissa osa-alueissa sekä riskienhallinnan ja viestintäverkkojen ja tietojärjestelmien tietoturvallisuuden hallinnan menettelyissä;

2) kriittisiä toimitusketjuja koskevien unionin tason koordinoitujen riskinarviointien tuloksien huomioimisesta toimialakohtaisessa riskienhallinnassa.

Riskienhallinnassa, riskienhallinnan toimintamallissa ja hallintatoimenpiteissä on noudatettava lisäksi NIS 2 -direktiivin 21 artiklan 5 kohdan nojalla annettavia Euroopan komission täytäntöönpanosäädöksiä.

10 § Johdon vastuu

Toimijan johto vastaa kyberturvallisuutta koskevan riskienhallinnan toteuttamisen ja valvonnan järjestämisestä sekä hyväksyy kyberturvallisuutta koskevan riskienhallinnan toimintamallin ja valvoo sen toteuttamista. Toimijan johdolla tulee olla riittävä perehtyneisyys kyberturvallisuutta koskevaan riskienhallintaan.

Johdolla tarkoitetaan toimijan hallitusta, hallintoneuvostoa ja toimitusjohtajaa sekä muussa niihin rinnastettavassa asemassa olevaa, joka tosiasiallisesti johtaa sen toimintaa.

1.1.3 Muuttuva valmiuslaki

Nykyisen valmiuslain (1552/2011) kokonaisuudistus on parhaillaan työn alla oikeusministeriön johdolla. Uudistuksen tavoitteena on saattaa valmiuslaki vastamaan nykyaikaista käsitystä yhteiskunnan kokonaisturvallisuudesta ja sitä uhkaa-



vista tekijöistä sekä erilaisten vaikutuksiltaan vakavien uhka- ja häiriötilanteiden tunnistamisesta. Oikeusministeriön mukaan hallituksen esitys on tarkoitus antaa eduskunnalle viimeistään syysistuntokaudella 2025. Hallituksen esityksen luonnos on tarkoitus lähettää julkiselle lausuntokierrokselle vuoden 2025 alkupuolella.

Valmiussuunnitelman osalta sähköverkonhaltijoiden on huomioitava 30.6.2025 toimitettavissa suunnitelmissa erityisesti valmiuslain päivittämisestä riippumattomat seikat, kuten henkilöstön, palveluntuottajien ja ajoneuvojen varaukset sekä kriittisten kohteiden suojaaminen ja valvon väistösuunnitelma.

Energiavirasto voi, muun muassa valmiuslain sähkön käytön rajoittamista koskevien säännösten muutosten merkittävydestä riippuen, vaatia sähköverkonhaltijoita päivittämään valmiussuunnitelmiaan uudelleen jo ennen seuraavia 30.6.2028 toimitettavia suunnitelmia.

1.2 Vaadittu sisältö ja aikataulu

Verkonhaltijoiden katsotaan täyttävän sähkömarkkinalain 28 §:n mukaiset velvoitteet toimittamalla Energiavirastolle:

- 1) Varautumissuunnitelman, jonka mukaisesti verkkonhaltija varautuu sähköverkkoon kohdistuviin normaaliolojen häiriötilanteisiin;
 - a. **Vuonna 2025 toimitettaviin suunnitelmiin on sisällytettävä yhtiön uusi riskikartoitus.**
- 2) Valmiussuunnitelman, jonka mukaisesti verkkonhaltija varautuu valmiuslaissa tarkoitettuihin poikkeusoloihin;
- 3) Varautumissuunnitelman ja valmiussuunnitelman pohjalta täytetyn SÄHKÖKOTKA 2021-työkalun, jolla verkkonhaltija arvioi oman varautumisensa tasoa varautumisen eri osa-alueilla. Työkalussa asetetaan myös kehittämistavoitteet seuraavan kolmen vuoden jaksolle. SÄHKÖKOTKA 2021-työkalu on ladattavissa Huoltovarmuuskeskuksen extranetistä Energiahuoltosektorin yhteisalueelta osoitteesta: <https://extranet.huoltovarmuus.fi/>. SÄHKÖKOTKA 2021-työkalusta pyydetään toimittamaan seuraavat tiedostot:
 - a. Raportti pdf-muodossa
 - b. Keskustelumuistio pdf-muodossa
 - c. Vastausdata Excel-muodossa



VAIHE 4: Paina Raportti näytölle-painiketta jolloin saat raportin näytölle nähtäväksi. Voit tulostaa raportin halutessasi. Samalla tavalla saat Keskustelumuistio näytölle-painikkeella Keskustelumuistion nähtäväksi ja tulostettavaksi. Raportin käsittelyn jälkeen siirry viimeiseen	RAPORTTI-sivu	<= Paluu toimenpiteisiin	Raportti näytölle
VAIHE 5: Tallenna asiakirja lopuksi haluamaasi paikkaan Tiedosto-valikon tallennuskomennolla. Tarvittaessa voit Datan tallennus -painikkeella siirtää arvioinnin tulokset erilliseen Excel-työkirjaan. Tallenna tämä työkirja tarvittaessa annetun ohjeen mukaisesti.		Keskustelumuistio näytölle	=> Datan tallennus
Paluu toimenpiteisiin -painikkeella pääset takaisin muokkaamaan kirjoittamiasi toimenpiteitä. Jos teet muutoksia toimenpiteisiin, sinun täytyy tehdä uudestaan myös vaiheet 4 ja 5.			

Kuva 1. SÄHKÖKOTKA 2021-työkalun raporttisivu.

Pyydetty SÄHKÖKOTKA-tiedostot löytyvät työkalun raporttisivulta kuvan 1. mukaisten "Raportti näytölle", "Keskustelumuistio näytölle" ja "Datan tallennus" painikkeiden takaa.

Vaaditut suunnitelmat on sähkömarkkinalain mukaisesti toimitettava Energiavirastolle **30.6.2025 mennessä**. Tämän jälkeen suunnitelmaa on päivitettävä vähintään kerran kolmessa vuodessa ja silloin, kun olosuhteissa tapahtuu merkittäviä muutoksia.

1.3 Seuraavissa suunnitelmissa painotettavat asiat

1.3.1 Riskikartoitus

Varautumissuunnitelman on vastattava ajankohtaisiin riskeihin. Energiaviraston mallipohjassa on vakiintuneesti pyydetty kuvaamaan yhtiön riskikartoitusprosessia sekä varautumista tiettyihin keskeisiin riskeihin. Olennaista onkin, että verkonhaltijat tunnistavat itse toimintaansa uhkaavat riskit ja varautuvat niihin asianmukaisesti. Myös kansallisessa täytäntöönpanossa oleva CER-direktiivi edellyttää, että "Kriittisten toimijoiden riskinarvioinneissa on otettava huomioon kaikki merkitykselliset luonnon ja ihmisen aiheuttamat riskit, jotka voivat johtaa poikkeamaan, mukaan lukien toimialojen tai rajatylittävät riskit, onnettomuudet, luonnonkatastrofit, kansanterveydelliset hätätilanteet ja hybridiuhat ja muut vihamieliset uhat, mukaan lukien direktiivissä (EU) 2017/541 säädetyt terrorismirikokset. Kriittisen toimijan riskinarvioinnissa on otettava huomioon se, missä määrin muut liitteessä tarkoitettujen toimialojen toimijat ovat riippuvaisia kriittisen toimijan tarjoamasta keskeisestä palvelusta, mukaan lukien tapauksen mukaan myös naapurijäsenvaltioissa ja kolmansissa maissa."

Riskikartoituksessa suositellaan hyödyntämään Huoltovarmuusorganisaation "Energiahuollon tuotannon ja toimintaketjujen riskeihin varautuminen" selvityksen tuloksia. Työn on tarkoitus valmistua toukokuussa 2025.

Seuraaviin 30.6.2025 mennessä toimitettaviin suunnitelmiin on liitettävä Energiaviraston Riskiarviopohja.xls-pohjan mukainen riskikartoitus, jossa kuvataan 10-15 keskeisintä yhtiön tunnistamaa riskiä, jotka voivat vaikuttaa sähkön jakelu- tai siirtopalvelun tarjontaan ml. keskeisimmät kyberturvallisuusriskit.

Näihin keskeisiin riskeihin varautumista on syytä edelleen kuvata suunnitelmassa. Esimerkiksi mallipohjan lukuun 8: Muihin häiriötilanteisiin varautuminen ja toimin-



ta häiriötilanteessa voi lisätä – jo tunnistettujen keskeisten riskien lisäksi - uusia alakohtia kohdasta 8.10 alkaen ja nimetä ne asianmukaisesti.

Suunnitelmien yhdenmukaisuuden vuoksi olemme kuitenkin tuoneet mallipohjan lukuun 8 kaksi uutta häiriötyyppiä kaikkien vastattavaksi: 8.8 Hybridivaikuttamiseen varautuminen sekä 8.9 Markkinahäiriöihin varautuminen.

1.3.2 Muutosmerkinnät

Varautumisen kehittäminen on iteratiivinen prosessi, eikä koko suunnitelmaa siksi ole tarkoitus uusia jokaisella päivityskierroksella. Suunnitelmien jatkuvuuden edistämiseksi myös varautumis- ja valmiussuunnitelmien mallipohjat on pyritty pitämään mahdollisimman ennallaan.

Seuraavissa suunnitelmissa ohjeistammekin verkonhaltijoita keskittymään erityisesti edellisissä suunnitelmissa havaitsemiensa puutteiden kehittämiseen tuomalla esiin miten vuonna 2022 tehdyssä suunnitelmassa esitetyt kehitystoimenpiteet on saatu tehtyä. **Mikäli mahdollista, päivitettyt kohdat on selkeyden vuoksi esitettävä sinisellä tekstillä.**

Suunnitelman alussa on myös hyvä ylläpitää listaa versiohistoriasta, josta käy ilmi, milloin suunnitelmaa on päivitetty, mitkä olivat keskeisimmät muutokset ja kuka oli päivityksen vastuuhenkilö.

1.3.3 Kehityskohteet

Verkonhaltijat ovat aiemmin tuoneet vaihtelevasti esille kehityskohteitaan. Seuraavien suunnitelmien tarkastuksessa painotetaan sitä, että kaikki **verkonhaltijat ovat tunnistaneet, vastuuttaneet ja aikatauluttaneet varautumis- ja valmiussuunnittelua koskevat kehityskohteensa**. Yhdenmukaisuuden vuoksi suosittelemme käyttämään tähän tarkoitukseen luotua SÄHKÖKOTKA-työkalun toimenpidesivua.

1.3.4 Valtioneuvoston asetus varautumissuunnitelmaan sisällytettävästä sähkönkäyttöpaikkojen etusijajärjestyksestä (TEM/2022/211)

9. joulukuuta 2022 voimaantulleen Valtioneuvoston asetuksen 4 §:n mukaisesti **sähköverkonhaltijoiden on päivitettävä sähkönkäyttöpaikkojen etusijajärjestys varautumissuunnitelman päivittämisen yhteydessä**. Seuraavat 30.6.2025 toimitettavat varautumissuunnitelmat ovat ensimmäiset varautumissuunnitelmat, joissa asetuksen 3 §:n mukainen muiden kuin kriittisten sähkönkäyttöpaikkojen etusijajärjestys on määritettävä.

3 §:n mukaisesti:

Verkonhaltijan varautumissuunnitelmassa on määritettävä muiden sähkönkäyttöpaikkojen kuin kriittisten sähkönkäyttöpaikkojen etusijajärjestys häiriö-, sähköpu-la- ja kriisitilanteita varten. Etusijajärjestyksen asettamisessa on huomioitava yhteiskunnan johtamisen ja turvallisuuden, väestön toimeentulon sekä elinkei-noelämän toimintakyvyn kannalta tärkeät sähkönkäyttöpaikat.



Muut sähkönkäyttöpaikat on luokiteltava vähintään kolmeen eri ryhmään seuraavasti:

- 1) sähkönkäyttöpaikat, joiden sähkönsaannin keskeyttämistä on vältettävä;*
- 2) sähkönkäyttöpaikat, joiden sähkönsaanti voi keskeytyä lyhyeksi ajaksi;*
- 3) sähkönkäyttöpaikat, joiden sähkönsaanti voi keskeytyä lyhyttä pidemmäksi ajaksi.*

Varautumissuunnitelmassa sähkönkäyttöpaikkojen etusijajärjestys on kuvattava mallipohjan uudessa luvussa 11.2 "Muiden sähkönkäyttöpaikkojen etusijajärjestys". Verkonhaltijoiden on suunnitelmassaan kuvattava vähintään: moneenko ryhmään sähkönkäyttöpaikat ryhmitellään, minkätyyppiset sähkönkäyttöpaikat kuhunkin ryhmään kuuluvat, kuinka monta sähkönkäyttöpaikkaa ryhmään kuuluu, ja mikä on kunkin ryhmän tärkeysluokka (ts. kuinka pitkäksi aikaa sähkönsaanti voi keskeytyä).

Sähkönkäyttöpaikkojen etusijajärjestyksen määrittelyssä suositellaan käyttämään apuna Huoltovarmuusorganisaation poolien yhdessä määrittämää taulukkoa eri toimialojen käyttöpaikkojen keskeytyskriittisyydestä. Taulukko on julkaistu tamikuussa 2024 HVO:n Sähköpoolin yhteisalueella.

1.4 Tietojen julkisuus

Varautumissuunnitelmat ja valmiussuunnitelmat ovat julkisuuslain (621/1999) 24 §:n 7 ja 8 kohtien mukaisesti kokonaisuudessaan salassa pidettäviä.

Sähköverkonhaltijoiden varautumissuunnittelua valvovana viranomaisena Energiavirasto määrittelee salassa pidettävän tiedon suojaustason tapauskohtaisesti tiedon salassa pidettävyyden mukaisesti. Suunnitelmiin ei ole syytä sisällyttää tarpeettomasti sellaista salassa pidettävää tietoa, jonka paljastuminen voi aiheuttaa vahinkoa "tiedonhallintalain 18 §:n 1 momentissa tarkoitetulle suojattavalle edulle". Varautumissuunnitelmaan ei esimerkiksi ole syytä ilmoittaa kriittisten kohteiden kuten konesalien ja varavalmomoiden sijaintia tai yksilöidä vastuuhenkilöiden nimiä vaan tehtävänimikkeet riittävät.¹

1.5 Mallipohjan soveltaminen

Energiavirasto on valmistanut verkonhaltijoiden suunnittelun tueksi liitteenä olevat mallipohja-asiakirjat.

Päivitetyt mallipohjat on luotu vuonna 2021 päivitetyn SÄHKÖKOTKA 2021-itsearviointityökalun kypsyyskysymysten pohjalta siten, että mallipohjien otsikkotasot vastaavat kypsyyskysymysten asettelua samassa järjestyksessä. Varautumissuunnitelman mallipohjasta on kuitenkin jätetty pois muutama yksittäinen kysymys ja palveluntuottajaosiossa on yhdistetty erityyppisiä palveluntuottajia koskevat otsikot yhteen. Mallipohjia on päivitetty edelleen vuonna 2024 edellisten

¹ Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa 1101/2019 3 §.



4090/040002/2024

suunnitelmien havaintojen, muuttuneen toimintaympäristön ja lainsäädäntömuutosten perusteella.

Kyberturvallisuuden hallinnan kartoittamiseksi **pyydämme kaikkia yhtiöitä vastaamaan suunnitelmassaan mallipohjan 9.1 kappaleessa olevaan kysymykseen:**

Rasti alta standardit, kybermaturiteetin mittaustyökalut, ohjeet ja tietoturvan hallintajärjestelmät, joita käytätte nyt tai olette aiemmin käyttäneet.

Voit halutessasi myös kommentoida miten ja mihin olette käyttäneet niitä.

☐ *Kybermittari,*

☐ *TIKKA 2016 –Tietoturvallisuuden arviointityökalu - tietoturvallisuuden itsearviointityökalu sähköverkkoyhtiöiden tietoturvallisuuden arviointiin,*

☐ *TIKKA Tietoturvallisuustilanteen kartoitustyökalu pienille yrityksille,*

☐ *ISO/IEC 27000 -sarja,*

☐ *ISA/IEC 62443 -sarja,*

☐ *ISO 9001 -sarja,*

☐ *NIST Special publication (SP) ja NIST Interagency/Internal Report (NISTIR) -sarjat,*

☐ *ISF Maturity Model,*

☐ *NIST Cybersecurity Capability Maturity Model (CSF),*

☐ *Cybersecurity Capability Maturity Model (C2M2),*

☐ *CIS Critical Security Controls (CSC),*

☐ *KATAKRI 2020,*

☐ *joku muu, mikä/mitkä? _____*

Avoin kommentti _____

Kaikkia mallipohjien tekstejä tulee muokata sähköverkonhaltijan tarpeiden mukaisesti. Kysymysmuodossa oleviin teksteihin ei ole tarkoitus vastata sellaisenaan vaan niiden tarkoitus on tuoda esille asioita, joita varautumis- ja valmiussuunnitelmassa odotetaan olevan.

Suunnitelmiin voi linkittää muita varautumiseen liittyviä dokumentteja etenkin, jos näitä ylläpidetään erikseen. Esimerkiksi vastuuhenkilöitä, yhteystietoja ja muita usein päivitettäviä tietoja voidaan ylläpitää erillisissä dokumenteissa, joihin varautumissuunnitelmassa viitataan. Vastaavasti varautumiseen liittyviä asioita on suotavaa jakaa pienempiin kokonaisuuksiin. Esimerkiksi kriisiviestintäsuunnitelmaa tai tietoturvapoliittikkaa ei ole tarkoituksenmukaista kokonaisuudessaan sisäl-

4090/040002/2024

lyttää varautumissuunnitelmaan, vaan niitä on suotavampaa ylläpitää erillisinä liitteinä, joihin varautumissuunnitelmassa viitataan. Näin varautumissuunnitelmasta ei muodostu liian isoa kokonaisuutta. Tällaisia yksityiskohtaisimpia liitteitä ei toimiteta Energiavirastolle suunnitelmien yhteydessä vaan ainoastaan erikseen pyydettyäessä.

Mallipohjan käyttö ei ole pakollista. Mikäli verkonhaltija tekee vapaamuotoiset varautumis- ja valmiussuunnitelmat, tulee suunnitelmissa kuitenkin huomioida ainakin näissä mallipohjissa esitetyt asiat. Verkonhaltijan tulee myös esittää SÄHKÖKOTKA 2021-työkalun kysymyskohtaisessa kommenttikentässä (kuva 2), missä kohdassa vapaamuotoista suunnitelmaa kyseiseen kysymykseen on vastaus. Vaihtoehtoisesti vapaamuotoisen suunnitelman otsikossa voi viitata SÄHKÖKOTKA:n kysymyksiin merkitsemällä SK #.

2. HÄIRIÖTILANTEIDEN HALLINAN VASTUUT JA JÄRJESTELYT	Vastaus	Painoarvo	Indeksi	Keskustelu / kommentit
Yhtiön toiminnan riskien analysointi	Ei koske	5	-	

Kuva 2. SÄHKÖKOTKA 2021 -työkalun kommenttikenttä.

1.6 Suunnitelmien toimittaminen Energiavirastolle

Suunnitelmat pyydetään toimittamaan Energiavirastoon turvapostilla osoitteeseen kirjaamo@energiavirasto.fi sekä kopiona varautumissuunnitelmat@energiavirasto.fi. Mikäli yrityksellänne ei ole käytössä turvapostipalvelua, voitte hyödyntää Energiaviraston turvapostipalvelua. Ole tällöin yhteydessä sähköpostilla osoitteeseen varautuminen@energiavirasto.fi.

Suunnitelman voi vaihtoehtoisesti toimittaa kirjattuna kirjeenä osoitteeseen: Energiavirasto, Lintulahdenkuja 2A, 00530 Helsinki.

Liitteet	Varautumissuunnitelman mallipohja Valmiussuunnitelman mallipohja
Jakelu	Sähkön kantaverkonhaltija Sähkön suurjännitteisen jakeluverkon haltijat Sähkön jakeluverkonhaltijat