Energimyndighetens anvisning om elnätsinnehavarnas förberednings- och beredskapsplanering

1.1 Relevant lagstiftning

Enligt 28 § i elmarknadslagen (588/2013)

> *Nätinnehavaren ska genom ändamålsenlig planering förbereda sig för störningar i elnätet under normala förhållanden, för genomförande av ransoneringsåtgärder som föranleds av störningar i tillgången på el i elsystemet och för sådana undantagsförhållanden som avses i beredskapslagen. Nätinnehavaren ska göra upp en beredskapsplan och i behövlig omfattning delta i beredskapsplanering som ska trygga försörjningsberedskapen. Beredskapsplanen ska uppdateras åtminstone en gång per tre år och när det sker en betydande förändring i omständigheterna.*
>
> *Närmare bestämmelser om innehållet i beredskapsplanen får utfärdas genom förordning av statsrådet. Bestämmelserna kan gälla nödvändigt ordnande av elnätsverksamhet och elöverföring eller eldistribution i syfte att säkerställa ledningen av och säkerheten i samhället, befolkningens försörjning och näringslivets funktionsförmåga.*
>
> *Beredskapsplanen och ändringar i den ska lämnas till Energimyndigheten. Energimyndigheten har rätt att inom sex månader från det att den mottagit beredskapsplanen kräva att nätinnehavaren gör ändringar i planen om den inte uppfyller de krav som föreskrivs.*

1.1.1 Lagstiftning om beredskap som ändras

Det nationella genomförandet av Europaparlamentets och rådets direktiv (EU) 2022/2557 (CER-direktivet) om kritiska entiteters motståndskraft pågår fortfarande när denna anvisning ges, så det är tills vidare oklart hur direktivet kommer att påverka skyldigheterna för elnätsinnehavarna i fråga om riskhantering. På basis av utkastet till regeringens proposition som var under offentligt hörande i början av 2024 kommer dock 28 § i elmarknadslagen inte att upphävas i samband med genomförandet av direktivet, vilket innebär att elnätsinnehavarna sannolikt även i fortsättningen ska lämna in sina beredskapsplaner till Energimyndigheten med tre års mellanrum.

På basis av det ovan nämnda ska elnätsinnehavarna utarbeta beredskapsplaner enligt 28 § i elmarknadslagen och lämna in dem till Energimyndigheten senast 30.6.2025, om inte något annat anvisas.

1.1.2 Lagstiftning om cybersäkerhet som ändras

Enligt 29 a § i elmarknadslagen

> *Nätinnehavare ska sörja för riskhanteringen i fråga om de kommunikationsnät och informationssystem som denne använder.*

Enligt förarbetena till 29 a § i elmarknadslagen ska hanteringen av informationssäkerhetsrisker dokumenteras och dokumentationen kan inkluderas i den beredskapsplan som avses i 28 §. Energimyndighetens tillsyn är i fråga om 29 a § i sig tillsyn i efterhand. Hanteringen av informationssäkerhetsrisker har dock en väsentlig koppling till nätinnehavarens beredskapsplanering och därför ska de grundläggande principerna och verksamhetsmodellerna för hanteringen av informationssäkerhetsrisker lyftas fram i beredskapsplanen.

Det föreslås att 29 a § i elmarknadslagen upphävs i samband med verkställandet av NIS2-direktivet. Avsikten är att skyldigheterna i NIS2-direktivet ska verkställas genom Cybersäkerhetslagen (XXX/2024). Genom lagen föreslås också att skyldigheten enligt 29 a § i elmarknadslagen som gäller elnätsinnehavarna om riskhantering i kommunikationsnät och informationssystem ska upphävas. Bestämmelser om riskhanteringen finns i det ursprungliga NIS-direktivet.

Energimyndigheten konstaterar att tryggandet av en störningsfri och kontinuerlig verksamhet i kommunikationsnäten och informationssystemen fortfarande är en central del av beredskapsplaneringen enligt 28 § i elmarknadslagen, med vilken nätinnehavaren ska förbereda sig på störningar i sitt elnät under normala förhållanden, genomförandet av de ransoneringsåtgärder som krävs på grund av störningar i eltillförseln till elsystemet och de undantagsförhållanden som avses i beredskapslagen. **Därför ska nätinnehavarna även i fortsättningen i sin beredskapsplan beskriva de saker som presenteras i kapitel 9 i mallen.**

När dessa anvisningar ges är det ännu oklart om den kommande cybersäkerhetslagen ska tillämpas på alla elnätsinnehavare. Enligt den föreslagna cybersäkerhetslagen ska aktörerna anmäla sig till de övervakande myndigheterna senast den 31 december 2024 om aktören uppfyller förutsättningarna för att omfattas av lagens tillämpningsområde. Verkställandet av lagen har dock fördröjts och anmälningstidtabellen förlängs sannolikt till nästa år.

Energimyndigheten kommer enligt den föreslagna cybersäkerhetslagen att vara tillsynsmyndighet inom elbranschen. Energimyndigheten ger närmare anvisningar om cybersäkerhetslagen inklusive anmälan till förteckningen över entiteter efter att lagen har trätt i kraft.

Enligt 3 § i den föreslagna cybersäkerhetslagen kan elnätsinnehavarna omfattas av lagens tillämpningsområde om:

> *(aktören) uppfyller eller överskrider villkoren för medelstora företag enligt artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG om definitionen av mikroföretag samt små och medelstora företag och som tillhandahåller sina tjänster eller bedriver sin verksamhet i en medlemsstat i Europeiska unionen;*

Dessutom tillämpas lagen på en elnätsinnehavare oberoende av dess storlek, om

> 1) *aktören tillhandahåller en tjänst som är väsentlig för att upprätthålla kritiska samhälleliga eller ekonomiska funktioner och som inte tillhandahålls av andra aktörer;*

2) *en störning av den tjänst som aktören tillhandahåller skulle ha en betydande påverkan på allmän ordning, allmän säkerhet eller folkhälsa;*

3) *en störning av den tjänst som aktören tillhandahåller kan medföra betydande systemrisker, särskilt för de sektorer där sådana störningar kan få gränsöverskridande konsekvenser; eller*

4) *aktören är kritisk på grund av sin särskilda betydelse på nationell eller regional nivå för en särskild sektor eller typ av tjänst, eller för andra sektorer i en medlemsstat i Europeiska unionen som är beroende av denna aktör.*

Enligt den föreslagna lagen kan närmare bestämmelser om ovan avsedda kriterier utfärdas genom förordning av statsrådet.

I enlighet med NIS2-direktivet ska också elnätsinnehavare som definieras som kritiska aktörer med stöd av CER-direktivet (EU) 2022/2557 tolkas att höra till tillämpningsområdet för NIS2-direktivet och därmed även Cybersäkerhetslagen. Detta torde regleras i samband med det nationella genomförandet av CER-direktivet.

Paragrafer om riskhantering i den föreslagna cybersäkerhetslagen:

7 § Riskhantering

En aktör ska identifiera, utvärdera och hantera de risker som hänför sig till säkerheten i de kommunikationsnät och informationssystem som den använder i sin verksamhet eller för att tillhandahålla sina tjänster. Hanteringen av cybersäkerhetsrisker ska förhindra eller minimera incidenternas inverkan på verksamheten, driftskontinuiteten, tjänstemottagarna och andra tjänster.

Aktören ska vidta sådana riskhanteringsåtgärder som är aktuella, proportionella och tillräckliga i förhållande till riskerna för de kommunikationsnät och informationssystem som används i verksamheten och kommunikationsnätets eller informationssystemets betydelse med tanke på aktörens verksamhet och tillhandahållande av tjänster.

8 § Handlingsmodell för hantering av cybersäkerhetsrisker

Aktören ska ha en uppdaterad handlingsmodell för hantering av cybersäkerhetsrisker för att skydda kommunikationsnät och informationssystem och deras fysiska miljö mot incidenter och deras verkningar.

I handlingsmodellen för hantering av cybersäkerhetsrisker ska de risker som hänför sig till kommunikationsnät och informationssystem och deras fysiska miljö identifieras med beaktande av ett tillvägagångssätt som beaktar alla riskfaktorer. I handlingsmodellen ska målen, förfarandena och ansvaren för hanteringen av cybersäkerhetsrisker samt de åtgärder enligt 9 § genom vilka kommunikationsnät och informationssystem och deras fysiska miljö skyddas mot cyberhot och incidenter (hanteringsåtgärder) fastställas och beskrivas.

9 § Åtgärder för hantering av cybersäkerhetsrisker

Aktörerna ska vidta proportionella tekniska, driftsrelaterade eller organisatoriska hanteringsåtgärder i enlighet med handlingsmodellen för hantering av cybersäkerhetsrisker för att hantera sådana risker som hänför sig till säkerheten i kommunikationsnät och informationssystem och förhindra eller minimera skadliga verkningar.

I handlingsmodellen och de hanteringsåtgärder som baserar sig på den ska åtminstone följande beaktas och uppdateras:

1) riktlinjerna för hantering av cybersäkerhetsrisker samt bedömningen av effektiviteten i fråga om åtgärderna,

2) de riktlinjer som gäller säkerheten i kommunikationsnät och informationssystem,

3) säkerheten vid förvärv, utveckling och underhåll av kommunikationsnät och informationssystem samt behövliga förfaranden för hantering av sårbarheter och delgivning av information om sårbarheter,

4) den övergripande kvaliteten och resiliensen i leveranskedjan i fråga om direkta leverantörers produkter och tjänsteleverantörers tjänster, de hanteringsåtgärder som är inbyggda i dem samt cybersäkerhetspraxis hos direkta leverantörer och tjänsteleverantörer,

5) tillgångsförvaltningen och identifieringen av funktioner som är viktiga med tanke på dess säkerhet,

6) personalsäkerheten och utbildningen i cybersäkerhet,

7) förfarandena för åtkomsthantering och autentisering,

8) riktlinjerna och förfarandena för användning av krypteringsmetoder samt vid behov åtgärderna för användning av säker elektronisk kommunikation,

9) upptäckandet och hanteringen av incidenter i syfte att återställa och upprätthålla säkerheten och driftssäkerheten,

10) säkerhetskopieringen, katastrofhanteringen, krishanteringen och den övriga driftskontinuiteten och vid behov användningen av säkrade reservkommunikationssystem,

11) grundläggande praxis för informationssäkerhet för att säkerställa verksamheten samt säkerheten i datakommunikationen, maskinvaran, programvaran och datamaterialet, samt

12) åtgärderna för att säkerställa den fysiska miljön, lokalsäkerheten och nödvändiga resurser i fråga om kommunikationsnät och informationssystem.

Åtgärderna ska ställas i relation till verksamhetens art och omfattning, de direkta konsekvenser som incidenten rimligtvis kan förutses ha, riskexponeringen i fråga om aktörens kommunikationsnät och informationssystem, sannolikheten för att incidenter inträffar och deras allvarlighetsgrad, kostnaderna för åtgärderna samt tillgängliga tekniska medel för att avvärja hot med beaktande av den aktuella utvecklingen.

Tillsynsmyndigheten kan inom sitt ansvarsområde meddela tekniska föreskrifter som preciserar riskhanteringsskyldigheterna om

1) sektorsspecifika särdrag som ska beaktas i handlingsmodellen för hantering av cybersäkerhetsrisker och i de delområden som avses i 2 mom. samt i förfarandena för riskhantering och hantering av informationssäkerheten i kommunikationsnät och informationssystem,

2) beaktandet av resultaten av de på unionsnivå samordnade riskbedömningarna av kritiska leveranskedjor i den sektorsspecifika riskhanteringen.

I riskhanteringen, handlingsmodellen för hantering av risker och hanteringsåtgärderna ska dessutom iakttas Europeiska kommissionens genomförandeakter som antas med stöd av artikel 21.5 i NIS 2-direktivet.

10 § Ledningens ansvar

Aktörens ledning svarar för genomförandet av och tillsynen över hanteringen av cybersäkerhetsrisker samt godkänner handlingsmodellen för hantering av cybersäkerhetsrisker och utövar tillsyn över genomförandet av den. Aktörens ledning ska ha tillräcklig förtrogenhet med hantering av cybersäkerhetsrisker.

Med ledning avses aktörens styrelse, förvaltningsråd och verkställande direktör samt någon annan i därmed jämförbar ställning som de facto leder dess verksamhet.

1.1.3 Lagstiftning om beredskap som ändras

Totalreformen av den nuvarande beredskapslagen (1552/2011) pågår som bäst under ledning av justitieministeriet. Målet med reformen är att få beredskapslagen att motsvara den moderna uppfattningen om samhällets övergripande säkerhet och de faktorer som hotar den samt identifieringen av olika hot- och störningssituationer med allvarliga konsekvenser. Enligt justitieministeriet är avsikten att överlämna regeringens proposition till riksdagen senast under höstsessionen 2025. Avsikten är att utkastet till regeringens proposition ska skickas på offentlig remiss i början av 2025.

I fråga om beredskapsplanen ska elnätsinnehavarna i de planer som lämnas in 30.6.2025 särskilt beakta faktorer som är oberoende av uppdateringen av beredskapslagen, såsom reserveringar av personal, tjänsteproducenter och fordon samt skydd av kritiska objekt och en plan för tillfälliga lokaler för kontrollrummet.

Energimyndigheten kan, bland annat beroende på betydelsen av ändringarna i beredskapslagens bestämmelser om begränsning av elanvändningen, kräva att elnätsinnehavarna uppdaterar sina beredskapsplaner på nytt redan före följande planer som ska lämnas in 30.6.2028.

1.2 Innehåll och tidsplan som krävs

Nätinnehavarna anses uppfylla de skyldigheter som fastställs i 28 § i elmarknadslagen, när de lämnar följande till Energimyndigheten:

1) en förberedningsplan för hur nätinnehavaren förbereder sig för störningar i elnätet under normala förhållanden

   a. **Planerna som lämnas in 2025 ska innehålla bolagets senaste kartläggning över risker.**

2) en beredskapsplan för hur nätinnehavaren förbereder sig för störningar i elnätet för sådana undantagsförhållanden som avses i beredskapslagen

3) Verktyget SÄHKÖKOTKA 2021 som fyllts i utifrån beredskapsplanerna och med vilket nätinnehavaren bedömer nivån på sin egen beredskap inom olika delområden. Med hjälp av verktyget ställs också utvecklingsmålen för de följande tre åren upp. SÄHKÖKOTKA 2021-verktyget kan laddas ner från Försörjningsberedskapscentralens extranet på adressen: https://extranet.huoltovarmuus.fi/. Vi ber er lämna in följande filer från verktyget SÄHKÖKOTKA 2021:

   a. Rapporten i pdf-format

   b. Diskussionspromemoria i pdf-format

   c. Svarsdata i excel-format

Bild 1. Rapportsidan för verktyget SÄHKÖKOTKA 2021.

De begärda filerna från SÄHKÖKOTKA finns på verktygets rapportsida enligt bild 1 bakom knappen "Rapport till skärmen", "Diskussionspromemoria till skärmen" och "Spara data".

De planer som krävs ska i enligt elmarknadslagen vara Energimyndigheten till hands till och med **30.6.2025**. Därefter ska planerna uppdateras åtminstone en gång per tre år och när det sker en betydande förändring i omständigheterna.

1.3 Frågor som ska betonas i följande planer

1.3.1 Kartläggning av risker

Beredskapsplanen ska motsvara aktuella risker. I Energimyndighetens mall har man av hävd ombetts beskriva bolagets process vid riskkartläggning och beredskapen för vissa centrala risker. Det väsentliga är att nätinnehavarna själva identifierar risker som hotar deras verksamhet och förbereder sig på dem på behörigt sätt. Även det nationella CER-direktivet förutsätter att "De kritiska aktörernas riskbedömningar ska beakta alla relevanta risker som orsakas av naturen och människan och risker som kan leda till avvikelser, inklusive branschrisker eller gränsöverskridande risker, olyckor, naturkatastrofer, folkhälsorelaterade nödsituationer och hybridhot och andra fientliga hot, inklusive terroristbrott enligt direktivet (EU) 2017/541. Vid riskbedömningen av en kritisk aktör ska beaktas i vilken mån andra aktörer inom de branscher som avses i bilagan är beroende av den centrala tjänst som den kritiska aktören tillhandahåller, inklusive i tillämpliga fall även i grannmedlemsstaterna och tredjeländer."

Rekommendationen är att resultaten av Försörjningsberedskapsorganisationens utredning ”Förberedelser inför risker i produktionen av energiförsörjning och verksamhetskedjor” utnyttjas för kartläggningen av risker. Arbetet planeras bli klart i maj 2025.

Följande planer som ska lämnas in senast 30.6.2025 ska åtföljas av en riskkartläggning i Excel-format där man beskriver de 15–20 mest centrala risker som bolaget identifierat och som kan påverka utbudet av eldistributions- eller överföringstjänster inklusive de viktigaste cybersäkerhetsriskerna. Energimyndigheten ger i samband med den slutliga anvisningen en Excel-mall där riskerna ska beskrivas.

Beredskapen för dessa centrala risker bör beskrivas ytterligare i planen. Till exempel i kapitel 8 i mallen: Till avsnittet beredskap för andra störningssituationer och agerande i störningssituationer kan – utöver redan identifierade centrala risker – läggas till nya underpunkter från och med punkt 8.10 och namnge dem på behörigt sätt.

För att planerna ska vara enhetliga har vi dock infört två nya störningstyper för alla i kapitel 8 i mallen: 8.8 Beredskap för hybridpåverkan samt 8.9 Beredskap för marknadsstörningar.

1.3.2 Ändringsanteckningar

Utvecklingen av beredskapen är en iterativ process och därför är det inte meningen att hela planen ska förnyas under varje uppdateringsomgång. För att främja kontinuiteten i planerna har man också strävat efter att hålla modellerna för beredskapsplanerna så oförändrade som möjligt.

I följande planer instruerar vi nätinnehavarna att fokusera särskilt på att utveckla de brister som observerats i tidigare planer genom att lyfta fram hur de utvecklingsåtgärder som presenterades i planen 2022 har genomförts. **Om möjligt ska de uppdaterade punkterna för tydlighetens skull presenteras med blå text.**

I början av planen är det också bra att upprätthålla en lista över versionshistoriken där det framgår när planen har uppdaterats, vilka de viktigaste ändringarna var och vem som ansvarade för uppdateringen.

1.3.3 Utvecklingsobjekt

Nätinnehavarna har tidigare i varierande grad lyft fram sina utvecklingsobjekt. Vid granskningen av följande planer betonas att alla **nätinnehavare har identifierat, fastställt ansvaren för och schemalagt sina utvecklingsobjekt i fråga om beredskapsplaneringen.** För enhetlighetens skull rekommenderar vi att man använder åtgärdssidan i SÄHKKOTKA-verktyget som skapats för detta ändamål.

1.3.4 Statsrådets förordning om företrädesordning för eldriftsställen som ska ingå i beredskapsplanen (TEM/2022/ 211)

Enligt 4 § i statsrådets förordning som trädde i kraft den 9 december 2022 **ska elnätsinnehavarna uppdatera företrädesordningen för eldriftsställena i samband med uppdateringen av beredskapsplanen**. Följande beredskapsplaner som ska lämnas in 30.6.2025 är de första beredskapsplanerna där företrädesordningen för andra än kritiska eldriftsställen enligt 3 § i förordningen ska fastställas.

Enligt 3 §:

I sin beredskapsplan ska nätinnehavaren utöver de eldriftsställen av kritisk betydelse som avses i 2 § också fastställa företrädesordning med tanke på störningssituationer, situationer med elbrist och krissituationer. Vid fastställandet av företrädesordningen ska hänsyn tas till sådana eldriftsställen som är viktiga för ledningen av och säkerheten i samhället, befolkningens försörjning och näringslivets funktionsförmåga.

Övriga eldriftsställen ska kategoriseras i tre kategorier enligt följande:

1) eldriftsställen där det ska undvikas avbrott i tillgången på el,

2) eldriftsställen där det får förekomma kortvariga avbrott i tillgången på el,

3) eldriftsställen där det får förekomma längre avbrott i tillgången på el.

I beredskapsplanen ska eldriftsställenas företrädesordning beskrivas i mallens nya kapitel 11.2 "Företrädesordning för övriga eldriftsställen". Nätinnehavarna ska i sin plan beskriva åtminstone: för hur många grupper eldriftsställena grupperas, vilka typer av eldriftsställen som hör till respektive grupp, hur många eldriftsställen som hör till gruppen, och vilken prioritetsklass varje grupp har (dvs. för hur länge kan eltillförseln avbrytas).

Vid fastställandet av företrädesordningen för eldriftsställen rekommenderas att man som hjälp använder den tabell som Försörjningsberedskapsorganisationens pooler tillsammans fastställt över hur kritiska elavbrotten vid driftställen inom olika branscher är. Tabellen publicerades i januari 2024 på Försörjningsberedskapsorganisationens gemensamma plattform Sähköpooli.

1.4 Tietojen julkisuus

Enligt 24 § 7 och 8 punkterna i offentlighetslagen (621/1999) är förberedninsplanerna och beredskapsplanerna helt sekretessbelagda handlingar.

I egenskap av en myndighet som övervakar elnätsinnehavarnas förberedningsplanering fastställer Energimyndigheten från fall till fall skyddsnivån för sekretessbelagda uppgifter enligt hur sekretessbelagd en uppgift är. Planerna bör inte i onödan innehålla sådana sekretessbelagda uppgifter som, om uppgifterna avslöjas, kan orsaka skada ”för sådana intressen som avses i 18 § 1 mom. i informationshanteringslagen”. Det är till exempel inte skäl att uppge var kritiska enheter som maskinhallar och reservkontrollrum är belägna eller specificera ansvarspersonernas namn utan uppgiftsbeteckningarna är tillräcklig information.[1]

1.5 Mallipohjan soveltaminen

Energimyndigheten har berett de bifogade malldokumenten som stöd för nätinnehavarnas planering.

De uppdaterade mallarna har skapats utifrån mognadsfrågorna i självutvärderingsverktyget SÄHKÖKOTKA 2021 som uppdaterades 2021 så att mallarnas rubriknivåer motsvarar mognadsfrågornas uppställning i samma ordning. Några enskilda frågor har dock utelämnats från mallen för beredskapsplanen och i avsnittet om serviceproducenter har rubrikerna för olika typer av serviceproducenter kombinerats. Mallarna uppdaterades ytterligare 2024 på basis av observationerna utifrån de föregående planerna, den förändrade verksamhetsmiljön och lagändringarna.

För att kartlägga hanteringen av cybersäkerheten **ber vi alla bolag att i sin plan svara på frågan i avsnitt 9.1 i mallen:**

Kryssa nedan för de standarder, verktyg för mätning av cybermaturitet och system för hantering av informationssäkerhet som ni använder eller har använt tidigare.

Om du vill kan du också kommentera hur och vad ni har använt dem till.

[ ] 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,

[1] Statsrådets förordning om säkerhetsklassificering av handlingar inom statsförvaltningen 1101/2019 3 §.

[ ] 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 _____

Alla texter i mallen bör omarbetas efter elnätsinnehavarens behov. De texter som finns i form av frågor bör inte besvaras som sådana, och nätinnehavaren bör lyfta fram omständigheter som förväntas ingå i förberedningsplanen.

Nätinnehavaren får länka andra beredskapsdokument i förberedningsplanen, särskilt om dokumenten uppdateras separat. Exempelvis uppgifter om ansvariga personer, kontaktuppgifter och andra uppgifter som uppdateras ofta kan ingå i separata dokument. I så fall ska nätinnehavaren hänvisa till sådana dokument i förberedningsplanen. På motsvarande sätt är det önskvärt att dela in beredskapsfrågor i mindre helheter. Det är till exempel inte ändamålsenligt att inkludera vare sig riskanalysen eller informationssäkerhetspolicyn i sin helhet i förberedningsplanen. Det är bättre att inkludera dem i separata bilagor och hänvisa till dem i förberedningsplanen. På så sätt utgör förberedningsplanen inte en alltför stor helhet. Sådana detaljerade bilagor ska inte lämnas till Energimyndigheten tillsammans med förberedningsplanen, utan endast på särskild begäran.

Det är inte obligatoriskt att använda mallen. Om nätinnehavaren gör upp fritt formulerade beredskapsplaner ska man i planerna dock beakta åtminstone det som presenteras i dessa mallar. Nätinnehavaren ska också presentera i det frågespecifika kommentarsfältet i verktyget SÄHKÖKOTKA 2021 (bild 2) var i den fritt formulerade planen svaret på den ifrågavarande frågan finns. Alternativt kan man i rubriken för den fritt formulerade planen hänvisa till frågorna i SÄHKÖKOTKA genom att markera SK #.

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

Bild 2. *SÄHKÖKOTKA 2021 -verktygets kommentarsfält.*

1.6 Inlämnande av planer till Energimyndigheten

Vänligen skicka planerna till Energimyndigheten med krypterad e-post till adressen kirjaamo@energiavirasto.fi samt som kopia till varautumissuunnitelmat@ener-

giavirasto.fi. Om ert företag inte använder krypterad e-post kan ni utnyttja Energimyndighetens tjänst för säker e-post. Kontakta i sådana fall per e-post adressen varautuminen@energiavirasto.fi.

Alternativt kan planen skickas som rekommenderat brev till adressen: Energimyndigheten, Fågelviksgränden 2A, 00530 Helsingfors.

Bilagor
Mall för förberedningsplan
Mall för beredskapsplan

Sändlista
Stamnätsinnehavare
Innehavare av högspänningsdistributionsnät
Distributionsnätsinnehavare