**Mall för elnätsinnehavarens förberedningsplan**

Innehållsförteckning

[1 BAKGRUND 3](#_Toc187847342)

[2 UTGÅNGSPUNKTER FÖR ELDISTRIBUTIONSBOLAGETS VERKSAMHET 5](#_Toc187847343)

[3 BASUPPGIFTER OM BOLAGETS FÖRBEREDNINGSPLANERING 5](#_Toc187847344)

[4 BOLAGETS RISKKARTLÄGGNING OCH BEREDSKAPSPLANERING 6](#_Toc187847345)

[5 ANSVARSOMRÅDEN OCH ARRANGEMANG FÖR HANTERING AV STÖRNINGAR 8](#_Toc187847346)

[6 BEREDSKAP FÖR AVVIKANDE VÄDERFÖRHÅLLANDEN 10](#_Toc187847347)

[7 AGERANDE VID STORSTÖRNINGAR ORSAKADE AV AVVIKANDE VÄDERFÖRHÅLLANDEN 13](#_Toc187847348)

[8 BEREDSKAP MOT ÖVRIGA STÖRNINGAR OCH ÅTGÄRDER VID STÖRNINGAR 15](#_Toc187847349)

[9 HANTERING AV RISKER I KOMMUNIKATIONSSYSTEM OCH DATASYSTEM OCH SÄKERSTÄLLANDE AV SYSTEMENS ANVÄNDBARHET 18](#_Toc187847350)

[10 SÄKERSTÄLLANDE AV TJÄNSTEPRODUCENTERNAS FUNKTIONSFÖRMÅGA 31](#_Toc187847351)

[11 REGIONALT SAMARBETE 32](#_Toc187847352)

# BAKGRUND

*Här kan du skriva en kort bakgrundsbeskrivning.*

*Beredskapsplanen sammanställer nätinnehavarens anvisningar om beredskap och hanteringen av störningar samt uppgifter om beredskapen. Med hjälp av planen kan man bedöma omfattningen av nätinnehavarens anvisningar och beredskap, hur aktuella och konsekventa anvisningarna är.*

*Alla texter i mallen ska redigeras enligt nätinnehavarens behov. Befintliga aktuella dokument kan länkas till beredskapsplanen. Kontaktuppgifter och uppgifter som ofta uppdateras kan finnas i separata dokument som man hänvisar till i beredskapsplanen.*

*Som stöd för utarbetandet av mallen har använts ordlistorna TSK 50 om övergripande säkerhet och TSK 52 om cybersäkerhet som Säkerhetskommittèn publicerat. För att förenhetliga terminologin rekommenderar vi att ordlistorna i fråga också används vid utarbetandet beredskapsplaner.*

*Den goda praxis som Energimyndigheten identifierat i och med beredskapsplanerna för 2019 kan utnyttjas som stöd för planeringen. Dessutom finns anvisningar i HVO-extranätets databank och i Energiförsörjningssektorns arbetsplattform. Anvisningar finns bland annat om följande teman:*

* *Tilannekuva-pelikirja (2021) (interaktivt om lägesbilden på finska)*
  + *Att forma lägesbilden samt bolagets interna kommunikation och kommunikationen till samarbetspartner*
* *Tiedonvaihto-pelikirja (2022) (interaktivt om att forma lägesbild och kommunikationen olika parter emellan på finska)* 
  + *Anvisningar om hur informationsutbytet mellan olika organisationer i en stor störningssituation görs effektivt samt hur man skapar en gemensam situationsförståelse som grund för den offentliga kommunikationen*
* *Anvisningen Viestintä sähköpulan uhatessa (2022) (på finska om kommunikationen vid hot om elbrist)*
* *Anvisningen Viestintä kantaverkon suurhäiriössä (2019) (på finska om kommunikationen vid storstörning i tamnätet)*
* *Utredningen Keskeytyskriittisten sähkönkäyttöpaikkojen priorisointi (2021) (på finska om prioritering av avbrottskritiska eldriftsställen)*
  + *Innehåller rekommendationer för fastställande och prioritering av kritiska objekt*
* *Tabell över prioritetsordningen för HVO-poolernas eldriftsställen (2024)*
* *Utredning om Norra Finlands räddningsverks beredskap att agera vid olyckor vid högspänningsobjekt (2021)*
  + *Innehåller bl.a. rekommendationer för beredskap inför olyckor och farliga situationer vid högspänningsobjekt*
* *KYBER-ENE Cybersäkerhet inom energibranschen 1–2*
  + *Praktiska metoder och åtgärder för att genomföra och utveckla cybersäkerheten, inklusive checklistor för bland annat IoT-lösningar.*

*Det finns aktuella anvisningar om övningsverksamhet bland annat på Försörjningsberedskapscentralens och Cybersäkerhetscentrets webbplatser:*

* [*Övningsanvisning för energibranschen - Försörjningsberedskapscentralen*](https://www.huoltovarmuuskeskus.fi/sv/publication/ovningsanvisning-for-energisektorn) *(2024)*
* [*Anvisning för att genomföra e-postövning | Cybersäkerhetscentret*](https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/ohje-sahkopostiharjoituksen-toteuttamiseen) *(2023) (på finska)*

*Utöver de ovan nämnda finns anvisningar för beredskap och kontinuitetshantering också på Cybersäkerhetscentrets webbplats:* [*Anvisningar för organisationer och företag | Cybersäkerhetscentret*](https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/anvisningar-och-guider/anvisningar-och-guider-organisationer-och-foretag) *samt i tjänsten eOppiva:* [*https://www.eoppiva.fi/sv/utbildningar/trygga-den-digitala-verksamheten-vid-storningar/*](https://www.eoppiva.fi/sv/utbildningar/trygga-den-digitala-verksamheten-vid-storningar/)

1. UTGÅNGSPUNKTER FÖR ELDISTRIBUTIONSBOLAGETS VERKSAMHET

## Eldistributionsbolaget i korthet

*En kort beskrivning.*

### Beredskap för störningar på eldistributionsbolaget

*En kort beskrivning.*

### De största störningarna som har identifierats i verksamheten

*Ange de största störningarna som utgångspunkt för planen. Utnyttja resultaten av en eventuell riskkartläggning.*

### Ledningssystem, riskhantering och kvalitetssäkring på eldistributionsbolaget

*En kort beskrivning och hänvisningar till dokumenten och systemen.*

# BASUPPGIFTER OM BOLAGETS FÖRBEREDNINGSPLANERING

## Ansvarsområden och arrangemang för förberedningsplanering

*Vem gör upp förberedningsplanen och vem deltar i förberedningsplaneringen? Vd ska godkänna planen innan denna lämnas till Energimyndigheten.*

***Obs! Ange inte de ansvariga personernas namn.*** *I enlighet med anvisningen är det inte ändamålsenligt att ange de ansvariga personernas namn, det räcker med att ange titlar.*

## Uppdatering av förberedningsplanen

*Beskriv processen för uppdatering av planen. Hur ofta uppdateras planen eller delar av planen?*

## Utvecklingsobjekt som identifierats utifrån föregående plan

*Vilka var de viktigaste utvecklingsobjekten som identifierades utifrån den föregående beredskapsplanen och de åtgärder som identifierades för att utveckla dem. Har de planerade åtgärderna genomförts och vilka delar av beredskapsplanen har ändrats utifrån dem (Obs. ändringsanteckningar i planen).*

BOLAGETS RISKKARTLÄGGNING OCH BEREDSKAPSPLANERING

*Syftet med detta kapitel är att lyfta fram hur nätinnehavaren kartlägger de risker som riktas mot den, förbereder sig på att hantera dem samt upprätthåller och utvecklar sin kompetens och medvetenhet om beredskapen.*

**Beredskapsplanering**

Beredskap för undantagstillstånd.

Upprätthållande av beredskapsplanen i kontinuitet till förberedningsplanerna samt övningar.

**Hantering av kontinuitet**

Hantering och återhämtning från kontinuitetshot i normaltid.

Upprätthållande av beredskapsplaner på basis av valda hotbilder samt övning av dessa situationer.

Föregripande riskhantering

Förutseende och hantering av osäkerhet i normaltid.

Systematisk identifiering och utvärdering av risker samt genomförande av riskhanteringsåtgärder.

## Föregripande riskhantering och riskanalys

*Beskrivning av bolagets riskbedömningsprocess och identifierade risker. Vem som deltar i riskanalysen, vem som ansvarar för riskanalysen och hur ofta riskanalysen uppdateras. Det rekommenderas att bolagets operativa ledning, var och en minst angående sina egna ansvarsområden i den utsträckning som möjligt, deltar i att utarbeta riskbedömningen.*

*När gjordes den senaste riskanalysen? Är riskerna indelade i olika kategorier till exempel utifrån ekonomiska effekter och sannolikheten för olika fenomen?*

*Har man inom bolaget bekanta sig med den nationella och regionala riskbedömningen och utnyttjat dem vid utarbetandet av riskbedömningen? Vilka risker har nätinnehavaren identifierat och vilka väsentliga risker försöker denne särskilt påverka genom denna plan? Har hanteringsåtgärder, ansvariga personer och tidsplaner för att vidta hanteringsåtgärder fastställts för väsentliga risker?*

*Riskregistret över de viktigaste (10–15 st.) riskerna som påverkar utbudet av eldistributions- eller överföringstjänster, inklusive cybersäkerhetsriskerna, ska bifogas till planen.*

## Planering av verksamhetens kontinuitetshantering

*Hur beaktas de hot och de för verksamheten kritiska affärsprocesser som identifierats i riskanalysen i planeringen av kontinuitetshanteringen? Vilka är tyngdpunktsområdena för bolagets beredskap under de följande tre åren?*

*Genom kontinuitetshanteringen skapas ett verksamhetssätt för hanteringen av allvarliga störningssituationer och verksamhetens kontinuitet och det omfattar en analys av de inledande händelsescenarierna, beslut om behovet av åtgärder som grundar sig på sannolikheten för händelserna och deras konsekvenser, utarbetande av planer och resursfördelning samt utbildning om och kontinuerligt underhåll av planerna.*

## Upprätthållande och uppdatering av medvetenheten om försörjningsberedskapen

*På vilket sätt upprätthåller och uppdaterar nätinnehavaren medvetenheten om försörjningsberedskapen? Syftet är att nätinnehavaren ska hålla sig uppdaterad om hur hoten utvecklas samt om hur åtgärderna i den egna kontinuitetsplaneringen fungerar och riktas rätt.*

## Utveckling av beredskapen tillsammans med intressentgrupperna inkl. beredskapsövningar

*Beskrivning av hur bolaget utvecklar beredskapen och hur man övar agerande i olika störningssituationer och hur ofta övar man beredskapen också tillsammans med samarbetspartner och myndigheter? Har bolaget deltagit i övningar som ordnats av myndigheterna, såsom RFV:s beredskapsövningar, informationsövningar eller PAPU-övningar?*

*Övar man förutom på företagets egen beredskap även på beredskap i leveranskedjor och -nätverk, inklusive serviceproducenter och materialleverantörer? Till exempel granskas beredskapsplanen och dess funktion testas under beredskapsövningarna och dessutom ordnas storstörnings-, brand- och räddningsövningar. Under beredskapsövningarna testas också beredskapen hos materialleveranskedjorna och serviceproducenterna.*

*Medierna har en viktig roll i att informera kunderna. Det är bra att se till att kontakterna med medierna upprätthålls kontinuerligt, varvid eventuella centrala journalister och informatörer har en god uppfattning om nätinnehavarens verksamhet och beredskapsfrågor. Det är bra att beakta medierna redan i planeringen av beredskapsverksamheten och när man utför övningar. På så sätt säkerställs att medierna i verkliga situationer får så korrekt och aktuell information som möjligt. När samarbetet fungerat väl redan under normala förhållanden kan medierna stödja bolaget med informeringen och undvika att eventuellt förmedla spekulativa eller motstridiga uppgifter från andra källor.*

*I planen är det också bra att lyfta fram följande i formen av en förteckning:*

* *Har bolaget en plan för beredskapsövningar? Hur långt sträcker sig planen tidsmässigt och vilka övningar ämnar bolaget delta i?*
* *Vilka övningar har man deltagit i under de senaste åren?*

1. ANSVARSOMRÅDEN OCH ARRANGEMANG FÖR HANTERING AV STÖRNINGAR

*Med ledningsansvar avses hantering av helhetsbilden och beslutsfattande.* Med handlingsansvar avses praktiska åtgärder.

## Ledningsansvar vid störningar och fel

*Beskriv de ansvariga personernas ledningsansvar vid störningar och fel. Har bolaget fastställt exempelvis en storstörningsorganisation och uppgifterna/ansvarsfördelningen för organisationen?*

## Verksamhetsansvar vid störningar och fel

*Beskriv de ansvariga personernas verksamhetsansvar vid störningar och fel. Har bolaget fastställt exempelvis en storstörningsorganisation och uppgifterna/ansvarsfördelningen för organisationen?*

Tabell 1 I arbetsbeskrivningar angivna uppgifter för att hantera störningar.

|  |  |  |
| --- | --- | --- |
| Företag | Uppgift | Telefon |
|  | t.ex. driftschef |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Kommunikations- och kriskommunikationsplaner vid olika störningar och fel

*Beskrivning av hur t.ex. kunder, samarbetspartner, myndigheter och medier informeras i störningssituationer. De ansvariga personerna för kommunikationen ska fastställas i planen.*

*I en välplanerad beredskap innehåller de på förhand fastställda beredskapsnivåerna principer för kommunikationen på varje beredskapsnivå. Aktörernas (t.ex. skiftmästare, driftschef, kommunikation) uppgifter har beskrivits enligt allvarlighetsklass. God praxis är att utnyttja medier via flera kanaler i genomförandet av kommunikationen samt att skicka information till en tjänst som är oberoende av plattform och har skalbara resurser. Det är också bra att upprätthålla en mer detaljerad kommunikations-/kriskommunikationsplan i en separat bilaga så att t.ex. kommunikationsanvisningar och meddelandemallar vid behov är lättillgängliga.*

*Ytterligare anvisningar för planeringen av kommunikationen finns t.ex. i spelboken Lägesbild, som finns på HVO-extranätet på plattformens gemensamma arbetsrum (Voimatalouspoolin yhteisalue). Syftet med spelboken Lägesbild är att hjälpa organisationerna att internt och tillsammans med sina samarbetspartner planera verksamhetsmodeller för användning av kommunikationsmedel under störningstid och skapa en lägesbild samt utveckla metoder som effektiviserar samarbetet.*

BEREDSKAP FÖR AVVIKANDE VÄDERFÖRHÅLLANDEN

*Beskrivning av hurdana störningar i klimatförhållandena man förbereder sig på och hur beredskapsåtgärderna skiljer sig från varandra enligt hur allvarlig situationen är eller i olika typer av situationer, till exempel vid storm och snöbelastning.*

*Obs! I detta kapitel ska man särskilt beskriva hur man på förhand har förberett sig på störningar orsakade av olika väderfenomen och vilka åtgärder som vidtas när en störningssituation hotar: t.ex. väderuppföljning, att larma personal, förutseende tekniska åtgärder t.ex. vid hot om snöbelastning.*

*I kapitel 7 beskrivs verksamhetsmodellerna vid störningar.*

## Fastställande av beredskapslägen vid störningar och fel

*Beskriv vilka beredskapslägen nätinnehavaren har och hur lägena har definierats.*

*Med vilka åtgärder höjs bolagets och tjänsteleverantörernas beredskap i olika beredskapslägen? Höjning av beredskap omfattar exempelvis kontroll av tillgången till och vid behov reservering av personalresurser, kommunikation, material, fordon, system och entreprenörer.*

## Introduktion för personalen och samarbetspartner i hur man agerar i störningssituationer

*Beskrivning av hur personalen och samarbetspartnerna har introducerats i olika störningssituationer och kompetensen har säkerställts.*

## Information till kunderna på förhand om störningssituationer

*Beskrivning av hur och med vilka kanaler kunderna informeras om störningssituationer och undantagsförhållanden (på förhand). Vem ansvarar för informeringen och hur upprätthålls beredskapen att informera?*

*Kontaktuppgifter och uppgifter som ofta uppdateras kan finnas samlade i ett separat dokument som man hänvisar till i beredskapsplanen. Det rekommenderas att kontaktuppgifterna innehåller kontaktuppgifterna till de viktigaste kunderna och till kontaktpersoner inom medierna. En stor del av kunderna följer i första hand medierna. För att informationen från olika källor ska vara så enhetlig och konsekvent som möjligt är det bra att erbjuda medierna tydlig och aktuell information om situationen.*

## Att ordna arbetstids-, måltids- och viloarrangemang

*Beskrivning av hur personalens och samarbetspartnernas arbetstider, måltider och vila har ordnats för att eldistributionsbolaget ska kunna agera i störningssituationer.*

## Beredskap för utrustnings- och materielunderhåll vid störningar

*Beskrivning av hur underhållet av nätinnehavarens och partnernas utrustning och materiel har ordnats särskilt vid längre störningar.*

## Reservering av nätmaterial

*Beskriv tillgången till det material och de reservdelar som behövs för reparation av elnätet.*

* *Vilka material har reserverats?*
* *På vilket sätt har underleveranstjänsterna säkerställts vid störningar?*
* *Är det möjligt att reservera kritiska reservdelar eller har bolaget med tjänsteleverantörer kommit överens om säkring av tillgången till delarna?*
* *Är det känt varifrån reservdelar eller andra material beställs och hur lång leveranstiden är?*
* *Har bolaget tillsammans med eldistributionsbolaget i grannskapet kartlagt samarbetsmöjligheterna?*
* *Har ansvariga personer fastställts?*

*Exempelvis följande material och verktyg är viktiga:*

* *nätmaterial och reservdelar*
* *fordon och annan utrustning*
* *operativ kommunikationstrafik och kommunikationsutrustning*
* *reservgeneratorer.*

## Reservering av material för ställverk och högspänningsnät

*Beskrivning av tillgängligheten till reservmaskiner, reservdelar och andra material för ställverk.*

* *Vilka material har reserverats?*
* *Hur har underleverantörstjänsterna tryggats med tanke på störningssituationen?*
* *Är det möjligt för eldistributionsbolaget eller serviceproducenterna att reservera kritiska reservdelar eller annat material med tanke på störningssituationer?*
* *Samarbetsmöjligheter med närliggande eldistributionsbolag?*
* *Har ansvarspersoner definierats?*

*När material och apparater reserveras ska man också beakta problem med tillgången till material i exceptionella situationer (t.ex. sanktioner eller pandemier).*

AGERANDE VID STORSTÖRNINGAR ORSAKADE AV AVVIKANDE VÄDERFÖRHÅLLANDEN

*Beskrivning av verksamheten särskilt vid storstörningar orsakade av väderfenomen.*

## Klassificering av störnings- och felsituationer samt åtgärder vid olika storstörningar

*Jfr punkt 6.1 "Fastställande av beredskapsnivåer vid för störnings- och felsituationer". Hur övergår man från att förbereda sig för en störning till att agera i en storstörningssituation?*

*Har nätinnehavaren definierat organisation för storstörningssituationer? Hur varierar organisationen för storstörningssituationer i omfattning och funktion enligt störningstyp (t.ex. storm, snöbelastning, åskväder) eller störningssituationens allvarlighet (t.ex. antalet elfria kunder)?*

## Uppföljning av störnings- och felsituationer och upprätthållande av lägesbilden

*Beskrivning av hur störnings- och felsituationer i nätet följs upp och hur informationen utnyttjas för lägesbilden.*

## Inrättande av ledningscentral/lägesbildscentral

*Beskriv hur och i vilken situation en ledningscentral/lägesbildscentral ska inrättas. Beskriv även ledningscentralens verksamhet, uppgifter och ansvariga personer samt uppdateringen av lägesbilden.*

*Vem ansvarar för uppdateringen av lägesbilden?*

*Det är bra att för lägesbilden samla in uppgifter om hur störningarna utvecklas, exempelvis från väderprognoser, informationssystemen för drift av nätet, fältaktörer, tjänsteleverantörer och andra samarbetsorganisationer, som Krivat.*

## Information till kunder vid långvariga störningar

*Beskriv vilka verktyg som används för information till bolagets kunder vid långvariga störningar och på vilket sätt.*

* *På vilket sätt ska bolaget säkerställa att kunderna får en så riktig bedömning som möjligt av situationen och elavbrottens längd hos telefonservicen, textmeddelandetjänsten, elavbrottskartan, sociala medier och meddelanden även vid storstörningar?*
* *Vem ansvarar för informeringen internt och externt.*
* *Kontakter till medierna, utnyttjande av medierna.*

*Kontaktuppgifter och uppgifter som ofta uppdateras kan finnas samlade i ett separat dokument som man hänvisar till i beredskapsplanen.*

## Responsmöten och responsenkäter efter störningar

*Beskriv på vilket sätt rapporteringen, responsmötena och responsenkäterna efter störningar ska arrangeras i organisationen. Vem ansvarar för responsmötena efter incidenter? Av vem begärs respons (t.ex. personal, samarbetspartner, kunder) och hur (t.ex. evenemang, intervjuer, webbenkäter)?*

*På vilket sätt beaktas till exempel följande faktorer vid rapporteringen och kartläggningen av utvecklingsområden efter incidenter?*

* *totalt antal fel (fel i hög-, mellan- och lågspänningsnäten)*
* *antal träd som har tagits bort från ledningarna*
* *antal reparationsresurser*
* *antal resurser vid kundservicen och andra delaktiga resurser*
* *reparationskostnader*
* *olyckor och farliga situationer*
* *antal samtal, responstider o.d.*
* *antal kunder utan elektricitet*
* *felens tidslängd*
* *SAIDI- och KAH-bedömningar*
* *antal standardersättningar*
* *framgång i media (positiva/neutrala/negativa nyheter)*

1. BEREDSKAP MOT ÖVRIGA STÖRNINGAR OCH ÅTGÄRDER VID STÖRNINGAR

*Beskriv hur bolagets beredskap beror på störningar och vilka instruktioner som har getts för olika störningar.*

## Beredskap för betydande tekniska fel och skador i eldistributionsnät och högspänningsdistributionsnät

*Beskriv vilka tekniska fel i distributions-/överföringsnätet bolaget har förberett sig för och på vilket sätt.*

## Beredskap mot epidemier

*Beskriv hur bolaget, i sin egen verksamhet, tjänsteleverantörernas verksamhet och tillhandahållandet av andra externa tjänster, har beaktat personalbrist som orsakas av epidemier, dvs. smittosamma sjukdomar som sprider sig till en stor del av befolkningen i regionen.*

*När personalresurserna minskar är det viktigt att identifiera kritiska funktioner och vid behov minska verksamheten i fråga om de processer för vilka avbrottet eller minskningen av verksamheten inte orsakar oskäliga olägenheter. När det gäller kritiska funktioner är det också skäl att satsa på att ersätta personer till exempel genom utbildning och arbetsrotation.*

## Beredskap mot storolyckor

*Beskriv hur bolaget har förberett sig för storolyckor. Med storolycka avses en olycka som bör anses vara särskilt allvarlig på grund av antalet döda eller skadade eller på grund av omfattningen av skador på miljön eller egendom eller på grund av olyckans art.*

*Eldistributionsbolagets huvudsakliga delområden i beredskapen mot storolyckor som orsakas av externa omständigheter är följande:*

* *skydd och säkerhet hos de egna anställda och tjänsteleverantörens anställda*
* *skydd av företagets egendom*
* *säkring av kontinuiteten i eldistributionen*

## Beredskap mot elbrist

*Beskriv på vilket sätt bolaget har förberett sig för elbrist och vilka planer bolaget har för elbrist (höjning av beredskapen, ledning, begränsning av effekten, information osv.).*

*Med elbrist (effektbrist) avses under normala förhållanden en situation där produktionen och importen inte räcker till för att täcka förbrukningen och då måste förbrukningen begränsas tillfälligt. Med elbrist avses en annan sak än ransonering av el under undantagsförhållanden. Stamnätsbolaget använder ett förfarande med tre steg för situationer när produktions- och konsumtionsläget skärps:*

* *Det är fråga om* ***möjlig elbrist*** *när prognoserna visar att den inhemska produktionen och importen inte räcker till för att täcka elförbrukningen under de närmaste timmarna eller dygnet. Aktörerna ombeds granska sina planer och förbereda sig på situationen.*
* ***Hög risk för elbrist*** *anses det vara när all elproduktion som finns tillgänglig i Finland är i bruk och det inte är möjligt att få mer el från grannländerna. Fingrid har varit tvungen att starta en snabb (15 min.) störningsreserv, dvs. gasturbiner och aktivera frikopplingsbara laster inom industrin. I Finland kan man inte upprätthålla en snabb reserv för störningar som motsvarar ett betydande fel.*
* ***Elbrist*** *(allvarlig effektbrist) anses ha uppstått när elproduktionen och importen inte räcker till för att täcka förbrukningen och elförbrukningen måste frikopplas utan kommersiella avtal. Distributionsnätsinnehavarna frikopplar förbrukningen kontrollerat enligt på förhand uppgjorda planer så att elavbrotten är högst ett par timmar och avbrotten inte riktas till funktioner som är viktiga för samhället.*

## Beredskap mot storstörningar i stamnätet

*Beskriv på vilket sätt bolaget har förberett sig för storstörningar i stamnätet samt för åtgärder i enlighet med systemskyddsplanen och återuppbyggnadplanen som föreskrivs i nätkoden om nödsituationer och återuppbyggnad (NC ER). Vilken plan har bolaget för åtgärder i storstörningar i stamnätet?*

*Det är fråga om storstörning i stamnätet när över hälften av förbrukningen är utan el eller hela stamnätet är spänningslöst i över tre minuter. Storstörningar kan bero på flera olika orsaker. En storstörning kan uppstå till följd av olika fel i överföringsnätet eller elproduktionen, naturfenomen, terrordåd, våld, vårdslöshet, okunskap och olyckor. En storstörning kräver flera allvarliga samtidiga fel i elsystemet.*

## Beredskap för lokal- och lagerförlust

*Beskrivning av hur man förbereder sig på förlust av lokaler och lager.*

*Obs! Planen för tillfälliga lokaler för kontrollrummet är en del av beredskapsplanen.*

## Beredskap för förlust av nyckelpersoner

*Har nätinnehavaren identifierat nyckelpersoner som utför kritiska uppgifter och förlusten av vilka som skulle vara av stor betydelse för bolagets verksamhet? Hur minimeras riskerna för förlust av nyckelpersoner?*

## Beredskap för hybridpåverkan

Hur har nätinnehavaren tillsammans med intressentgrupper förberett sig på det ökade hotet om hybridpåverkan? T.ex. informationspåverkan som riktas mot personalen och kunderna, cyberpåverkan, underrättelse som riktas mot bolaget, intrång i bolagets lokaler samt sabotage av nätkomponenter.

## Beredskap inför störningar på marknaden

Hur har nätinnehavaren förberett sig inför störningar på marknaden? T.ex. kraftiga variationer i elpriset och deras inverkan på kundernas elanvändning, konkurser bland elförsäljarna samt störningar i anslutning till datahub.

## Beredskap mot andra störningar

*Här kan du ange om nätinnehavaren har identifierat andra väsentliga risker som denne har beredskap mot.*

HANTERING AV RISKER I KOMMUNIKATIONSSYSTEM OCH DATASYSTEM OCH SÄKERSTÄLLANDE AV SYSTEMENS ANVÄNDBARHET

*Enligt 29 a §, som är en ny paragraf i elmarknadslagen, ska nätinnehavare sörja för riskhanteringen i fråga om de kommunikationsnät och informationssystem som denne använder. Även av denna anledning är informationssäkerhetspolicyn och beredskapen mot informationssäkerhetsrisker en allt mer ökande del av förberedningsplaneringen. Därför har de skilts åt och utgör en separat helhet i planen.*

*Vi rekommenderar att cyberhot beaktas som en del av organisationens övergripande riskhantering och att de beskrivs närmare i styckena 4.1 och 4.2.*

*För att trygga basnivån för elnätsinnehavarens verksamhet under normala förhållanden och undantagsförhållanden ska man på företagsnivå kontinuerligt förbereda sig på hot mot cyberverksamhetsmiljön (en verksamhetsmiljö som består av ett eller flera digitala informationssystem). Sådana hot är bl.a.:*

* *en allvarlig störning i ett kritiskt informations- och kommunikationssystem som direkt och avsevärt stör elnätsinnehavarens verksamhet, till exempel ett överbelastningsangrepp.*
* *ett allvarligt problem med apparaternas lokaler som påverkar funktionen hos flera datasystem*
* *en allvarlig störning i datatrafiken som till exempel kan påverka organisationens kommunikationsförmåga eller tillgången till tjänster*
* *allvarlig personuppgiftsincident*

*Beredskap inför hot mot cyberverksamhetsmiljön kallas cybersäkerhet. Cybersäkerhet kan definieras som en målbild där man kan lita på cyberverksamhetsmiljön och där dess verksamhet tryggas. Störningar i verksamheten i cyberverksamhetsmiljön orsakas ofta av ett realiserat informationssäkerhetshot, informationssäkerheten är därmed en central faktor när man strävar efter cybersäkerhet. Utöver informationssäkerheten strävar man efter cybersäkerhet bland annat genom åtgärder vars syfte är att trygga den fysiska världens funktioner som är beroende av den störda cybermiljön.*

*Då man medinformationssäkerhet avser tillgången till* ***information****, dess integritet och konfidentialitet, betyder cybersäkerhet säkerhet i ett digitalt och nätverksbaserat samhälle eller en digital organisation och cybersäkerhetens inverkan på deras funktioner. Cybersäkerhet är inte bara ett engångsprojekt i en föränderlig värld, utan det måste upprätthållas och utvecklas kontinuerligt.*

*Verksamhetsmodellen för datatekniska hotsituationer kan också beskrivas i en separat anvisning.*

## Hantering av cybersäkerhet

*En beskrivning av hanteringen av cybersäkerhet inom bolaget, dvs. cybersäkerhetspolitiken, -strategin och -programmet. Cybersäkerhetsprogrammet grundar sig på en cybersäkerhetsstrategi. Cybersäkerhetsstrategin fastställer mål, målens prioritet, ansvar och uppföljning för organisationens cybersäkerhet. I den enklaste formen innehåller cybersäkerhetsstrategin en lista över cybersäkerhetsmålen och en plan för att uppnå dem.*

*Hurdant är företagets cybersäkerhetsprogram. Syftet med programmet är att definiera hanteringsmodellen, den strategiska utvecklingen av cybersäkerheten och ledningens stöd med beaktande av riskerna med de objekt som ska skyddas och de mål som organisationen ställt upp. Har man inom bolaget definierat exempelvis*

* *Datasäkerhetsprinciper och centrala begrepp. Tar cybersäkerhetsprogrammet ställning till alla risker som framgår av riskbedömningarna antingen genom att godkänna dem eller genom att fastställa de försiktighetsåtgärder som anses nödvändiga, såsom skydd, svar och återhämtning på goda grunder?*
* *Aktuella datasäkerhetsanvisningar och -bestämmelser. Hur har man säkerställt att kund- och personuppgifter hanteras i enlighet med dataskyddslagstiftningen (GDPR) om skydd av personuppgifter i Finland och EU?*
* *Övervakningspraxis för cybersäkerhet. Har denna övervakningspraxis presenterats för organisationens personal genom samarbetsförfarande?*
* *Uppgifter och ansvarspersoner i anslutning till skötseln av informationssäkerheten, kontakter till samarbetspartner, samarbetsnätverk och myndigheter. Hur har tjänsteproducenterna för sin del introducerats i och förbundit sig till den cybersäkerhetsstrategi, -förfaranden och -anvisningar som företaget implementerat?*
* *Informationssäker hantering av handlingar och dokument* *(inkl. nätverksinformation)*
* *Personalens deltagande, utbildning, kunskapsdelning och tillräckliga färdigheter*
* *Programmets kontinuitet och utveckling. Åtnjuter programmet stöd av företagets ledning på en kontinuerlig basis? Uppdateras programmet i samband med anskaffning, utveckling och underhåll av datasystem?*
* *Genomförs interna och externa auditeringar och tester? Utförs det årliga tekniska datasäkerhetsgranskningar i organisationens olika system och utförs de av utomstående? Har man övervägt att låta en aktör inom informationssäkerhet testa informationssäkerhetsnivån av typen red / purple team?*

***OBS! Vi ber alla bolag att fylla i enkäten nedan.***

*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,*

*[]* ***NIST SP ja IR -sarjat****, NIST Special Publication* [*https://csrc.nist.gov/publications/sp*](https://csrc.nist.gov/publications/sp) *ja* [*https://csrc.nist.rip/publications/PubsSPs.html*](https://csrc.nist.rip/publications/PubsSPs.html) *ja NIST Interagency/Internal Report* [*https://csrc.nist.gov/publications/nistir*](https://csrc.nist.gov/publications/nistir) *ja* [*https://www.nist.gov/nist-pub-series/nist-interagencyinternal-report-nistir*](https://www.nist.gov/nist-pub-series/nist-interagencyinternal-report-nistir)

*[]* ***ISF****, Information Security Forum* [*https://www.securityforum.org/*](https://www.securityforum.org/)

*[]* ***NIST CSF****, Cyber Security Framework* [*https://www.nist.gov/cyberframework*](https://www.nist.gov/cyberframework)

*[]* ***C2M2****, Cybersecurity Capability Maturity Model - Yhdysvaltain energiaministeriön tarjoama kyberturvallisuusvalmiuksien kypsyysmalli* [*https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2*](https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2)

*[]* ***CIS Critical Security Controls (CSC),***[*https://www.cisecurity.org/controls*](https://www.cisecurity.org/controls)

*[]* ***KATAKRI 2020****,*

*[] joku muu, mikä/mitkä? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

*Avoin kommentti \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

## Cybersäkerhetsarkitektur

*Beskrivning av företagets cybersäkerhetsarkitektur. Med hjälp av cybersäkerhetsarkitekturen beskrivs organisationens säkerhetsprocesser, cybersäkerhetssystem och personalstruktur samt deras förhållande till organisationens mål och strategiska planer. Cybersäkerhetsarkitekturen skapar förutsättningar för att planera och utveckla organisationens cybersäkerhet som en helhet i stället för punktmässiga lösningar, såsom enskilda lösningar för hanteringen av identitet eller åtkomst.*

*Med hjälp av cybersäkerhetsarkitekturen kan man närma sig skyddet av kritiska system och information via kända arkitekturmetoder. Till sådana metoder hör bland annat segmentering av nät, underhållslösningar, krypteringsmetoder och spårningsloggar och de kan användas tillsammans med metoder för åtkomst, såsom monitorering, returnering eller verifiering. När cybersäkerhetsarkitekturen planeras att fungera tillsammans med organisationens affärsstrategi fungerar den som input bl.a. för riskanalyser och konfigurering av objekt som ska skyddas.*

* *Utvärderas krav på cyberarkitektur för organisationens system och nätverk regelbundet och i samband med på förhand fastställda situationer, såsom systemändringar? Har ansvaret för uppdateringen av kontinuitetshanteringsplanerna fastställts i samband med system- och nätändringar? Är uppdateringen av planerna bunden till årsklockor hos organisationen?*
* *Hur har kontinuiteten i avtalshanteringen, säkerställandet av avtalens existens samt kännedomen om avtalens innehåll säkerställts?*
* *Hur har hanteringen av underleverantörer och säkerställandet av deras säkerhet genomförts?*
* *Segmenteras näten på fysisk och logisk nivå? Hur har säkerhetslösningarna för externa och interna nät genomförts? Testas det att differentieringen av näten fungerar regelbundet eller åtminstone efter alla nätändringar (t.ex. ändringar i brandväggsreglerna)? Hur har man beaktat förhindrandet av angrepp som fortskrider mellan organisationens olika funktioner i segmenteringen av näten?*
* *Har apparater, system och nätverk separerats från varandra utifrån användningsändamål? Finns det till exempel utrustning som endast är avsedd för betalning av fakturor och som inte får eller kan användas för något annat?*
* *Har beroendeförhållanden mellan organisationens olika funktioner identifierats? Utnyttjas identifiering av beroendeförhållandena bl.a. vid segmentering av system och nätverk?*
* *Har säkerhetsmekanismer och lösningar för fjärradministration för enheter och program genomförts med beaktande av hur kritiska de är?*
* *Beaktas i valet av leverantörer för program och applikationer om leverantören följer principerna för säker applikationsutveckling?*
* *Krypteras uppgifterna på hårddiskar i bärbara enheter för den händelse att de tappas bort eller stjäls? Är det möjligt för organisationen att låsa enheterna eller ta bort uppgifterna på enheterna med hjälp av fjärradministrationsförbindelser?*
* *Har organisationen fastställt policyer för säker användning av mobila enheter, inklusive fjärradministration och installation av applikationer?*
* *Har de mest kritiska filerna och konfigurationerna säkerställts genom säkerhetskopior som är fria från den operativa verksamhetens datanät, s.k. kylförvaringslösningar (offline säkerhetskopior)? Har behovet av säkerhetskopiering kartlagts och dimensionerats till en tillräcklig nivå? Är ansvaret för säkerhetskopiering tydligt mellan er och systemleverantörerna?*
* *Finns det för organisationens system och nätverk en uppdaterad utrustningsförteckning där man specificerar till exempel utrustningstyper, modeller, märken, ledningar och strömkällor för att påskynda återhämtningen från avvikelsen?*

## Identitets- och åtkomsthantering

*Beskrivning av identitets- och åtkomsthanteringen. Det enklaste sättet att definiera och hantera identiteter är att skapa användarrättigheter och avlägsna onödiga identiteter. Identitetsaktörerna kan vara organisationens interna eller externa individer, men också anordningar, system eller processer som behöver rättigheter till skyddade objekt. Upprätthållandet av rättigheterna förutsätter spårbarhet och säkerställer att alla har en giltig identitet samt att rättigheterna avlägsnas efter att behovet har upphört.*

*Åtkomsthanteringen omfattar fastställande av tillträdeskrav, krav på beviljande av rättigheter samt upphävande av rättigheter när rättigheter till objektet inte längre behövs. Hanteringen av åtkomsten till organisationens skyddade objekt ska beakta riskerna för organisationens mål och kritisk infrastruktur.*

* *Är hanteringen och granskningen av användarnamn regelbunden?*
* *Har loggningen definierats i anslutning till identitets- och åtkomsthantering och hur länge förvaras loggarnas innehåll? Vilka av användarnas åtgärder loggas utöver de som ingår i åtkomsthanteringen?*
* *Har systemen för lagring av observationer som är väsentliga för tillsynsmetoderna, såsom loggning, skyddats så att olovlig ändring eller förstöring av uppgifterna i dem förhindras?*
* *Används tillsynsmetoderna på behörigt sätt så att informationssäkerhetsincidenter och eventuella sårbarheter upptäcks och utreds för att minska riskerna?*
* *Har möjligheten att använda huvudanvändarrättigheter begränsats för normala användare? Hur övervakas huvudanvändarnas åtgärder och på vilken nivå? Hur länge förvaras loggarna i anslutning till övervakningen och hur säkerställs dessa?*
* *Finns det gemensamma användarkoder i bruk? Hur hanteras dessa och har man planerat att avstå från dem?*
* *Har systemet för hantering av användarrättigheter dubblerats? Har man planerat hur systemet kan förbigås i en nödsituation till exempel för att aktivera huvudanvändarnas användarnamn?*

## Kontinuitetshantering av kritiska data- och datakommunikationssystem

*Beskrivning av hur kontinuiteten i verksamheten har säkerställts för informationssystemens och datakommunikationssystemens del. Kontinuitetshanteringen omfattar identifiering av hot mot verksamheten och deras effekter samt verksamhetssätt för hantering av störningssituationer och funktionernas kontinuitet under alla förhållanden.*

*I klassificeringen om hur kritiska funktionerna är prioriteras återställande av system och funktioner i katastrofsituationer. Nättrafiken och kommunikationsförbindelserna samt till exempel användarrättigheterna spelar en viktig roll när det gäller att inleda och föra återhämtningsåtgärderna framåt. Som stöd för prioriteringen kan man använda tanken från timme till nästa timme, dvs. utan vilken organisationen inte klarar sig ens en timme, och vilket i sin tur till exempel inte hindrar att reparationsåtgärder inleds efter en eller två dagar och vilka saker som är sådana att man med undantag av skador till ryktet kan återkomma till om exempelvis en vecka. Prioriteringsordningen kan variera beroende på affärsverksamhet/tjänst inom organisationen och därför är det viktigt att på förhand kommunicera dessa behov med organisationens IT- och OT-personal.*

*Det vore bra om organisationen i samband med prioriteringen av återhämtningen också definierade eventuella lagstiftningskrav som gäller den, såsom eventuella 24/7/365 funktioner som kräver funktionssäkerhet i alla situationer.*

*Har man till exempel*

* *Identifierat centrala datasystem och datakommunikationssystem och gjort en förteckning av dem på basis av hur kritiska de är för verksamheten*
* *Utarbetat planer för kontinuiteten för datasystem och datakommunikationssystem*
* *Säkerställt att upprätthållandet och underhållet av systemen är tillgängligt även i störnings- och undantagssituationer*
* *Skött kopieringen av säkerhetsskäl regelbundet för datasystem och datakommunikationssystem*
* *Kopieringen av säkerhetsskäl för datasystemen och datakommunikationssystemen har skötts regelbundet och man har övat på att återställa säkerhetskopiorna årligen. Rapporteras resultaten av återställningen, såsom framgången, till ledningen?*

## Identifiering av allvarlig sårbarhet eller störning i informationssäkerheten och återhämtning från den

*Beskrivning av hur man strävar efter att identifiera allvarliga sårbarheter, störningar och angrepp i datanätet och hurdana anvisningar personalen har om en sådan informationssäkerhetsincident upptäcks. Beskrivning av hur man återhämtar sig från genomförda informationssäkerhetsincidenter och -angrepp.*

* *Hur har ansvaret för myndighetsrapportering (t.ex. NIS) fördelats och hurdan är rapporteringsprocessen?*
* *Hur samlar man in och upprätthåller tillräcklig kompetens och information om de tekniska sårbarheterna i data- och datakommunikationssystemen?*
* *Hur sköts loggningen? Vad innehåller loggen och hur länge förvaras den?*
* *Hur upptäcks informationssäkerhetshändelser automatiskt? Hur och med vilka verktyg lyfts misstänkta informationssäkerhetsincidenter fram? Hurdan förmåga har er organisation och era tjänsteleverantörer (t.ex. stöd- och underhållstjänster, lokalvård, entré- och säkerhetstjänster, matförsörjning eller datakommunikationsleverantörer) eller era samarbetspartner att reagera tekniskt på informationssäkerhetsincidenter dygnet runt?*
* *Hur reagerar man automatiskt på informationssäkerhetsincidenter som lyfts fram? Hur ser handlingsplanerna ut? Hur återhämtar man sig från incidenten?*
* *Hur har ansvaret för de olika rollerna inom informationssäkerheten fördelats till er organisations personal (t.ex. ledningen, servicecheferna och entrévakterna) samt till samarbetspartner och underleverantörer?*
* *Har ni utfört övningar för era processer för hantering av informationssäkerhetsincidenter självständigt och tillsammans med samarbetspartner? Hur riktar ni övningsverksamheten och utreder årligen behoven av utbildning och övningar i er organisation? Har ni i er organisation inlett ett övningsprogram för att främja kontinuerlig utbildning inom olika funktioner?*
* *Har uppgifterna om minst en (datasäkerhetsansvarig) person eller roll som vid behov är tillgänglig samt datatillsynsorganet (SOC) förmedlats till myndigheterna för anmälan av datasäkerhetsincidenter?*

## Tillförseln av el till kritiska data- och datakommunikationssystem

*Beskrivning av säkerställandet av elförsörjningen till system som är kritiska med tanke på hanteringen av verksamhetens kontinuitet enligt hur kritiskt objektet det är fråga om.*

* *Hur har elmatnings- och datakommunikationskablarna i apparatutrymmena skyddats mot externa hot och hur har kablarna för viktiga apparatutrymmen verifierats?*
* *Säkerställs elförsörjningen till de datasystem, datakommunikation och kontrollrum som används för styrning i under normala förhållanden med reservkraftmaskiner eller obrutna elförsörjningsanordningar (UPS) med tanke på störningar?*
* *Hur har upprätthållandet av reservkraftmaskinernas, ackumulatorernas och elmatningsutrustningens kondition och testning ordnats.*
* *Har ansvarspersonerna fastställts bland annat i anslutning till reservkraftmaskiner, ackumulatorer och eltillförsel?*

## Skydd av kritiska data- och datakommunikationssystem och övrig säkerhet för lokaler

*Beskrivning av hur informationssystem, kontrollrum och transformatorstationer skyddas mot fysiska fenomen eller händelser.*

* *Hur har t.ex. viktiga utrustnings- och kontrollrum skyddats mot elektroniska störningar?*
* *Hur är de apparater som används vid ställverken strukturellt skyddade för att tåla höga överspänningar och elektromagnetiska störningar i lokalerna?*
* *Används tillförlitliga och högklassiga system för övervakning av förhållandena?*
* *Hur har man ombesörjt för säkerheten vid lokalerna och passerkontrollen? Har t.ex. fysiska säkerhetsområden definierats och klassificerats enligt deras betydelse i olika tillträdes- och skyddsklasser? Är säkerhetsområdena skyddade med elektroniska passerkontroll- och inbrottslarmsystem som sparar händelserna samt med videoövervakning? Hur länge och var förvaras ovan nämnda loggar och inspelningar?*
* *Inspekteras kritiska objekt regelbundet?*
* *Uppmuntras personalen att göra observationer av fordon och personer som rör sig nära kritiska objekt, obemannade luftfarkoster (drönare) samt fotografering av objekten?*
* *Har de anställda skolats in i en processmodell gällande förberdning för och rapportering av undantagssituationer?*
* *Har övervakningssystemens nät separerats från andra nät? Hur och varifrån kommer man t.ex. åt kameraövervakningen?*
* *Hur samarbetar nätinnehavaren med olika myndigheter för att skydda kritiska objekt mot skadegörelse och militär verksamhet?*
* *Har ansvarspersoner definierats och hur uppdateras ansvaren eller ansvarspersonerna?*
* *Är passerkontrollsystemet testat med tanke på datasäkerheten?*
* *Hur har man genomfört och gett anvisningar om hur utomstående (t.ex. varuleverantörer, servicetjänster och leverantörer av utrustning) kan röra sig i olika lokaler? Har personer från leverantörer, servicetjänster eller leverantörer av utrustning genomgått en säkerhetsutredning?*
* *Hur begränsas giltighetstiden för besökarnas och den egna personalens passerkort? Har en process fastställts för besöken? Hur har man gett anvisningar och begränsat antalet besökare som rör sig i lokalerna?*

## Reservsystem för kritiska data- och datakommunikationssystem

*Beskrivning av reservsystem och åtgärder för övergång till reservsystem. För vilka system finns reservsystem?*

* *Har till exempel lokalerna för apparater i funktionskritiska system verifierats (t.ex. fördubblats) och placerats tillräckligt långt från varandra geografiskt?*
* *Har driftcentralen ett reservkontrollrum i en annan byggnad än det egentliga kontrollrummet?*
* *Om reservkontrollrummet är beläget längre bort än på promenaddistans, hur har transporten av personal mellan kontrollrummen ordnats eller planerats att ordnas?*
* *Existerar det tillfälliga lokaler för situationer där kontrollrum och andra normala arbetsutrymmen inte är i bruk?*
* *Är dokumenteringen av reservsystemen för datakommunikations- och informationssystemen uppdaterad? Finns det aktuella fysiska kopior av dokumenten? Är placeringen av dessa kopior känd?*
* *Är ansvarspersonerna fastställda och har de tillräckliga kunskaper, färdigheter, ansvar och befogenheter? Finns en eller flera ansvarspersoner med tillräckliga beslutsrättigheter alltid tillgänglig?*
* *Hur fattar ansvarspersonen beslut om övergång till reservsystemet?*
* *Har reservkommunikationssätt, verktyg och -kanaler planerats och testats för störningssituationer där grundläggande informationsteknik eller datanät inte är tillgängliga?*
* *Har man funderat på hur systemen ska drivas om man inte får kontakt med systemen på distans eller om normala kontrollrum inte är tillgängliga?*
* *Har man förberett sig på en situation där normala kommunikationsmedel inte kan användas när en eventuell skadlig aktör är inne i systemen?*
* *Har man förberett sig på olika scenarier där systemen inte kan återställas i funktionsdugligt skick till exempel genom säkerhetskopior?*

SÄKERSTÄLLANDE AV TJÄNSTEPRODUCENTERNAS FUNKTIONSFÖRMÅGA

*Beskrivning av hur nätinnehavaren har säkerställt kontinuiteten i funktionsförmågan och en tillräcklig mängd personal hos de parter som deltar i hanteringen av störningssituationer. I synnerhet de tjänsteproducenter som deltar i hanteringen av störningssituationer är centrala, men även andra tjänsteproducenters funktionsförmåga ska säkerställas och beaktas i beredskapsplanen.*

*Obs! Rubrikerna i mallen har formulerats så att de gäller alla tjänsteproducenter i allmänhet, men i verktyget SÄHKÖKOTKA finns tjänsteproducenterna specificerade enligt bransch:*

* *Tjänsteproducenter för eldistributionsnätet*
* *Tjänsteproducenter för ställverk och högspänningsnät*
* *Tjänsteproducenter för data- och datakommunikationssystem*

## Hantering av risker i anslutning till tjänsteproducenter och minimering av konsekvenserna

*Beskrivning av hur riskerna i anslutning till tjänsteproducenterna och hur konsekvenserna av dessa risker för nätinnehavarens verksamhet har kartlagts.*

*Har nätinnehavaren till exempel säkerställt tjänsteproducentens:*

* *verksamhetssätt för ledning under krissituationer*
* *tillräcklig utbildning i beredskapsfrågor för personer som sköter kritiska uppgifter*
* *informationssäkerhetspraxis*
* *anskaffning av tillbehör, material och bränsle*
* *avtal med ersättande tjänsteproducenter*

*Har man för nätinnehavarens del fastställt ansvarspersoner som säkerställer att tjänsteproducenternas funktionsförmåga har beaktats på behörigt sätt i avtalen och i tjänsteproducentens praktiska verksamhet.*

## Fastställande av kritiska nivåer för tjänsteproducenter

*Har olika kritiska nivåer fastställts för tjänsteproducenterna och hur säkerställs funktionsförmågan och ersättningsbarheten i synnerhet för de mest kritiska tjänsteproducenternas del?*

## Möjligheter att ersätta tjänsteproducenternas resurser och styrsystem

*Beskrivning av hur tjänsteproducenternas resurser och styrsystem kan ersättas t.ex. med ett annat företag som producerar tjänster?*

## Tjänsteproducenternas verksamhetsmodell och samarbete med nätinnehavaren i allvarliga störningssituationer

*Hur har nätinnehavaren säkerställt att tjänsteproducentens verksamhetsmodeller är kompatibla med nätinnehavarens verksamhet och att samarbetet med nätinnehavaren fungerar smidigt i allvarliga störningssituationer?*

REGIONALT SAMARBETE

## Eldriftsställen av kritisk betydelse

*Beskrivning av hur eldriftsställen av kritisk betydelse enligt 2 § i statsrådets förordning (ANM/2022/211) har definierats för störnings-, elbrist- och krissituationer och beaktats i nätinnehavarens beredskap. Vilka eldriftsställen av kritisk betydelse har nätinnehavaren identifierat inom sitt ansvarsområde? Har definitionen gjorts i samarbete med kunderna?*

*Hur har eldriftsställen av kritisk betydelse beaktats i nätinnehavarens kund- och användarstödsystem?*

*Obs! Enligt SRF 2 § ska man i första hand sträva efter att trygga eltillförseln till eldriftsställen av kritisk betydelse för att upprätthålla funktioner som är nödvändiga med tanke på ledningen av samhället och säkerheten. Avsikten är inte att klassificera eldriftsställen som är av kritisk betydelse enligt prioriteringsgrupperingen för driftställen enligt punkt 11.2 utan de bildar en egen grupp.*

## Företrädesordning för övriga eldriftsställen

*Beskrivning av hur företrädesordningen har fastställts för andra eldriftsställen än de av kritisk betydelse som avses i 2 § i statsrådets förordning (ANM/2022/211) i fall av störnings-, elbrist- och krissituationer och hur företrädesordningen har beaktats i nätinnehavarens beredskap. Har definitionen gjorts i samarbete med kunderna? Obs! Fastställandet av företrädesordningen gäller alla nätinnehavarens driftställen*

*Hur har driftställenas företrädesordning beaktats i nätinnehavarens kund- och användarstödsystem?*

*Nätinnehavarna ska i sin plan åtminstone beskriva*

* *i hur många grupper eldriftsställena grupperas,*
* *vilken typ av eldriftsställen som hör till respektive grupp,*
* hur många eldriftsställen som hör till gruppen, *och*
* *prioritetsklass för varje grupp (dvs. för hur lång tid eltillförseln kan avbrytas).*

*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.*

*Andra eldriftsställen än de som är av kritisk betydelse ska enligt 2 § klassificeras i minst tre olika grupper 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.*

*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.*

## Samarbete och lägesbild med räddningsmyndigheterna

*Beskrivning av hur samarbetet med räddningsmyndigheterna har ordnats i störnings- och felsituationer.*

*Beskrivning av hur lägesbilden förmedlas med räddningsmyndigheten.*

## Samarbete med andra myndigheter

*Beskrivning av hur samarbetet och kommunikationen med andra myndigheter (t.ex. polisen) har ordnats.*

*Hur har bolaget organiserat och sörjt för praxis för rapportering om avvikande händelser och anmälningar till myndigheterna (NIS-anmälningar till Energimyndigheten, Skypo, KTK, CKP osv.)?*

*Enligt polisens anvisningar (ID-2537733) ska observerade hot, avvikande händelser och brott utan dröjsmål anmälas till nödcentralen och polisen enligt nedanstående anvisningar, så att man omedelbart kan bedöma vilka åtgärder som behöver vidtas och inleda dessa.*

*Anmälningssätt:*

***1) Ring nödnumret 112 om det är fråga om***

*- en hotfull situation eller ett brott som pågår eller precis har inträffat i anslutning till ett kritiskt objekt, där den misstänkta gärningsmannen är på platsen eller precis har avlägsnat sig*

*- gärningsmannen har avlägsnat sig, men det finns spår som kan säkras på platsen, eller det finns t.ex. inspelningar från en övervakningskamera om gärningen och gärningsmannen eller uppgifter om ett fordon som gärningsmannen använt*

*- aktivitet som avviker från det normala i närheten av objekten, t.ex. fotografering av objekten, drönare*

***2) Gör en brottsanmälan*** *https://poliisi.fi/sv/gor-en-brottsanmalan*

*- ringa brott som begås på objekten i icke-brådskande situationer*

*- gärningen har begåtts tidigare och det inte finns några observationer eller spår mm. att säkra av gärningsmannen*

***3) Anmälan om andra iakttagelser som har väckt misstankar på platser***

*- ingen akut hotsituation och inget brott har upptäckts*

*- anteckna händelsen och skicka uppgifterna per e-post till*

*havainnot.krp@poliisi.fi och palaute@supo.fi*

## Samarbete med andra distributionsnätsbolag

*Beskrivning av hur man samarbetar med andra bolag i störningssituationer och i beredskapen inför dem. Kommer man mellan bolagen överens om t.ex. fördelning av resurser för att repararea fel och ordnande av reservmatningsförbindelser?*

## Samarbete med stamnätsbolaget

*Beskriv samarbetet med stamnätsbolaget vid allvarliga störningar: storstörningar i stamnätet, elbrist och ransoneringsplaner samt distributionsnätinnehavarens roll i samarbete med stamnätsbolaget.*

## Samarbete med fjärrvärmebolag

*Beskrivning av hur kontakten med fjärrvärme- och energibolagen har ordnats.*

## Samarbete med vattenbolag

*Beskrivning av hur man samarbetar med vattenbolagen i störningssituationer och i beredskapen för dem.*

## Samarbete med telebolag

*Beskrivning av hur man samarbetar med telebolagen i störningssituationer och i beredskapen inför dem. Känner nätinnehavaren till telebolagens mest kritiska basstationer och hur kommer man överens om prioritetsordningen för återställning el till basstationerna?*

## Samarbete med kommuner

*Beskrivning av hur man samarbetar med kommunerna i störningssituationer och i beredskapen för dem.*

## Samarbete med andra aktörer (t.ex. försvarsmakten, vägunderhållare)

*Beskrivning av hur man samarbetar med andra centrala aktörer i störningssituationer och i beredskapen inför dem. Hur kommer man överens om t.ex. prioriteringen av vägunderhållet i områdena fel repareras om snötäcket eller trädbeståndet hindrar reparationsgruppen från att nå området?*