**Sähköverkonhaltijan varautumissuunnitelman mallipohja**

Sisällysluettelo

[1 TAUSTAA 3](#_Toc188021022)

[2 SÄHKÖNJAKELUYHTIÖN TOIMINNAN LÄHTÖKOHDAT 4](#_Toc188021023)

[3 YHTIÖN VARAUTUMIS- JA VALMIUSSUUNNITTELUN PERUSTIEDOT 5](#_Toc188021024)

[4 YHTIÖN RISKIKARTOITUS JA VARAUTUMISSUUNNITTELU 5](#_Toc188021025)

[5 HÄIRIÖTILANTEIDEN HALLINNAN VASTUUT JA JÄRJESTELYT 8](#_Toc188021026)

[6 POIKKEAVIIN SÄÄOLOIHIN VARAUTUMINEN 9](#_Toc188021027)

[7 TOIMINTA POIKKEAVIEN SÄÄOLOSUHTEIDEN AIHEUTTAMISSA SUURHÄIRIÖTILANTEISSA 11](#_Toc188021028)

[8 MUIHIN HÄIRIÖTILANTEISIIN VARAUTUMINEN JA TOIMINTA HÄIRIÖTILANTEESSA 13](#_Toc188021029)

[9 VIESTINTÄVERKKOJEN SEKÄ TIETOJÄRJESTELMIEN RISKIEN HALLINTA JA KÄYTETTÄVYYDEN VARMISTAMINEN 16](#_Toc188021030)

[10 PALVELUTUOTTAJIEN TOIMINTAKYVYN VARMISTAMINEN 27](#_Toc188021031)

[11 ALUEELLINEN YHTEISTYÖ 29](#_Toc188021032)

# TAUSTAA

*Tähän voi kirjoittaa lyhyen taustakuvauksen.*

*Varautumissuunnitelma kokoaa yhteen verkonhaltijan varautumista ja häiriönhallintaa koskevan ohjeiston ja tiedot varautumisesta. Suunnitelman avulla on arvioitavissa verkonhaltijan ohjeiston ja varautumisen kattavuus, ohjeiden ajantasaisuus ja ristiriidattomuus.*

*Kaikkia mallipohjan tekstejä tulee muokata verkonhaltijan tarpeiden mukaisesti. Varautumissuunnitelmaan voi linkittää olemassa olevia ajantasaisia dokumentteja. Yhteystiedot ja usein päivitettävät tiedot voivat olla erillisissä dokumenteissa, joihin varautumissuunnitelmassa viitataan.*

*Mallipohjan tekemisessä on käytetty tukena Turvallisuuskomitean julkaisemia Kokonaisturvallisuuden sanastoa TSK 50 sekä Kyberturvallisuuden sanastoa TSK 52. Termistön yhtenäistämiseksi suosittelemme käyttämään kyseisiä sanastoja myös varautumis- ja valmiussuunnitelmien laatimisessa.*

*Suunnittelun tukena voi hyödyntää Energiaviraston vuoden 2019 varautumissuunnitelmista tunnistamia hyviä käytäntöjä. Sen lisäksi ohjeistusta löytyy HVO-extranetin Tietopankista sekä Energiahuoltosektorin työtilasta. Ohjeita löytyy mm. seuraavista teemoista:*

* *Tilannekuva-pelikirja (2021)*
	+ *Tilannekuvan tuottaminen sekä yhtiön sisäinen ja yhteistyökumppaneiden välinen viestintä*
* *Tiedonvaihto-pelikirja (2022)*
	+ *Ohjeistusta siitä miten suurhäiriötilanteen tiedonvaihto eri organisaatioiden välillä tehdään tehokkaasti sekä miten muodostetaan yhteinen tilanneymmärrys julkisen viestinnän perustaksi*
* *Viestintä sähköpulan uhatessa -ohje (2022)*
* *Viestintä kantaverkon suurhäiriössä -ohje (2019)*
* *Keskeytyskriittisten sähkönkäyttöpaikkojen priorisointi -selvitys (2021)*
	+ *Sisältää suosituksia kriittisten kohteiden määrittämisestä sekä niiden priorisoinnista*
* *Taulukko HVO-poolien sähkönkäyttöpaikkojen etusijajärjestyksestä (2024)*
* *Pohjois-Suomen pelastuslaitosten valmiudet toimia suurjännitekohteiden onnettomuuksissa -selvitys (2021)*
	+ *Sisältää mm. suosituksia suurjännitekohteiden onnettomuus- ja vaaratilanteiden varautumiseen*
* *KYBER‐ENE Energia‐alan kyberturvaaminen 1‐2*
	+ *Käytännönläheisiä menetelmiä ja toimia kyberturvallisuuden toteuttamiseen ja kehittämiseen, sisältäen tarkastuslistoja muun muassa IoT-ratkaisuihin.*

*Harjoittelun osalta tuoretta ohjeistusta löytyy mm. Huoltovarmuuskeskuksen ja Kyberturvallisuuskeskuksen sivuilta:*

* [*Energia-alan harjoitusohje - Huoltovarmuuskeskus*](https://www.huoltovarmuuskeskus.fi/julkaisu/energia-alan-harjoitusohje) *(2024)*
* [*Ohje sähköpostiharjoituksen toteuttamiseen | Kyberturvallisuuskeskus*](https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/ohje-sahkopostiharjoituksen-toteuttamiseen) *(2023)*

*Edellä mainittujen lisäksi ohjeistusta varautumiseen sekä jatkuvuudenhallintaan löytyy myös Kyberturvallisuuskeskuksen sivuilta:* [*Tietoturvaohjeita yrityksille | Kyberturvallisuuskeskus*](https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-organisaatioille-ja-yrityksille) *sekä eOppiva-palvelusta:* [*https://www.eoppiva.fi/koulutukset/turvaa-digitaalinen-toiminta-hairiotilanteissa/*](https://www.eoppiva.fi/koulutukset/turvaa-digitaalinen-toiminta-hairiotilanteissa/)

SÄHKÖNJAKELUYHTIÖN TOIMINNAN LÄHTÖKOHDAT

## Sähkönjakeluyhtiö lyhyesti

*Lyhyt kuvaus.*

### Häiriöihin varautuminen sähkönjakeluyhtiössä

*Lyhyt kuvaus.*

### Merkittävimmät häiriötilanteet, jotka on toiminnassa tunnistettu

*Kirjataan merkittävimmät häiriötilanteet suunnitelman lähtökohdaksi. Hyödynnetään mahdollisen riskikartoituksen tuloksia.*

### Sähkönjakeluyhtiön johtamisjärjestelmä, riskienhallinta ja laadunvarmistus

*Lyhyt kuvaus ja viittaus dokumentteihin sekä järjestelmiin.*

# YHTIÖN VARAUTUMIS- JA VALMIUSSUUNNITTELUN PERUSTIEDOT

## Varautumissuunnittelun vastuut ja järjestelyt

*Kuka laatii varautumissuunnitelman ja ketä varautumissuunnitteluun osallistuu? Toimitusjohtajan on hyväksyttävä varautumissuunnitelma ennen sen toimittamista Energiavirastolle.*

***Huom! Ei vastuuhenkilöiden nimiä.*** *Ohjeen mukaisesti varautumissuunnitelmaan ei ole tarkoituksenmukaista yksilöidä vastuuhenkilöiden nimiä vaan tehtävänimikkeet riittävät.*

## Varautumissuunnitelman päivittäminen

*Kuvaus suunnitelman päivitysprosessista. Miten usein suunnitelmaa tai suunnitelman osia päivitetään?*

## Edellisessä suunnitelmassa tunnistetut kehityskohteet

*Mitkä olivat keskeisimmät edellisessä varautumissuunnitelmassa tunnistetut kehityskohteet ja niiden kehittämiseksi tunnistetut toimenpiteet. Onko suunnitellut toimenpiteet toteutettu ja mihin varautumissuunnitelman osiin niiden perusteella on tehty muutoksia (Huom. muutosmerkinnät suunnitelmaan).*

YHTIÖN RISKIKARTOITUS JA VARAUTUMISSUUNNITTELU

*Tässä luvussa on tarkoitus tuoda esille, miten verkonhaltija kartoittaa siihen kohdistuvia riskejä, varautuu niiden hallintaan sekä ylläpitää ja kehittää varautumiseen liittyvää osaamistaan ja tietoisuuttaan.*



## Ennakoiva riskienhallinta ja riskien analysointi

*Kuvaus yhtiön riskiarviointiprosessista ja tunnistetuista riskeistä. Ketkä osallistuvat riskiarvion tekoon, kuka vastaa riskiarviosta ja miten usein riskiarviota päivitetään.* *Suositeltavaa on, että yhtiön operatiivinen johto, kukin vähintään omalta vastuualueeltaan mahdollisuuksiensa mukaan osallistuu arvion laadintaan.*

*Milloin viimeisin riskiarvio on tehty? Onko riskit jaettu luokkiin esim. ilmiöiden todennäköisyyden ja taloudellisen vaikutuksen perusteella?*

*Onko yhtiö tutustunut kansalliseen ja alueelliseen riskiarvioon ja hyödyntänyt niitä riskiarvion laadinnassa)? Millaisia riskejä verkonhaltija on tunnistanut ja mihin keskeisiin riskeihin tällä suunnitelmalla erityisesti pyritään vaikuttamaan? Onko keskeisille riskeille määritelty hallintatoimet, vastuuhenkilöt ja aikataulut hallintatoimien toteuttamisesta?*

*Riskirekisteri keskeisimmistä (10-15 kpl) sähkön jakelu- tai siirtopalvelun tarjontaan vaikuttavista riskeistä ml. kyberturvallisuusriskit on toimitettava suunnitelman liitteenä.*

## Jatkuvuudenhallinnan suunnittelu

*Miten riskianalyysissa tunnistetut uhat ja liiketoiminnan kriittiset prosessit huomioidaan jatkuvuuden hallinnan suunnittelussa? Mitkä ovat yhtiön varautumisen painopistealueet seuraavat kolme vuotta?*

*Jatkuvuuden hallinnalla luodaan toimintatapa vakavien häiriötilanteiden hallinnalle ja toiminnan jatkuvuudelle ja se kattaa alkutapahtuma-skenaarioiden analyysin, tapahtumien todennäköisyyteen ja vaikutuksiin perustuvat päätökset toimenpiteiden tarpeesta, suunnitelmien laatimisen ja resursoinnin sekä suunnitelmien koulutuksen ja jatkuvan ylläpidon.*

## Huoltovarmuustietoisuuden ylläpito ja päivittäminen

*Millä tavoin verkonhaltija huolehtii huoltovarmuustietoisuuden ylläpitämisestä ja päivittämisestä? Tarkoituksena on, että verkonhaltija pysyy ajan tasalla uhkien kehittymisestä sekä oman jatkuvuussuunnittelun toimenpiteiden toimivuudesta ja oikeasta kohdentamisesta.*

## Varautumisen kehittäminen yhdessä sidosryhmien kanssa ml. varautumisharjoitukset

*Kuvaus siitä, miten yhtiössä kehitetään varautumista sekä miten harjoitellaan toimintaa erilaisissa häiriötilanteissa ja miten usein varautumista harjoitellaan myös yhteistyökumppaneiden ja viranomaisten kanssa? Onko yhtiö osallistunut viranomaisten järjestämiin harjoituksiin kuten AVI:n valmiusharjoituksiin, TIETO- tai PAPU-harjoituksiin?*

*Harjoitellaanko yrityksen oman varautumisen lisäksi toimitusketjujen ja -verkostojen varautumista ml. palveluntuottajat ja materiaalitoimittajat? Esimerkiksi varautumissuunnitelma katselmoidaan ja sen toimivuus testataan varautumisharjoituksissa ja lisäksi järjestetään suurhäiriö-, palo- ja pelastusharjoituksia. Varautumisharjoituksissa testataan myös materiaalitoimitusketjujen ja palveluntuottajien varautuminen.*

*Asiakkaiden informoinnissa tiedotusvälineillä on merkittävä rooli. On hyvä huolehtia siitä, että kontakteja tiedotusvälineisiin ylläpidetään jatkuvasti, jolloin mahdollisilla luottotoimittajilla ja tiedottajilla on hyvä käsitys verkonhaltijan toiminnasta ja varautumiseen liittyvistä asioita. Tiedotusvälineet on hyvä ottaa huomioon jo varautumisen toiminnan suunnittelussa ja toimintaa harjoiteltaessa. Näin varmistetaan, että todellisissa tilanteissa tiedotusvälineet saavat mahdollisimman oikeata ja ajantasaista tietoa. Ja kun yhteistyö on ollut hyvää jo normaalioloissa, voivat tiedotusvälineet osaltaan tukea yhtiön tiedotusta ja välttää mahdollisesti muista lähteistä tulevien spekulatiivisten tai ristiriitaisten tietojen välittämistä.*

*Suunnitelmassa on myös hyvä tuoda esiin listauksena:*

* *Onko yhtiöllä varautumisharjoitteluun liittyvä suunnitelma? Kuinka pitkälle ajalle suunnitelma on ja mihin harjoituksiin aiotaan osallistua?*
* *Mihin harjoituksiin on osallistuttu viime vuosina?*

# HÄIRIÖTILANTEIDEN HALLINNAN VASTUUT JA JÄRJESTELYT

*Johtamisvastuulla tarkoitetaan kokonaiskuvan hallintaa ja päätöksentekoa. Toimintavastuilla tarkoitetaan käytännön toimia*.

## Johtamisvastuut häiriö- ja vikatilanteissa

*Kuvaus vastuuhenkilöiden johtamisvastuista häiriö- ja vikatilanteissa. Onko yhtiössä määritelty esim. suurhäiriöorganisaatio ja sen mukaiset tehtävät/vastuut?*

## Toimintavastuut häiriö- ja vikatilanteissa

*Kuvaus vastuuhenkilöiden toimintavastuista häiriö- ja vikatilanteissa. Onko yhtiössä määritelty esim. suurhäiriöorganisaatio ja sen mukaiset tehtävät/vastuut?*

Taulukko 1 Toimenkuvissa olevat häiriöiden hallintatehtävät.

|  |  |  |
| --- | --- | --- |
| Yritys | Tehtävä | Puhelin |
|  | esim. käyttöpäällikkö |  |
|  |  |  |
|  |  |  |

## Viestintä- ja kriisiviestintäsuunnitelmat eri häiriö- ja vikatilanteissa

*Kuvaus miten esim. asiakkaille, yhteistyötahoille, viranomaisille ja medialle viestitään häiriötilanteissa. Suunnitelmassa on määriteltävä myös vastuuhenkilöt viestinnän osalta.*

*Hyvin suunnitellussa varautumisessa ennalta määritetyt varautumistasot sisältävät periaatteet kunkin varautumistason viestintää varten. Toimijoiden (esim. vuoromestari, käyttöpäällikkö, viestintä) tehtävät on kuvattu vakavuusluokkien mukaan. Hyvä käytäntö on hyödyntää viestinnän toteutuksessa monikanavaista mediaa sekä toimittaa tietoa alustariippumattomaan ja resursseiltaan skaalautuvaan palveluun. Yksityiskohtaisempaa viestintä-/kriisiviestintäsuunnitelmaa on myös hyvä ylläpitää erillisessä liitteessä, jotta esim. viestintäohjeet ja viestipohjat ovat tarvittaessa helposti saatavilla.*

*Viestinnän suunnitteluun löytyy lisäohjeita esim. Tilannekuva -pelikirjasta, joka on saatavilla HVO-extranetistä Voimatalouspoolin yhteisalue -työtilasta). Tilannekuva-pelikirjan tarkoituksena on auttaa organisaatioita suunnittelemaan sisäisesti ja yhteistyökumppaneidensa kanssa häiriöaikaisten viestivälineiden käytön toimintamalleja ja tilannekuvan tuottamista sekä kehittämään yhteistyötä tehostavia menetelmiä.*

POIKKEAVIIN SÄÄOLOIHIN VARAUTUMINEN

*Kuvaus millaisiin ilmastollisiin häiriöihin varaudutaan ja miten varautumistoimenpiteet eroavat tilanteen vakavuuden mukaan tai erityyppisissä tilanteissa esim. myrsky- ja lumikuormatilanteissa.*

*Huom. Tässä luvussa kuvattava erityisesti, miten erilaisten sääilmiöiden aiheuttamiin häiriöihin on varauduttu ennalta ja millaisia toimenpiteitä tehdään häiriötilanteen uhatessa: esim. sään seuranta, henkilöstön hälyttäminen, ennakoivat tekniset toimenpiteet esim. lumikuorman uhatessa.*

*Luvussa 7 kuvataan toimintamallit häiriötilanteessa.*

## Häiriö- ja vikatilanteisiin liittyvien valmiustilojen määrittäminen

*Kuvaus minkälaisia valmiustiloja verkonhaltijalla on ja miten ne on määritelty.*

*Millä toimenpiteillä eri valmiustiloissa nostetaan omaa ja palveluntuottajien valmiutta? Valmiuden nostamiseen liittyy esimerkiksi henkilöresurssien, viestinnän, materiaalien, kaluston, järjestelmien ja urakoitsijoiden saatavuuden tarkistaminen ja tarvittaessa varaaminen.*

## Henkilöstön ja yhteistyökumppaneiden perehdytys toimimaan häiriötilanteissa

*Kuvaus kuinka henkilöstön ja yhteistyökumppaneiden perehdytys erilaisiin häiriötilanteisiin on tehty ja osaaminen on varmistettu.*

## Asiakkaiden ennalta tiedottaminen häiriötilanteista

*Kuvaus miten ja millä kanavilla asiakkaille tiedotetaan häiriötilanteista ja poikkeusoloista (ennalta). Kuka vastaa tiedottamisesta ja miten tiedottamisen valmiuksia ylläpidetään?*

*Yhteystiedot ja usein päivitettävät tiedot voivat olla kootusti erillisessä dokumentissa, johon varautumissuunnitelmassa viitataan. Yhteystiedoissa suositellaan olevan keskeisten asiakkaiden yhteystiedot ja tiedotusvälineiden yhteyshenkilöiden yhteystiedot. Suuri osa asiakkaista seuraa ensisijaisesti tiedotusvälineitä. Jotta informaatio eri lähteistä olisi mahdollisimman yhdenmukaista ja ristiriidatonta, tiedotusvälineille on hyvä tarjota selkeätä ja ajantasaista tietoa tilanteesta.*

## Työaika-, ruokailu ja lepojärjestelyiden järjestäminen

*Kuvaus miten henkilöstön ja yhteistyökumppaneiden työajat, ruokailu ja lepo on järjestetty, jotta sähkönjakeluyhtiö pystyy toimimaan häiriötilanteessa.*

## Varuste- ja kalustohuoltoon varautuminen häiriötilanteissa

*Kuvaus miten verkonhaltijan ja kumppaneiden varusteiden ja kaluston huolto on järjestetty etenkin pidemmissä häiriötilanteissa.*

## Verkostomateriaalin varaaminen

*Kuvaus sähköverkon korjaustöihin tarvittavien materiaalien ja varaosien saatavuudesta.*

* *Mitä materiaaleja on varattu?*
* *Miten alihankintapalvelut on turvattu häiriötilannetta ajatellen?*
* *Onko mahdollista varata kriittisiä varaosia tai onko niiden saatavuuden varmistamisesta sovittu palveluntuottajien kanssa?*
* *Tiedetäänkö mistä varaosat tai muut materiaalit tilataan sekä niiden toimitusaika?*
* *Onko selvitetty yhteistyömahdollisuuksia naapurisähkönjakeluyhtiön kanssa?*
* *Onko määritelty vastuuhenkilöt?*

*Esim. seuraavat materiaalit ja välineet ovat olennaisia:*

* *Verkostomateriaalit ja varaosat*
* *Ajoneuvot ja muu kalusto*
* *Operatiivinen viestiliikenne ja -kalusto*
* *Varavoimakoneet*

## Sähköasema- ja suurjänniteverkostomateriaalin varaaminen

*Kuvaus sähköasemien varakoneiden, laitteiden varaosien ja muiden materiaalien saatavuudesta.*

* *Mitä materiaaleja on varattu?*
* *Miten alihankintapalvelut on turvattu häiriötilannetta ajatellen?*
* *Onko sähkönjakeluyhtiön tai palveluntuottajien mahdollista varata kriittisiä varaosia tai muita materiaaleja häiriötilanteita ajatellen?*
* *Yhteistyömahdollisuudet naapurisähkönjakeluyhtiön kanssa?*
* *Onko määritelty vastuuhenkilöt?*

*Materiaalien ja laitteiden varaamisessa on huomioitava myös poikkeuksellisten tilanteiden (esim. pakotteiden tai pandemian) aiheuttamat saatavuusongelmat.*

TOIMINTA POIKKEAVIEN SÄÄOLOSUHTEIDEN AIHEUTTAMISSA SUURHÄIRIÖTILANTEISSA

*Kuvaus toiminnasta erityisesti sääilmiöistä aiheutuvissa suurhäiriötilanteissa.*

## Häiriö- ja vikatilanteiden luokittelu sekä toimenpiteet eri suurhäiriötilanteissa

*Vrt. kohta 6.1 ”Häiriö- ja vikatilanteisiin liittyvien valmiustilojen määrittäminen”. Miten häiriöön varautumisesta siirrytään toimimaan suurhäiriötilanteessa?*

*Onko verkonhaltija määrittänyt suurhäiriöorganisaation? Miten suurhäiriöorganisaation laajuus ja toiminta vaihtelee häiriötyypeittäin (esim. myrsky, lumikuorma, ukkoset) tai häiriötilanteen vakavuuden (esim. sähköttömien asiakkaiden määrä) mukaan?*

## Häiriö- ja vikatilanteiden seuranta ja tilannekuvan ylläpito

*Kuvaus miten verkon häiriö- ja vikatilanteita seurataan ja miten tietoa hyödynnetään tilannekuvassa.*

## Johtamiskeskuksen/tilannekuvakeskuksen perustaminen

*Kuvaus miten ja missä tilanteessa johtamiskeskus/tilannekuvakeskus perustetaan. Kuvattava myös johtamiskeskuksen toimintaa, tehtäviä, vastuuhenkilöitä sekä tilannekuvan ylläpitoa.*

*Kuka vastaa tilannekuvan ylläpidosta?*

*Tilannekuvaa varten on syytä kerätä tietoja häiriötilanteen kehittymisestä esim. sääennusteista, verkon käyttötoiminnan tietojärjestelmistä, kenttätoimijoilta, palveluntuottajilta sekä muilta yhteistyöorganisaatioilta esim. Krivat:n kautta.*

## Asiakkaiden tiedottaminen pitkäkestoisissa häiriötilanteissa

*Kuvattava millä välineillä ja miten asiakkaille tiedotetaan pitkäkestoisissa häiriötilanteissa.*

* *Miten varmistetaan, että asiakkaat saavat esim. vikapuhelinpalvelusta, tekstiviestipalvelusta, somesta ja tiedotteista mahdollisimman oikean arvion tilanteesta ja lämmityskatkojen kestosta myös suurhäiriötilanteissa?*
* *Kuka vastaa tiedottamisesta sisäisesti ja ulkoisesti.*
* *Kontaktit tiedotusvälineisiin, tiedotusvälineiden hyödyntäminen.*

*Yhteystiedot ja usein päivitettävät tiedot voivat olla kootusti erillisessä dokumentissa, johon varautumissuunnitelmassa viitataan.*

## Häiriötilanteiden jälkeiset palautetilaisuudet ja -kyselyt

*Kuvaus miten organisaatiossa järjestetään häiriötilanteen jälkeinen raportointi sekä palautetilaisuudet ja -kyselyt. Kuka vastaa tilanteen jälkeisistä palautetilaisuuksista? Keneltä palautetta pyydetään (esim. henkilöstö, yhteistyökumppanit, asiakkaat) ja miten (esim. tilaisuudet, haastattelut, nettikyselyt)?*

*Miten esimerkiksi seuraavia asioita huomioidaan tilanteen jälkeisessä raportoinnissa ja kehityskohteiden arvioinnissa?*

* *vikojen kokonaismäärä (sj-, kj-, pj-viat)*
* *johdoilta poistettujen puiden määrä*
* *korjausresurssien määrä*
* *asiakaspalvelu- ja muiden tilanteeseen osallistuvien resurssien määrä*
* *korjauskustannukset*
* *tapaturmat ja vaaratilanteet*
* *puheluiden määrät, vastausajat ym.*
* *sähköttömien asiakkaiden määrä*
* *vikojen kestoajat*
* *SAIDI ja KAH -arviot*
* *vakiokorvausten määrä*
* *onnistuminen mediassa (positiiviset/neutraalit/negatiiviset uutiset)*

MUIHIN HÄIRIÖTILANTEISIIN VARAUTUMINEN JA TOIMINTA HÄIRIÖTILANTEESSA

*Kuvaus miten yhtiön varautuminen riippuu häiriötilanteesta ja minkälaiset toimintaohjeet erilaisiin häiriötilanteisiin on?*

## Sähkönjakeluverkon ja suurjännitteisen jakeluverkon merkittäviin teknisiin vikoihin ja vaurioihin varautuminen

*Kuvaus millaisiin jakelu-/siirtoverkon teknisiin vikoihin varaudutaan ja miten niihin varaudutaan.*

## Epidemioihin varautuminen

*Kuvaus miten toiminnassa on huomioitu epidemiasta eli suureen osaan alueen väestöstä levinneestä tartuntataudista aiheutuva henkilöstövaje omassa toiminnassa, palvelutoimittajien toiminnassa ja muiden ulkoisten palvelujen tarjonnassa.*

*Henkilöresurssien vähetessä on keskeistä tunnistaa kriittiset toiminnot ja supistaa tarvittaessa toimintaa niiden prosessien osalta, joiden osalta keskeytys tai toiminnan supistaminen eivät tuota kohtuutonta haittaa. Kriittisten toimintojen osalta on myös syytä panostaa henkilöiden korvattavuuteen esim. koulutuksilla ja tehtäväkierrolla.*

## Suuronnettomuuksiin varautuminen

*Kuvaus miten toiminnassa on varauduttu suuronnettomuuksiin. Suuronnettomuudella tarkoitetaan onnettomuutta, jota on kuolleiden, loukkaantuneiden, ympäristöön tai omaisuuteen kohdistuneiden vahinkojen määrän taikka onnettomuuden laadun perusteella pidettävä erityisen vakavana.*

*Suuronnettomuuteen, joka aiheutuu ulkopuolisesta syystä, sähkönjakeluyhtiön varautumisen keskeiset osa-alueet ovat:*

* *oman ja palvelutoimittajan henkilöstön suojaaminen ja turvallisuus*
* *yrityksen omaisuuden suojaaminen*
* *sähkönjakelun jatkuvuuden varmistaminen*

## Sähköpulaan varautuminen

*Kuvaus miten sähköpulatilanteeseen on varauduttu ja minkälaiset suunnitelmat yhtiöllä on sähköpulatilanteen varalle (valmiuden nosto, johtaminen, tehonrajoitus, tiedottaminen yms.).*

*Sähköpulalla (tehopula) normaalioloissa tarkoitetaan tilannetta, jossa tuotanto ja tuonti eivät riitä kattamaan kulutusta ja tällöin kulutusta joudutaan hetkellisesti rajoittamaan. Sähköpulalla tarkoitetaan eri asiaa kuin poikkeusoloissa tehtävällä sähkönsäännöstelyllä. Kantaverkkoyhtiö käyttää tuotanto- ja kulutustilanteen kiristyessä kolmiportaista menettelyä:*

* ***Sähköpula mahdollinen*** *on kyseessä silloin, kun ennusteiden perusteella on ennakoitavissa, että kotimainen tuotanto ja tuonti eivät riitä kattamaan sähkönkulutusta lähitunteina tai vuorokautena. Toimijoita pyydetään tarkastamaan suunnitelmansa ja varautumaan tilanteeseen.*
* ***Sähköpulan riski suuri*** *katsotaan syntyneeksi, kun kaikki Suomesta saatavilla oleva sähköntuotanto on käytössä eikä naapurimaista ole mahdollista saada lisää sähköä. Fingrid on joutunut käynnistämään nopeaa (15 min.) häiriöreserviään, eli kaasuturpiineja ja aktivoimaan irtikytkettäviä kuormia teollisuudessa. Suomessa ei kyetä ylläpitämään mitoittavaa vikaa vastaavaa määrää nopeaa häiriöreserviä.*
* ***Sähköpula*** *(vakava tehopulatilanne) katsotaan syntyneeksi, kun sähköntuotanto ja tuonti eivät riitä kattamaan kulutusta ja sähkönkulutusta joudutaan kytkemään irti ilman kaupallisia sopimuksia. Jakeluverkonhaltijat suorittavat kulutuksen kytkemisen irti ennalta laadittujen suunnitelmien mukaisesti hallitusti siten, että sähkökatkot ovat enimmillään pari tuntia, eikä katkoksia kohdisteta yhteiskunnan kannalta tärkeisiin toimintoihin.*

## Kantaverkon suurhäiriöön varautuminen

*Kuvaus miten kantaverkon suurhäiriöön sekä hätätilaa- ja käytönpalautusta koskevan verkkosäännön (NC ER) mukaisiin järjestelmän varautumissuunnitelman ja käytönpalautumissuunnitelman toimenpiteisiin on varauduttu. Minkälainen suunnitelma yhtiöllä kantaverkon suurhäiriössä toimimiseksi?*

*Kantaverkossa on suurhäiriö, kun yli puolet kulutuksesta on ilman sähköä tai koko kantaverkko on jännitteetön yli kolme minuuttia. Suurhäiriö voi johtua useista eri syistä. Suurhäiriö voi syntyä erilaisten siirtoverkon tai sähköntuotannon vikojen, luonnonilmiöiden, terroritekojen, väkivallan, huolimattomuuden, tietämättömyyden ja onnettomuuksien seurauksena. Suurhäiriö edellyttää useita samanaikaisia vakavia vikoja sähköjärjestelmässä.*

## Toimitila- ja varastomenetykseen varautuminen

*Kuvaus miten toimitila- ja varastomenetykseen varaudutaan.*

*Huom. Valvomon väistösuunnitelma on osana valmiussuunnitelmaa.*

## Avainhenkilömenetykseen varautuminen

*Onko verkonhaltija tunnistanut kriittisiä tehtäviä suorittavia avainhenkilöitä kenen menetyksellä olisi suuri merkitys yhtiön toimintaan? Miten avainhenkilömenetyksen riskejä minimoidaan?*

## Hybridivaikuttamiseen varautuminen

Miten verkonhaltija on yhdessä sidosryhmien kanssa varautunut kasvaneeseen hybridivaikuttamisen uhkaan? Esim. henkilöstöön ja asiakkaisiin kohdistuvaan informaatiovaikuttaminen, kybervaikuttamiseen, yhtiöön kohdistuvaan tiedusteluun, tunkeutumiseen yhtiön tiloihin sekä verkkokomponenttien sabotaasiin?

## Markkinahäiriöihin varautuminen

Miten verkonhaltija on varautunut markkinahäiriöihin? Esim. voimakkaisiin sähkönhinnan vaihteluihin ja niiden vaikutuksiin asiakkaiden sähkönkäyttöön, sähkön myyjien konkursseihin sekä datahubiin liittyviin häiriöihin.

## Muihin häiriötilanteisiin varautuminen

*Tässä voi nostaa esille, mikäli verkonhaltija on tunnistanut muita olennaisia riskejä, joihin se varautuu.*

VIESTINTÄVERKKOJEN SEKÄ TIETOJÄRJESTELMIEN RISKIEN HALLINTA JA KÄYTETTÄVYYDEN VARMISTAMINEN

*Sähkömarkkinalain 29 a §:n mukaisesti verkonhaltijan on huolehdittava käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta. Tästäkin syystä tietoturva ja kyberuhkiin varautuminen ovat kasvava osa varautumissuunnittelua ja siksi ne on erotettu suunnitelmaan omaksi kokonaisuudekseen.*

*Suosittelemme kyberuhkien huomioimista osana organisaation kokonaisriskienhallintaa ja kuvailemaan ne tarkemmin kappaleissa 4.1 ja 4.2.*

*Sähköverkonhaltijan toiminnan perustason turvaamiseksi normaali- ja poikkeusoloissa tulee yritystasolla jatkuvasti varautua kybertoimintaympäristöön (yhdestä tai useammasta digitaalisesta tietojärjestelmästä muodostuva toimintaympäristö) kohdistuviin uhkiin. Tällaisia uhkia ovat mm:*

* *vakava kriittisen tieto- ja viestintäjärjestelmän häiriötilanne, joka haittaa välittömästi ja merkittävästi sähköverkonhaltijan toimintaa, esimerkiksi palvelunestohyökkäys.*
* *vakava laitetilaongelma, joka vaikuttaa usean tietojärjestelmän toimintaan*
* *vakava häiriö tietoliikenteessä, jolla voi olla esimerkiksi vaikutuksia organisaation viestintäkyvykkyyteen tai palveluiden saatavuuteen*
* *vakava tietosuojaloukkaus*

*Kybertoimintaympäristöön kohdistuviin uhkiin varautumista kutsutaan kyberturvallisuudeksi. Kyberturvallisuus voidaan määritellä tavoitetilaksi, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Kybertoimintaympäristön toiminnan häiriytyminen aiheutuu usein toteutuneesta tietoturvauhkasta, joten kyberturvallisuuteen pyrittäessä tietoturva on keskeinen tekijä. Tietoturvan lisäksi kyberturvallisuuteen pyritään muun muassa toimenpiteillä, joiden tarkoituksena on turvata häiriytyneestä kybertoimintaympäristöstä riippuvaiset fyysisen maailman toiminnot.*

*Siinä missä tietoturvalla tarkoitetaan* ***tiedon*** *saatavuutta, eheyttä ja luottamuksellisuutta, kyberturvallisuus tarkoittaa digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuutta ja sen vaikutusta niiden toimintoihin. Kyberturvallisuus ei ole muuttuvassa maailmassa vain kertaluontoinen projekti, vaan sitä on ylläpidettävä ja kehitettävä jatkuvasti.*

*Toimintamalli tietoteknisissä uhkatilanteissa voidaan kuvata myös erillisessä ohjeessa.*

## Kyberturvallisuuden hallinta

*Kuvaus yrityksen Kyberturvallisuuden hallinnasta eli kyberturvallisuuspolitiikasta, -strategiasta ja -ohjelmasta. Kyberturvallisuusohjelman perustana toimii kyberturvallisuusstrategia. Kyberturvallisuusstrategia määrittelee organisaation kyberturvallisuustavoitteet, tavoitteiden prioriteetin, vastuut ja seurannan. Yksinkertaisimmassa muodossa kyberturvallisuusstrategia pitää sisällään listan kyberturvallisuustavoitteista ja suunnitelman niiden saavuttamiseksi.*

*Millainen on yrityksen kyberturvallisuusohjelma. Ohjelman tarkoitus on määritellä hallintamalli, kyberturvallisuuden strateginen kehittäminen ja johdon tuki, huomioiden suojattavien kohteiden riskit ja organisaation asettamat tavoitteet. Onko määritelty esim.*

* *Tietoturvaperiaatteet ja keskeiset käsitteet. Ottaako kyberturvallisuusohjelma kantaa kaikkiin riskiarvioissa ilmeneviin riskeihin joko hyväksyen ne tai määrittäen tarpeellisiksi nähdyt varotoimet kuten suojaus, vastaus ja palautuminen perustellusti?*
* *Ajantasaiset tietoturvaohjeet ja -määräykset. Miten on varmistettu, että asiakas- ja henkilötietoja käsitellään Suomen ja EU:n henkilötietojen suojaa koskevan tietosuojalainsäädännön (GDPR) mukaisesti?*
* *Kyberturvallisuuden valvontakäytänteet. Onko nämä valvontakäytänteet esitelty yhteistoimintamenettelyssä organisaation henkilöstölle?*
* *Tietoturvallisuuden hoitamiseen liittyvät tehtävät ja vastuuhenkilöt, kontaktit yhteistyökumppaneihin, yhteistyöverkostoihin ja viranomaisiin. Miten palveluntuottajat on omalta osaltaan perehdytetty ja sitoutettu yrityksen käytössä olevaan kyberturvallisuusstrategiaan, -menettelyihin ja -ohjeistuksiin?*
* *Asiakirjojen ja dokumenttien (ml. verkostotietojen) tietoturvallinen hallintatapa*
* *Henkilöstön osallistuminen, koulutus, tiedonjako ja riittävät taidot*
* *Ohjelman jatkuvuus ja kehittäminen. Onko ohjelmalla yrityksen johdon jatkuva tuki? Päivitetäänkö ohjelmaa tietojärjestelmien hankinnan, kehittämisen ja huollon yhteydessä?*
* *Toteutetaanko sisäisiä ja ulkoisia auditointeja ja testauksia? Tehdäänkö vuosittaisia ulkopuolisten tekemiä teknisiä tietoturvatarkastuksia organisaation eri järjestelmiin? Onko harkittu tietoturvatoimijan tekemää red / purple team -tyyppistä tietoturvan tason testausta?*

***HUOMIO! Pyydämme kaikkia yhtiöitä täyttämään alla olevan kyselyn.***

*Rasti alta standardit, kybermaturiteetin mittaustyökalut 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 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 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

## Kyberturvallisuusarkkitehtuuri

*Kuvaus yrityksen kyberturvallisuusarkkitehtuurista. Kyberturvallisuusarkkitehtuurin avulla kuvataan organisaation turvallisuusprosessien, kyberturvallisuusjärjestelmien ja henkilöstön rakenne sekä näiden suhde organisaation tavoitteeseen ja strategisiin suunnitelmiin. Kyberturvallisuusarkkitehtuuri luo edellytykset suunnitella ja kehittää organisaation kyberturvallisuutta kokonaisuutena pistemäisten ratkaisuiden, kuten yksittäisten identiteetin- tai pääsynhallintaratkaisujen, sijasta.*

*Kyberturvallisuusarkkitehtuurin avulla voidaan lähestyä kriittisten järjestelmien ja tiedon suojaamista tunnettujen arkkitehtuurimenetelmien kautta Tällaisiin menetelmiin kuuluvat mm. verkkojen segmentointi, ylläpitoratkaisut, salausmenetelmät ja jäljityslokit ja niitä voidaan käyttää yhdessä saatavuuteen liittyvien menetelmien kuten monitoroinnin, palautusmenetelmien tai varmennuksen kanssa. Kun kyberturvallisuusarkkitehtuuri suunnitellaan toimimaan yhdessä organisaation liiketoimintastrategian kanssa, toimii se syötteenä mm. riskianalyyseille ja suojattavien kohteiden konfiguroinnille.*

* *Arvioidaanko organisaation järjestelmien ja verkkojen vaatimuksia kyberarkkitehtuuriin säännöllisesti ja ennalta määriteltyjen tilanteiden, kuten järjestelmämuutosten yhteydessä? Onko jatkuvuudenhallintasuunnitelmien päivitys vastuutettu järjestelmä- ja verkkomuutosten yhteydessä? Onko suunnitelmien päivitys sidottu organisaation vuosikelloihin?*
* *Miten sopimuksien hallinnan jatkuvuus, sopimusten olemassaolon varmistaminen sekä sopimusten sisällön tunteminen on varmistettu?*
* *Miten alihankkijoiden hallinta sekä heidän turvallisuutensa varmistaminen on toteutettu?*
* *Segmentoidaanko verkkoja fyysisellä ja loogisella tasolla? Miten ulko- ja sisäverkkojen turvallisuusratkaisut on toteutettu? Testataanko verkkojen eriyttämisen toimivuutta säännöllisesti tai vähintään kaikkien verkkomuutosten jälkeen (esim. palomuurisääntöjen muutokset)? Miten verkkojen segmentoinnissa on huomioitu hyökkäyksien etenemisen estäminen organisaation eri toimintojen välillä?*
* *Onko laitteita, järjestelmiä ja verkkoja eriytetty toisistaan käyttötarkoituksien perusteella? Onko olemassa esimerkiksi vain laskujen maksamiseen tarkoitetut laitteet, joita ei saa tai voi käyttää mihinkään muuhun?*
* *Onko organisaation eri toimintojen väliset riippuvuudet tunnistettu? Hyödynnetäänkö riippuvuuksien tunnistamista mm. järjestelmien ja verkkojen segmentoinnissa?*
* *Onko laitteiden ja ohjelmistojen suojausmekanismit ja etähallintaratkaisut toteutettu ottaen huomioon niiden kriittisyys?*
* *Huomioidaanko ohjelmisto- ja sovellustoimittajien valinnassa noudattaako toimittaja turvallisen sovelluskehityksen periaatteita?*
* *Salataanko kannettavien laitteiden kovalevyjen tiedot hukkaamisen tai varastamisen varalta? Onko organisaation mahdollista lukita laitteet tai poistaa laitteilla olevat tiedot etähallintayhteyksien avulla?*
* *Onko organisaatiossa määritelty politiikat mobiililaitteiden turvalliselle käytölle ml. etähallinta ja sovellusten asentaminen?*
* *Onko kriittisimmät tiedostot ja konfiguraatiot varmistettu operatiivisen toiminnan tietoverkoista irti oleviin varmuuskopioihin, ns. kylmäsäilytysratkaisuihin (offline varmuuskopioihin)? Onko varmuuskopioinnin tarpeet kartoitettu ja mitoitettu riittävälle tasolle? Onko varmuuskopioinnit vastuut selvät teidän ja järjestelmätoimittajien kesken?*
* *Onko organisaation järjestelmien ja verkkojen osalta olemassa ajantasainen laitelistaus, jossa eritellään esimerkiksi laitetyypit, mallit, merkit, johdot sekä virtalähteet poikkeamasta palautumisen nopeuttamiseksi?*

## Identiteetin- ja pääsynhallinta

*Kuvaus identiteetin- ja pääsynhallinnasta. Identiteettien määrittely ja hallinta on yksinkertaisimmillaan käyttöoikeuksien perustamisesta ja tarpeettomien identiteettien poistamista. Identiteetti-tahot voivat olla organisaation sisäisiä tai ulkoisia yksilöitä, mutta myös laitteita, järjestelmiä tai prosesseja, jotka tarvitsevat oikeudet suojattuihin kohteisiin. Oikeuksien ylläpitäminen edellyttää jäljitettävyyttä, varmistaen kaikkien identiteettienvoimassaolon, sekä oikeuksien poistamista tarpeen päättymisen jälkeen.*

*Pääsynhallinta sisältää pääsyvaatimusten määrittelyn, oikeuksien myöntämisen vaatimusten perusteella sekä oikeuksien poistamisen, kun oikeuksia kohteeseen ei enää tarvita. Organisaation suojattaviin kohteisiin tapahtuvan pääsynhallinnan tulee ottaa huomioon riskit organisaation tavoitteille ja kriittiselle infrastruktuurille.*

* *Onko käyttäjätunnusten hallinta ja katselmointi säännöllistä?*
* *Onko lokitus määritelty liittyen identiteetin- ja pääsynhallintaan ja miten kauan lokien sisältöä säilytetään? Mitä käyttäjien toimia lokitetaan pääsynhallintaan sisältyvien toimien lisäksi?*
* *Onko valvontamenetelmiin oleellisesti kuuluvien havaintojen tallennusjärjestelmien kuten lokituksen suojaus toteutettu niin että niiden sisältämän tiedon luvaton muuttaminen tai tuhoaminen estetään?*
* *käytetäänkö valvontamenetelmiä asianmukaisesti, siten että tietoturvapoikkeamat ja mahdolliset haavoittuvuudet havaitaan ja selvitetään riskien vähentämiseksi?*
* *Onko pääkäyttöoikeuksien käyttöä rajoitettu normaaleilta käyttäjiltä? Kuinka pääkäyttäjien toimia valvotaan ja millä tasolla? Kuinka kauan valvontaan liittyviä lokeja säilytetään ja miten nämä varmistetaan?*
* *Onko käytössä yhteyskäyttöisiä tunnuksia? Kuinka näitä hallinnoidaan ja onko näistä luopuminen suunniteltu?*
* *Onko käyttövaltuuksienhallintajärjestelmä kahdennettu? Onko suunniteltu, kuinka järjestelmä voidaan ohittaa hätätilanteessa esimerkiksi pääkäyttäjien tunnusten aktivoimiseksi?*

## Kriittisten tieto- ja tietoliikennejärjestelmien jatkuvuuden hallinta

*Kuvaus miten toiminnan jatkuvuus on tietojärjestelmien ja tietoliikennejärjestelmien osalta varmistettu. Jatkuvuuden hallinta sisältää toiminnan uhkien tunnistamisen ja niiden vaikutukset, sekä toimintatavan häiriötilanteiden hallinnalle ja toimintojen jatkuvuudelle kaikissa olosuhteissa.*

*Kriittisyysluokittelussa priorisoidaan järjestelmien ja toimintojen palauttamisjärjestys katastrofitilanteessa. Verkkoliikenne ja viestintäyhteydet, sekä esimerkiksi käyttövaltuudet ovat tärkeässä osassa palautumistoimien käynnistämisessä ja eteenpäin viemisessä. Priorisoinnin tukena voi käyttää tunti tunnilta ajattelua tukena eli mitä ilman organisaatio ei pärjää tuntiakaan, ja mikä puolestaan ei esimerkiksi estä korjaustoimien käynnistämistä päivän tai kahden kuluttua ja mitkä asiat ovat sellaisia, että mainehaittaa lukuun ottamatta asiaan voidaan palata vaikkapa viikon päästä. Priorisointijärjestys voi vaihdella liiketoiminto/ palvelu kohtaisesti organisaation sisällä, minkä vuoksi näiden tarpeiden kommunikointi organisaation IT- ja OT-henkilöstölle etukäteen on tärkeää.*

*Organisaation olisi hyvä määritellä palautumisen priorisoinnin yhteydessä myös mahdolliset siihen kohdistuvat lainsäädännölliset toimintavaatimukset, kuten mahdolliset 24/7/365 kaikissa tilanteissa toimintavarmuutta edellyttävät toiminnot.*

*Onko esim.*

* *Tunnistettu keskeiset tieto- ja tietoliikennejärjestelmät ja luetteloitu ne toimintakriittisyyden perusteella*
* *Laadittu tieto- ja tietoliikennejärjestelmien jatkuvuussuunnitelmat*
* *Varmistettu, että järjestelmien yllä- ja kunnossapito ovat saatavilla myös häiriö- ja poikkeustilanteissa*
* *Tietojärjestelmien ja tietoliikennejärjestelmien varmuuskopiointi hoidettu säännöllisesti*
* *Tietojärjestelmien ja tietoliikennejärjestelmien varmuuskopiointi hoidettu säännöllisesti ja varmuuskopioiden palautusta harjoiteltu vuosittain. Raportoidaanko palautumisen tuloksista kuten onnistumisesta johdolle?*

## Vakavan tietoturvahaavoittuvuuden tai -häiriön tunnistaminen ja siitä toipuminen

*Kuvaus miten vakavat tietoturvahaavoittuvuudet, -häiriöt ja tietoverkkohyökkäykset pyritään tunnistamaan ja minkälaiset toimintaohjeet henkilöstölle on, jos tällainen tietoturvapoikkeama havaitaan. Kuvaus myös miten toteutuneista tietoturvahäiriöistä ja -hyökkäyksistä palaudutaan.*

* *Miten viranomaisilmoitukset (esim. NIS) on vastuutettu ja minkälainen prosessi ilmoituksille on?*
* *Miten tieto- ja tietoliikennejärjestelmien teknisistä haavoittuvuuksista kerätään ja ylläpidetään riittävää osaamista ja tietoa?*
* *Miten lokitus on hoidettu? Mitä loki sisältää ja kuinka kauan lokeja säilytetään?*
* *Miten tietoturvatapahtumia havainnoidaan automaattisesti? Miten ja millaisilla työkaluilla epäilyt tietoturvapoikkeamat nostetaan näkyviin? Millainen kyvykkyys organisaatiollanne sekä palveluntarjoajillanne (esim. tuki- ja ylläpitopalvelut, laitoshuolto, aula- ja turvallisuuspalvelut, ruokahuolto tai tietoliikennetoimittajat) tai yhteistyökumppaneillanne on reagoida teknisesti tietoturvapoikkeamiin 24/7?*
* *Miten nostettuihin tietoturvapoikkeamiin reagoidaan automatisoidusti? Millaiset toimintasuunnitelmat ovat? Miten tapahtumasta palaudutaan?*
* *Miten tietoturvan eri roolit on vastuutettu organisaationne henkilökunnallenne (esim. johto, palvelupäälliköt sekä aulavahdit) sekä yhteistyökumppaneille ja alihankkijoille?*
* *Oletteko harjoitelleet tietoturvahäiriönhallintaprosessejanne itsenäisesti ja yhteistyökumppaneiden kanssa? Kuinka kohdistatte harjoitustoimintaa ja selvitätte koulutuksen ja harjoitusten tarpeita organisaatiossanne vuosittain? Oletteko käynnistäneet organisaatiossanne harjoitusohjelman eri toiminnallisuuksien jatkuvan kouluttamisen edistämiseksi?*
* *Onko vähintään yhden (tietoturvasta) vastuullisen tarvittaessa saatavilla olevan henkilön tai roolin, sekä tietoturvavalvomon (SOC) tiedot välitetty viranomaisille tietoturvapoikkeamien ilmoittamista varten?*

## Kriittisten tieto- ja tietoliikennejärjestelmien sähkönsyötöt

*Kuvaus toiminnan jatkuvuuden hallinnan kannalta kriittisten järjestelmien sähkönsyötön varmistamisesta kohteen kriittisyyden mukaisesti.*

* *Miten laitetilojen sähkösyöttö- ja tietoliikekaapelointi on suojattu ulkoisia uhkia vastaan ja miten kaapelit ovat tärkeiden laitetilojen osalta varmennettu?*
* *Varmistetaanko normaaliolojen häiriötilanteiden varalta ohjaukseen käytettävien tietojärjestelmien, tietoliikenteen ja valvomotilojen sähkönsyöttö varavoimakonein tai katkeamattomin sähkönsyöttölaittein (UPS)?*
* *Miten varavoimakoneiden, akustojen ja sähkösyöttölaitteiden kunnonhallinta ja testaus on järjestetty.*
* *Onko vastuuhenkilöt määritelty mm. varavoimakoneiden, akustoihin ja sähkönsyöttöön liittyen?*

## Kriittisten tieto- ja tietoliikennejärjestelmien suojaamisasiat ja muu tilaturvallisuus

*Kuvaus tietojärjestelmien, valvomotilojen ja sähköasemien suojaamisesta fyysisiä ilmiöitä tai tapahtumia vastaan.*

* *Miten esim. tärkeät laite- ja valvomotilat on suojattu sähköisiä häiriöitä vastaan?*
* *Miten sähköasemilla käytettävät laitteet ovat rakenteellisesti suojattu kestämään tiloissa esiintyviä korkeita ylijännitteitä ja sähkömagneettisia häiriöitä?*
* *Onko käytössä luotettavat ja korkeatasoiset ja olosuhteiden valvontajärjestelmät?*
* *Miten tilaturvallisuudesta ja kulunvalvonnasta on huolehdittu? Onko esim. määritelty fyysiset turva-alueet ja luokiteltu ne tärkeyden mukaan eri kulkuoikeus- ja suojausluokkiin? Onko turva-alueet suojattu sähköisillä, tapahtumat tallentavilla kulunvalvonta- ja murtohälytysjärjestelmillä sekä videovalvonnalla? Kauanko ja missä edellä mainittujen lokeja ja tallenteita säilytetään?*
* *Onko valvontajärjestelmien verkot eriytetty muista verkoista? Miten ja mistä esim. kameravalvontaan pääsee käsiksi?*
* *Miten verkonhaltija tekee yhteistyötä eri viranomaisten kanssa kriittisten kohteiden suojaamiseksi vahingontekoja ja sotilaallista toimintaa vastaan?*
* *Onko määritelty vastuuhenkilöt ja miten vastuita tai vastuuhenkilöitä päivitetään?*
* *Onko kulunvalvontajärjestelmä tietoturvatestattu?*
* *Kuinka ulkopuolisten (esim. tavarantoimittajien, huoltopalveluiden ja laitetoimittajien) kulkeminen eri tiloissa on toteutettu ja ohjeistettu? Onko tavarantoimittajien, huoltopalveluiden tai laitetoimittajien henkilöt turvallisuusselvitetty?*
* *Kuinka vierailijoiden ja oman henkilöstön kulunvalvontakorttien voimassaoloaikaa rajoitetaan? Onko vierailuille määritelty prosessi? Kuinka vierailijoiden liikkumista tiloissa on ohjeistettu ja rajoitettu?*

## Kriittisten tieto- ja tietoliikennejärjestelmien varajärjestelmät

*Kuvaus varajärjestelmistä ja toimista varajärjestelmiin siirtymiseksi. Mistä järjestelmistä on olemassa varajärjestelmät.*

* *Onko esimerkiksi toimintakriittisten järjestelmien laitetilat varmennettu (esim. kahdennettu) ja maantieteellisesti riittävän etäällä toisistaan?*
* *Onko käyttökeskuksella varavalvomo, joka sijaitsee eri rakennuksessa kuin varsinainen valvomo?*
* *Mikäli varavalvomo sijaitsee kävelymatkan ulkopuolella, miten henkilöstön kuljetus valvomoiden välillä on järjestetty tai suunniteltu järjestettäväksi?*
* *Onko väistöpaikkoja olemassa tilanteita varten, joissa valvomot ja muut normaalit työskentelytilat eivät ole käytössä?*
* *Onko tietoliikenne- ja tietojärjestelmien varajärjestelmien dokumentointi ajan tasalla? Onko dokumenteista olemassa ajantasaiset fyysiset kopiot? Onko näiden kopioiden sijainti tiedossa?*
* *Onko vastuuhenkilöt määritetty ja onko heillä riittävät tiedot, taidot, vastuut ja valtuudet? Onko yksi tai useampi riittävät päätöksenteko-oikeudet omaava vastuuhenkilö aina tavoitettavissa?*
* *Miten vastuuhenkilö tekee päätöksen varajärjestelmään siirtymisestä?*
* *Onko varaviestintätavat, työkalut ja -kanavat suunniteltu ja testattu häiriötilanteita, joissa perustietotekniikka tai tietoverkot eivät ole käytettävissä, varten?*
* *Onko mietitty, miten järjestelmiä operoidaan, mikäli niihin ei saa yhteyttä etänä tai mikäli normaalit valvomotilat eivät ole käytettävissä?*
* *Onko varauduttu tilanteeseen, jossa normaaleja viestintävälineitä ei voi käyttää mahdollisen haitallisen toimijan ollessa järjestelmien sisässä?*
* *Onko varauduttu erilaisiin skenaarioihin, joissa järjestelmiä ei voida palauttaa toimintakuntoon esimerkiksi varmuuskopioista?*

PALVELUTUOTTAJIEN TOIMINTAKYVYN VARMISTAMINEN

*Kuvaus miten verkonhaltija on varmistanut jatkuvuuden hallintaan osallistuvien kumppaneiden toimintakyvyn ja henkilöstön riittävyyden häiriötilanteissa. Erityisesti häiriönhallintaan osallistuvat palveluntuottajat ovat keskeisiä, mutta myös muiden palveluntuottajien toimintakyky on varmistettava ja huomioitava varautumissuunnitelmassa.*

*Huom. Mallipohjassa otsikointi on muotoiltu koskettamaan yleisesti kaikkia palveluntuottajia, mutta SÄHKÖKOTKA-työkalussa on palveluntuottajat eriteltynä toimialoittain:*

* *Sähkönjakeluverkon palveluntuottajat*
* *Sähköasemien ja suurjänniteverkon palveluntuottajat*
* *Tieto- ja tietoliikennejärjestelmien palveluntuottajat*

## Palvelutuottajariskien hallinta ja vaikutusten minimointi

*Kuvaus miten palveluntuottajiin liittyviä riskejä ja niiden vaikutuksia verkonhaltijan toimintaan kartoitettu.*

*Onko verkonhaltija varmistanut esim. palveluntuottajan:*

* *kriisijohtamisen toimintatavat*
* *kriittisiä tehtäviä hoitavien henkilöiden riittävän koulutuksen varautumisasioihin*
* *tietoturvakäytännöt*
* *tarvike-, materiaali- ja polttoainehankinnat*
* *sopimukset korvaavien palveluntuottajien kanssa*

*Onko määritelty verkonhaltijan osalta vastuuhenkilöt, jotka varmistavat, että palveluntuottajien toimintakyky on asianmukaisesti huomioitu sopimuksissa ja palveluntuottajan käytännön toiminnassa.*

## Palveluntuottajien kriittisyystasojen määrittäminen

*Onko palveluntuottajille määritelty eri kriittisyystasoja ja miten erityisesti kriittisimpien palveluntuottajien toimintakyky ja korvattavuus varmistetaan?*

## Palvelutuottajien resurssien ja ohjausjärjestelmien korvattavuus

*Kuvaus miten palveluntuottajien resurssit ja ohjausjärjestelmät ovat korvattavissa esim. toisella palveluja tuottavalla yrityksellä?*

## Palvelutuottajien toimintamalli ja yhteistyö verkonhaltijan kanssa vakavissa häiriötilanteissa

*Miten verkonhaltija on varmistanut, että palveluntuottajan toimintamallit ovat yhteensopivia verkonhaltijan toiminnan kanssa ja, että yhteistyö verkonhaltijan kanssa toimii sujuvasti vakavissa häiriötilanteissa?*

ALUEELLINEN YHTEISTYÖ

## Kriittiset sähkönkäyttöpaikat

*Kuvaus miten Valtioneuvoston asetuksen (TEM/2022/211) 2 § mukaiset kriittiset sähkönkäyttöpaikat on määritelty häiriö-, sähköpula- ja kriisitilanteita varten ja huomioitu verkonhaltijan varautumisessa. Mitä kriittisiä sähkönkäyttöpaikkoja verkonhaltija on vastuualueeltaan tunnistanut? Onko määrittely tehty yhteistyössä asiakkaiden kanssa?*

*Miten kriittiset sähkönkäyttöpaikat on huomioitu verkonhaltijan asiakastieto- ja käytöntukijärjestelmissä?*

*Huom. VNA 2 §:n mukaisesti kriittisten sähkönkäyttöpaikkojen sähkönsaanti on ensisijaisesti pyrittävä turvaamaan yhteiskunnan johtamisen ja turvallisuuden kannalta välttämättömien toimintojen ylläpitämiseksi. Kriittisiä sähkönkäyttöpaikkoja ei ole tarkoitus luokitella kohdan 11.2 mukaisessa käyttöpaikkojen etusijaryhmittelyssä vaan ne muodostavat oman ryhmänsä.*

## Muiden sähkönkäyttöpaikkojen etusijajärjestys

*Kuvaus miten muiden kuin Valtioneuvoston asetuksen (TEM/2022/211) 2 § mukaisten kriittisten sähkönkäyttöpaikkojen etusijajärjestys on määritelty häiriö-, sähköpula- ja kriisitilanteita varten ja miten se on huomioitu verkonhaltijan varautumisessa. Onko määrittely tehty yhteistyössä asiakkaiden kanssa? Huom. etusijajärjestyksen määrittely koskee kaikkia verkonhaltijan käyttöpaikkoja*

*Miten käyttöpaikkojen etusijajärjestys on huomioitu verkonhaltijan asiakastieto- ja käytöntukijärjestelmissä?*

*Verkonhaltijoiden on suunnitelmassaan kuvattava vähintään:*

* *moneenko ryhmään sähkönkäyttöpaikat ryhmitellään;*
* *minkä tyyppiset sähkönkäyttöpaikat kuhunkin ryhmään kuuluvat;*
* kuinka monta sähkönkäyttöpaikkaa ryhmään kuuluu; *ja*
* *mikä on kunkin ryhmän tärkeysluokka (ts. kuinka pitkäksi aikaa sähkönsaanti voi keskeytyä).*

*Etusijajärjestyksen asettamisessa on huomioitava yhteiskunnan johtamisen ja turvallisuuden, väestön toimeentulon sekä elinkeinoelämän toimintakyvyn kannalta tärkeät sähkönkäyttöpaikat.*

*Muut sähkönkäyttöpaikat kuin 2 §:n mukaiset kriittiset 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.*

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

## Yhteistyö ja tilannekuva pelastusviranomaisten kanssa

*Kuvaus miten yhteistoiminta pelastusviranomaisten kanssa on järjestetty häiriö- ja vikatilanteissa.*

*Kuvaus, miten tilannekuva välittyy pelastusviranomaisen kanssa.*

## Yhteistyö muiden viranomaisten kanssa

*Kuvaus miten yhteistyö ja viestintä muiden viranomaisten (esim. poliisi) kanssa on järjestetty.*

*Kuinka yhtiö on organisoinut ja huolehtinut poikkeavien tapahtumien ja ilmoitusten raportointikäytännöt viranomaisille (Energiavirastolle tehtävät NIS-ilmoitukset, Supo, KTK, KRP jne.)?*

## Yhteistyö muiden jakeluverkkoyhtiöiden kanssa

*Kuvaus miten muiden kanssa tehdään yhteistyötä häiriötilanteissa sekä niihin varautumisessa. Sovitaanko yhtiöiden välillä esim. viankorjausresurssien jakamisesta ja varasyöttöyhteyksien järjestämisestä?*

## Yhteistyö kantaverkkoyhtiön kanssa

*Kuvataan yhteistyö kantaverkkoyhtiön kanssa vakavissa häiriötilanteissa: kantaverkon suurhäiriö, sähköpula ja säännöstelysuunnitelmat sekä jakeluverkonhaltijan rooli yhteistyössä kantaverkkoyhtiön kanssa.*

## Yhteistyö kaukolämpöyhtiöiden kanssa

*Kuvaus miten yhteydenpito kaukolämpö- ja energiayhtiöiden kanssa on järjestetty.*

## Yhteistyö vesiyhtiöiden kanssa

*Kuvaus miten vesiyhtiöiden kanssa tehdään yhteistyötä häiriötilanteissa sekä niihin varautumisessa.*

## Yhteistyö teleyhtiöiden kanssa

*Kuvaus miten teleyhtiöiden kanssa tehdään yhteistyötä häiriötilanteissa sekä niihin varautumisessa. Onko verkonhaltijan tiedossa teleyhtiöiden kriittisimmät tukiasemat ja miten häiriötilanteessa sovitaan tukiasemien sähköjen palauttamisen prioriteettijärjestys?*

## Yhteistyö kuntien kanssa

*Kuvaus miten kuntien kanssa tehdään yhteistyötä häiriötilanteissa sekä niihin varautumisessa.*

## Yhteistyö muiden tahojen kanssa (esim. puolustusvoimat, teiden kunnossapitäjät)

*Kuvaus miten muiden keskeisten tahojen kanssa tehdään yhteistyötä häiriötilanteissa sekä niihin varautumisessa. Miten esim. viankorjausalueiden teiden kunnossapidon priorisoinnista sovitaan, mikäli lumipeite tai puusto estää korjausryhmän pääsemisen alueelle?*