**Maakaasuverkonhaltijan**

**varautumissuunnitelman mallipohja**

Sisällysluettelo

[1 TAUSTAA 3](#_Toc160105630)

[2 MAAKAASUNJAKELUYHTIÖN TOIMINNAN LÄHTÖKOHDAT 4](#_Toc160105631)

[3 YHTIÖN VARAUTUMISSUUNNITTELUN PERUSTIEDOT JA VARAUTUMISEN KEHITTÄMINEN 5](#_Toc160105632)

[4 HÄIRIÖTILANTEIDEN HALLINNAN VASTUUT JA JÄRJESTELYT 6](#_Toc160105633)

[5 KRIITTISIIN HÄIRIÖTILANTEISIIN VARAUTUMINEN 8](#_Toc160105634)

[6 TOIMINTA HÄIRIÖTILANTEISSA 9](#_Toc160105635)

[7 VIESTINTÄVERKKOJEN JA TIETOJÄRJESTELMIEN RISKIEN HALLINTA 11](#_Toc160105636)

[8 TEKNISTEN RESURSSIEN JA JÄRJESTELMIEN KÄYTETTÄVYYDEN VARMISTAMINEN 20](#_Toc160105637)

[9 PALVELUNTUOTTAJIEN TOIMINTAKYVYN VARMISTAMINEN 24](#_Toc160105638)

[10 ALUEELLINEN YHTEISTYÖ VAKAVISSA HÄIRIÖTILANTEISSA 25](#_Toc160105640)

# 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 myös kootusti erillisessä dokumentissa, johon 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.*

*Varautumissuunnittelun kehittämisen tueksi löytyy ohjeistusta 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*
* *Fyysisen suojauksen ohje (2022)*
	+ *Ohjeistusta siitä, miten fyysinen turvallisuus tulisi tarkoituksenmukaisesti ja riittävissä määrin huomioida osana energia-alan kohteiden suojaamista. Ohje tarjoaa energia-alan toimijoille keskeisiä tietoja ja valmiuksia liittyen fyysisen turvallisuuden suunnitteluperiaatteisiin sekä eri suojautumisen keinoihin, kuten turvajärjestelmiin, rakenteelliseen suojaukseen sekä hallinnollisiin prosesseihin.*
* *KYBER‐ENE Energia‐alan kyberturvaaminen 1‐2*
	+ *Käytännönläheisiä menetelmiä ja toimia kyberturvallisuuden toteuttamiseen ja kehittämiseen, sisältäen tarkastuslistoja muun muassa IoT-ratkaisuihin.*

*HVO-extranetin lisäksi ohjeistusta varautumiseen sekä jatkuvuudenhallintaan löytyy myös esim. kyberturvallisuuskeskuksen verkkosivuilta:* [*https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-organisaatioille-ja-yrityksille*](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/)

# MAAKAASUNJAKELUYHTIÖN TOIMINNAN LÄHTÖKOHDAT

## Maakaasunjakeluyhtiö lyhyesti

Lyhyt kuvaus.

## Maakaasunjakeluyhtiön strategia

Lyhyt kuvaus.

## Häiriöihin varautuminen maakaasunjakeluyhtiössä

Lyhyt kuvaus.

## Merkittävimmät häiriötilanteet, jotka on toiminnassa tunnistettu

Kirjataan merkittävimmät häiriötilanteet suunnitelman lähtökohdaksi. Hyödynnetään mahdollisen riskikartoituksen tuloksia.

## Maakaasunjakeluyhtiön johtamisjärjestelmä, riskienhallinta ja laadunvarmistus

Lyhyt kuvaus ja viittaus dokumentteihin sekä järjestelmiin.

# YHTIÖN VARAUTUMISSUUNNITTELUN PERUSTIEDOT JA VARAUTUMISEN KEHITTÄMINEN

## 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.*

## Yhtiön toiminnan riskien analysointi

*Kuvaus ketkä osallistuvat riskiarvion tekoon, kuka vastaa riskiarviosta ja miten usein riskiarviota päivitetään.*

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

*Millaisia riskejä verkonhaltija on tunnistanut ja mihin keskeisiin riskeihin tällä suunnitelmalla erityisesti pyritään vaikuttamaan? Onko keskeisille riskeille määritelty hallintatoimet, vastuuhenkilöt ja aikataulut hallintatoimien toteuttamisesta?*

*Tarkempi riskirekisteri voi olla esim. erillisenä liitteenä.*

## Varautumissuunnitelman päivittäminen ja kehittäminen

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

*Mitä kehityskohteita varautumisessa on tunnistettu? Millä aikataululla varautumista parannetaan ja onko kehityskohteille määritelty vastuuhenkilöt?*

## 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? 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:*

* *Mihin harjoituksiin on osallistuttu viime vuosina?*
* *Mihin harjoituksiin aiotaan osallistua tulevaisuudessa?*
1. HÄIRIÖTILANTEIDEN HALLINNAN VASTUUT JA JÄRJESTELYT

*Tässä luvussa on tarkoitus tuoda esille varautumiseen tähtäävät hallinnolliset keinot, kuten organisaatiojärjestelyt, vastuiden määrittelyt sekä henkilöstön ohjeistukset ja koulutukset.*

## 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?*

## Toimenkuvissa olevat häiriöiden hallintatehtävät

*Voidaan ylläpitää myös erillisenä liitteenä.*

## Henkilöstön ja palveluntuottajien perehdytys toimimaan häiriötilanteissa

*Kuvaus miten henkilöstö ohjeistetaan ja koulutetaan häiriötilanteiden varalle.*

*Maakaasunjakeluyhtiön päivystäjä on avainasemassa toimintojen käynnistämisessä. Hänelle täytyy luoda selkeät toimintamallit eri tilanteisiin. Otsikoitu ajantasainen yhteystietolista nopeuttaa yhteydenottoa oikeisiin henkilöihin.*

## Työaika-, ruokailu ja lepojärjestelyiden järjestäminen

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

1. KRIITTISIIN HÄIRIÖTILANTEISIIN VARAUTUMINEN

*Kuvaus, millaisiin häiriötilanteisiin yhtiössä varaudutaan ja miten yhtiön varautuminen riippuu häiriötilanteesta? Millaiset toimintaohjeet erilaisiin häiriötilanteisiin on?*

## Siirtoverkon teknisiin vikoihin ja vaurioihin varautuminen

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

## Maakaasutuotannon teknisiin vikoihin ja vaurioihin varautuminen

Kuvaus, millaisiin teknisiin vikoihin varaudutaan ja miten niistä selvitään.

## ****Maakaasuasiakkaiden teknisiin vikoihin ja vaurioihin varautuminen****

Kuvaus, millaisiin teknisiin vikoihin varaudutaan ja miten niistä selvitään.

## 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, maakaasunjakeluyhtiön varautumisen keskeiset osa-alueet ovat:*

* *oman ja palvelutoimittajan henkilöstön suojaaminen ja turvallisuus*
* *yrityksen omaisuuden suojaaminen*
* *maakaasujärjestelmän toiminnan jatkuvuuden varmistaminen*

*Henkilöstön turvallisuuden varmistamiseksi maakaasunjakeluyhtiö laatii ja ylläpitää toimipaikan pelastussuunnitelmia sekä harjoittelee suunnitelmien mukaista toimintaa säännöllisesti.*

## Maakaasun saatavuuteen sekä markkinahäiriöihin varautuminen (mm. polttoaine, maakaasumarkkinat)

*Kuvaus, miten toiminnassa on varauduttu maakaasun saatavuuden häiriöihin ja markkinahäiriöihin.*

## Avainhenkilömenetykseen varautuminen

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

## Muihin häiriötilanteisiin varautuminen

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

1. TOIMINTA HÄIRIÖTILANTEISSA

## Viestintä- ja kriisiviestintäsuunnitelmat

*Kuvaus, miten esim. asiakkaille, yhteistyötahoille, viranomaisille ja medialle viestitään häiriötilanteissa.*

*Tarkempaa kriisiviestisuunnitelmaa on hyvä ylläpitää erillisessä liitteessä.*

*Onko määritelty vastuuhenkilöt?*

## 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.*

## Häiriö- ja vikatilateiden seuranta ja seurantajärjestelmä

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

## Johtamiskeskuksen/tilannekuvakeskuksen perustaminen käyttöönotto

*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. verkon käyttötoiminnan tietojärjestelmistä, kenttätoimijoilta, palveluntuottajilta sekä muilta yhteistyöorganisaatioilta.*

## Asiakkaiden ennalta tiedottaminen häiriötilanteista ja poikkeusoloista

*Kuvataan, miten asiakkaille tiedotetaan häiriötilanteista ja poikkeusoloista (ennalta) ja kuka on vastuussa.*

## Asiakkaiden tiedottaminen pitkäkestoisissa häiriötilanteissa

*Kuvattava, millä välineillä ja miten asiakkaille tiedotetaan pitkäkestoisissa häiriötilanteissa. Miten varmistetaan, että asiakkaat saavat mahdollisimman oikean arvion tilanteesta ja häiriötilanteen kestosta?*

## Asiakaspalvelun toimintamalli häiriötilanteissa

*Kuvataan asiakaspalvelun toimintamalli häiriötilanteissa.*

*Kuvattava myös, miten asiakaspalvelun osalta varaudutaan kasvavaan tiedontarpeeseen.*

## Häiriötilanteiden jälkeiset palautetilaisuudet ja -kyselyt

*Kuvaus, miten organisaatiossa järjestetään häiriötilanteen jälkeinen raportointi sekä palautetilaisuudet ja -kyselyt. Kuka vastaa tilanteen jälkeisistä palautetilaisuuksista?*

VIESTINTÄVERKKOJEN JA TIETOJÄRJESTELMIEN RISKIEN HALLINTA

***Tämä luku koskee lain mukaan ainoastaan siirtoverkonhaltijaa, eikä jakeluverkonhaltijoilla ole velvoitetta toimittaa tämän luvun tietoja.***

*Energiavirasto kuitenkin kannustaa myös jakeluverkonhaltijoita varautumaan ja huolehtimaan viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta. Jakeluverkonhaltijat voivat vapaaehtoisesti sisällyttää luvun tiedot Energiavirastolle toimitettavaan suunnitelmaan tai käsitellä kohdat sisäisesti, mutta poistaa ne Energiavirastolle toimitettavasta suunnitelmasta.*

*Maakaasumarkkinalain 34 a §:n mukaisesti* ***siirtoverkonhaltijan*** *on huolehdittava käyttämiinsä viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien hallinnasta. Tästäkin syystä tietoturvapolitiikka ja tietoturvariskeihin varautuminen ovat osa varautumissuunnittelua ja siksi ne on otettu suunnitelmaan omaksi kokonaisuudekseen.* *Riskienhallinnassa on otettava huomioon: 1) järjestelmien ja tilojen turvallisuus; 2) tietoturvauhkien ja häiriöiden käsittely; 3) liiketoiminnan jatkuvuuden hallinta; 4) riskien seuranta sekä järjestelmien tarkastukset ja testaukset; 5) mahdollisten kansainvälisten standardien noudattaminen.*

*Suosittelemme kyberuhkien huomioimista osana organisaation kokonaisriskienhallintaa ja kuvailemaan ne tarkemmin kappaleessa 3.2.*

*Verkonhaltijan 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 verkonhaltijan 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.*
* *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 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 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 ja https://csrc.nist.rip/publications/PubsSPs.html ja NIST Interagency/Internal Report https://csrc.nist.gov/publications/nistir ja https://www.nist.gov/nist-pub-series/nist-interagencyinternal-report-nistir*

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

*[] NIST CSF, Cyber Security Framework 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*

*[] CIS Critical Security Controls (CSC), 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?*

## Tietojärjestelmien 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/palvelukohtaisesti 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 on 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 tieto- ja tietoliikennejärjestelmien teknisistä haavoittuvuuksista hankintaan 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?*
1. *Onko vähintään yhden (tietoturvasta) vastuullisen tarvittaessa saatavilla olevan henkilön tai roolin, sekä tietoturvavalvomon (SOC) tiedot välitetty viranomaisille tietoturvapoikkeamien ilmoittamista varten?* TEKNISTEN RESURSSIEN JA JÄRJESTELMIEN KÄYTETTÄVYYDEN VARMISTAMINEN

## Verkostomateriaalin varaaminen

*Kuvaus maakaasuverkon 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 muiden jakeluverkonhaltijoiden kanssa?*

*Onko määritelty vastuuhenkilöt?*

*Esim. seuraavat materiaalit ja välineet ovat olennaisia:*

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

*Varavoimakoneet*

## Kriittisten järjestelmien 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 toiminnan ohjaukseen käytettävien tietojärjestelmien, tietoliikenteen ja valvomotilojen sähkönsyötön varmistamisesta varavoimakonein sekä katkeamattomin sähkönsyöttölaittein (UPS)?*
* *Miten varavoimakoneiden, akustojen ja sähkösyöttölaitteiden kunnonhallinta ja testaus on järjestetty?*
* *Miten varavoimakoneiden polttoainejakelu on varmistettu?*
* *Onko vastuuhenkilöt määritelty mm. varavoimakoneiden, akustoihin ja sähkönsyöttöön liittyen?*

## Kriittisten järjestelmien suojaamisasiat ja muu tilaturvallisuus

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

* *Miten esim. tärkeät laite- ja valvomotilat on suojattu sähköisiä häiriöitä vastaan?*
* *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 järjestelmien 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 määritelty 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?*
* *Miten toimitilamenetykseen varaudutaan?*

## Polttoainejakelun varmistaminen

*Kuvaus polttoainejakelun varmentamisesta.*

*Verkonhaltijan on selvitettävä omalla alueella tai lähiseudulla olevat huoltoasemat, joiden sähkönsaanti on varmistettu. Näiden kanssa tulee tehdä ennakkoon sopimus maakaasunjakeluyhtiön ajoneuvojen tankkausjärjestelyistä.*

*Onko määritelty vastuuhenkilöt?*

1. PALVELUNTUOTTAJIEN 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.*

## Palveluntuottajien kriittisyystasojen määrittäminen

*Listaa palveluntuottajat kriittisyystasoittain.*

## Palvelutuottajariskien hallinta ja vaikutusten minimointi

*Miten palveluntuottajiin liittyviä riskejä ja niiden vaikutuksia verkonhaltijan toimintaan kartoitettu.*

*Kuvattava miten erityisesti kohdassa 8.1. tunnistettujen kriittisimpien palveluntuottajien toimintakyky ja korvattavuus varmistetaan.*

*Onko verkonhaltija varmistanut esim. palveluntuottajan:*

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

*Hankitaanko keskeisiä palveluita useammalta kuin yhdeltä palveluntuottajalta tai onko korvaavien palveluntuottajien kanssa sovittu etukäteen?*

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

## Palveluntuottajien resurssien ja ohjausjärjestelmien korvattavuus

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

## Maakaasuverkon palveluntuottajien toimintamalli vakavissa häiriötilanteissa

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

1. ALUEELLINEN YHTEISTYÖ VAKAVISSA HÄIRIÖTILANTEISSA

## Asiakkaiden kriittiset käyttöpaikat

*Kuvaus miten kriittiset maakaasun käyttöpaikat on määritelty ja huomioitu varautumisessa ja vakavissa häiriötilanteissa. Onko määrittely tehty yhteistyössä asiakkaiden kanssa?*

## Yhteistyö ja tilannekuva pelastusviranomaisten kanssa

*Kuvaus, miten yhteistoiminta kunnan valmiusjohtoryhmän ja pelastusviranomaisten sekä poliisin kanssa on järjestetty häiriö- ja vikatilanteissa.*

*Kuvaus, miten tilannekuva välittyy pelastusviranomaisen kanssa.*

## Viranomaislinja (puheyhteys) eri viranomaisten kanssa

*Kuvaus, miten viestintä viranomaisten kanssa on järjestetty. Onko esim. VIRVE-verkon puheryhmiä on käytössä?*

## Yhteistyö siirtoverkkoyhtiön kanssa

*Kuvataan yhteistyö siirtoverkkoyhtiön kanssa vakavissa häiriötilanteissa.*

## Yhteistyö ja yhteydenpito muihin keskeisiin osapuoliin

*Kuvataan yhteistyö ja yhteydenpito muiden keskeisten osapuolten kanssa.*

*Muita keskeisiä osapuolia voivat olla esim.*

* *muut jakeluverkonhaltija*
* *kaukolämpöyhtiöt*
* *teleyhtiöt*
* *kunnat*
* *teiden kunnossapitäjät*