Kymsote

Kymenlaakson
sosiaali- ja terveyspalvelut

# Tietoturvapolitiikka

## Kymsotessa sovellettava tietoturvapolitiikka

# Sisällysluettelo



## Selitteet

| Termi | Selite |
|---|---|
| Riski | epävarmuuden vaikutus tavoitteisiin.<br><br>Riski ilmaistaan tavallisesti riskin todennäköisyyden ja riskin tulona. Riski on tässä yhteydessä kielteinen, ei-toivottu tapahtuma tai seuraus. |
| Suojattava kohde | organisaation toiminnan kannalta merkityksellinen kohde, joka halutaan suojata riskien varalta.<br><br>Suojattava kohde voi olla esimerkiksi tieto, tietojärjestelmä, prosessi, fyysinen tila, yksittäinen asiakirja tai työasema. |
| Tietoturva | järjestelyt, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus. |
| Tietoturvahäiriö | yksi tai useampi toisiinsa liittyvä odottamaton tai ei-toivottu tietoturvatapahtuma, joka vaarantaa tietojen ja palvelujen tietoturvan ja vaikuttaa organisaation toimintaan epäsuotuisasti. |
| Tietoturvaprosessi | tietoturvallisuuden hallintaan sisältyvät prosessit, joita on eritelty politiikan luvussa ”Tietoturvallisuuden hallinta.” |
| Tietoturvauhka | mahdollisesti toteutuva haitallinen tapahtuma tai kehityskulku, joka kohdistuu tietoturvaan ja toteutuessaan vaarantaa sen. |
| Turvallisuusselvitys | henkilön nuhteettomuuden tai luotettavuuden varmistamiseksi Turvallisuusselvityslaissa (2014/726) säädetyllä tavalla laadittava selvitys henkilön taustasta. |

## 1. Johdanto

Tietoturvapolitiikka määrittää periaatteet, toimintatavat ja vastuut, joita noudatetaan Kymsoten tietoturvallisuuden toteuttamisessa ja kehittämisessä.

Tietojen, käsittelyprosessien, tietojärjestelmien, teknisen ympäristön sekä toimitilojen turvallisuus on välttämätön edellytys Kymsoten toiminnalle. Potilas- ja asiakastietojen saatavuus, virheettömyys ja ajantasaisuus tukevat Kymsoten vastuulla olevaien laaja-alaisten sosiaali- ja terveyspalveluiden tuottamista. Käsiteltävien tietojen arkaluonteisuus ja suuri määrä edellyttävät tietojen luottamuksellisuuden varmistamista tietojen koko elinkaaren ajan.

Kymsoten tietoturvatyötä ohjaavat lainsäädäntö, viranomaisohjeet, Kymsoten strategia sekä organisaation johdon asettamat vaatimukset. Tärkeimmät organisaation tietoturvallisuutta ohjaavat lait on eritelty Kymsoten tietosuojapolitiikassa.

Tietoturvapolitiikkaa täydentävät tietoturvan eri osa-alueita kuvaavat yksityiskohtaisemmat ohjeet ja prosessikuvaukset, jotka löytyvät Kymsoten intranetin tietoturvasivuilta. (Etusivu > Meidän tapamme toimia > Tietoturva)

## 2. Soveltamisala

Tietoturvapolitiikka koskee kaikkea Kymsoten ja sen tytäryhtiöiden toimintaa sekä lisäksi yhteistyökumppaneita siinä laajuudessa, kun ne toimittavat palveluita Kymsotelle tai käsittelevät Kymsoten vastuulla olevia tietoja. Jokainen Kymsotelle työskentelevä henkilö palvelusuhteesta riippumatta on velvoitettu noudattamaan tietoturvapolitiikkaa sekä sitä täydentäviä tietoturvaohjeita.

## 3. Tietoturvatavoitteet

Kymsoten tietoturvassa noudatetaan seuraavia tietoturvatavoitteita:

### Tietoturvan hallinta ja suunnittelu

- Tietoturvatoiminta on Kymsotessa suunnitelmallista, systemaattista ja kattavaa.
- Tietoturvallisuuden suunnittelussa ja hallinnassa otetaan huomioon saatavuus, eheys ja luottamuksellisuus.
    - Saatavuuden avulla varmistetaan, että tiedot ovat kaikkien niitä tarvitsevien saatavilla viivytyksettä ajasta ja paikasta riippumatta käyttöoikeuksien puitteissa.
    - Eheyden avulla varmistetaan, että tiedot ovat virheettömiä, kattavia ja ajantasaisia.
    - Luottamuksellisuuden avulla varmistetaan, että tietoihin pääsevät vain niihin oikeutetut henkilöt ja että tietojen luvaton käyttö havaitaan sekä siihen reagoidaan.
- Tietoturvaan liittyvät toimenpiteet dokumentoidaan siten, että tietoturva kyetään arvioimaan ja osoittamaan Kymsoten johdolle ja sidosryhmille.

### Henkilöstön toiminnan tietoturvallisuus

- Henkilöstöltä edellytetään tietoturvallista työskentelyä.

- Henkilöstön toiminnan tietoturvallisuutta tuetaan selkeillä ohjeilla, helppokäyttöisillä tietoturvaratkaisuilla, perehdytyksillä ja koulutuksilla.

**Riskit ja kehittäminen**

- Kymsoten vastuulla olevien tietojen, järjestelmien ja käsittelyprosessien riskit tunnistetaan, arvioidaan ja käsitellään. Riskilähtöisen tietoturvallisuuden hallinnan tavoitteena on löytää oikea tasapaino tietoturvainvestointien sekä niiden avulla saavutettavien hyötyjen välillä.
- Tietoturva otetaan huomioon kaikissa kehittämistoimenpiteissä heti alusta alkaen ja tietoturva sovitetaan yhteen muiden toiminnallisten vaatimusten kanssa. Erityisesti digitalisoituvien toimintaprosessien tietoturvallisuus suunnitellaan potilasturvallisuus ja käytettävyysnäkökohdat huomioiden.

**Seuranta, häiriöt ja jatkuvuus**

- Palveluiden saatavuus ja toiminnan jatkuvuus varmistetaan sekä normaalitilanteessa että poikkeusoloissa.
- Tietoturvahäiriöihin varaudutaan siten, että toiminta kyetään palauttamaan takaisin normaalitilaan nopeasti.
- Tietoturvan toteutuminen varmistetaan säännöllisellä seurannalla, testauksilla ja harjoittelulla, joiden tulosten perusteella arvioidaan kehittämistarpeita sekä toteutetaan kehittämistoimenpiteitä jatkuvan parantamisen periaatteen mukaisesti.

## 4. Organisointi ja vastuut

Tietoturvallisuuden kokonaisuudesta vastaa Kymsoten toimitusjohtaja sekä muu ylin johto nimettyjen vastuualueidensa mukaisesti. Erityisesti tietoturva kuuluu Tietohallintojohtajan vastuulle.

Kymsoten Tietoturva- ja tietosuojaryhmä toimii ylimmän johdon apuna kuntayhtymän tietoturvan kehityksessä sekä seurannassa. Tietoturva- ja tietosuojatyöryhmä ylläpitää ja kehittää tietoturvallisuutta, luo yleisiä periaatteita, antaa niihin liittyviä tarkentavia ohjeita sekä osallistuu tietoturvaa koskevien ratkaisujen suunnitteluun.

Kunkin palveluketjun nimetty vastuuhenkilö vastaa tietoturvallisuuden toteutumisesta ja kehittämisestä palveluketjuun kuuluvien toimintojen osalta.

Tietoturvaprosessien toimivuudesta ja kehittämisestä vastaa kunkin tietoturvaprosessin nimetty vastuuhenkilö.

Jokainen Kymsotelle työskentelevä henkilö palvelusuhteesta riippumatta on velvollinen perehtymään annettuihin tietoturvaohjeisiin, seuraamaan tietoturvaohjeiden päivityksiä, noudattamaan annettuja tietoturvaohjeita sekä raportoimaan havaitsemistaan tietoturvapuutteista esimiehelleen tai ohjeistetun ilmoituskäytännön kautta.

Jokainen esimies vastaa omien alaistensa perehdyttämisestä, ohjaamisesta, kouluttamisesta ja seurannasta.

Hankintojen ja projektien tietoturvallisuudesta vastaa hankinnan nimetty projektipäällikkö.

Tietosuojavastaavan tehtävänä on tietosuojan toteutumisen seuranta ja ohjaaminen. Tietosuojavastaava on otettava mukaan ajoissa henkilötietoihin liittyvien tietoturva-asioiden valmisteluun.

Ulkoistettuihin palveluihin liittyvät tietoturvan vastuuhenkilöt sekä Kymsoten, että palveluntuottajan puolella määritellään sopimuskohtaisesti.

Tietoturvavastuut on yksilöity tarkemmin tietoturvallisuuden vastuutaulukossa.

## 5. Tietoturvallisuuden hallinta

Tietoturvallisuuden hallinta Kymsotessa koostuu joukosta tietoturvaprosesseja, jotka on esitelty lyhyesti seuraavissa kappaleissa. Tarkemmat kuvaukset ja ohjeet eri tietoturvaprosesseista löytyvät Kymsoten intranetin tietoturvasivuilta.

### Suunnittelu ja vuosikello

Tietoturvallisuutta toteutetaan Kymsotessa sekä vuosikellon mukaisina etukäteen suunniteltuina toimenpiteinä, että reagoimalla tilanteisiin tarpeen mukaan.

Vuositasolla suunnitellaan tietoturvallisuuteen liittyvät tehtävät, työmäärät, aikataulut, vastuut sekä tarvittavat henkilöresurssit ja taloudelliset panostukset. Vuositason tietoturvasuunnitelma yhdistetään Kymsoten muuhun toiminnan suunnitteluun ja vuosikelloon.

Suunnitelman toteutumista seurataan ja suunnitelmaa täsmennetään tarpeen mukaan vuoden aikana.

### Suojattavien kohteiden hallinta

Kymsoten toiminnan kannalta merkitykselliset tiedot, järjestelmät, prosessit ja tekniset ympäristöt tunnistetaan, luokitellaan ja dokumentoidaan. Suojattavista kohteista ylläpidetään ajantasaista luetteloa.

### Tietoturvariskien hallinta

Kymsotessa arvioidaan systemaattisesti tietoihin ja niiden käsittelyyn kohdistuvia tietoturvariskejä. Riskit käsitellään siten, että jäännösriskit asettuvat hyväksyttävälle tasolle. Riskienhallintaa käytetään lisäksi päätöksenteon tukena tilanteissa, joissa on havaittu puutteita olemassa olevissa tietoturvaratkaisuissa.

Riskienhallinnassa noudatetaan dokumentoitua riskienhallintamenettelyä, jonka avulla varmistetaan erityyppisten riskien yhteismitallinen arviointi ja käsittely.

Tietoturvallisuuteen kohdistuvat riskit voivat johtaa huomattaviin taloudellisiin menetyksiin. Toisaalta ylisuojaaminen johtaa tarpeettomiin kustannuksiin ja voi vaikeuttaa päivittäistä työskentelyä. Näistä seikoista johtuen riskienhallinta on tärkeä apuväline Kymsoten tietoturvallisuuden ohjauksessa.

**Tietoturvavaatimusten hallinta**

Kymsoten suojattaville kohteille määritellään tietoturvavaatimukset riskilähtöisesti ottaen huomioon sekä lainsäädännön että toiminnan asettamat vaatimukset. Tietoturvavaatimuksia ylläpidetään siten, että ne vastaavat muuttuvan turvallisuusympäristön asettamia vaatimuksia.

Tietoturvavaatimuksia tarkastellaan rinnakkain tietosuojavaatimusten, lääkintälaitevaatimusten, toiminnan laatuvaatimusten, potilasturvallisuusvaatimusten sekä muiden toimintaa ja hankintoja ohjaavien vaatimusten kanssa.

Erityyppisiä hankintoja varten muodostetaan valmiita joukkoja tietoturvavaatimuksista, joita voidaan hyödyntää hankinnoissa ja projekteissa. Tietoturvavaatimusten muodostamisessa hyödynnetään viranomaisten laatimia valmiita kriteeristöjä.

**Henkilöstön toiminnan tietoturvallisuus**

Henkilöstön toiminnan tietoturvallisuutta ohjataan tietoturvaohjeilla, perehdytyksillä, koulutuksilla sekä hyvällä esimiestyöllä. Henkilöstön tietoturvaosaaminen ja toiminnan turvallisuus varmistetaan seurannan avulla.

Jokainen Kymsotelle työskentelevä henkilö palvelusuhteesta riippumatta on velvoitettu perehtymään annettuihin tietoturvaohjeisiin, seuraamaan tietoturvaohjeiden päivityksiä, noudattamaan annettuja tietoturvaohjeita sekä raportoimaan havaitsemistaan tietoturvapuutteista.

Kymsotelle työskentelevät henkilöt allekirjoittavat tietojen ja tietojärjestelmien käyttö ja salassapitositoumuksen. Lisäksi turvallisuuden kannalta kriittisemmissä tehtävissä työskenteleville henkilöille voidaan tehdä turvallisuusselvitys.

**Järjestelmien ja teknisten ympäristöjen tietoturva**

Järjestelmien ja teknisten ympäristöjen tietoturvavaatimukset määritellään. Vaatimusten toteutuminen varmistetaan katselmoinnein ja testauksin ennen käyttöönottoa. Järjestelmien käyttöönotot toteutetaan yhdenmukaisen tietoturvallisen käyttöönottomenettelyn mukaisesti. Järjestelmien ja teknisten ympäristöjen tietoturvallisuutta seurataan ja kehitetään säännöllisesti.

**Hankintojen tietoturva**

Hankintojen yhteydessä määritellään noudatettavat tietoturvavaatimukset. Hankintaprosessin yhteydessä varmistetaan katselmoinnin ja testauksin tietoturvavaatimusten täyttyminen. Tietoturvavaatimukset liitetään hankintasopimuksiin. Hankintojen tietoturvavaatimuksia seurataan ja ylläpidetään säännöllisesti.

### Häiriöhallinta

Tietoturvahäiriöiden tunnistaminen, arviointi ja käsittely toteutetaan yhdenmukaisen häiriöhallintaprosessin mukaisesti. Häiriötilanteet arvioidaan ja korjataan viivytyksettä sekä niiden toistuminen pyritään estämään. Häiriöiden yhteydessä tehdään lakien edellyttämät viranomaisilmoitukset ja informoidaan eri sidosryhmät.

### Seuranta, auditoinnit ja jatkuva parantaminen

Kymsoten tietoturvatilannetta sekä tietoturvaprosessien toimivuutta seurataan säännöllisesti. Kaikkien tietoturvallisuuden vastuuhenkilöiden kuuluu arvioida oman vastuualueensa tietoturvallisuus vähintään kerran vuodessa sekä raportoida kehittämistarpeista oman vastuualueensa osalta.

Tietoturva-auditointeja tehdään säännöllisesti ja auditointien tuloksia hyödynnetään osana tietoturvan jatkuvaa parantamista.

Tietoturvatilanne raportoidaan Kymsoten ylimmälle johdolle vuosittain. Ylimmän johdon tulee arvioida tietoturvan tilanne sekä tarvittaessa käynnistää toimenpiteitä havaittujen puutteiden korjaamiseksi.

## 6. Tietoturvarikkomukset ja sanktiot

Tietoturvaohjeiden sekä lainsäädännön vastainen toiminta käsitellään tapauskohtaisesti ennalta määritellyn prosessin mukaisesti. Tietoturvarikkomusten mahdollisiin seuraamuksiin sovelletaan Seuraamustaulukkoa. Rikosoikeudellisen lainsäädännön piiriin kuuluvat rikkomukset ilmoitetaan aina poliisille.

# Muutoshistoria

| Muutoshistoria | | | |
|---|---|---|---|
| **Versio** | **Päivä** | **Tekijä** | **Kuvaus** |
| 0.1 | | Teemu Kiiveri | Asiakirjan pohja ja luonnosversio tehty |
| 0.2 | | Kymsoten asiantuntijat ja Huld OY | Luonnosversiota muokattu |
| 0.3 | 12.11.2020 | YT-toimikunta | Asiakirja esitelty ja käyty läpi |
| 0.4 | 17.11.2020 | Työsuojelutoimikunta | Asiakirja esitelty ja käyty läpi |
| 1.0 | 1.12.2020 | Kymsote Jory | Politiikka hyväksytty |