

Kärkölen kunnan tietoturvapolitiikka

11.10.2021

1. JOHDANTO

Kärkölen kunnan toiminta ja palvelutuotanto perustuvat merkittävilä osin tietoon sekä koulutettuun ja tietoturvatietoiseen henkilöstöön ja hyvän hallinnon periaatteiden noudattamiseen. Sähköisen ja muussa muodossa olevan tiedon ja tietojen käsittelyn turvaaminen on osa kunnan toimintaa ja kokonaisturvallisuuden ylläpitämistä.

Tietoturvapoliitikassa kunnan johto määrittelee tietoturvaan liittyvän toiminnan tavoitteet, vastuut ja periaatteet Kärkölen kunnassa. Tämä politiikka toimii perustana yksityiskohtaisemmille määräyksille ja -ohjeille sekä käytännöille, joiden avulla tietoturvatyö liitetään osaksi kunnan toimintaa.

Tämä politiikka koskee jokaista Kärkölen kunnan työntekijää, viranhaltijaa, luottamushenkilöä ja kunnan lukuun toimivaa, joka työnsä tai toimeksiantonsa puitteissa käsittelee kunnan omistamaa tai hallinnoimaa tietoa.

Tätä politiikkaa sovelletaan kaikkeen tietoon riippumatta esitystavasta, muodosta tai elinkaaren vaiheesta.

2. TIETOTURVATYÖN TAVOITTEET

Kunnan tietoturvatyötä tehdään kunnan johdon ohjauksessa jatkuvaan kehittämiseen perustuen. Kehitysprosessissa arvioidaan kunnan toimintaympäristöön kohdistuvia tekijöitä, asetetaan tavoitteet¹ ja laaditaan suunnitelmat niiden saavuttamiseksi. Suunnitelmat johdetaan työkäytännöiksi ja tavoitteiden toteutumista seurataan säännöllisesti sekä tulosten perusteella muutetaan käytäntöjä aiempaa turvallisemmiksi.

Kärkölen kunnan tietoturvatyön tavoitteena on:

- luoda ja ylläpitää luotettavaa ja turvallista ympäristöä kunnassa tapahtuvalle tiedon käsittelylle
- varmistaa mahdollisimman häiriötön ja turvallinen toiminta sekä palvelutuotanto
- huolehtia vaatimusten mukaisesta tietojen (erityisesti henkilötietojen) käsittelystä kaikissa tilanteissa
- tukea kunnan turvallisuuskulttuurin kehittämistä

¹ Muiden muassa vaatimukset (lait ja asetukset), sisäiset ja ulkoiset riskit, sopimusvelvoitteet, soveltuvat kansalliset tietoturvaa koskevat standardit ja kriteeristöt, julkishallintoa koskevat suositukset ja hyvät käytännöt, henkilöstön ja kuntalaisten toiveet.

3. TIETOTURVA

Tietoturvalla tarkoitetaan hallinnollisia ja teknisiä toimia, joilla varmistetaan tiedon:

Luottamuksellisuus	tiedot ovat vain niiden käyttöön oikeutettujen saatavilla
Eheys	tietoja eivät voi muuttaa muut kuin siihen oikeutetut
Käytettävyys	tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä

Tietoturva koostuu tiedon luottamuksellisuuden, eheyden, saatavuuden ja tarvittaessa kiistämättömyyden varmistamisesta. Käytännössä näistä tietoturvan 'peruspilareista' huolehditaan Kärkölen kunnalle tärkeän tiedon sekä tietojärjestelmien ja -verkkojen osalta muiden muassa seuraavasti:

- luottamuksellisuus saavutetaan estämällä valtuudeton käyttö sekä luokittelemalla ja tarvittaessa salaamalla käsiteltävä tietosisältö.
- eheys varmistetaan niin, että tietoa ei voida muuttaa ilman asianmukaisia valtuuksia ja, että yritykset käsitellä tietoa tai järjestelmiä ilman valtuuksia havaitaan. Eheyden varmistaminen sisältää myös varoimet tiedon tahattoman vääristymisen estämiseksi inhimillisen tai teknisen häiriön seurauksena.
- saatavuuden varmistamiseksi ylläpidetään riittävää kapasiteettia, vikasietoisia toteutuksia, varmuuskopiokäytäntöjä sekä käytetään luotettavaksi todettuja teknisiä ratkaisuja.
- kiistämättömyyden toteutumista tuetaan kattavilla ja keskitetyillä tapahtumien kirjaus- ja lokienhallintakäytännöillä.

4. KOKONAISTURVALLISUUS

Kärkölän kunnassa kokonaisturvallisuudella tarkoitetaan alla kuvattuja osa-alueita, jotka yhdessä tietoturvakäytäntöjen kanssa muodostavat eheän kokonaisuuden kunnan tiedon, tietojärjestelmien ja -verkkojen sekä ihmisten, kunnan kiinteistöjen ja muun omaisuuden suojaaksi.

Kokonaisturvallisuuden hallinta edellyttää kunnan toimintaympäristön kattavaa tuntemusta, toiminnan suunnittelua, osaamisen ylläpitoa, viestintää sekä jatkuvaa seurantaa ja muutosten hallintaa.

Tietosuoja: Velvoittavien tietosuojasäädösten mukaiset toimenpiteet, joilla varmistetaan henkilön riittävä yksityisyyden suoja ja muut sitä turvaavat oikeudet henkilötietoja käsitellessä.

Riskienhallinta: Kaikki kunnan toiminnot ja organisaatiotasot kattava järjestelmällinen toiminta kunnan sisäisten ja ulkoisten riskien hallitsemiseksi kunnan kannalta tarkoituksenmukaisia ja kustannustehokkaita ratkaisuja käyttämällä.

Riskienhallinnassa pyritään ennakoiuuteen jälkikäteen reagoinnin sijaan, tavoitteena laatia riskienhallintasuunnitelma kaikille kriittisiksi luokitelluille palveluille ja järjestelmille.

Tietoturvan ja kokonaisturvallisuuden kehittäminen liitetään riskienhallinnan kautta kunnan johtamisjärjestelmään ja tätä kautta koko kunnan toiminnan kehittämiseen.

Jatkuvuuden hallinta: Hallinnolliset ja tekniset toteutukset (esim. valmius-, jatkuvuus-, toipumis- ja pelastussuunnitelmat sekä niihin liittyvät prosessit), joilla kunnan toimintojen ja palveluiden jatkuvuus turvataan normaalioloissa, häiriötilanteissa sekä poikkeusoloissa.

Jatkuvuudesta huolehditaan ylläpitämällä, harjoittelemalla ja testaamalla tarvittavia jatkuvuus- ja muita suunnitelmia. Lisäksi toimintaympäristön tilaa seurataan aktiivisesti ja mahdollisiin poikkeamiin ja häiriöihin reagoidaan tietoturvapoikkeamien hallintaprosessin mukaisesti.

Henkilöstöturvallisuus: Tietoturvatyötoimenpiteet, joita suoritetaan henkilöstöprosessin kaikissa vaiheissa: ennen palvelussuhdetta, sen aikana ja sen päättymisen yhteydessä.

Fyysinen turvallisuus: Toimenpiteet, järjestelmät ja rakenteet, joiden avulla kunnan tiloja ja siellä olevia ihmisiä, kuljetuksia, matkatyötä sekä tietoa ja muuta omaisuutta suojataan fyysisiltä ja kiinteistö- ja ympäristövahingoilta, vahingoittamisyrityksiltä ja oikeudettomilta henkilöiltä.

Sopimushallinnan keinoin samat vaatimukset saatetaan tarvittavilta osin koskemaan myös kunnan sidosryhmiä.

5. ORGANISOINTI JA VASTUUT

Kunnan keskeisimmät tietoturvatoinimijat ja heidän vastuunsa on kuvattu seuraavassa taulukossa.

Toimija	Vastuut
Kunnanhallitus	<ul style="list-style-type: none">– Tietoturvallisuusjärjestelyt, tietojärjestelmien toiminta ja yhteen toimivuus– Tietoturvallisuustoimenpiteet sekä poikkeusoloihin varautuminen– Tietoturvapoliitikan hyväksyminen
Kansliapäällikkö	<ul style="list-style-type: none">– Tietoturvan järjestäminen ja toteutumisen raportointi kunnanhallitukselle– Tietoaineistojen ja tietojärjestelmien tietoturvallisuudesta– Tietojen siirtämisestä tietoverkossa– Tietoaineistojen turvallisuuden varmistamisesta– Tietojärjestelmien käyttöoikeuksien hallinnasta– Lokitietojen keräämisestä tietojärjestelmien käytöstä ja luovutuksesta– Valmistelee tietoturvapoliitikasta johdettavat tietoturva-asiakirjat
Toimialajohtaja	<ul style="list-style-type: none">– Tietoturvan toteutuminen omalla toimialallaan sekä toteutumisen raportointi– Tietoturvan toimeenpano ja kehittäminen toimialallaan– Operatiivisten tietojärjestelmien tietoturvalisen käytön ohjeistaminen yhteistyössä tietojärjestelmän vastuuhenkilön kanssa
Henkilöstö	<ul style="list-style-type: none">– Määräysten ja ohjeiden noudattaminen sekä ei-toivottujen tapahtumien ilmoittaminen välittömästi omalle esimiehelle tai kansliapäällikölle
Esimies	<ul style="list-style-type: none">– Tietoturvaperehdytys, omaisuuden hallinta, avainten ja työvälineiden luovutus ja palautus sekä käyttö- ja pääsyoikeuksien hallinnan toteuttaminen
Tietosuojaavastaava	<ul style="list-style-type: none">– Henkilötietojen käsittelyn valvonta ja yhteistyö valvontaviranomaisten kanssa– Henkilökunnan ja johdon tukeminen tietosuoja-asioissa– Tietosuojaan liittyvä sisäinen viestintä
Tietojärjestelmän pääkäyttäjä	<ul style="list-style-type: none">– Tietoturvan, tietosuojan ja käyttöoikeuksien hallinta tietojärjestelmässä– Tietojärjestelmän käytön seuranta ja rekisteriselosteen laatiminen
Henkilöstöpäällikkö	<ul style="list-style-type: none">– Tietoturvan toteutuminen henkilöstöprosessin kaikissa vaiheissa (työsuhteen alkaessa, työsuhteen aikana ja päättyessä)
Johtoryhmä	<ul style="list-style-type: none">– Tietoturvan toteutumisen asianmukaisuuden ja riittävyyden seuranta

6. TIETOTURVAN JÄRJESTÄMISEN PERIAATTEET

Kärkölen kunnan tietoturvatyössä noudatetaan seuraavia periaatteita:

1. Tietoturvaa ja kokonaisturvallisuutta johdetaan järjestelmällisesti
2. Riskienhallintaa toteutetaan arvioimalla uhka- ja riskiympäristöä säännöllisesti kaikilla toimialoilla

3. Toiminnan jatkuvuutta uhkaaviin häiriöihin varaudutaan ennakolta ylläpitämällä, harjoittelemalla ja testaamalla tarvittavia jatkuvuuteen liittyviä suunnitelmia
4. Henkilötietojen käsittelyyn kiinnitetään erityistä huomiota huolehtimalla tietosuojasäädösten vaatimusten täyttymisestä
5. Kunnan määrittelemät tietoturva-vaatimukset huomioidaan mahdollisimman varhaisessa vaiheessa toiminnan, hankintojen ja teknisten järjestelmien suunnittelua sekä sisällytetään kaikkiin sopimuksiin
6. Tietoturvadokumentaatiota prosesseineen pidetään ajan tasalla
7. Henkilöstön osaamisesta huolehditaan koulutussuunnitelman mukaisilla jatkuvilla perehdytys- ja koulutuskäytännöillä
8. Tietoturvan toteutumista tuetaan sisäisellä ja ulkoisella viestinnällä
9. Tietojärjestelmät ja tietojenkäsittely toteutetaan hyvän tiedonhallintatavan mukaisesti, joka mahdollistaa tarvittavien asiakirjojen julkisuuden, tiedon asianmukaisen arkistoinnin ja hävittämisen

7. TIEDON JA TIETOJÄRJESTELMIEN KÄYTTÖ

Kärkölen kunnan tietojärjestelmäympäristössä käytetään kunnan tietohallinnon hyväksymiä tietojärjestelmiä, laitteita ja ohjelmistoja, jotka on tarkoitettu työtehtävien hoitamista varten.

Pääsyoikeudet kunnan tietoverkkoon ja -järjestelmiin sekä käyttöoikeudet kunnan omistamaan ja hallinnoimaan tietoon myönnetään käyttövaltuuspolitiikan mukaisesti työtehtävien hoitoon tarvittavassa laajuudessa.

8. TIETOTURVADOKUMENTAATION YLLÄPITO

Tämän tietoturvapolitiikan säännöllisestä katselmoinnista vastaa sen omistajana kansliapäällikkö tai hänen nimeämänsä taho.

Tästä politiikasta johdettu muu tietoturvadokumentaatio katselmoidaan ja päivitetään sekä hyväksytään kansliapäällikön ohjaamalla tavalla.

Kärkölen kunnan tietoturvadokumentaatio on kokonaisuudessaan henkilökunnan saatavilla kunnan sisäisissä informaatiokanavissa työtehtävien edellyttämässä laajuudessa.

OHJEEN VOIMAANTULO JA AJAN TASALLA PITÄMINEN

Tämä ohje tulee voimaan 11.10.2021.

Kunnanhallitus valtuuttaa kansliapäällikön hyväksymään tähän ohjeeseen sellaiset vähäiset korjaukset ja täsmennykset, jotka ovat tarpeellisia sen ajan tasalla pitämiseksi.

Ohje tuodaan kunnanhallituksen käsittelyyn, kun toiminnassa tai lainsäädännössä tapahtuu sellaisia merkittäviä muutoksia, jotka edellyttävät ohjeen laajaa päivittämistä.