

Tietoturvan ja tietosuojan johtaminen

Organisointi, vastuut, seuranta ja resursointi

Tiivistetty esitys tarkastuslautakunnan arviointia varten

JOHTAMINEN

VASTUUT

SEURANTA

RESURSSIT



28.9.2026



Johtamisen organisointi - tavoitemalli

Vastuu kulkee poliittisesta johdosta operatiiviseen toimeenpanoon ja toimialoille.



Johdon yhteenveto

Kokonaisuus on vahvistunut vuonna 2026, mutta johtamisen rakenteita tulee edelleen vakiinnuttaa.

Selkeä vastuu

Tietoturvapäällikön virka perustettiin 1.6.2026. Tehtävään kuuluu tietoturvan kokonaisvaltainen suunnittelu, toteutus ja valvonta. Tietosuojavastaavan toimi täytetty EU:n tietosuoja-asetuksen mukaisesti.

Politiikka ohjaa

Tietoturva- ja tietosuojapolitiikka on keskeinen ohjaava asiakirja ja perusta käytännön ohjeille.

Seuranta on käytössä

Tietotilinpäätös, työryhmä, poikkeamat, koulutukset ja auditoinnit muodostavat seurantakokonaisuuden.

Kehitystarpeet

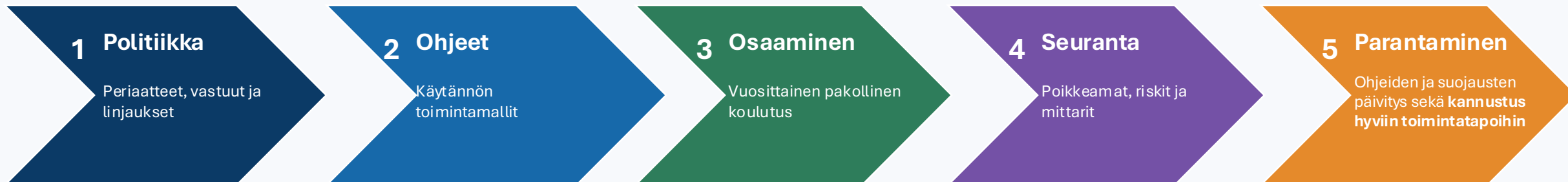
Suora johdon raportointi, valvontaoikeudet, osaamisen ylläpito ja budjetointi vaativat huomiota.

Keskeinen arvio

Johtamismalli sisältää olennaiset roolit ja seurannan elementit. Seuraava vaihe **on vahvistaa säännöllinen raportointiryhti**, mitattavat tavoitteet sekä tietoturvan ja tietosuojan oma taloudellinen ohjaus. Tämä vahvistaa riippumattomuutta.

Politiikasta käytännön toimintaan

Ohjaus toteutuu politiikan, ohjeiden, koulutuksen, seurannan ja jatkuvan parantamisen ketjuna.

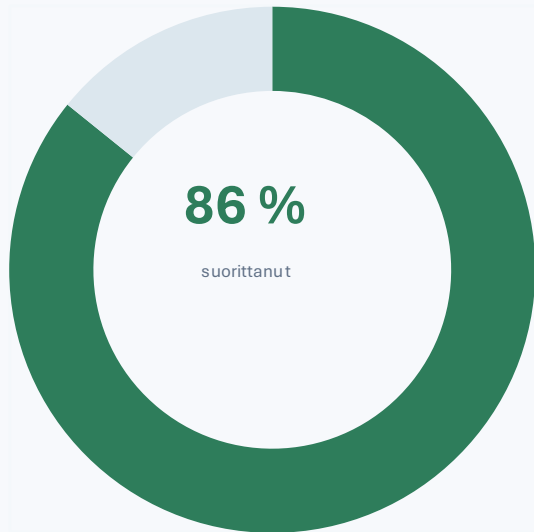


Riskiperusteisuus yhdistää ketjun

Velvoitteet ja suojaustoimet määritellään tiedon käsittelyyn liittyvien havaittujen riskien perusteella. Poikkeamat dokumentoidaan, käsitellään ja hyödynnetään toimintatapojen kehittämisessä.

Koulutus ja tietoturvatietoisuus - toteumaraportti

Vuosittainen koulutusvelvoite koskee henkilöstöä ja luottamushenkilöitä.



2 167 henkilöä, joilla

Hyväksytty koulutussuoritus.

2 525 henkilöä

Vertailuryhmä: 2 299 työntekijää
ja 226 luottamushenkilöä.

Johtamisen näkökulma

Koulutuksen suoritusaste on vahva. Seurantaan tarvitaan kuitenkin yhdenmukainen raportointi, ajantasainen koulutusympäristö ja selkeä käsittely puuttuville suorituksille.

Huomio: koulutusjärjestelmä on vaihtunut Eduhousesta Graniteen.

Seuranta ja raportointi

Tietotilinpäätös toimii vuosittaisena kokonaiskuvana, jota täydentävät jatkuva seuranta ja tarkastukset.



KPMG:n IT-tarkastus tilikaudelta 2024 raportoitiin johdolle.

Mittarit ja kehityssuunta

Tietotilinpäätöksiä on laadittu vuodesta 2019 alkaen. Mittarit kattavat toimintaympäristön, tiedot, riskit ja palvelut.

**Toimintaympäristö** Työasemat, käyttäjät, puhelimet, palvelupyynnot ja häiriöt

**Tietovarannot** Tietovarannot, järjestelmät ja tietosuojaselosteet

**Riskit ja arviot** Vaikutustenarvioinnit ja turvallisuusselvitykset

**Tietopyynnot** Julkisuuslain mukaiset pyynnot ja rekisteröityjen oikeudet

**Poikkeamat** Tietoturva- ja tietosuojapoikkeamat ilmoitusjärjestelmässä

**Kasvava tekninen ympäristö**
Työasemien ja tietojärjestelmien määrä ja riippuvuussuhteet kasvaneet, mikä on lisännyt palvelupyyntöjä ja häiriöilmoituksia.

**Lisääntyvä tiedonkäsittely**
Turvapostin käyttö, vaikutustenarvioinnit ja tietopyynnot ovat lisääntyneet.

**Arvioinnin kehitystarve**
Viiden vuoden muutosta kuvaava numeerinen aikasarja puuttuu tästä aineistosta. Trendit tulee täydentää päätöksenteon tueksi.

Vastuut käytännössä

Vastuut on kuvattu politiikassa, mutta toteutumista on ylläpidettävä koulutuksella, valvonnalla ja raportoinnilla.

Kaupunginhallitus

Seuraa kokonaisuutta ja toimii rekisterinpitäjänä alaisissaan toiminnoissa

Lautakunnat

Rekisterinpitäjän vastuu toimialojensa palveluissa

Rekisterin vastuuhenkilö

Tietosuoja, riskienhallinta ja selosteen lainmukaisuus

Esihenkilöt ja johto

Vastuiden tunteminen, koulutukset ja käytännön valvonta

ICT-tuottajat

Tekniset tietoturvavastuut ja laatukokousten valvonta

Valvonnan ydin: koulutusten suoritusaste, riskitoimien toteutuminen ja poikkeamien käsittely.

Resursointi ja ulkoiset palvelut

Henkilöresurssi on vahvistunut, mutta **tietoturvalla ja tietosuojalla ei ole erillistä budjettia**.

Tietoturva

1 tietoturvapäälikkö. Virka 1.6.2026 alkaen vähensi aiempaa resurssivajetta.

Tietosuoja

1 päätoiminen tietosuojavastaava ja 1 sivutoiminen asiantuntija sivistyspalveluissa.

Ostopalvelut

SIEM-SOC, auditointipalvelut sekä Netum Oy:n tietosuoja-asiantuntijat erityiskysymyksiin.

Budjetointi

Ei erillistä tietoturvan tai tietosuojan budjettia. Seuraavalle vuodelle on esitetty 10 000 euroa tietoturva-auditointeihin.

Osaamisen jatkuvuus

Tietoturvapäälikön koulutus-, konferenssi- ja verkostoitumismahdollisuudet edellyttävät ennakoitavaa rahoitusta.

Suosittelavat johtamistoimet

Painopiste siirtyy rakenteiden perustamisesta niiden säännölliseen ja mitattavaan käyttöön.

1

Vakiinnuta raportointirythmi

Tietoturvapäällikön ja tietosuojavastaavan säännöllinen raportointi kaupunginjohtajalle ja kaupunginhallitukselle.

2

Määritä valvontaoikeudet

Riittävät työkalut, käyttöoikeudet ja näkyvyys kaupungin tietoturvan seurantaan.

3

Aseta mittaritavoitteet

Tavoitearvot, viiden vuoden aikasarjat ja poikkeamien vakavuusluokittelu.

4

Vahvista budjetointi

Auditoinnit, kouluttautuminen ja jatkuva osaamisen ylläpito omaksi kokonaisuudeksi.

5

Päivitä tekoälyohjaus

Tekoälypolitiikan ja käytännön ohjeiden säännöllinen päivitys sekä noudattamisen seuranta.

Arvioinnissa huomioitavat rajaukset

Tarkennettavat tiedot

Koulutusympäristön ajantasainen nimi ja teknisten suojausten kattavuuden mittarit tulee varmistaa.

Puuttuva aikasarja

Kehitystä ei voi arvioida täsmällisesti ilman vuosittaisia vertailulukuja.

Tavoitteita määriteltävä

Tietoturvan ja tietosuojan tavoitteita on määriteltävä ja seurattava niiden toteutumista

Johtopäätös

Kaupungilla on toimiva perusrakenne tietoturvan ja tietosuojan johtamiseen. Jatkossa läpinäkyvyyttä ja arvioitavuutta **vahvistavat erityisesti säännöllinen johdon raportointi, vertailukelpoiset mittarit ja ennakoitava resursointi.**

Kyberturvallisuuden tilannekuva on muuttunut – ja paljon

Kyberuhat vaativat varautumista:

Kyberrikollisuus on muuttunut ammattimaiseksi ja taloudellisesti merkittäväksi toiminnaksi, jossa hyödynnetään tietojenkalastelua, haittaohjelmia, haavoittuvuuksia ja hyökkäyspalveluita.

Hyökkääjät voivat edetä murtoon tai kiristykseen jopa 20 minuutissa, joten organisaatioiden on tunnistettava arkaluonteisen datan sijainti, käyttö ja käsittely sekä varauduttava poikkeustilanteisiin ja järjestelmien palauttamiseen

Kyberturvallisuuden tilannekuva on muuttunut

Tekoäly edellyttää ihmisen valvontaa: Copilot-tekoälyn ja ohjelmistoagenteiksi kutsuttujen järjestelmien todettiin nopeuttavan prosessointia ja tukevan ohjelmistokehitystä, mutta niiden tuotoksia on ymmärrettävä ja valvottava.

Kriittinen ajattelu, huolellisesti suunnitellut syötteet ja prompt injection -uhkien tunnistaminen ovat keskeisiä, koska syöteinjektio voi tapahtua dokumenttien, kuvien tai rajapintojen kautta.

Tekoäly nopeuttaa myös kyber rikollisten toimintaa.

Henkilöstön koulutukseen on panostettava tekoälyn osalta.

Kyberturvallisuuden tilannekuva on muuttunut

Kvanttiturvallisuuteen on valmistauduttava ajoissa: Arvioitu (VM), että kvanttitietokone voisi vuonna 2030 pystyä murtamaan 2048-bittisen RSA-salauksen tunneissa (nyt vuosia)

Salattua dataa voidaan kerätä jo nyt myöhempää murtamista varten, minkä vuoksi organisaatioiden tulisi inventoida järjestelmät, arvioida riskit, suunnitella kvanttiturvallisuus ja ottaa huomioon muun muassa PQC (Post-Quantum Cryptography), hybridisalaus sekä kvanttistrategia hankinnoissa.

Kyberturvallisuuden tilannekuva on muuttunut

Digitaalinen riippuvuus on strateginen kysymys:

EU:n teknologisen suvereniteetin haasteena on riippuvuus Yhdysvalloista ja Kiinasta, joista noin 80 prosenttia EU:n digituotteista tulee.

Teknologiakilpailu, suurten teknologiatoimijoiden valta, alustojen datankeruu ja datakeskukset kytkeytyvät seminaarin mukaan geopolitiikkaan, demokratian tulevaisuuteen ja EU:n tarpeeseen vahvistaa omaa rooliaan.