Tampereen seudun sähköisten viestintävälineiden käyttösäännöt

Sisällys

1 Yleistä 3
2 Työnantajan tarjoamien työvälineiden yksityiskäyttö 3
3 Internetin käyttörajoitukset 4
4 Sähköpostiviestien ja -osoitteiden määritelmät sekä käsittely 4
4.1 Määritelmät ja käyttötarkoitukset 4
4.2 Sähköpostiosoitteiden julkaiseminen 5
4.3 Sähköpostiviestien käsittely 5
4.3.1 Yleistä sähköpostien käsittelystä 5
4.3.2 Huijaukset ja tietojenkalastelu 6
4.3.3 Sähköpostien rajoittaminen ja suodattaminen 7
4.3.4 Roskapostiviestit 7
4.3.5 Perille menemättömät sähköpostiviestit 8
4.3.6 Väärään osoitteeseen saapuneet sähköpostiviestit 8
4.3.7 Organisaation sähköpostiviestien käsittely 8
4.3.8 Työsähköpostiviestien käsittely 9
4.3.9 Yksityisten viestien käsittely 9
4.3.10 Muiden sähköpostiviestien käsittely 10
4.4 Palvelussuhteen tai opiskeluoikeuden päättyminen 10
4.5 Menettely työntekijän ollessa väliaikaisesti tai pysyvästi poissa 10
5 Sähköiset kyselyt 11
6 Sähköisten viestien salaus ja todentaminen 11
7 Sähköisen kalenterin käyttö 12
7.1 Tilanvarauskäytännöt 13
8 Teamsin käyttö viestinnässä ja kokouksissa 13
9 Tekstiviestien ja (sosiaalisen median) viestintäpalveluiden käyttö 15
10 Tekoälyratkaisut 16
11 Käytön valvonta sekä lokitietojen kerääminen ja säilyttäminen 17
12 Näiden määräysten valvonta 18
13 Dokumentin versiohistoria 19

1 Yleistä

Työnantajalla on velvollisuus kirjallisesti ohjeistaa, mihin ja miten sähköisiä viestintäratkaisuja, sovelluksia ja tietoverkkoa käytetään huomioiden muun muassa tekoälyratkaisut. Tämän dokumentin keskeisenä tarkoituksena on sääntöjen lisäksi myös ohjeistaa käyttäjiä ja varmistaa viestinnän osapuolten oikeusturva sekä parantaa verkon ja järjestelmien tietoturvaa ja tietosuojaa.

Sähköisten viestintävälineiden käyttösääntöjen linjaukset koskevat kaikkia Tampereen seudun tietohallintoyhteistyössä mukana olevia kuntia. Ne koskevat myös kaikkia järjestelmistä vastaavia toimijoita, joiden kanssa seudun kunnilla on voimassa oleva sopimus.

Nämä käyttösäännöt toteuttavat voimassa olevaa lainsäädäntöä kuten:

- lakia sähköisen viestinnän palveluista (917/2014)
- EU:n yleistä tietosuoja-asetusta (GDPR)
- tietosuojalakia (1050/2018)
- lakia yksityisyyden suojasta työelämässä (759/2004)
- lakia julkisen hallinnon tiedonhallinnasta (906/2019)
- EU:n tekoälyasetusta (EU) 2024/1689
- lakia eräiden tekoälyjärjestelmien valvonnasta (1377/2025)
- digipalvelulakia (306/2019)
- yhteistoimintalakia (1333/2021)

2 Työnantajan tarjoamien työvälineiden yksityiskäyttö

Työnantaja tarjoaa ohjelmistoineen henkilöstölle tietotekniikkaan liittyvät laitteet, jotka ovat tarkoitettu työtehtävien hoitamiseen. Omia yksityiselämän laitteita ei ole tarkoitettu työasioiden hoitamiseen, ellei asiasta ole poikkeustapauksessa erikseen työantajan kanssa sovittu ja tietoturvallisuudesta huolehdittu.

Lähtökohtaisesti työantajan laitteita ja tietojärjestelmiä ei saa käyttää omien työhön liittymättömien asioiden (nk. yksityisasioiden) käsittelyyn, kaupalliseen yritystoimintaan tai yhdistystoimintaan. Poikkeuksena tästä on esimerkiksi työsuhde-etuna myönnetty työpuhelin.

Voit kuitenkin halutessasi tallentaa ja käsitellä pienimuotoisesti omia yksityisasioitasi työtunnuksiisi sidotussa OneDrive-työtilassasi. Tällöin sinun pitää nimetä kansio erikseen etuliitteellä "Yksityinen", jotta tiedostot voidaan tarvittaessa erotella työantajan omistamasta työtietosisällöstä. Lisäksi pienimuotoinen työnantajan laitteiden muu yksityiskäyttö, kuten henkilökohtaisten laskujen maksaminen tai internet selailu omalla ajalla, on sallittua.

Rikoksia ei saa tehdä eli ei esimerkiksi saa tallentaa mitään laitonta materiaalia!

Työnantaja ei ratko yksityiskäyttöön liittyviä ongelmia eikä vastaa yksityiskäytöstä mahdollisesti koituneista vahingoista. Työ- tai virkasuhteen päätyttyä työvälineille tallennetut yksityiset aineistot hävitetään työnantajan toimesta.

Sähköisten viestimien käyttäjien on syytä pohtia, mitä kaikkia riskejä omaan sähköiseen viestintään ja laitteiden käyttöön liittyy sekä pyrkiä huomioimaan ja minimoimaan kyseiset riskit.

Käyttäytymisen tulee olla asiallista riippumatta käytettävästä viestintävälineestä. Työntekijän, harjoittelijan ja opiskelijan, jotka käyttävät kunnan sähköisiä viestintävälineitä tai muuten edustavat työnantajaa, tulee muistaa viesteissään lojaliteettivelvollisuus työnantajaa kohtaan. Lojaliteettivelvoite tarkoittaa, että työntekijän on toimittava työnantajan edun mukaisesti. Työntekijän on vältettävä kaikkea, mikä on ristiriidassa hänen asemassaan olevalta työntekijältä kohtuuden mukaan vaadittavan menettelyn kanssa. Hän ei saa toiminnallaan aiheuttaa työnantajalleen vahinkoa.

3 Internetin käyttörajoitukset

Jokainen käyttäjä on vastuussa siitä, että hänen tiedostonsa, sähköpostiviestinsä sekä internetkäyttönsä on lakien, ohjeiden ja hyvän tavan mukaista.

Tietoliikenneverkon toiminnan ja tietoturvan takaamiseksi seuraavat toiminnot ovat kiellettyjä:

- palomuurien, virustorjunnan ym. kiertäminen tai tietojärjestelmän turvamekanismien tarkoituksellinen ohittaminen
- työjärjestelmiin liittymättömien vertaisverkko-ohjelmien käyttö, sillä niiden kautta voi mahdollisesti tarttua haittaohjelmia ja niiden käyttöön voi liittyä tekijänoikeusrikkomuksia
- työtehtäviin liittymättömien ohjelmien, musiikki- ja videotiedostojen sekä pelien lataaminen tai jakaminen kuntien tietoverkkoon ilman työnantajan lupaa
- työtehtäviin liittymättömien mahdollisesti vaarallisten sivujen selailu.

Kunnat voivat rajoittaa teknisillä estoilla internetissä olevien palvelujen ja www-osoitteiden käyttöä seudun kuntien verkosta ja laitteilta.

Työkäyttöön liittymättömissä internetin palveluissa ei saa käyttää samoja salasanoja kuin sisäverkon järjestelmissä.

Salasanojen tallentaminen Internet-selaimen muistiin ei ole suositeltavaa. Salasanojen hallintaan soveltuu työaseman työpöydältä löytyvästä Yritysportaalista ladattava KeePass-ohjelma.

4 Sähköpostiviestien ja -osoitteiden määritelmät sekä käsittely

4.1 Määritelmät ja käyttötarkoitukset

Sähköpostiviestit on tässä jaettu neljään eri luokkaan sen mukaisesti, millaiseen osoitteeseen ne liittyvät.

- **Organisaation sähköpostiviesti** on kunnan tai yksikön organisaatio-osoitteeseen tullut tai sitä kautta lähetetty viesti.

- **Työsähköpostiviesti** on työntekijälle työkäyttöön annettuun henkilökohtaiseen sähköpostiosoitteeseen (esimerkiksi maija.mehilainen@tampere.fi) tullut tai sitä kautta lähetetty työtehtäviin liittyvä viesti.
- **Henkilökohtainen sähköpostiviesti** on työnantajan antamaan sähköpostiosoitteeseen liittyvä henkilökohtainen (=yksityinen) viesti.
- **Muu sähköpostiviesti** on käyttäjän ulkopuoliseen sähköpostiosoitteeseen esimerkiksi gmail-osoitteeseen tullut tai sitä kautta lähetetty viesti.

Työntekijöiden henkilökohtaiset työsähköpostiosoitteet muodostuvat käyttäjän nimestä. Tähän muotoon (esimerkiksi etunimi.sukunimi@tampere.fi) tekevät poikkeuksen nimikaimat, joiden osoitteisiin lisätään tarvittaessa erotteleva osa. Ulkopuolisille käyttäjille käytetään ext-alkuisia sähköpostiosoitteita. Luonnollisen henkilön sähköpostiosoite on EU:n yleisen tietosuoja-asetuksen (GDPR) tarkoittama henkilötieto.

Työnantajalla on oikeus määrätä tietojärjestelmistään sekä työntekijöiden sähköpostitilien käytöstä. Työnantaja voi päättää sähköpostitilin antamisesta tai pois ottamisesta työntekijän käytöstä työsuhteen aikana tai työsuhteen päättymisen jälkeen. Työnantaja voi tarvittaessa myös laittaa työntekijän sähköpostiin automaattisen vastausvietin esimerkiksi pitkän poissaolon ajaksi.

4.2 Sähköpostiosoitteiden julkaiseminen

Julkaisemisella tarkoitetaan sähköpostiosoitteen ilmaisemista muun muassa kunnan puhelinluettelossa, muussa julkaisussa, verkkosivuilla, käyntikorteissa tai hakemistopalveluissa.

Kunta voi julkaista organisaatio-osoitteet sekä työntekijöidensä työsähköpostiosoitteet niiltä osin kuin se on tarpeen palveluiden käytön ja tehtävien hoidon kannalta.

Ohjeita:

Kuntien työntekijöiden tulee välttää sähköpostiosoitteiden julkaisemista verkkosivuilla tekstimuotoisena, koska se lisää osoitteeseen lähetettävien roskapostien määrää. Sen sijaan on suositeltavaa kertoa osoitteen muodostamistapa eikä varsinaista osoitetta eli esimerkiksi se, että ne ovat muotoa etunimi.sukunimi@tampere.fi.

4.3 Sähköpostiviestien käsittely

4.3.1 Yleistä sähköpostien käsittelystä

Tampereen seudun sähköpostijärjestelmässä työsähköpostiviestien automaattinen ohjaaminen postijärjestelmän ulkopuoliseen sähköpostiosoitteeseen on kielletty ja teknisesti estetty, jotta lähettäjän tietämättä luottamuksellista tai salassa pidettävää tietoa ei päädy salaamattomana julkisen verkon puolelle.

Työsähköpostiosoitteen käyttö yksityiseen kaupalliseen tarkoitukseen tai poliittiseen mainontaan on kiellettyä lukuun ottamatta henkilökunnan ammattiyhdistysten ja kunnan oppilaitosten opiskelijajärjestöjen toimintaa.

Ketjukirjeitä tai yleisesti roskapostiksi tulkittavia viestejä ei saa lähettää Tampereen seudun sähköpostijärjestelmästä.

Asiakkaiden sähköpostiosoitteet pitää laittaa piilokopiokenttään aina, kun heille lähetetään esimerkiksi tiedotteita tai palautekyselyitä, joissa on useita vastaanottajia.

Työsähköpostiosoitetta tulee käyttää vain sellaisiin verkkopalveluihin rekisteröitymiseen, joilla on selkeä yhteys työtehtäviin.

Ohjeita:

Tampereen seudun työsähköpostiosoitteisto sisältää kymmenien tuhansien henkilöiden tietoja. Useilla henkilöillä on nimikaimoja ja viestin vastaanottajaa valittaessa on aina tarkistettava, että nimen lisäksi myös organisaatio ja tehtävänimike ovat oikein. Erityisen huolellinen kannattaa olla silloin, kun lähettää sähköpostia matkapuhelimella tai tablettitietokoneella. Pientä näyttöä käyttäessä on suurempi riski tehdä virheitä, kun valitsee viestilleen oikeaa vastaanottajaa tai tarkistaa sähköpostiosoitetta.

Vastaanottaja-kenttään kuuluu laittaa ne henkilöt tai tahot, joille asia ensisijaisesti kuuluu ja/tai joilta edellytetään toimenpiteitä. Kopio-kenttään vastaavasti tulee laittaa henkilöt tai tahot, joille asia halutaan tiedoksi.

Piilokopion käyttäminen on suositeltavaa silloin, kun viestitään laajalla jakelulla tai vastaanottajat eivät saa nähdä toistensa sähköpostiosoitteita. Henkilön sähköpostiosoite tai asiakassuhde voi olla salassa pidettävä tieto.

Virheelliselle tai väärälle vastaanottajalle lähetetty viesti tulee peruuttaa, jos se on mahdollista. Outlookissa se yleensä onnistuu vain Tampereen seudun oman postijärjestelmän niiltä sisäisiltä käyttäjiltä, jotka eivät vielä ole kyseistä postia avanneet.

4.3.2 Huijaukset ja tietojenkalastelu

Sähköpostitse tehdyt huijaukset, tietojenkalastelut ja haittaohjelmaperäiset hyökkäykset ovat lisääntyneet ja jatkuvasti tulee uusia tapoja.

Tietojen kalastelussa huijari pyrkii keräämään luottamuksellisia tietoja käyttäjän avulla. Näissä rikollisten tekemissä huijauksissa käytetään erittäin monimutkaista tekniikkaa ja oveluutta, jonka vuoksi kaikkia haitallisia sähköposteja ei saada täysin suodatettua pois. Tästä syystä myös sähköpostin käyttäjän oma toiminta on erittäin merkittävässä roolissa hyökkäysten ja huijausten torjumisessa.

Mieti ennen kuin avaat sähköpostin liitetiedostoja tai klikkaat viesteissä olevia linkkejä.

- Suhtaudu epäluuloisesti tuntemattomalta lähettäjältä saamiisi viesteihin, etenkin jos viestissä on liitteitä tai linkkejä. Sama pätee myös tuntemiisi lähettäjiin, koska lähettäjän tiedot voidaan väärentää tai hänen sähköpostitilinsä on voitu kaapata.

- Mikäli viesti on selkeästi epäilyttävä (olet esimerkiksi voittanut jotain tai saat ”ilmaista” rahaa), poista viesti sitä enempää tutkimatta. Mikäli avasit epäilyttävän viestin ja klikkasit siinä olevaa linkkiä tai avasit esimerkiksi viestin liitetiedoston, ota välittömästi yhteys Tukikeskukseen, vaikka näyttäisi siltä, että mitään ei tapahtunut.

Epäselvissä tilanteissa voit toimia seuraavilla tavoilla:

- Kysy viestin lähettäjältä, lähettikö hän viestin tarkoituksella sinulle. Älä kuitenkaan kysy tätä vastaamalla viestiin tai soittamalla viestissä yhteystietoina annettuihin numeroihin, sillä huijari on voinut antaa omia yhteystietojaan eli tarkasta yhteystiedot jostain muualta.
- Odota yli vuorokausi avaamatta viestiä. Tyypillisesti virustorjunta ja haittaohjelmien suodatus oppivat jatkuvasti tunnistamaan uusia haitallisia linkkejä tai liitteitä. Täten viestin avaaminen vasta myöhemmin on turvallisempaa kuin heti sen saavuttua.
- Myös Tukikeskuksen kautta voit kysyä apua asian selvittämisessä.

4.3.3 Sähköpostien rajoittaminen ja suodattaminen

Kunnilla on oikeus ohjelmallisesti tarkistaa sähköpostiviestit ja niiden liitetiedostot mahdollisten virusten ja muiden haittaohjelmien osalta sekä rajoittaa mahdollisesti haitallisten, viallisten tai liian suurien tai monilukuisten liitetiedostojen vastaanottamista ja lähettämistä. Samalla kunnilla on oikeus myös poistaa viruksia ja muita haittaohjelmia sisältävät viestit ja liitetiedostot. Yksittäisen viestin suodattamisesta tai tuhoamisesta ei tiedoteta viestin lähettäjälle.

Ylläpitäjillä on oikeus selvittää viestien turvallisuuteen liittyviä asioita ja sen myötä myös puuttua sähköpostien kulkuun sähköpostijärjestelmän palvelutason tai turvallisuuden takaamiseksi.

4.3.4 Roskapostiviestit

Tampereen seudun sähköpostipalvelua suojataan ja roskapostiongelmaa pienennetään suodattamalla viestit, jotka saapuvat tunnetuista roskapostia välittävistä palvelimista tai jotka luokitellaan roskapostiksi otsikkotietojensa tai automaattisen sisältöanalyysin perusteella. Esto toteutetaan teknisin menetelmin sähköpostipalvelussa. Suodatetut viestit voidaan myös asettaa karanteeniin tai tuhota käyttäjän puolesta.

Yksittäinen roskapostiviesti voidaan suodattaa tai tuhota ilman, että siitä on tarve tiedottaa viestinnän osapuolille tai palauttaa tuhottua viestiä lähettäjälle.

Ohjeita:

Älä vastaa roskapostiin – vastaamalla osoitat sähköpostiosoitteesi toimivaksi, ja se lisätään roskapostittajien jakelulistoille.

Jos automaattisesta roskapostien suodatuksesta huolimatta saat häiritsevässä määrin roskapostia, ilmoita asiasta Tukikeskukseen.

Roskaposti-kansioon tai karanteeniin päätyneet roskapostit voi ja on hyvä poistaa eli niille ei välttämättä tarvitse tehdä muuta. Jos käyttäjän Outlookissa on mahdollista ilmoittaa kalastelusta, niin sitä kannattaa käyttää. Lähettäjän estäminen sen sijaan ei yleensä ole suositeltavaa eli se auttaa vain yritysten

lähettämiin mainoskirjetyyppisiin posteihin, kun muissa roskaposteissa tai huijauksissa postin lähettäjäksi on usein väärennetty joku sivullinen henkilö, jonka estäminen ei auta ketään.

Jos roskapostiin päätynyt viesti ei ole roskapostia, niin valitse postin kohdalla ”Ei roskapostia” toiminto, jolloin posti siirretään Saapuneet kansioon. Tässä tapauksessa ei yleensä ole syytä määritellä lähettäjän postiosoitetta luotettavaksi, koska kyseisen tahon tili saatetaan kaapata myöhemmin ja sieltä voi alkaa tulla huijauksia tai muuta roskapostia.

4.3.5 Perille menemättömät sähköpostiviestit

Sähköpostiviestin lähettäjällä on vastuu viestin perillemenosta.

Käyttäjien tulee huolehtia, että omassa sähköpostilaatikossa on riittävästi tilaa uusien sähköpostien vastaanottamiseen ja lähettämiseen.

Ohjeita:

Mikäli saapuvan viestin vastaanottajan osoite ei ole vastaanottavan sähköpostijärjestelmän tiedossa, lähettää järjestelmä viestin lähettäjälle automaattisesti virheilmoituksen. Vastaanottajan järjestelmä yleensä lähettää ilmoituksen lähettäjälle myös, jos vastaanottajan sähköposti on täynnä. Käyttäjien tulee siivota omia turhia sähköpostejaan riittävän usein, jotta oma postilaatikko ei pääse täyttymään.

4.3.6 Väärään osoitteeseen saapuneet sähköpostiviestit

Mikäli sähköpostin käyttäjä saa toiselle henkilölle tarkoitetun sähköpostiviestin, on hänellä salassapitovelvollisuus niin viestin sisällöstä kuin olemassaolostakin.

Ohjeita:

Toiselle henkilölle (esimerkiksi kaimalle) tarkoitettu sähköpostiviesti on ohjattava edelleen oikeaan osoitteeseen, jos osoite on varmuudella tiedossa. Lisäksi viestin lähettäjää pitää informoida siitä, että viesti on tullut alun perin väärälle vastaanottajalle. Mikäli oikeaa osoitetta ei ole tiedossa, on viestin vastaanottajan lähetettävä alkuperäiselle lähettäjälle tieto virheellisestä osoitteesta ja hävitettävä saapunut viesti.

Kunnan tai viranhaltijan toimivaltaan kuulumaton, ilmeisestä erehdyksestä tai tietämättömyydestä lähetetty sähköpostiviesti on siirrettävä hallintolain (434/2003) 21 §:n mukaisesti toimivaltaiseksi katsotulle viranomaiselle, jos se on tiedossa ja siirrosta on ilmoitettava viestin lähettäjälle. Ellei siirto ole mahdollinen, viesti palautetaan ja hävitetään.

Lähetys- ja palautusvelvollisuudet tai -ohjeet eivät koske haitallisia posteja tai muuta roskapostia.

4.3.7 Organisaation sähköpostiviestien käsittely

Organisaatio-osoitteen tulee kuvata sitä toimintoa, jota varten osoite on perustettu (esimerkiksi tampereenpalvelupiste@tampere.fi)

Jokaiselle organisaatio-osoitteelle tulee nimetä vähintään yksi vastuuhenkilö, jolla tulee olla myös varahenkilö. Vastuuhenkilö määrittelee sen, miten saapuneet viestit käsitellään, käsittely varmistetaan ja saatetaan tiedoksi muille käsittelijöille.

Jos saapuneessa viestissä on kuittauspyyntö, lähetetään kuittausviesti ilman tarpeetonta viivettä. Kuittauspyyntö tarkoittaa tässä yhteydessä viestin saatteessa olevaa virallista pyyntöä eikä lähettäjän sähköpostijärjestelmän lähettämää ”Lähettäjä on pyytänyt kuittauksen” -ilmoitusta.

Sähköisessä asioinnissa viranomaisen on viipymättä ilmoitettava sähköisen asiakirjan vastaanottamisesta lähettäjälle kuittausviestillä. Automaattikuittauksia ei tule käyttää muissa kuin erityisesti sitä varten suunnitelluissa asiointijärjestelmissä.

Organisaation sähköpostiviestejä käsitellään julkisuuslain (621/1999) edellyttämällä tavalla. Julkisuuslaissa säädetään muun muassa, mikä on viranomaisen asiakirja, mitkä ovat salassa pidettävät tiedot ja milloin on oikeus saada tieto asiakirjasta.

Työnantajalla on tarvittaessa esteetön pääsy organisaatiosähköpostiosoitteisiin saapuneisiin viesteihin. Näitä sähköpostiosoitteita ei saa käyttää yksityiseen viestintään.

Vastuuhenkilöille määritellään tarvittava pääsy organisaatio-osoitteen postilaatikkoon heidän henkilökohtaisilla tunnuksillaan. Organisaatiopostilaatikoita ei käytetä yhteiskäyttötunnuksilla, kuin erikseen sallituissa perustelluissa poikkeustapauksissa.

4.3.8 Työsähköpostiviestien käsittely

Työsähköpostiosoitteella toimitettuja viestejä käsitellään pääsääntöisesti vastaanottajalle osoitettuina henkilökohtaisina viesteinä.

Ennen kuin otat sähköpostikeskusteluun mukaan lisää jäseniä tai lähetät viestejä eteenpäin, varmista, että aiempi viestikeskustelu ei sisällä mitään uudelle vastaanottajalle kuulumatonta sisältöä (esimerkiksi sisäisiä yhteistyökumppanille tai asiakkaalle kuulumattomia asioita tai jotain salassa pidettävää/suojattavaa tietoa).

Ohjeita:

Sähköpostiviestin aihekentässä (=otsikko) voi käyttää saatesanoja helpottamaan vastaanottajaa ymmärtämään nopeasti sen mitä häneltä odotetaan viestin käsittelyn suhteen. Esimerkkejä saatesanaksi: Tiedoksi, Luettavaksi, Kommentoitavaksi tai Tehtäväksi + määräaika. Voit myös käyttää Outlookin suuri tärkeys, pieni tärkeys tai seuranta -tunnisteita sekä muita postin luokitteluvaihtoehtoja.

Vastattaessa työsähköpostiin on suositeltavaa käyttää ”Vastaa kaikille” -toimintoa, ellei ole perustellusti tarve poistaa jakelusta joitain henkilöitä, joille vastaus ei kuulu.

Jos viestiä ei ole syytä levittää, voi olla hyvä selvästi kirjoittaa viestin alkuun siitä huomautus esimerkiksi ”Älä jatkolähetä tätä sähköpostia eteenpäin!”.

Älä tulosta sähköposteja paperille, ellei se ole välttämätöntä. Jos tulostat, niin käytä turvatulostusta aina kun se on mahdollista.

4.3.9 Yksityisten viestien käsittely

Työntekijän henkilökohtaiset (=yksityiset) viestit tulee erottaa selvästi työhön liittyvistä (=työnantajalle kuuluvista) viesteistä.

Jos työntekijä saa työsähköpostiosoitteeseensa henkilökohtaisia viestejä, hänen tulee joko poistaa tai siirtää ne omiin kansioihinsa, joiden nimestä yksityisyys on nähtävissä (esim. yksityisasiat). Tämä koskee sekä saapuvia että lähetettyjä viestejä.

Palvelussuhteen päätyttyä tai työntekijän kuollessa sähköpostilaatikkoon tai muihin sähköisiin välineisiin jääneet henkilökohtaiset viestit poistetaan eikä niitä luovuteta kuolinpesälle.

4.3.10 Muiden sähköpostiviestien käsittely

Kunnan ulkopuolinen sähköpostiosoite on yksityisasia, jota ei tässä tarkemmin ohjata. Työntekijä ei saa käyttää ulkopuolista sähköpostiosoitetta kuntaan liittyviin työtehtäviin ilman perusteltua hyvää syytä ja sen perusteella työnantajan antamaa lupaa.

Ulkopuoliseen sähköpostiosoitteeseen liittyvillä käyttäjätunnuksilla ei saa käyttää samoja salasanoja kuin kunnan järjestelmien käyttäjätunnuksilla.

Ulkopuolisen sähköpostiosoitteen ja -palvelun käyttö henkilökunnan tietokoneilta aiheuttaa riskejä sille, että postien mukana tulee haittaohjelmia. Tästä ja työajankäyttöön liittyvistä syistä henkilökohtaisten postipalveluiden käyttöä tulee välttää työpaikan tietokoneilla ja työaikana.

4.4 Palvelussuhteen tai opiskeluoikeuden päättyminen

Henkilön käyttöoikeus kunnan antamaan sähköpostiosoitteeseen päättyy siihen liittyvän palvelussuhteen, opiskeluoikeuden tai muun vastaavan päättyessä. Ulkopuolisten henkilöiden käyttöoikeuksien voimassaolosta vastaa tunnukselle määritelty vastuuhenkilö, yleensä käyttöoikeutta puoltaneen yksikön esihenkilö. Käyttöoikeuden päättymisen jälkeen ei enää oteta vastaan henkilölle lähetettyjä viestejä.

Ohjeita:

Ennen palvelussuhteen tai käyttöoikeuden päättymistä sähköpostikäyttäjän on hyvä ilmoittaa verkostolleen sähköpostiosoitteensa poistumisesta ja poistaa henkilökohtaiset viestit. Tärkeät tai tarpeelliset työviestit voi työntekijä tallentaa ns. offline-tiedostoon, jonka saa välitettyä esihenkilölle tai seuraajalle.

Sähköpostit sekä OneDrive-tallennuspaikan tiedostot ovat tarvittaessa palautettavissa 30 päivää palvelussuhteen päättymisen jälkeen.

Jos työntekijä on estynyt tai lakkaa hoitamasta tehtäviään jo ennen työsuhteen päättymistä, tulee esihenkilön ottaa yhteys Tukikeskukseen, jotta sähköpostin vastaanotto keskeytetään tai estetään jo siinä vaiheessa.

4.5 Menettely työntekijän ollessa väliaikaisesti tai pysyvästi poissa

Työnantajalla on oikeus lain yksityisyyden suojasta työelämässä (759/2004, 18–20§) asettamissa rajoissa saada käyttöönsä työnantajalle kuuluvat, sen toiminnan jatkumisen kannalta välttämättömät, viestit työntekijän ollessa estyneenä. Työntekijälle työsähköpostiosoitteella lähetettyjen tai tämän lähettämien viestien selville saaminen ja niiden avaaminen perustuu ensisijaisesti työntekijän suostumukseen sekä siihen että työntekijän luottamukselliset henkilökohtaiset viestit ovat erotettavissa työnantajalle selvästi kuuluvista viesteistä.

Ohjeita:

Mikäli työntekijä ei ole antanut toiselle, työnantajan hyväksymälle henkilölle edellä mainittua suostumusta taikka vakavan sairauden, kuoleman tai muun todellisen syyn takia häneltä ei voida saada suostumusta, voi hänen esihenkilönsä tai yksikön/organisaation päällikkö Tukikeskuksen avulla selvittää ja avata työntekijän poissa ollessa työsähköpostiviestit. Viestien etsinnän ja avaamisen syy, siihen osalliset ja ajankohta sekä kenelle avatusta viestistä on annettu tieto, on kirjattava ja ilmoitettava ilman aiheetonta viivytystä työntekijälle.

Jos työntekijä on pidempään estynyt tai lakkaa hoitamasta tehtäviään, tulee esihenkilön ottaa yhteyttä Tukikeskukseen, jotta sähköpostin vastaanotto keskeytetään tai estetään.

Kun kyse on työntekijän ennakoidusta poissaolosta, työntekijän ja esihenkilön on huolehdittava työntekijän sähköpostin asianmukaisesta hoidosta. Suositeltavin tapa on antaa tehtävään valitulle henkilölle postilaatikon lukuoikeus.

Suositeltavaa on myös laittaa Outlookiin poissaoloviesti. Poissaoloviestin sisällössä tulee huomioida järkevä kompromissi informatiivisuuden ja tietoturvan välillä.

Lisätietoja tämän asian soveltamisesta löytyy Työelämän tietosuojan käsikirjasta.

5 Sähköiset kyselyt

Ulkopuolelta tuleviin kyselyihin on syytä suhtautua epäileväisesti, sillä osa niistä on huijauksia tai puhdasta tietojen kalastelua rikollisiin tai vilpillisiin tarkoituksiin. Lähettäjä on helppo väärentää miksi tahoksi tahansa eli vaikka kysely näyttäisi tulevan esimerkiksi yhteistyökumppanilta, se ei välttämättä pidä paikkaansa. Kyselyitä voi tulla myös medialta tai yhteistyökumppanin kilpailijalta, joka voi yrittää saada tietoa kilpailijastaan tai esimerkiksi menossa olevasta kilpailutuksesta tai hankinnasta luvattomasti.

Kunnan henkilöstölle tarkoitetuissa ulkopuolelta lähetettävissä kyselyissä tulee olla nimetty sisäinen yhteyshenkilö, joka sisäisestä osoitteesta etukäteen tiedottaa kyselyn kohderyhmää kyselyn tarkoituksesta.

Kyselytyökalua valittaessa täytyy selvittää työkalun tallentamien tietojen sijainti, jotta voidaan varmistua siitä, että tietoja käsitellään turvallisesti ja henkilötietojen osalta EU:n yleisen tietosuoja-asetuksen mukaisesti.

Mikäli vastaajan henkilötietoja, esimerkiksi nimi ja sähköpostiosoite, välittyy vastauksien käsittelijöille, täytyy kyselyn alussa tämä selkeästi kertoa vastaajalle.

6 Sähköisten viestien salaus ja todentaminen

Salassa pidettävät asiakirjat tai muuta luottamuksellista informaatiota sisältävät viestit pitää lähettää aina suojattuina, vaikka vastaanottaja muuta ehdottaisi tai toivoisi.

Sähköpostit välittyvät ilman erityistoimenpiteitä aina suojatusti Tampereen kaupungin kanssa samassa postijärjestelmässä olevien Tampereen seudun kahdeksan muun kunnan kanssa (Hämeenkyrö, Kangasala, Lempäälä, Nokia, Orivesi, Pirkkala, Vesilahti ja Ylöjärvi).

Lisäksi tiettyjen ulkopuolisien toimijoiden osalta on toteutettu ns. TLS-salaus, joten viestit välittyvät automaattisesti suojattuina näihin organisaatioihin.

Käyttäjä voi erikseen salata muille tahoille lähetettävät viestit seudun sähköpostijärjestelmään erikseen hankittua salausmenetelmää käyttäen. Salaamisesta on olemassa erilliset ohjeet.

Salassa pidettävän tai suojattavan sisällön (esim. henkilötunnukset) käsittelyssä pitää aina olla erityisen huolellinen ja tarkistaa, että:

- sähköpostin vastaanottaja on valittu oikein ja että hänellä on oikeus saada tietoonsa salassa pidettäviä tietoja,
- yhteyshenkilö, kenen kanssa viestitään esimerkiksi Teamsilla äänen, videokuvan ja/tai pikaviestien välityksellä on oikein valittu,
- tietoja tai tiedostoja jaetaan tai näytetään vain tarpeellisessa laajuudessa.

7 Sähköisen kalenterin käyttö

Kokouksiin tulee ensisijaisesti lähettää kutsut sähköisinä kalenterikutsuina.

Kalenterimerkinnöissä on muistettava tietosuoja. Mitään salassa pidettävää aineistoa ei pidä tallentaa tai liittää kalenterikutsun yhteyteen siten, että se on sivullisille nähtävissä. Erityisesti otsikossa tämä asia on huomioitava, sillä se näkyy resurssikalentereissa kaikille.

Pääsääntöisesti Outlookin tai Teamsin kalentereihin ei pidä tallentaa salassa pidettäviä tietoja. Mikäli kuitenkin tällaista tietoa on välttämätöntä tallentaa kalenterimerkintään, tulee kalenterimerkintä merkitä yksityiseksi.

Ohjeita:

Kutsujan tulisi varmistaa etukäteen kalenterityökaluja käyttäen, että ajankohta olisi sopiva mahdollisimman monelle, jotta vältyttäisiin turhalta jälkikäteiseltä uusien ajankohtien etsimiseltä.

On syytä välttää sellaisien ajankohtien varaamista, jotka kokonaan tai osittain ajoittuvat virka-ajan ulkopuolelle tai vievät suuren osan tyypillisestä lounasajankohdasta. Mikäli muita vaihtoehtoja ei näytä löytyvän, on hyvä varmistaa ennen varaamista osallistujilta, onko tällainen ajankohta ok.

Mikäli osallistuja haluaa välittää kalenterikutsun edelleen jollekin toiselle henkilölle, olisi tästä hyvä vähintäänkin informoida alkuperäistä kutsun lähettäjää. Tämä koskee erityisesti läsnä kokouksia, joihin on saatettu varata sopivan kokoinen neuvottelutila tai tarjoiluja perustuen alkuperäiseen kutsulistaan. Myös asiasisältö saattaa olla tietosuoja-/luottamuksellisuussyistä sellainen, ettei kutsua pidä ilman lupaa lähettää eteenpäin.

Sähköisen kalenterikutsun vastaanottajan tulee hyväksyä tai hylätä kutsu siten, että siitä lähtee ilmoitus kutsujalle. Näin kutsuja saa kalenteriinsa tiedon siitä, ketkä ovat tulossa paikalle ja tarvittaessa hän voi ehdottaa uutta aikaa.

Sähköiseen kalenteriin tulee tehdä merkinnät työaikana olevista tapahtumista sisältäen muun muassa kokoukset, koulutukset ja muut tapaamiset. Kalenteriin tulisi selkeästi (mielellään "Poissa"-määreellä) merkitä myös lomat ja muut poissaolot, jolloin henkilö ei ole lainkaan töissä.

Kalenterin merkinnät voi tarvittaessa merkitä yksityiseksi. Tällöin on huomioitavaa, että myöskään ne henkilöt, joille kalenterinäkymät on jaettu, eivät saa kyseisen merkinnän sisältöä avattua.

Hakutoiminnolla voi etsiä tarvittaessa myös jälkikäteen merkintöjä.

Kalenteri voidaan halutessa jakaa avoimeksi kaikille tai määritellyille työntekijöille tai työntekijäryhmille. Tällöin kaikki merkinnät, jotka eivät ole yksityisiä, ovat näkyvissä jaetun kalenterin katselijoille. Kalenterin jaon yhteydessä voi määritellä sen, mitä toiset työntekijät voivat kalenterillasi tehdä tai siitä nähdä. Perusasetuksena kannattaa pitää sellaista asetusta, joka sallii toisten henkilöiden nähdä kalenterimerkinnöistä otsikon, ajan ja paikan, mutta ei muuta. Mikäli kalenteria ei ole ollenkaan jaettu toisille, pystyvät he kuitenkin palavereja järjestäessään tarkistamaan kalenterin avulla, onko henkilö vapaana vai varattuna kyseisenä aikana.

Palaverien/kokousten tilavarauksissa tulisi välttää oletettuun osallistujamäärään nähden kapasiteetiltaan räikeästi ylisuurten tilojen varaamista, koska tämä saattaa aiheuttaa ongelmia muille, jotka myöhemmin yrittävät löytää isommalle kokoukselle sopivaa tilaa.

7.1 Tilanvarauskäytännöt

Kokous- ja neuvottelutilat (resurssikalenterit) tulee olla nimetty yhdenmukaisesti, loogisesti ja helposti löydettäviksi toimipaikan nimen perusteella. Jokainen pystyy tekemään varauspyyntöjä resurssikalentereihin lisäämällä tilan resurssina omaan kalenteriin tekemäänsä kalenterikutsuun. Varauksien tekeminen suoraan neuvotteluhuoneen tai resurssin kalenteriin on normaalisti teknisesti estetty. Osa resurssikalentereista edellyttää sovitun tahon hyväksyntää ennen kuin varaus vahvistetaan. Erikseen hyväksyttävistä varauksista tulee aina sähköpostiin kuittaus siitä, onko varaus hyväksytty vai hylätty. Varauksia tulee tehdä vain tiloihin, joihin varaajalla on kulkuoikeus tai muutoin sovittu tilan haltijan kanssa pääsystä.

8 Teamsin käyttö viestinnässä ja kokouksissa

Teams-yhteydet ovat salattuja ja niitä voidaan pitää riittävän turvallisina salassa pidettävienkin asioiden käsittelemiseen, mikäli tarpeellista. Tämä kuitenkin edellyttää varmaa tietoa siitä, ketkä henkilöt ovat keskustelussa tai palaverissa mukana ja kyseinen salassa pidettävä tieto on luvallista näille kaikille kertoa tai luovuttaa. Tässä on tarve huomioida se, että neuvottelussa voi olla mukana henkilöitä myös nimettömänä puhelimella tai yksittäisen nimen takana voi olla useampikin henkilö yhteisen näytön ja kaiuttimien kautta. Henkilöitä voi tulla palaveriin myös lisää sen aikana.

Tampereen seudun järjestämissä kokouksissa ei saa käyttää ulkoisia tekoälyosallistujia, jotka tallentavat kokouksen tai laativat siitä yhteenvedon, jos siitä ei ole erikseen sovittu ja kyseisen tekoälykomponentin tietoturvallisuutta

varmistettu. Kokouksen järjestäjä vastaa tallentamisesta sekä tallenteen ja transkription jakamisesta.

Tarvittaessa viestin lähettävä osapuoli voi tehdä poiston Teams-keskustelussa, jolloin tieto poistuu kaikilta sekä myös palvelimelta. Eli mikäli on välttämätöntä välittää esimerkiksi jonkun henkilön henkilötunnus Teams-sovelluksen pikaviestiosuudella, niin se pitää viesteistä poistaa, jottei se jää tarpeettomasti tallennetuksi sovellukseen.

Aina pitää olla erityisen huolellinen siitä, että

- yhteyshenkilö(t), kenen kanssa neuvottelua käydään tai pikaviestitään, on oikein kutsuttu
- käyttäjä tietää mitä tietoja hän saa luovuttaa muille keskustelun osapuolille
- tiedostoja jaetaan tai näytetään vain tarpeellisessa laajuudessa
- pikaviesteihin liitetyt salassa pidettävät tai suojattavat tiedot poistetaan heti kun vastapuoli on viestit saanut.

Lisätietoa on seudullisessa Tietojenkäsittely pilvipalveluissa -ohjeessa.

Ohjeita:

Teams kokouksista voi tehdä kuva- ja äänitallenteen sekä myös tekstitallenteen keskustelusta. Tallentaminen mahdollistaa kokouksen tai koulutuksen sisällön kertaamisen ja sen näkemisen myös niille, jotka eivät pysty kokoukseen osallistumaan sovittuna aikana. Tekstitallenne (litterointi, transkriptio) mahdollistaa nopeasti etsiä tietoa kokouksen sisällöstä ilman tarvetta kuunnella koko tallennetta. Se mahdollistaa myös tekoälyn (Copilot) avulla muistion, tiivistelmän, kysymysten tai hakujen tekemisen jälkikäteen kokouksesta. On syytä kuitenkin huomioida, että tekstitallenteessa voi olla useitakin virheitä sanoissa, jotka tekniikka on tunnistanut väärin. Usein esimerkiksi nimet tai lyhenteet saattavat olla tallenteella virheellisesti kirjoitettuja eli joka tapauksessa tiedot on syytä aina tarkastaa ennen käyttöä.

Kokouksen järjestäjä on velvollinen selvittämään tallennuksen tarpeellisuuden ja käyttämisen sekä tekee päätöksen tallentamisesta. Tallentamisesta tulee kertoa kokouksen tai tilaisuuden alussa ja mielellään jo kutsussa. On hyvä myös kertoa se, miten tallennetta käytetään ja kauanko sitä säilytetään. Järjestäjä voi myös tarvittaessa keskeyttää tai päättää tallentamisen, mikäli kokouksessa halutaan keskustella ilman tallentamista. Jos tilaisuudessa on ulkopuolinen esiintyjä, tulee häneltä kysyä etukäteen lupa, saako esityksen hänen puolestaan tallentaa.

Mikäli tallennat kokouksen, on hyvä antaa Teamsin tehdä siitä myös tekstitallenne.

Jos Teams kokouksen osallistujalistassa havaitaan ulkoinen tekoälyavustaja, jota ei ole etukäteen sovittu tai hyväksytty, on se syytä heti todeta ääneen. Kokouksen järjestäjän tai tekoälyavustajan tuoneen osallistujan tulee poistaa avustaja ennen kokouksen jatkamista.

9 Tekstiviestien ja (sosiaalisen median) viestintäpalveluiden käyttö

Matkapuhelimesta tai tietojärjestelmästä matkapuhelimeen lähetettävät tekstiviestit (SMS-viestit) ja multimediaviestit (MMS-viestit):

- Mikäli asiakkaalle lähetetään salassa pidettäviä tietoja pitää asiakkaalta pyytää ensin suostumus ja varmistaa matkapuhelinnumero. Asiakkaan pitää olla tunnistettu. Suostumus pitää kirjata asiakastietojärjestelmään tai liittää muulla tavoin osaksi asiakastietoja.
- Huomioi, että MMS-viestit käyttäytyvät eri lailla kuin SMS-viestit, jos niitä lähettää usealle vastaanottajalle. MMS-viestien vastaanottajat näkevät kaikkien vastaanottajien puhelinnumerot ja tämä on kiellettyä silloin kun asiakassuhde on salassa pidettävä. Yleisesti asiakasviestinnässä tämä ei ole hyvä asia. Monet puhelinmallit lähettävät alun perin tekstiviestinä kirjoitetun viestin MMS-viestinä, jos sen pituus ylittää tietyn rajan tai viestiin sisällyttää erikoismerkkejä esimerkiksi hymiöitä. Tämä asia vaihtelee lähettäjän tahon puhelinmalliin liittyen.

WhatsApp, Facebook, Instagram, Messenger, Signal, Snapchat, X, LinkedIn tai muita vastaavia julkisiin pilvipalveluihin perustuvia viestintäpalveluita ei saa käyttää suojattavien henkilötietojen, kuten henkilötunnuksien, eikä salassa pidettävien tietojen käsittelyyn. Sama koskee myös erilaisia asiakasrajapinnassa käytettäviä keskusteluvälineitä tai chat-palveluita.

Edellä mainituissa sovelluksissa usein riskinä on se, että ne tallentavat viestejä keskustelussa mukana oleville laitteille sekä myös ulkoiseen pilvipalveluun, joista ne voivat päätyä sivullisille ja tietojen elinkaarta ei pystytä hallitsemaan. Mikäli vastaanotat salassa pidettäviä tietoja esimerkiksi kuntalaisilta näillä viestintävälineillä, siirrä tarvittavat tiedot heti turvallisempaan paikkaan ja poista ne omalta osaltasi turvattomasta viestintäsovelluksesta pienentääksesi riskejä.

Älä sokeasti luota sosiaalisen median kautta tuleviin viesteihin, sillä sosiaalisessa mediassa on helppo tehdä toisten nimissä tunnuksia tai kaapata toisen henkilön sähköinen identiteetti. Henkilön oikea valokuva ja/tai nimi palvelussa ei takaa, että tunnuksen haltija on kyseinen henkilö itse.

TikTok- ja Telegram-sovelluksien, sekä muidenkin tietoturvan tai tietosuojan kannalta epäluotettavissa maissa tehtyjen viestintäsovellusten, asentaminen ja käyttö työlaitteilla on kiellettyä. Jos TikTok tai Telegram ovat välttämättömiä työtehtävissä, sallitaan siihen käyttöön erillinen työlaite, jolla ei tehdä muita työtehtäviä.

Ohjeita:

Se, kuinka turvallinen ja luotettava internetin verkkopalvelu tai puhelinsovellus on, vaikuttaa merkittävästi siihen, mihin tarkoitukseen palvelua voit käyttää. Tärkeää on yleensäkin huomioida, onko palvelun käyttämä yhteys salattu sekä minne ja miten tiedot tallennetaan. Oleellista on myös se, kenellä on järjestelmään syötettyjen tietojen omistus- ja/tai käyttöoikeus sekä kenelle tiedot näkyvät tai kuka niitä pääsee katsomaan. Tärkeää on myös tutustua kyseisen palvelun käyttöehtoihin (sallitaanko esimerkiksi työkäyttö ja mitä se maksaa) sekä palvelun tietosuojaan (esimerkiksi miten käyttäjän tietoja suojataan, käytetään tai luovutetaan ja missä niitä säilytetään).

Se, että joku palvelu on jo käytössä jossain muussa organisaatiossa ei vielä takaa sitä, että se olisi laillinen, turvallinen tai järkevä käyttää!

Aina pitää tarkastaa hyvin, että viestin saajan numero tai nimi on sama, jonka asiakas tai yhteistyökumppani on kertonut.

Viestistä pitää käydä ilmi selvästi kuka ja missä roolissa viestin lähettää.

Muista tietosuoja ja tietoturva myös valmisteilla olevissa asioissa eli älä tiedota niistä sosiaalisessa mediassa ennen kuin ne ovat julkisia. Julkisista artikkeleista kannattaa jakaa vain sellaisia linkkejä, jotka aukeavat ilmaiseksi luettaviksi kansalaisille. Esimerkiksi Tampereen kaupungin uutisia ei kannata jakaa vain tilaajille aukeavina Aamulehden Tähtijuttuina, vaan kaupungin oman nettisivun linkkinä alkuperäiseen tiedotteeseen.

10 Tekoälyratkaisut

Tampereen seudun Microsoft-ympäristössä työtunnuksilla kirjautuneena Microsoft Copilot -tuoteperheen käyttö on sallittua. Työntekijöitä kannustetaan kokeilemaan ja käyttämään toimisto-ohjelmien sisällä toimivia tekoälyratkaisuja. Lisäksi kannattaa hyödyntää tiettyihin tarkoituksiin valmiiksi räätälöityjä tekoälyapureita (nk. agentteja, botteja), jotka keskustelevat määrittelemästäsi aineistosta ja suorittavat automaatioita antamiesi ohjeiden perusteella. Voit myös tehdä omia apureita ja jakaa niitä sisäiseen käyttöön.

Copilotin lisäksi Tampereen seudulla voidaan hyödyntää organisaation (kunnan) varmistamia ja järjestämiä muita tekoälyratkaisuja. Tällaisilla ratkaisuilla tarkoitetaan tekoälypalveluja, joiden käyttö on etukäteen arvioitu käyttötarkoitukseen soveltuvana niin tietosisällön, lainsäädännön kuin viranomaistoiminnan vaateiden mukaisesti.

Työtunnuksilla kirjautuneena voit käsitellä Copilotin avulla myös sisäisiä ja salassa pidettäviä tietoja ellei sitä ole kyseisen tiedon osalta erikseen kielletty. Työtunnuksia käytettäessä Copilotille annetut tiedot tai tiedostot eivät päädy Tampereen seudun ulkopuolelle eikä Microsoft käytä niitä tekoälyn kouluttamiseen.

Julkisissa tekoälyratkaisuissa ei saa käsitellä salassa pidettävää tai sisäiseen käyttöön tarkoitettua tietoa. Julkisilla tekoälyratkaisuilla tarkoitetaan tässä ohjeessa kuluttajakäyttöön suunnattuja tuotteita, jotka ovat kenen tahansa käytettävissä tai sellaisia kaupallisia tuotteita, joita ei ole taustaselvitetty ja hyväksytty työkäyttöön. Julkisissa tekoälypalveluissa käyttäjän antamia tietoja tai dokumentteja saatetaan käyttää esimerkiksi palvelun kehittämiseen tai palvelua tuottavan yrityksen muihin omiin käyttötarkoituksiin. Esimerkkejä kuluttajille suunnatuista tekoälypalveluista ovat ChatGPT, Gemini ja Grok.

Lähtökohtana on, että sopiva työkalu valitaan keskitetysti tarjotuista ratkaisuista. Uusien tekoälyratkaisujen lisääminen käytettäväksi tehdään keskitetysti ja käyttöönotto projektoidaan.

Tekoälyratkaisuja ei oteta käyttöön ilman tarvittavia vaikutustenarviointeja (muutos- ja kustannusvaikutukset, tietoturvan ja tietosuojan vaikutukset, perusoikeusvaikutusten arviointi). Erityisen tärkeää tämä on suuririskisessä tekoälyn käytössä (EU:n tekoälyasetus (EU) 2024/1689). Kunta voi teknisesti kokonaan estää haitallisiksi tai vaarallisiksi arvioitujen tekoälypalvelujen käytön.

Tekoälyratkaisusta tehdään aina taustaselvitys (esimerkiksi projektipäällikön koordinoimana), jossa arvioidaan käytettävän ratkaisun soveltuvuus riskiperusteisesti toimintaan ja toimintaympäristöön huomioiden digitaalinen turvallisuus ja lainsäädännön vaatimukset.

Tekoälyratkaisulle täytyy määrittää omistaja ja vastuuhenkilö. Uusia ratkaisuja hankittaessa ja käyttöönotettaessa tulee olla yhteydessä kunnan tietohallinnon asiantuntijoihin. Osaan palveluista liittyy mutkikkaita käyttö- ja lisenssiehtoja sekä tietoturvaan ja tietosuojaan liittyviä asioita, jotka pitää arvioida ennen käyttöönottoa. Tuotteita ei saa koskaan käyttää niiden käyttöehtojen vastaisesti.

Oman kunnan tekoälyn hallintamallissa tai vastaavassa ohjeistuksessa voidaan määritellä toimeenpanoa ja tarkentavia käytäntöjä. Seudun kuntien tulee pitää kirjaa tekoälyratkaisuistaan (tekoälyrekisteri).

Käyttöönotossa tulee aina soveltaa oman kunnan hyväksymiä tekoälyn eettisiä periaatteita. Seudun ja kunnan oman ohjeistuksen määrittelemissä rajoissa palvelualueet ja toimintayksiköt määrittelevät itse, mitä työkaluja ja käyttötapoja on eri työtehtävissä sallittua käyttää.

Kun kunta ulkoistaa palveluitaan toimeksiantona, pitää huolehtia siitä, että ulkoistuskumppani noudattaa Tampereen seudun tekoälyn käytön linjauksia.

Dataa ja tekoälyä hyödyntäviä palveluita kehitetään kuntalaisten hyväksi ja heitä kuunnellen. Tekoälyjärjestelmä ei voi tyypillisesti oppia kaikkia mahdollisia tilanteita. Virhepäätelmän tai teknisen vian riski on aina olemassa. Kun järjestelmä on ihmisen kontrollissa, voidaan reagoida yllättäviin tilanteisiin ja vaikutuksiin. Ihmisen kontrolli tulee pysyä kaikissa tekoälyratkaisujen elinkaaren vaiheissa suunnittelusta käytön lopettamiseen.

Kun tekoälyä käytetään sisällön tuottamiseen, on tekoälyn tuottamat materiaalit aina tarkistettava ennen käyttöä tai edelleen lähettämistä. Kielimalleihin perustuva tekoäly saattaa yhdistellä tietoja väärin, materiaali voi sisältää salassa pidettävää tietoa ja vakuuttavan oloinen teksti voi olla täysin perätön.

Materiaalien julkaisija on vastuussa sisällöstä. Mikäli tekoäly tuottaa vaarallista tai muuten epäilyttävää ja sopimatonta materiaalia, pitää tilanne dokumentoida kopioimalla tekstit, ottamalla kuvakaappauksia tai tallentamalla mahdolliset virhe- ja lokitiedot analysointia varten. Poikkeamista pitää ilmoittaa eteenpäin ensisijaisesti kyseisen tekoälyratkaisun vastuuhenkilölle, mutta tarvittaessa myös havaitsijan omalle esihenkilölle tai Tukikeskukseen. Tietoturva- ja tietosuojapoikkeamista ilmoitetaan kunnan sovitun prosessin mukaisesti tietoturvasta ja tietosuojasta vastaaville henkilöille.

Tekoälysovelluksia ei saa käyttää rikollisiin tarkoituksiin tai kiusaamiseen eikä pilailumielessäkään esimerkiksi niin sanottujen deep fake -huijausvideoiden tekemiseen.

11 Käytön valvonta sekä lokitietojen kerääminen ja säilyttäminen

Internetin, laitteiden ja sovellusten käytöstä tallentuu erilaisia lokitietoja tilanteen mukaan käytettyyn laitteeseen, työnantajan palvelimille, tietoturvajärjes-

telmiin, tietoliikenneoperaattorille sekä käytetyn pilvipalvelun tai palvelun/sovelluksen palvelimille. Lokitietojen tallennusaika vaihtelee tarpeen ja toimijan mukaan.

Internet-liikennettä saa raportoida tilastollisesti ainoastaan siten, ettei se kytkeydy yksittäisiin käyttäjiin. Lokitietoja kerätään automaattisesti ja niitä käytetään virhetilanteiden, ongelmien ja mahdollisten väärinkäytösten selvittämiseen, tietoturvan ja tietosuojan parantamiseen sekä palveluiden kehittämiseen.

Työasemiin, mobiililaitteisiin ja verkon välimuistipalvelimiin voi tallentua myös kokonaisia www-sivuja, joita käyttäjä on selannut. Tietojen säilytysaika käyttäjän laitteissa riippuu muun muassa selaimen asetuksista. Käyttäjän tulee ottaa huomioon, että saman koneen mahdolliset muut käyttäjät voivat päästä käsiksi näihin tietoihin. Käyttäjä voi itse poistaa laitteisiinsa tallentuvia tietoja internet-selaimen asetusten kautta.

12 Näiden määräysten valvonta

Näiden määräysten valvonnasta vastaavat kunkin kunnan esihenkilöt, tietohallinto sekä ICT-palvelusta vastaavat tahot. Mikäli sähköisten viestintävälineiden käyttäjä havaitsee näiden käyttösääntöjen vastaista menettelyä omassa tai muiden toiminnassa, tulee siitä viivytyksettä ilmoittaa omalle esihenkilölle ja/tai oman kunnan tietohallinnolle. Jokaisen tulee myös ilmoittaa havaitsemistaan tietoturvallisuuteen liittyvistä puutteista, väärinkäytöksistä tai niiden epäilyistä eteenpäin tietohallinnon erikseen ohjeistamalla tavalla. Mikäli kyseiseen tilanteeseen ei ole soveltuvaa ohjetta käytettävissä, tulee ilmoitus tehdä omalle esihenkilölle ja/tai Tukikeskukseen, jotka puolestaan välittävät tiedon eteenpäin.

Jos henkilö toimii vastoin näitä sääntöjä, hänen käyttöoikeuksiaan voidaan rajoittaa joko väliaikaisesti tai pysyvästi. Lisäksi työnantaja voi ryhtyä muihin tarvittaviin työoikeudellisiin ja rikosoikeudellisiin toimenpiteisiin ja vaatia vahingonkorvauksia.

Nämä käyttösäännöt päivitetään tarvittaessa. Päivitystarvetta seuraa Seudun tietoturvaryhmä. Organisaatiomuutoksista, laeista tai muista vastaavista muutoksista johtuvia teknisiä korjauksia tähän dokumenttiin voi Seudun tietoturvaryhmä tehdä ilman erillistä uutta laajempaa hyväksyntäkäsittelyä.

13 Dokumentin versiohistoria

Versio (päivämäärä)	Päivittäjä tai hyväksyjä	Tehdyt muutokset
23.3.2016	Tietohallinnon seudullinen johtoryhmä	Versio, johon on yhdistetty Tampereen kaupungin ja seudun aiemmat erilliset linjaukset.
9.5.2016	Tietohallinnon seudullinen johtoryhmä	Ensimmäinen hyväksytty versio.
18.12.2020	Seudun tietoturvaryhmä	Useita teknisiä korjauksia dokumentin sisältöön.
22.11.2023	Tietohallinnon seudullinen johtoryhmä	Lakimuutoksista, SOTE-irtautumisesta ja sovellusten muutoksista johtuvia päivityksiä useimpiin lukuihin sekä kokonaan uusi tekoälyä käsittelevä luku.
28.1.2026	Tietohallinnon seudullinen johtoryhmä	Useita muutoksia, joista isoimmat liittyen yksityiskäyttöön (luku 2), kalenterien salassa pidettäviin tietoihin (luku 7), Teams kokouksiin (luku 8), tekoälyyn (luku 10) ja valvontaan/lokitukseen (luku 11).