Utajärven kunta

TIETOTURVAPOLITIIKKA

Johdanto

Tiedon käsittely on oleellinen osa Utajärven kunnan toimintaa ja palveluiden tuottamista. Tietojenkäsittelyn tehokkuus ja virheettömyys ovat keskeisiä tekijöitä palvelutuotannon tehokkuudelle ja laadulle. Käytettävät tietoaineistot sisältävät usein asiakkaisiin, työntekijöihin ja toimintaan liittyvää tietoa, joka on lainsäädännön perusteella suojattava.

Tiedon turvaaminen on oleellista koko organisaation toiminnan kannalta. Tietoturvan hyvä hallinta edellyttää toiminnan jatkuvaa seurantaa, pitkäjänteistä suunnittelua ja riittävää resursointia erilaisten uhkatilanteiden varalta. Tietoturvan toteuttaminen vaatii sovittujen ohjeiden ja toimintatapojen noudattamista, koulutusta ja viestintää.

Tietoturvapolitiikka on Utajärven kunnan johdon kannanotto tietoturvan toteuttamiseen. Se määrittelee ne yleisperiaatteet, tavoitteet ja vastuut, joita noudatetaan tietoturvan toteuttamisessa ja kehittämisessä.

Utajärven kunnanhallituksen vahvistama tietoturvapolitiikka kattaa Utajärven kunnan kaikkeen toimintaan liittyvät tietojenkäsittelyn tehtävät. Jokaisen Utajärven kunnan viranhaltijan, työntekijän ja luottamushenkilön sekä toimintayksikön tietojen ja tietojärjestelmien käyttäjän on tunnettava tietoturvapolitiikka ja noudatettava sen perusteella annettuja ohjeistuksia ja määräyksiä. Organisaation ulkopuolisten toimijoiden tulee myös sitoutua noudattamaan tätä tietoturvapolitiikkaa, kansallisia normeja sekä ohjeita ehtona tehtäviensä mukaiselle pääsylle toimintayksikön tietojärjestelmiin ja niiden tietoaineistoihin.

Tietoturvapolitiikkaa täydentävät ja täsmentävät erilaiset tietoturvaperiaatteet, käyttöohjeistukset ja säännökset, joita ovat:

- ICT-järjestelmien käyttäjäsitoumus Utajärven kunnan henkilöstölle (liite 1).

Tietoturva ja tietosuoja

Tietoturva tarkoittaa tietojen käsittelyn ja arkistoinnin turvaamista. Tietoturva rakentuu tiedon luottamuksellisuudesta, eheydestä, saatavuudesta, käytettävyydestä ja kiistämättömyydestä sekä tietojen käsittelyn valvonnasta.

Tietoturvaan kuuluvat tietoturvaorganisaatio, tietojen käsittelijöiden toimintatavat, tietojen turvaamisen menetelmät, välineet ja toimenpiteet, työhön osoitetut resurssit sekä välineistön ja tilojen tietoturvaominaisuudet.

Hyväksytyn tietoturvapolitiikan mukainen tietoturva sisältyy luonnollisena osana kaikkeen toimintaan. Tietoturvan kehittäminen ja ylläpito ovat osa toimintayksikön yleistä turvallisuustoimintaa, riskien hallintaa ja sisäistä valvontaa.

Tietosuojalla tarkoitetaan henkilötietojen suojaamista valtuudettomalta ja henkilöä vahingoittavalta käsittelemiseltä. Tietosuojaan kuuluvat yksityisten henkilöiden yksityisyydensuoja sekä sitä turvaavat oikeudet ja edut henkilötietoja käsiteltäessä. Sosiaali- ja terveyspalveluita tuottavan toimintayksikön tietosuojaa ohjaavat voimakkaasti asiakastietojen käsittelystä säädetyt lait ja määräykset.

Tietoturvan tavoitteet

Utajärven kunnan tietoturvatyön tavoitteena on turvata kunnan toimintaa tukevien tietojärjestelmien ja tietoverkkojen keskeytymätön toiminta, havaita ja estää tietojen ja tietojärjestelmien luvaton käyttö, tiedon tahaton tai tahallinen tuhoaminen tai vääristäminen sekä minimoida niistä mahdollisesti aiheutuvat vahingot.

Tietoturvatason tulee mukautua tilanteen, palvelun, standardien ja lakien edellyttämiin vaatimuksiin. Lähtökohtana on, että kunnan tiedot ja tietojärjestelmät suojataan asianmukaisesti sekä normaali että poikkeusoloissa hallinnollisin ja teknisin toimenpitein. Normaaliajan toiminnan tietojenkäsittelyn turvaamisen lisäksi varaudutaan toiminnan keskeyttäviin uhkatilanteisiin ja niistä toipumiseen.

Tietoturvatyön tavoitteena on sisällyttää hyväksytyn tietoturvapolitiikan ja sitä täydentävien tietoturvaperiaatteiden ja –ohjeiden mukainen tietoturva luonnollisena osana kaikkeen Utajärven kunnan toimintaan. Tämä tarkoittaa henkilökunnan, yhteistyökumppaneiden ja alihankkijoiden sitouttamista Utajärven kunnan tietoturvakäytäntöihin ja vastuuttamista huolehtimaan käsiteltävien tietojen tietoturvasta. Tietoturvatyön tavoitteena on ylläpitää kuntalaisten ja eri sidosryhmien luottamusta kuntayhtymän tarjoamiin perinteisiin ja sähköisiin palveluihin sekä niiden tietoturvan, tietosuojan ja yksityisyydensuojan toteutumiseen.

Organisointi ja vastuut

Organisointi

Kokonaisvastuu tietoturvan toteutumisesta on Utajärven kunnan hallituksella ja kunnanjohtajalla. Kunnan johto päättää kunnan kokonaisturvallisuuden eri osa-alueiden kehittämistoiminnan tavoitteista, organisoinnista, resursseista ja toimintavaltuuksista sekä nimeää tietoturvavastaavan ja tietosuojavastaavan.

Kunnan tietoturvatyön kokonaisuudesta vastaa tietoturvaryhmä kunnan johdolta saamiensa resurssien ja toimintavaltuuksien puitteissa. Tietoturvaryhmä käsittelee tietoturvan linjaukset ja ohjeet ennen kuin ne esitellään johdolle hyväksyttäväksi ja vastaa tietoturva-asioista tiedottamisesta Kunnan ulkopuolelle ja kunnassa yleisellä tasolla. Kunnanjohtajan nimeämään tietoturvaryhmään kuuluvat ainakin xxxxxxxxx (ketä kunta sitten tähän määrääkään?). Kunnanjohtaja nimeää tietoturvatyöryhmälle puheenjohtajan ja koollekutsujan.

Kunnan asiakastietoja sisältävien henkilörekistereiden suojaamisesta ja valvonnasta vastaa tietosuojavastaava. XXXXX kunnan tietosuojavastaavana toimii xxxxxxxx.

XXXX vastaa XXXX kunnan hallinnollisen tietoturvan järjestämisestä, kehittämisestä ja seurannasta.

Oulunkaaren kuntayhtymä tuottaa Utajärven kunnan sosiaali- ja terveydenhuollon palvelut ja vastaa omaan toimintaansa liittyvästä tietoturvan kokonaisuudesta.

Oulunkaaren kuntayhtymä tuottaa Utajärven kunnalle tekniset ICT-palvelut. Oulunkaaren kuntayhtymän tietohallintopäällikkö vastaa kuntayhtymän ja kunnan teknisen tietoturvan järjestämisestä, kehittämisestä ja seurannasta. Tietohallintopäällikkö toimii Oulunkaaren kuntayhtymän tietoturvavastaavana.

Vastuut

Utajärven kunnan eri palvelualat vastaavat tietoturvan toteutumisesta omassa toiminnassaan sekä hankkimissaan ostopalveluissa. Palvelualojen johdon ja kuntaan nimettyjen tietoturva- ja tietosuojavastaavien tulee huomioida toiminnan erityispiirteet ja lainsäädäntö sekä selventää tietoturvavastuut omissa yksiköissään.

Jokaiselle tietovarastolle ja tietojärjestelmälle määritetään omistaja, joka vastaa järjestelmänsä toiminnasta ja tietoturvan kehittämisestä ja toteuttamisesta. Omistajien tehtävänä on mm. kartoittaa tietojärjestelmiensä toimintaan liittyvät riskit, huolehtia tietojenkäsittelyn luottamuksellisuudesta, tietojen oikeellisuudesta, pääsyn valvonnasta ja toimintojen jatkuvuudesta. Jokaisesta tietojärjestelmästä laaditaan tarvittavat dokumentit.

Kunnan työntekijöiden vastuulla on huolehtia siitä, että heidän työtehtävissään käsittelemät, organisaatiolle kuuluvat tiedot jäävät organisaation haltuun ellei niitä muilla määräyksillä ole määrätty hävitettäviksi.

Esimiesten tehtävänä on vastata siitä, että työntekijöillä on oikeudet tehtävän edellyttämässä laajuudessa tarvittaviin tietojärjestelmiin ja tietoihin, myös työtehtävien mahdolliset muutokset huomioiden. Työsuhteen päättyessä on huolehdittava käyttöoikeuksien poistamisesta tietojärjestelmiin. Esimiesten tehtävänä on huolehtia myös siitä, että alaiset saavat riittävän perehdytyksen ja koulutuksen tietoturvaan ja siitä, että työntekijät ymmärtävät tietoturvan merkityksen. Esimiehiltä odotetaan esimerkillistä ja vastuullista tietoturvakäyttäytymistä.

Tietoturvan toteutus

Tietoturvan toteuttamisen perusteena on tässä dokumentissa kuvattu ja kunnan hallituksen hyväksymä Utajärven kunnan tietoturvapolitiikka. Tietoturvan toteuttamisen lähtökohtana on tietoturvapolitiikan tehokas viestiminen koko organisaatiolle.

Utajärven kunnan tietoturvaperiaatteet perustuvat kansallisiin, yleisiin ja toimialakohtaisiin tietoturvaa, henkilörekistereitä, hyvää tiedonhallintatapaa ja tiedon laatua ohjaaviin velvoittaviin säädöksiin, ohjeisiin ja standardeihin. Lainsäädännön ja ohjeistusten muutokset otetaan huomioon toimintayksikön tietoturvan kehittämisessä.

Tietoturvan tavoitteiden saavuttaminen on jatkuva prosessi, joka tapahtuu hallinnollisten ja teknisten ratkaisujen avulla. Käyttäjien toimintaa ohjataan käyttösäännöillä ja toimintaohjeilla sekä tietoturvakoulutuksella. Kunnan työntekijöiden käytössä on verkko-oppimateriaali, joka antaa yleisen perehdytyksen tietoturva- ja tietosuoja-asioihin. Tavoitteena on, että jokainen työntekijä suorittaa verkko-opintokokonaisuuden ja osoittaa osaamisensa siihen tarkoitetulla testillä.

Jokaisen kunnan tietoverkkojen ja tietojärjestelmien käyttäjän tulee noudattaa hyväksyttyjä tietoturvaperiaatteita ja –ohjeita, joiden noudattamiseen jokainen käyttäjä sitoutuu allekirjoittamalla ICT-järjestelmien käyttäjäsitoumuksen. Käyttäjäsitoumuksen allekirjoittaminen on edellytys tehtävien mukaisten tietojärjestelmien ja tietoaineistojen käyttöoikeuksien saamiselle. Esimiesten tehtävänä on valvoa tietoturvaohjeiden noudattamista ja tietoturvan toteutumista yksiköissään ja työntekijöiden keskuudessa.

Käytännön teknisestä tietoturvasta ja sen ohjeistuksesta vastaavat palveluntuottajat, joille palvelun toteutus on sopimuspohjaisesti luovutettu. Kaikkiin palvelusopimuksiin sisällytetään tietoturvaan liittyvät vaatimukset, velvoitteet, häiriötilanteiden toimintamallit ja määritellään vastuuhenkilöt läpi koko palveluketjun. Palvelutuottajan vastuulla on raportoida tietoturvaan kohdistuvista merkittävistä ris-

keistä välittömästi palvelusopimuksessa määritellyille yhteyshenkilöille. Jokaisen työntekijän velvollisuus on ilmoittaa havaitsemistaan tietoturvaan liittyvistä puutteista tai väärinkäytöksistä esimiehelleen tai tietosuojavastaavalle.

Jokaisella kuntayhtymän tietojärjestelmällä on nimetty omistaja, joka osaltaan vastaa tietojärjestelmän tietoturvan toteutumisesta. Järjestelmän omistajuuteen liittyvät tiedot dokumentoidaan rekisteri- ja tietojärjestelmäselosteessa. Kaikki tietojärjestelmät ja tietovarastot on luokiteltava niissä käsiteltävien tietojen ja tunnistettujen tietoturvariskien mukaisesti. Tietojen ja tietojärjestelmien omistajien on tehtävä luokittelua vastaavat riskikartoitukset ja tietoturvaohjeet käyttäjille sekä huolehdittava, että työntekijät saavat riittävän koulutuksen. Riskikartoitusten toteutumista ja ohjeiden noudattamista on seurattava aktiivisesti. Lisäksi omistajien on ylläpidettävä ajantasaisia varautumissuunnitelmia, joissa on kuvattu vastuuhenkilöt, roolit ja toimintamallit riskien toteutumisen varalta.

Tietoturvan seuranta ja valvonta

Tietoturvapolitiikan ja –ohjeiden noudattamisen valvonta on tärkeä osa kunnan sisäistä valvontaa. Tietoturvatyöryhmä ja kunnan johtoryhmä seuraavat teknisen ja hallinnollisen tietoturvan toteutumista ja niillä on oikeus toimeenpanna tietoturva-auditointeja.

Käyttäjien ja tietojärjestelmien ylläpitäjien tulee ilmoittaa havaitsemastaan tietoturvan puutteesta, tietoturvaan liittyvästä väärinkäytöksestä tai epäilemästään tietoturvarikkomuksesta esimiehelleen, tietosuojavastaavalle tai tietoturvavastaavalle.

Esimiesten tehtävänä on valvoa tietoturvan toteutumista omassa yksikössään ja raportoida tietoturvaloukkauksista tietosuojavastaavalle tai tietoturvavastaavalle.

ICT-palveluiden tuottajilla on velvollisuus raportoida säännöllisesti tietoturvaan liittyvistä palvelutasojen täyttymisestä ja riskeistä tietohallintopäällikölle.

Tietosuojavastaavan tehtävänä on valvoa kuntayhtymän potilas- ja asiakastiedon käsittelystä säädetyn lain ja ohjeistusten toteutumista ja ryhtyä toimenpiteisiin havaittujen tietosuojan heikkouksien korjaamiseksi.

Tietoturvavastaavan tehtävänä on seurata ja valvoa kuntayhtymän tietojärjestelmien tietoturvan toteutumista ja ryhtyä toimenpiteisiin havaittujen tietoturvan heikkouksien korjaamiseksi.

Tietoturvaloukkauksissa tai tietoturvaan liittyvässä uhkatilanteessa tietohallintopäälliköllä on oikeus sulkea tietty tietoliikenneyhteys, tietojärjestelmä, käyttäjätunnus tai laite. Tietohallintopäällikön on viipymättä tai heti kun se on mahdollista, informoitava asianosaisia tehdyistä toimenpiteistä ja mahdollisista jatkotoimenpiteistä.

Tiedottaminen

Tietoturva-asioihin liittyvästä sisäisestä tiedottamisesta vastaavat tietoturvatyöryhmä ja tietohallinpäällikkö yhteistyössä kunnan viestinnän kanssa. Tietohallintopäällikkö, tietosuoja-asiantuntija ja ICT-palvelutuottajat ylläpitävät käyttäjien saatavilla käytännön tietoturvaohjeita ja tiedottavat akuuteista tietoturvauhkista sekä suojautumiskeinoista. Ensisijainen sisäisen viestinnän tiedotuskanava on kunnan intranet.

Tietoturva-asioihin liittyvästä ulkoisesta tiedottamisesta vastaa tietohallintopäällikkö yhdessä kunnan viestinnän kanssa. Poikkeusolojen tiedottamisesta vastaa kunnanjohtaja.

Liitteet:

Liite 1. ICT-järjestelmien käyttäjäsitoumus

Muutoshistoria

Versio	Päivämäärä	Muutoksen sisältö	Tekijä / hyväksyjä
0.1	30.6.2016	XXXXXX kunnan tietoturvapolitiikka	Matti Matero
1.0		Tietoturvapolitiikan hyväksyminen	Kunnanhallitus XXXXX kunta