Tietoturvapolitiikka

Hyväksytty:
Voimaantulo 1.1.2025

Pöytyän kunta | Puh. (02) 481 000 | Kehityksentie 6, 21800 Kyrö
www.poytya.fi
Kyrön toimipiste, Kehityksentie 6, 21800 Kyrö
Riihikosken virastotalo, Yläneentie 11 b, c-rappu, 21870 Riihikoski

Pöytyä

Sisällys

Pöytyä

1. Keskeisiä käsitteitä

Tietoturva
Tietoturvalla varmistetaan tietojen luottamuksellisuus, eheys ja saatavuus. Tietoturvaan sisältyy muun muassa tietojen, tietoaineistojen, laitteistojen, ohjelmistojen, tietoliikenteen, tilojen ja toiminnan turvaaminen. Tietoturva liittyy tietosuojaperiaatteiden toteuttamiseen muun muassa organisatorisilla ja teknisillä toimenpiteillä.

Tietosuoja
Tietosuoja tarkoittaa jokaisen oikeutta henkilötietojensa suojaan. Se turvaa rekisteröityjen oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä. Tietosuoja määrittelee ne perusperiaatteet, miten, milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä.

Luottamuksellisuus
Luottamuksellisuus eli se, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla. Tiedot suojataan luotettavasti ja oikeus käsitellä tietoja perustuu työtehtävien mukaiseen tarpeeseen ja vähimpien oikeuksien periaatteeseen. Tietojen ja järjestelmien käyttäjät tunnistetaan luotettavasti.

Eheys
Eheys eli se, että tietoja eivät voi muuttaa muut kuin siihen oikeutetut. Tietojen ja tietojen käsittelymenetelmien oikeellisuus, laatu ja kiistämättömyys varmistetaan. Tieto suojataan luvattomalta tai vahingossa tapahtuvalta tiedon muuttamiselta tai poistamiselta.

Saatavuus
Saatavuudella tarkoitetaan tiedon hyödynnettävyyttä haluttuna aikana. Tiedot sekä liittyvät järjestelmät ja palvelut ovat niihin oikeutettujen saavutettavissa.

Tietoturvaloukkaus
Tietoturvaloukkaus on oikeudeton puuttuminen tietoon tai tietojärjestelmään. Loukkaus voi olla luonteeltaan fyysinen tai tekninen. Yleisimpiä tietoturvaloukkauksen muotoja ovat käyttäjätunnusten ja salasanojen väärinkäyttö, tietomurto, palvelunestohyökkäys, tietojen varastaminen ja haittaohjelmat.

Henkilötietojen tietoturvaloukkaus
Henkilötietojen tietoturvaloukkaus eli tietoturvaloukkaus, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvattomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta. Kuvattuja loukkauksia voivat olla esimerkiksi hävinnyt tiedonsiirtoväline (kuten USB-muisti), varastettu tietokone, haittaohjelmatartunta tai päätöksen postitus väärälle henkilölle.

Pöytyä

2. Tietoturvaperiaatteet ja -tavoitteet

Tieto on keskeisessä roolissa Pöytyän kunnan toiminnassa ja palvelutuotannossa. Tietoturvan periaatteita noudatetaan kaikissa kunnan tietojen käsittelyn elinkaaren vaiheissa. Tiedon elinkaarella tarkoitetaan kaikkia käsittelyn vaiheita, keräämisestä sen hävittämiseen. Periaatteiden noudattaminen koskee kaikkea tietoa riippumatta siitä, miten se on tuotettu, saatu, jaettu tai tallennettu ja riippumatta siitä, onko tieto tuotettu tietokoneella, käsin, tulostamalla, kopioimalla, kuvaamalla tai puhumalla. Tietoresurssien käyttäjien on tärkeää ymmärtää näiden resurssien merkitys kunnan palvelutavoitteiden saavuttamisessa.

Kunnan johto määrittelee tässä politiikassa tietoturvallisuuden ja tietosuojan puitteet, linjaukset, tavoitteet ja vastuut. Politiikka luo perustan kunnan tietoturvatoiminnalle, -ohjeistukselle ja -koulutukselle, ja se sisältää myös linjaukset tietosuoja-asioiden käsittelylle kunnassa. Tietoturvapolitiikka sitoo kunnan kaikkia toimialoja ja kaikkia työntekijöitä sekä luottamushenkilöitä, ja se tulee huomioida sopimuksissa yhteistyökumppanien kanssa.

Tietoturvaperiaatteilla varmistetaan tietojen luottamuksellisuus, eheys ja käytettävyys ja täten kunnan palvelutuotannon, prosessien ja muiden toimintojen luotettavuus, laatu sekä jatkuvuus. Lähtökohtana tietoturvaa koskevissa päätöksissä ovat viranomaissäädökset sekä hyvä tiedonhallinta- ja -käsittelytapa.

Tietoturvatyön päämäärät ovat:

1. Tunnistaa kunnan toiminnalle tärkeät tiedot, tietojärjestelmät ja tietojenkäsittelyprosessit.
2. Aikaansaada ja ylläpitää näiden tietojen ja järjestelmien luotettavuus, eheys ja käytettävyys vähintään sen tasoisena, mitä säädökset ja hyvä hallintotapa kunnan toiminnalta ja hallinnolta edellyttävät.
3. Suunnitella, toteuttaa, seurata ja arvioida kunnan tietojen käsittelyä ja hallintaa siten, että se täyttää sekä ulkopuolelta tulevat vaatimukset että kunnan omat tavoitteet.
4. Varautua tietoriskeihin ja minimoida toteutuvista riskeistä aiheutuneet vahingot.
5. Huomioida tietojen käsittelyn näkökulma kunnan valmiussuunnitelmissa sekä muussa varautumisessa häiriötilanteisiin ja poikkeusoloihin.
6. Turvata kuntalaisten ja henkilöstön yksityisyyden suoja siten kuin sitä koskevissa säädöksissä edellytetään.
7. Pitää yllä hyvää tietoturvatietoisuutta ja -osaamista kunnan koko henkilöstön keskuudessa.

Kunnan kaikessa toiminnassa pitää huomioida sekä yleinen tietoturvallisuus että erityisesti henkilötietoihin liittyvä tietosuoja. Niistä huolehtiminen ei ole erillistä toimintaa vaan osa kunnan jatkuvaa palvelu- ja hallintotyötä,

johtamista ja kokonaisturvallisuutta. Vastuu tietoturvallisuudesta koskee siten koko organisaatiota. Mahdollisiin epäkohtiin, kuten tietoturvapoikkeamiin tai tietosuojan loukkauksiin, puututaan työnjohdollisin ja tarvittaessa myös rikosoikeudellisin keinoin.

Tietoturvapolitiikka tiedotetaan sisäisesti henkilöstölle ja se julkaistaan kunnan internetsivuilla.

3. Tietoturvallisuuden suunnittelu

Tietoturvapolitiikkaa toteuttavat käytännön yksityiskohtaisemmat toimenpiteet määritellään tietoturvaohjeistuksissa. Ohjeistuksien pääsisällön tulee olla kunnan koko toiminnan kattava, mutta siihen voi sisältyä myös palvelualueittain laadittavia tarkentavia osia. Ohjeistuksissa tulee ottaa huomioon tunnistetut tietoriskit ja esittää riittävät, kohtuulliset toimet niiden hallitsemiseksi. Ohjeistukset ovat tarkistettava vuoden välein ja päivitettävä havaittujen tarpeiden mukaisesti. Ne voivat sisältää myös salassa pidettäviä tietoja, mikä tulee huomioida asiakirjan säilyttämisessä ja jakelussa.

4. Tietoturva- ja tietosuojatyössä keskeiset roolit ja vastuut

4.1 Ylimmän johdon vastuu

Kunnanhallitus hyväksyy tietoturvapolitiikan ja johtaa tietoturvallisuustoimintaa kunnassa kunnanvaltuuston talousarviossa tähän osoittamien resurssien puitteissa. Tietosuojavastaava vastaa tietoturvapolitiikkaa toteuttavan ohjeistuksen, tiedotuksen ja koulutuksen järjestämisestä ja vahvistaa politiikan jalkauttamiseksi tarkoitetut sisäiset toimintaohjeet.

Toimialajohtajat vastaavat kunnan tietoturvapolitiikan ja -ohjeiden noudattamisesta toimialoilla sekä tarvittaessa tarkentavien toimialakohtaisten lisäohjeiden antamisesta. Lisäksi toimialajohtajat vastaavat siitä, että toimialan tietovarannoille ja tietojärjestelmille on nimetty päävastuuhenkilöt eli omistajat (vrt. 3.4).

4.2 Esihenkilöiden vastuut

Sen lisäksi, mitä edellä todettiin ylimmän johdon vastuusta, kunkin toimialan, tulosalueen ja toimintayksikön esihenkilö vastaa johtamansa toiminnan osalta seuraavista:

- toimintaa varten koottavien, ylläpidettävien ja käytettävien tietojen tarvemäärittely sekä tärkeys- ja turvallisuusluokittelu; viimeksi mainittu sisältää mm. tietojen suojaamisen tarpeet

- käyttöoikeuksien myöntämisen periaatteet ja rajoitukset em. tietoihin
- resurssien määrittely ja varaaminen toiminnan edellyttämään tietojenkäsittelyyn siten, että käsittely on säädösten, hyvän hallintotavan ja tämän tietoturvapolitiikan mukaista
- alaisensa henkilöstön tietoturva-, tietosuoja- ja tietojenkäsittelyosaamisen varmistaminen ja tarvittaessa tähän liittyvän lisäkoulutuksen järjestäminen; erityisesti on huolehdittava tietoturva- ja tietosuoja-asioiden kattavaan käsittelyyn osana uusien työntekijöiden perehdyttämistä
- alaisensa henkilöstön käyttöoikeustarpeiden määrittäminen ja ilmoittaminen niiden toimeenpanijoille (esimerkiksi tietohallintoon ja kunnan eri sovellusten pääkäyttäjille) sekä tällaisten oikeuksien päättymisen varmistaminen tarvittaessa, kuten ao. henkilön palvelussuhteen päättyessä
- työtehtävien jakaminen ja rajaaminen siten, että tiedonhallinnan kannalta vaaralliset työyhdistelmät vältetään
- vaitiolositoumusten vaatiminen luottamuksellisten tietojen käsittelijöiltä
- johtamansa toiminnan ja henkilöstön valvonta siten, että tämän tietoturvapolitiikan mukainen tietoturvallisuus toteutuu, ja mahdollisten epäkohtien viivytyksetön käsittely
- salassapito- ja tietosuojasitoumuksen allekirjoittaminen (henkilöstö ja luottamushenkilöt)

Toimialajohtajien vastuulla on nimetä toimialan tietovarannoille ja -järjestelmille päävastuuhenkilöt eli omistajat (ks. kohta 3.4).

4.3 Tietosuojavastaava

Kunnanhallitus nimeää kunnalle tietosuojasäädösten edellyttämän tietosuojavastaavan. Tehtävä on ensisijaisesti asiantuntija- ja neuvonantajarooli, jota voidaan hoitaa joko päätoimisena tai oman varsinaisen tehtävän ohella siten kuin nimeämispäätöksessä tarkennetaan.

Tietosuojavastaavan tehtäviin kuuluu

- huolehtia yhdessä kunnan palvelualueiden vastuuhenkilöiden kanssa siitä, että kunnan tietojenkäsittelyn turvallisuutta koskevat vaatimukset tulevat selvitetyiksi ja riskit arvioiduiksi
- kehittää ja koordinoida tietosuojaa ylläpitäviä ja parantavia toimintatapoja
- tukea esimiehiä ja tietoresurssien omistajia turvallisuussuunnittelussa ja suunnitelmien toimeenpanossa
- johtaa kuntatason tietoturvallisuussuunnitelman ja -ohjeiden valmistelua sekä varmistaa niiden tarkoituksenmukainen jakelu ja esilläpito
- katselmoida mahdolliset palvelualueittain tai muuten rajatummin laadittavat ja sovellettavat tietoturvallisuussuunnitelman osat ja ohjeet

- suunnitella tietosuojaa koskevaa koulutusta ja valvoa sen toteutuksia
- avustaa yksityisyydensuojan huomioinnissa kunnan hankintojen valmistelussa
- toimia tarvittaessa kunnan tietosuojaryhmän puheenjohtajana tai kokoonkutsujana
- raportoida kunnan johdolle tietosuojan tilasta vähintään kerran vuodessa

Tietosuojavastaavan tehtäviä voidaan tarvittaessa tarkentaa nimeämispäätöksessä tai tehtävänkuvauksessa.

Tietosuojavastaavan tehtävät ja rooli kunnan organisaatiossa määräytyy EU:n yleisen tietosuoja-asetuksen (2016/679) sekä tätä täydentävän kansallisen tietosuojalain (1050/2018) mukaan.

4.4 Tiedon tai tietojärjestelmän omistajan vastuut

Kunnan käytössä oleville tietovarannoille on nimettävä omistaja eli päävastuuhenkilö, joka vastaa siitä, että tieto on tarpeiden mukaista, oikeaa ja ajan tasalla. Tämä koskee sekä digitaalista että muussa muodossa olevaa tietoa.

Tietovarannon omistajan vastuulle kuuluu:
- tietojen luokittelu tärkeyden, saatavuuden (toiminnan jatkuvuuden) ja luottamuksellisuuden näkökulmasta
- tietoihin kohdistuvien riskien arviointi; henkilötietojen tapauksessa arviointi tulee tehdä EU:n yleisen tietosuoja-asetuksen ja sitä täydentävän kansallisen tietosuojalainsäädännön edellyttämällä tavalla ja laajuudella
- tietojen suojaamiseen liittyvien vaatimusten ja tavoitteiden määrittely, edellä mainitut luokittelut ja arvioinnit huomioiden

Toimialajohtajat toimivat toimialojensa tietovarantojen omistajina. Tarvittaessa toimialajohtaja voi valtuuttaa tietovarannon omistajaksi esihenkilön, jonka vastuulla olevaa toimintaa kyseinen tietovaranto ensisijaisesti palvelee. Yksittäisen erillisen tietoaineiston omistajaksi toimiajajohtaja voi määrätä myös henkilön, joka ensisijaisesti luo tai tuottaa tiedon.

Toimialajohtajat toimivat toimialojensa käytössä olevien tietojärjestelmien omistajina ja nimeävät päävastuuhenkilöt. Toimialajohtaja voi valtuuttaa esihenkilön toimimaan tietojärjestelmän omistajana. Hän voi olla sama henkilö, joka omistaa järjestelmällä käsiteltävät tiedot. Järjestelmän omistajan tietoturvavastuita ovat:
- yhden tai useamman pääkäyttäjän nimeäminen järjestelmälle; pääkäyttäjänä voi myös olla omistaja itse

- pääkäyttäjän toteutettavaksi tarkoitettujen järjestelmäkohtaisten käyttöoikeusperiaatteiden ja -sääntöjen määrittely sekä muu pääkäyttäjän työn ohjeistaminen
- järjestelmällä toteutettavaan tietojenkäsittelyyn liittyvän riskiarvion ja riskienhallintasuunnitelman tekeminen tai teettäminen
- sen varmistaminen, että tietojärjestelmässä on siinä käsiteltävien tietojen kannalta riittävät suojaukset ja käyttöoikeuksien määrittelyn mahdollisuudet kunkin käyttäjän tai käyttäjäryhmän työnkuvan mukaisesti
- asianmukaisten tietoturvaa ja tietosuojaa koskevien sopimusehtojen sisällyttäminen järjestelmän hankinta- ym. sopimuksiin
- tietojärjestelmäselosteen laadinta ja ylläpito

Tietojärjestelmän omistaja pitää nimetä jo siinä vaiheessa, kun järjestelmää hankitaan, jotta hän voi huomioida vastuulleen kuuluvat asiat hankinnassa (mm. vaatimusmäärittelyssä). Omistaja on yleensä se henkilö, joka on vastuussa kyseisestä tiedon käsittelyprosessista tai muutoin tuntee sen parhaiten.

4.5 Henkilöstön vastuut

Jokainen kunnan puolesta tietoja käsittelevä henkilö (omaan henkilöstöön kuuluva tai ulkopuolinen) on velvollinen suojelemaan kunnan tietoresursseja luvattomalta pääsyltä, luvattomalta muuttamiselta, tuhoamiselta tai perusteettomalta julkitulolta. Jokainen tiedon käyttäjä ja käsittelijä on myös velvollinen noudattamaan kunnan tietoturva- ja -suojaohjeistoja. Jokaisen on raportoitava havaitsemistaan tietoturvauhista ja -rikkeistä. Tämä koskee myös henkilötietojen käsittelyyn liittyvää tietosuojaa.

Tarkemmat henkilöstölle tarkoitetut tietoturva- ja tietosuojaohjeet laaditaan erikseen tietosuojaryhmän hyväksymällä tavalla ja tarkkuudella. Ohjeiston tulee olla saatavilla ja työntekijöiden luettavissa kaikilla kunnan työpaikoilla joko tulostettuna tai sähköisessä muodossa kunnan tietoverkossa.

4.6 Tietosuojaryhmä

Kunnanjohtaja nimeää tietosuojavastaavan esityksestä jäsenet kunnan tietosuojaryhmään. Ryhmän kokoonpanossa tulee huomioida kunnan tiedonhallinnan eri osa-alueet ja toimialojen edustus. Ryhmän päätehtävänä on tukea kunnan ylintä johtoa ja toimialojen johtoa sekä tietosuojavastaavaa näiden tietosuojaa koskevissa vastuissa. Ryhmän tehtävänä on myös käsitellä erityisen laajat tai monimutkaiset tietosuojan kehittämiseen ja toteutumiseen liittyvät kysymykset.

Ryhmällä ei ole itsenäistä viranomaistoimivaltaa, mutta se voi valmistella ehdotuksia tai suosituksia toimivaltaisten viranhaltijoiden tai luottamuselinten käsiteltäväksi ja päätettäväksi.

4.7 Tietohallinnon henkilöstö

Kunnan tietohallinnon henkilöstön (ml. esihenkilö) vastuulla on suunnitella ja toteuttaa kunnan tietojenkäsittely-ympäristö tietoturvapolitiikan ja -ohjeiden mukaisena sekä lain sallimin keinon valvoa, että tietotekniikkaa hyödyntävä tietojenkäsittely toteutuu tavoitteiden mukaisesti. Mahdolliset poikkeamat on viipymättä raportoitava tietosuojavastaavalle.

Tietohallinnon henkilöstön tietoturvatehtävät ja -vastuut voidaan tarvittaessa sopimuksellisesti siirtää myös ulkoiselle palveluntoimittajalle.

5. Tietojen ja tietojärjestelmien käytön periaatteet

Kunnan tietoja ja tietojärjestelmiä käytettäessä tulee noudattaa seuraavia tietoturvallisuutta edistäviä periaatteita ja sääntöjä:

- Kunnan käytössä oleva tieto sekä tietojärjestelmät, tietotekniset laitteet ja ohjelmistot on tarkoitettu työtehtävien hoitamista varten.
- Kunnan tietojärjestelmäympäristössä saa käyttää ainoastaan tietohallinnon hyväksymiä tietojärjestelmiä, laitteita ja ohjelmistoja.
- Tietotekniset asennustyöt saa suorittaa vain tietohallinto tai sen valtuuttama taho.
- Kunnan toimintaa ja palveluita tukevat tietojärjestelmät luokitellaan tärkeyden ja suojaustarpeiden näkökulmasta, ja niille nimetään omistaja.
- Käyttöoikeudet kunnan tietoon ja tietojärjestelmiin myönnetään työtehtävien hoitoon tarvittavassa laajuudessa. Käyttöoikeudet hyväksyy käyttäjän esihenkilön hakemuksen perusteella tietojärjestelmän omistaja tai hänen valtuuttamansa taho.
- Tietoturvallisuutta koskeviin laiminlyönteihin ja väärinkäytöksiin puututaan välittömästi kunnan normaalein kurinpidollisin keinoin tai lainsäädännön edellyttämällä tavalla.
- Tiedon turvalliset käsittelytavat ja tietoturvapoikkeamien hallintakäytännöt kuvataan tarpeelliseksi katsotulla tarkkuudella erillisissä ohjeissa.

6. Tietoturvaosaamisen ja -tietoisuuden ylläpito

Uudessa tehtävässä aloittava työntekijä perehdytetään tietoturvan ja tietosuojan perusteisiin ja ohjeisiin, painottaen hänen omiin työtehtäviinsä. Perehdytyksen läpiviennistä vastaa lähin esihenkilö. Pöytyän kunta velvoittaa jokaisen työntekijän hyväksymään salassapito- ja tietosuojasitoumuksen palvelussuhteen alkaessa.

Tietoturvallisuuden ja tietosuojan osaamista vahvistetaan vuosittain sisäisen tiedotuksen, ohjeistuksen ja tarpeen mukaan erikseen järjestettävien koulutusten muodossa.

Ylimmän johdon tulee erityisesti varmistaa, että tietoturvallisuuden ja tietosuojan ylläpidosta, kehittämisestä ja johtamisesta nimenomaisesti vastaaville tarjotaan riittävä hallinnollinen ja tekninen koulutus.

Osaamisen varmistamiseksi koko henkilöstöltä edellytetään säännöllistä tietoturva- ja tietosuojakoulutuksen suorittamista. Tietoturva- ja tietosuojakoulutusta edellytetään myös luottamushenkilöiltä.

7. Seuranta, raportointi ja kehittäminen

Jokainen on velvollinen seuraamaan (valvomaan) tietoturvallisuuden ja tietosuojan toteutumista edellä kuvattujen tehtäviensä ja vastuualueidensa mukaisesti. Tietoturva- ja -suojajärjestelyt toteutetaan siten, että turvallisuusloukkausten selvittäminen on jälkikäteen kohtuudella mahdollista.

Tietosuojavastaava raportoi tietosuojan toteutumisesta ja erityisesti mahdollisista poikkeamista kunnan johdolle. Tarvittaessa viranomaisille ja rekisteröidylle raportoidaan lainsäädännön ja kunnan ohjeistuksen mukaisesti.

Tämän tietoturvapolitiikan sisältö tulee katselmoida tietosuojaryhmässä vuosittain ja tarvittaessa päivittää.