



RÄÄKKYLÄN KUNNAN

TIETOTURVA- JA TIETOSUOJAPOLITIikka

Hyväksytty: Rääkkylän kunnanhallitus 23.04.2018 § 66

DOKUMENTIN VERSIOTIEDOT			
Versio	Pvm	Muutosten kuvaus	Tekijä
1	21.3.2018	Tietosuojaryhmä käsitellyt	Raita Joutsensaari
	11.4.2018	Johtoryhmä käsitellyt	Raita joutsensaari

Sisällys

1. Johdanto.....	1
2. Tietoturvan ja tietosuojan tavoitteet	1
3. Tietoturva ja tietosuoja – käsitteitä.....	2
4. Organisointi ja vastuut.....	2
5. Riskienhallinta	3
6. Tietoturvan ja tietosuojan toteutus.....	3
7. Tietoturvan ja tietosuojan toteutumisen seuranta ja valvonta.....	4
8. Dokumentit ja keskeinen lainsäädäntö	4



1. JOHDANTO

Tietoturva- ja tietosuojapolitiikkaan on koottu Räikkylän kunnassa noudatettavat tietoturvan ja tietosuojan tavoitteet, periaatteet, toteuttamisen organisointitavat ja vastuut. Palvelujensa toiminnan varmistamiseksi Räikkylän kunta on sitoutunut kaikessa toiminnassaan lainsäädäntöön perustuvaan tietoturvan ja tietosuojan ylläpitoon ja sen jatkuvaan kehittämiseen.

Tietoturva- ja tietosuojan parantaminen on osa kunnan toiminnan kehittämistä, jatkuvuuden varmistamista ja sisäistä valvontaa.

Tietoturva- ja tietosuojapolitiikkaan pohjautuvat suunnitelmat, ohjeet ja määräykset kattavat kaikki tietojen käsittelytoiminnot koko tiedon elinkaaren ajan, riippumatta siitä, missä muodossa tieto on. Ohjeet ja määräykset koskevat kaikkia Räikkylän kunnan työntekijöitä, luottamushenkilöitä, toimielimiä ja Räikkylän kunnan toimeksiantoja tekeviä palveluntuottajia. Sopimuksia tehtäessä huomioidaan palveluntuottajien riittävä tietoturva- ja tietosuojataso.

Tietoturva- ja tietosuojatyötä tehdään yhteistyössä Pohjois-Karjalan tietotekniikka Oy:n kanssa (myöhemmin PTTK). PTTK Oy toimittaa kunnan ICT- palvelut, tietojärjestelmät ja tietotekniset laitteet.

2. TIETOTURVAN JA TIETOSUOJAN TAVOITTEET

Kunnassa käsitellään erilaisia henkilötietoja, taloustietoja ja hallinnon asiakirjoja. Osa näistä tiedoista on salassa pidettävää, arkaluonteista tai muuten luottamuksellista tietoa.

Räikkylän kunnan tietoturva- ja tietosuojatyön tavoitteena on

- mitoittaa ja järjestää käyttöympäristö ja resurssit siten, että toiminta on tehokasta ja se edistää tietoturvan ja tietosuojan toteutumista kunnan eri toiminnoissa
- turvata tärkeiden tietojärjestelmien ja tietoverkkojen häiriötön toiminta
- varmistaa, että toiminnassa käytettävän tieto on oikeaa, ajantasaista, luotettavaa ja sitä käsitellään lainmukaisesti
- että julkinen tieto on helposti löydettävissä ja käytettävissä
- rekisteröidyn laissa määriteltyjen oikeuksien turvaaminen
- varmistaa, että tiedot eivät joudu tahattomasti tai tahallisesti asiattomien haltuun tai tuhottavaksi
- varmistaa, että tietoja ja tietojärjestelmiä käyttävät vain henkilöt, joilla on niihin oikeus työtehtäviensä hoitamiseksi
- noudattaa henkilötietojen käsittelyssä periaatteita, joita ovat kohtuullisuus ja läpinäkyvyys, käyttötarkoitussidonnaisuus, tietojen minimointi, täsmällisyys, säilytyksen rajoittaminen, eheys ja luottamuksellisuus
- dokumentoinnilla osoittaa, että lainmukaisuusperiaatteita on noudatettu.

Tietojärjestelmätoimintojen keskeytyksistä ja häiriöistä huolimatta kunnan toiminta ja palvelut on pystyttävä hoitamaan vähintään PTTK Oy:n kanssa ennalta sovitulla minimitasolla. Luotettavuus riippuu palveluketjusta, joka muodostuu PTTK Oy:n tuottamista toimivista työasemista, tietoliikenneverkoista, konesalipalveluista, tietojärjestelmistä ja kunnan käyttäjistä. Normaalityönnön jatkuvuuden turvaamisen lisäksi poikkeusolojen valmiuden luominen ja ylläpito on välttämätön osa PTTK Oy:n kunnille tuottamaa tietojenkäsittelyn turvallisuutta.

3. TIETOTURVA JA TIETOSUOJA – KÄSITTEITÄ

Tietoturva tarkoittaa tietojen, palvelujen, järjestelmien ja tietoliikenteen suojaamista ja varmistamista niihin kohdistuvien riskien hallitsemiseksi lainsäädännöllisillä, hallinnollisilla, teknisillä ja muilla toiminnoilla sekä normaali- että poikkeusoloissa.

Tietoturvallisuus kattaa kaikenlaiset tietojenkäsittelytehtävät sisältäen myös erityyppisten dokumenttien arkistoinnin. Tietoturvallisuustoimet koskevat sähköisessä, puhutussa ja kirjallisessa muodossa olevan tiedon käsittelyä, säilyttämistä, luovutusta ja siirtoa.

Tietoturvallisuuteen sisältyy

- hallinnollinen turvallisuus (johtaminen ja hallinnointi)
- henkilöturvallisuus (osaaminen, roolit, riittävyys)
- fyysinen turvallisuus (toimitilojen ja laitteiden fyysinen suojaaminen)
- tietoliikenneturvallisuus (tiedon siirron turvaaminen)
- laitteistoturvallisuus (tietokoneiden, puhelinten ym. suojaaminen)
- ohjelmistoturvallisuus (käyttövarmuus, jatkuvuus, käyttöoikeudet)
- tietoaineiston turvallisuus (sähköisten ja paperisten dokumenttien käsittely ja seuraaminen)

Tietoturvallisuustyö on tietoturvallisuuden saavuttamiseksi tehtävien toimenpiteiden suunnittelua ja toteuttamista. Toimintaan kuuluvat tietojen turvaamisen menetelmät, välineet ja toimenpiteet, työhön osoitetut resurssit sekä välineistön tietoturvaominaisuudet.

Tietosuojalla tarkoitetaan henkilöiden yksityisyyden, suojaamista, luottamuksen turvaamista sekä oikeuksien ja oikeusturvan varmistamista henkilötietoja käsiteltäessä. Hyvä tietosuoja edellyttää hyvää tietoturvasoaa.

4. ORGANISOINTI JA VASTUUT

Kunnanhallitus hyväksyy kunnan tietoturva- ja tietosuojapolitiikan ja vastaa tietoturvan ja tietosuojan toteuttamisen edellytyksien luomisesta asetettujen tavoitteiden saavuttamiseksi.

Räikkylän kunnan johtoryhmä vastaa tietoturva- ja tietosuojapolitiikan toteutuksesta hallinnollisella tasolla sekä tietoturvan ja tietosuojan integroimisesta kunnan kokonaistoimintastrategiaan. Johtoryhmä varmistaa toimintaan kuuluvien tietojen turvaamisen ja suojaamisen menetelmät, välineet ja toimenpiteet, työhön osoitetut resurssit sekä välineistön tietoturvaominaisuudet.

Tietoturva- ja suojaryhmän (ICT-ryhmä) tehtävänä on käynnistää toimenpiteet vakavien tietoturvaongelmien korjaamiseksi sekä käsitellä tietosuojarikkomukset ennalta suunnitellun prosessin mukaisesti. Tietoturva- ja suojaryhmän muihin tehtäviin kuuluvat tietoturvaan ja

tietosuojaan liittyvien suunnitelmien ja ohjeistuksien laatiminen ja käytäntöön vieni sekä koulutusten järjestäminen. Ryhmä valmistelee ja ohjaa kunnan tietoturvan ja tietosuojan käytännön toteutusta ja kehittämistoimenpiteitä sekä niihin liittyvää riskienhallintaa.

Tietoturvavastaava vastaa tietoturvan seurannasta, raportoinnista ja kehittämisestä yhdessä muiden tietoturvaryhmän jäsenien kanssa.

Tietosuojavastaava valvoo ja seuraa tietosuojan toteutumista tietosuojan valvontasuunnitelman mukaisesti ja raportoi havaitsemistaan puutteista ja esittää parannusehdotuksia niihin tietoturva- ja johtoryhmälle. Tietosuojavastaava on mukana uusien tietojärjestelmien hankintaprosessissa.

Esimiehet vastaavat siitä, että työntekijät perehdytetään tietoturva- ja tietosuoja-asioihin ja -ohjeistuksiin ja että työntekijät ymmärtävät lakien ja asetusten merkityksen työtehtävissään. Esimiesten tehtäviin kuuluu havainnoida ja reagoida tietoturva- ja tietosuojaongelmiin.

Lisäksi **jokainen Räikkylän kunnan työntekijä ja luottamushenkilö** on vastuussa tietoturvan ja tietosuojan toteuttamisesta omalta osaltaan. Jokainen työntekijä vastaa siitä, että henkilötietoja käsitellessään noudattaa niitä koskevia lakeja ja annettua ohjeistusta.

5. RISKIENHALLINTA

Kunnanhallitus vastaa koko kunnan osalta sisäisestä valvonnasta ja riskienhallinnasta. Riskien hallinta on osa sisäistä valvontaa. Toimielimet vastaavat omien tehtäväalueidensa sisäisestä valvonnasta ja riskienhallinnan järjestämisestä.

Tietoturvan ja tietosuojan riskejä arvioi kunnan johtoryhmä ja riskien hallintaprosessista vastaavat toimialojen palvelualueiden johtajat ja esimiehet.

Tietoturva- ja tietosuojariskeistä raportoidaan toimielimille ja kunnanhallitukselle sisäisen valvonnan ja riskienhallinnan ohjeessa määrätyllä tavalla.

6. TIETOTURVAN JA TIETOSUOJAN TOTEUTUS

Räikkylän tietoturvan ja tietosuojan perusta on Räikkylän kunnanhallituksen vahvistama tietoturva- ja tietosuoja politiikka. Lisäksi laaditaan tietoturva- ja tietosuoja suunnitelma, jossa kuvataan keskeiset toimintatavat ja – menetelmät tietojen käsittelylle. Henkilöstön tietosuojaoppaassa ohjeistetaan tiedonkäsittelyä käytännön tasolla.

Tietoturva- ja tietosuoja suunnitelmaan liittyvät PTTK:n tietojärjestelmistä laatimat toipumis-, varautumis- ja valmiussuunnitelmat, joissa kuvataan toimenpiteet ja menetelmät toiminnan jatkuvuuden turvaamiseksi sekä toiminnan palauttamiseksi normaalitasolle häiriötilanteiden jälkeen.

Tietoturvaa ja tietosuoja koskevasta viestinnästä henkilöstölle ja tarvittaessa palveluntuottajille vastaavat palvelualuejohtajat ja esimiehet. Henkilöstölle tiedotetaan tietoturvaan ja tietosuojaan liittyvistä ohjeista tai niiden muutoksista ja järjestetään riittävä koulutus.

7. TIETOTURVAN JA TIETOSUOJAN TOTEUTUMISEN SEURANTA JA VALVONTA

Tietoturvan ja tietosuojan toteutumisesta laaditaan vuosittain tietosuojan valvontasuunnitelma, jonka pohjalta tietoturvan ja tietosuojan toteutumista seurataan tietoturvaryhmässä ja kunnan johtoryhmässä.

Jokaisen Räikkylän kunnan työntekijän ja luottamushenkilön tulee ilmoittaa havaitsemistaan tietoturva- ja tietosuojapuutteista, tietoturvaan ja tietosuojaan liittyvistä väärinkäytöksistä tai epäilemistään tietoturva- ja tietosuojarikkomuksista esimiehelle ja tietoturvavastaavalle.

Tietoturvapoikkeamat käsitellään ennalta suunnitellun ja ohjeistetun prosessin mukaisesti.

8. DOKUMENTIT JA KESKEINEN LAINSÄÄDÄNTÖ

Tietoturva- ja tietosuojapolitiikassa määriteltyjen tavoitteiden saavuttamiseksi ja prosessien kehittämisen turvaamiseksi kunnassa laaditaan:

- Tietoturva- ja tietosuojasuunnitelma
- Henkilöstön tietosuojaopas
- Tietosuojan valvontasuunnitelma
- Tietoaineistojen käsittelyohje

PTTK laatii

- Toipumissuunnitelmat (palvelin- ja verkkolaitekohtaiset)
- Varautumissuunnitelmat (järjestelmäkohtaiset)
- ICT-Valmiussuunnitelma

Tietoturva- ja tietosuojatyötä ohjaavaa keskeistä lainsäädäntöä ovat:

- Arkistolaki (831/1994)
- Euroopan parlamentin ja neuvoston tietosuoja-asetus (EU) (679/2016)
- Hallintolaki (434/2003)
- Henkilötietolaki (523/1999) 31.12.2018 saakka
- Julkisuuslaki (Laki viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallinta-tavasta 621/1999)
- Julkisuusasetus (Asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta 1030/1999)
- Kuntalaki (410/2015)
- Laki sähköisistä allekirjoituksista (14/2003)
- Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)
- Laki yksityisyyden suojasta työelämässä (759/2004)
- Laki valmiuslain muuttamisesta (198/2000)
- Henkilötietojen käsittelyä koskevia erityissäännöksiä on lukuisissa eri aloja koskevissa laissa.

Tulossa

- Tietosuoja laki (1.1.2019 alkaen)
- Tiedonhallintalaki
- Erityislakien päivitykset asetuksen mukaiseksi