Tietoturva- ja tietosuojapolitiikka

Joroisten kunta

Versio 1.0

16.5.2018

Hyväksytty kunnanvaltuustossa 18.6.2018 § 23

Sisällysluettelo

1 Johdanto 3
2 Tietoturva- ja tietosuojapolitiikan tarkoitus ja tausta 3
3 Keitä tietoturva- ja tietosuojapolitiikka koskee 3
4 Tietoturvallisuus 3
5 Tietosuoja 4
5.1 Menettely tietosuojan vaarantuessa 5
6 Kokonaisturvallisuus 5
7 Riskienhallinta 6
8 Varautuminen ja jatkuvuudenhallinta 6
9 Turvallisuus 6
10 Roolit ja vastuut 7
11 Tietojärjestelmien käyttö 7
12 Tietoturvan seuranta, ylläpito ja kehittäminen 7

Liite 1 ROOLIT JA VASTUUT
Liite 2 TIETOTURVA- JA TIETOSUOJARIKKOMUSTEN SEURAAMUSTAULUKKO
Liite 3 TIETOTURVA- JA TIETOSUOJASITOUMUS

1 Johdanto

Tietoturva ja tietosuoja ovat Joroisten kunnassa kiinteä osa päivittäistä toimintaa, ja lähtökohta luottamukselliselle viranomaistoiminnalle.

Tietosuojalla tarkoitetaan henkilön yksityisyyden suojaamista ja henkilötietojen oikeaoppista käsittelyä niin, että henkilön yksilöivää tietoa ei paljastu siihen oikeudettomille tiedon elinkaaren missään vaiheessa.

Tietoturvatyö tarkoittaa tiedon suojaamiseksi tehtävien toimenpiteiden suunnittelua ja sen mukaista toteuttamista.

Tässä politiikassa ja sen liitteissä määritellään mitä tietoturva ja tietosuoja Joroisten kunnassa tarkoittaa. Lisäksi politiikassa kuvataan kunnan tietoturvan ja tietosuojan keskeiset periaatteet, tavoitteet, roolit ja vastuut.

Tämä politiikka katselmoidaan ja päivitetään tarvittavilta osin vuosittain. Dokumentti on kokonaisuudessaan saatavilla kunnan intranetissä sekä internet-sivuilla.

2 Tietoturva- ja tietosuojapolitiikan tarkoitus ja tausta

Tämä politiikka toimii kunnan ylimpänä turvallisuusasiakirjana, sekä perustana toimialojen omille toimintaperiaatteille ja ohjeille, jotka tarkentavat tässä politiikassa annettuja määräyksiä.

Tämä politiikka kuvaa tietoturvan ja tietosuoja roolit kunnan toiminnoissa ja palveluissa, perustuen tehtyihin riskiarvioihin ja toimintaa säätelevien lakien vaatimuksiin.

3 Keitä tietoturva- ja tietosuojapolitiikka koskee

Tämä politiikka on kunnanhallituksen hyväksymä ja koskee koko kuntakonsernia sekä niitä sidosryhmiä (yhteistyö- ja sopimuskumppanit) jotka käsittelevät kunnan omistamaa tai hallinnoimaa tietoa.

Politiikassa esitetyt periaatteet ja käytännöt koskevat kaikissa tiedon elinkaaren vaiheissa (~~luonti~~, tuottaminen, kerääminen, säilytys, siirto, luovuttaminen, hävittäminen) ja kaikissa muodoissa (mm. paperi, sähköinen, optinen, puhuttu) olevaa tietoa.

4 Tietoturvallisuus

Tietoturvallisuus kattaa tietoturvaan ja tietosuojaan liittyvät toteutukset. Tietoturvalla kunnassa tarkoitetaan kaikissa muodoissa olevan tiedon (sekä tietojärjestelmien, tietoliikenteen,

palveluiden ja niiden käyttöympäristöjen) turvaamista siten, että tiedon alkuperäisyys, luottamuksellisuus, eheys ja saatavuus kyetään varmistamaan.

Periaatteena on, että tietoturvallisuuskäytännöt kattavat kaikki kunnan tietojenkäsittelytehtävät sisältäen myös asiakirjahallinnon sekä arkistoinnin ottaen huomioon toimialojen ja työyksiköiden perusluonteen ja tietoturvatarpeet. Tietoturvallisuus pyritään integroimaan kiinteästi kunnan palveluihin ja toimintaan, sekä jokaisen käyttäjän työtapoihin.

Tietoturvallisuutta toteutetaan käytännössä seuraavilla:

- **Asenne**: Tiedon käsittelijä ymmärtää tietoturvan merkityksen ja omat vastuunsa, sekä on motivoinut noudattamaan tätä politiikkaa sekä tästä politiikasta johdettuja tietoturvaohjeita ja -määräyksiä.
- **Eheys:** Tieto, tietojärjestelmät ja paperiasiakirjojen arkistot ovat luotettavia, oikeellisia ja ajantasaisia. Toisin sanoen tieto ei ole muuttunut teknisen vian seurauksena tai tietoa ei ole muutettu ihmisen toimesta tahallisesti tai tahattomasti.
- **Kiistämättömyys:** Tiedonkäsittelytoimenpiteiden suorittamista siten, että käsittelyn osapuolet voidaan yksiselitteisesti tunnistaa sekä toimenpiteiden aikana että jälkikäteen.
- **Luottamuksellisuus:** Tieto on vain siihen oikeutettujen saatavissa eikä sitä paljasteta tai muutoin saateta sivullisten tietoon. Tiedon käsittelyssä noudatetaan julkisuuslakia sekä erikseen, toiminnoittain/järjestelmittäin, hyväksyttyjä tietojen turvaluokituksien mukaisia sääntöjä ja ohjeita.
- **Pääsynvalvonta:** Tietoa tai tietojärjestelmää ei voi käyttää ilman lupaa ja ettei arkistotiloihin tai vastaaviin pääse ilman kontrolloitua pääsynvalvontaa.
- **Saatavuus:** Tieto ja tietojärjestelmät ovat käytettävissä ja käyttökelpoisia valtuutetuille käyttäjille ja tietojärjestelmille, sovituilla tavoilla ja sovittuun aikaan.

Kunnan tietoturvatyön periaatteet ja toteutukset perustuvat ensisijassa julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) ohjeisiin ja suosituksiin, JHS-suosituksiin, tietoturvatasojen määrittelemiin Perustaso -vaatimuksiin (Tietoturvallisuusasetus 681/2010) ja tietosuojavaltuutetun toimiston antamiin ohjeisiin.

5 Tietosuoja

Henkilötietoja kerätään vain siinä laajuudessa ja vain siksi ajaksi kuin kunnan tarjoamien palveluiden tuottaminen edellyttää. Henkilötietojen käsittelijöillä on käyttöoikeus vain niihin tietoihin, joita palvelun tuottamisessa tarvitaan. Tietoja voidaan luovuttaa kolmansille osapuolille lakeihin perustuvien luovutustarpeiden nojalla. Tietoja ei luovuteta muihin tarkoituksiin ilman asiakkaalta pyydettyä käyttötarvekohtaista lupaa.

Toiminnassa muodostuvista henkilörekistereistä on julkisesti tarjolla tietosuojaselosteet, joista käy ilmi rekistereiden sisältämät tiedot ja käyttötarkoitus.

Joroisten kunnan toimiessa rekisterinpitäjänä palveluntarjoaja voi siirtää henkilötietoja Euroopan unionin, Euroopan talousalueen tai muiden maiden, joiden Euroopan Komissio on todennut takaavan riittävän tietosuojan tason, ulkopuolelle ainoastaan Joroisten kunnan etukäteisellä kirjallisella suostumuksella.

Tietoturva- ja tietosuojaryhmän riskiarvion mukaisesti Joroisten kunta tekee sopimuksen kumppaneiden ja palveluntarjoajien kanssa henkilötietojen käsittelystä.

Joroisten kunta noudattaa laissa ja asetuksissa voimassa olevia velvollisuuksia rekisterinpitäjänä ja henkilötietojen käsittelijänä, sekä sitoutuu turvaamaan rekisteröidyn oikeudet. (Euroopan unionin yleinen tietosuoja-asetus (EU 679/2016), Tietosuojalaki (2018), Tiedonhallintalaki (2019)

Joroisten kunta edellyttää, että henkilöstö on osallistunut tietoturva- ja tietosuojakoulutuksiin ja todentaa osaamisen mm. verkko-oppimisympäristössä suoritetun testin avulla. Lisäksi henkilöstö allekirjoittaa tietoturva- ja tietosuojasitoumuksen (liite 3).

Rekisterinpitäjänä (Joroisten kunta) on se toimija, jonka käyttötarkoitusta varten henkilötiedot on kerätty. Rekisterinpitäjä vastaa siitä, ja sen on pystyttävä osoittamaan se, että henkilötietojen käsittelyä koskevia periaatteita on noudatettu:

- käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys
- käyttötarkoitussidonnaisuus
- tietojen minimointi
- tietojen täsmällisyys
- tietojen säilytyksen rajoittaminen
- tietojen eheys ja luottamuksellisuus

5.1 Menettely tietosuojan vaarantuessa

Tietosuojaloukkaukseksi katsotaan kaikki henkilötietojen käsittelyä koskevien lakien ja asetusten, tämän politiikan sekä kunnan tarkempien periaatteiden ja ohjeistuksien vastainen toiminta.

Jo pelkkä epäily tietosuojaloukkauksesta johtaa asian selvittämiseen. Selvittäminen aloitetaan kunnan sisäisenä toimintana. Jos tietosuojaloukkaus arvioidaan lainsäädännön perusteella rangaistavaksi toiminnaksi tai rangaistavuudesta on olemassa riittävä epäilys, asian käsittely annetaan viranomaiselle.

Jos henkilötietojen tietosuojaloukkauksesta todennäköisesti aiheutuu rekisteröidyn oikeuksiin ja vapauksiin kohdistuva korkea riski, rekisterinpitäjän on ilmoitettava siitä rekisteröidyille ja valvontaviranomaiselle ilman aiheetonta viivytystä (72h).

Muu, ei lainsäädännöllisesti rangaistavaksi toiminnoksi luettava, mutta tietosuojaa vaarantava toiminta johtaa kunnan sisäiseen seuraamusmenettelyyn, jossa tietosuojaloukkaus voi johtaa

huomautukseen, varoitukseen tai työsuhteen päättämiseen. Tietoturva- ja tietosuojapolitiikan liitteessä 2 on Joroisten kunnan seuraamustaulukko.

Joroisten kunnan nimetty tietosuojavastaava toimii yhteyshenkilöinä valvontaviranomaisille sekä rekisteröidyille, joita tietosuojaloukkaus koskee.

6 Kokonaisturvallisuus

Kunnan kokonaisturvallisuus koostuu riskienhallintaan, varautumiseen ja turvallisuuteen liittyvistä prosesseista ja niiden toteutuksista. Tietoturva- ja tietosuojapolitiikka on osa kunnan kokonaisturvallisuuden hallintaa.

7 Riskienhallinta

Riskienhallinta toimii kunnan kokonaisturvallisuuden perustana. Riskienhallinnan avulla kunnan palveluihin, toimintoihin ja tietoihin kohdistuvia riskejä hallitaan järjestelmällisesti ja koko organisaation laajuisesti. Riskienhallinta kuuluu jokaisen työntekijän vastuulle.

EU:n yleinen tietosuoja-asetus edellyttää vaikutuksen arvioinnin (DPIA) tekemistä. Vaikutustenarvioinnin tarkoituksena on kuvata henkilötietojen käsittelyä, arvioida käsittelyn tarpeellisuutta ja oikeasuhteisuutta sekä arvioida henkilötietojen käsittelystä aiheutuvia riskejä ja tarvittavia toimenpiteitä, joilla riskeihin puututaan. Vaikutustenarviointi on tehtävä, kun henkilötietojen käsittelyyn todennäköisesti kohdistuu korkea riski. Vaikutustenarvioinnin tarkoituksena on auttaa rekisterinpitäjää tietosuoja-asetuksen vaatimusten noudattamisessa ja noudattamisen osoittamisessa.

8 Varautuminen ja jatkuvuudenhallinta

Kunta on varautunut erilaisiin, toimintaa häiritseviin tai toiminnan keskeyttäviin uhkatilanteisiin, kriiseihin ja niistä toipumiseen ennakolta. Tämä tapahtuu kehittämällä ja ylläpitämällä seuraavia varautumiseen ja jatkuvuudenhallintaan liittyviä suunnitelmia:

- **Valmiussuunnitelma** toiminnan, palveluiden ja järjestelmien hallinnoimiseksi häiriö- ja poikkeusoloissa joka sisältää:
- **Jatkuvuussuunnitelmat** toiminnan kannalta kriittisille palveluille, toiminnoille ja tietojärjestelmille niiden jatkuvuuden turvaamiseksi
- **Toipumissuunnitelmat** kriittisille tietojärjestelmille ja -verkoille niiden mahdollisimman nopean toipumisen, toiminnan uudelleenaloittamisen ja jatkamisen varmistamiseksi
- **Lakisääteiset pelastussuunnitelmat** ihmisten ja omaisuuden suojelemiseksi, sekä vahinkojen minimoimiseksi onnettomuustilanteissa

9 Turvallisuus

Tietoturvan ja tietosuojan ohella keskeisimpiä turvallisuuden osa-alueita kunnassa ovat:

Turvallisuusjohtaminen on turvallisuuden toteutumisen ohjaamista ja valvomista kaikilla tietoturvaprosessin kuvaamilla osa-alueilla.

Henkilöstöturvallisuus on kunnan ja sidosryhmien henkilöstöön kohdistuvien ja henkilöstöstä aiheutuvien riskien hallintaa. Periaatteena on, että tietoturva ja tietosuoja huomioidaan työ- / virkasuhteen kaikissa vaiheissa.

Fyysinen turvallisuus koostuu järjestelyistä joilla kunnan tiloja, ihmisiä, tietoa ja muuta omaisuutta suojataan vahingoilta ja vahingoittamisyrityksiltä.

10 Roolit ja vastuut

Tietoturvan ja tietosuojan toteuttaminen on jatkuvaa, laaja-alaista ja kaikille toimijoille kuuluvaa toimintaa. Periaatteena on, että sen toteuttamiseen osallistuvat kunnan ja sidosryhmien henkilöstö, osana omaa yleistä toimintavastuutaan. Käytännössä tämä tarkoittaa hyvien periaatteiden ja ohjeiden noudattamista sekä tietoturvan- ja tietosuojan huomioimista kaikessa tekemisessä.

Ylin vastuu tietoturvasta, tietosuojasta, riskienhallinnasta ja varautumisesta on kunnanhallituksella. Ohjaus- ja kehittämistyössä tarvittava muu erityisasiantuntemus ja nimetyt turvallisuusvastuut kuvataan liitteessä 1.

11 Tietojärjestelmien käyttö

Kunnan periaatteiden mukaisesti tietojärjestelmät ovat tarkoitettu työtehtävien hoitamiseen eikä niitä tule käyttää kunnan omistaman tai hallinnoiman tiedon vaarantumiseen johtavaan toimintaan. Kunnalle tai sen toiminnalle mahdollisesti aiheutetun haitan korvausvastuussa on ensisijassa vaarantumisen aiheuttaja.

Käyttäjien toimintaa ohjataan tästä politiikasta johdetuilla periaatteilla ja -ohjeilla. Tiedon ja tietojärjestelmien väärinkäyttöön puututaan kunnan normaalein kurinpitomenettelyin.

12 Tietoturvan seuranta, ylläpito ja kehittäminen

Kunnan tietoturva- ja tietosuojatavoitteiden toteutumista seurataan säännöllisesti laaditun vuosikellon mukaisesti. Seuranta perustuu tietoturva- ja tietosuojaprosessin mukaisiin mitattaviin tavoitteisiin ja raportointikäytäntöihin, sekä yhteisesti sovittuihin teknisen valvonnan keinoihin.

Tietoturvan ja tietosuojan ylläpidossa ja kehittämisessä keskeisessä roolissa on osaaminen mitä toteutetaan säännöllisillä koulutus- ja viestintäkäytännöillä. Tämä politiikka ja periaatteet koulutetaan koko kunnan henkilöstölle normaalin perehdytysprosessien mukaisesti.

Tarvittavien ulkoisten sidosryhmien tietoturva- ja tietosuojaosaamisesta vastaa kyseisen toimialan johto. Periaate on, että kaikki, jotka käsittelevät kunnan omistamaa tai hallinnoimaa tietoa saavat riittävät edellytykset tiedon asianmukaiseen käsittelyyn.

LIITE 1: ROOLIT JA VASTUUT

Luottamushenkilöstö

- Vastaa tietoturvallisuuden toteuttamisesta omissa luottamustehtävissään

Kunnanhallitus

- Päättää kunnan tietoturvapolitiikasta
- Vastaa tietoturvapolitiikan toteutumisesta

Kunnanjohtaja

- Päättää käytännön tietoturvan toteuttamistavoista (tietoturvasuunnitelma)
- Raportoi ja tekee kehittämisehdotuksen kunnanhallitukselle tietoturvapolitiikkaan liittyen
- Tietoriskien ja tietoturvapoikkeamien hallinnan koordinointi

Kunnan johtoryhmä/toimialajohtajat

- Valmistelee tietoturva- ja tietosuojapolitiikan ja tietoturvasuunnitelman kehittämiseen ja käytäntöön viemiseen liittyvät asiat yhteistyössä tietoturvapäällikön kanssa
- Edistää tietoturva- ja tietosuojatietoisuutta toimialoilla ja henkilöstön keskuudessa
- Tietoturvaan ja tietosuojaan liittyvän viestinnän tukeminen ja toteuttaminen yhdessä tietoturvapäällikön kanssa

Tietoturva- ja tietosuojaryhmä

- käsittelee, kommentoi, antaa lausuntoja ja hyväksyy tietosuojaan, tietoturvaan ja kyberturvallisuuteen liittyviä ohjeita ja linjauksia
- käsittelee merkittävät tietosuojaan ja tietoturvaan liittyvät poikkeamat
- käsittelee ja hyväksyy osaltaan projektit sovituissa tarkastuspisteissä
- kehittää ja edistää organisaation tietoturvan ja tietosuojan toteutumista
- tarkastaa henkilötietoja sisältävien sopimusten tietoturvan ja tietosuojan

Tietoturvapäällikkö (tietohallintojohtaja)

- Valmistelee tietoturva- ja tietosuojapolitiikan ja suunnitelman kehittämiseen ja käytäntöön viemiseen liittyvät asiat yhteistyössä johtoryhmän kanssa
- Vastaa henkilöstön tietoturvakoulutusten järjestämisestä

- Vastaa tietoturvaan liittyvän raportoinnin kunnan johtoryhmälle

Tietosuojavastaava

- Antaa rekisterinpitäjälle tai henkilötietojen käsittelijälle sekä henkilötietoja käsitteleville työntekijöille tietoja ja neuvoja
- Seuraa, että noudatetaan EU tietosuoja-asetusta, muita tietosuojalainsäännöksiä ja rekisterinpitäjän tai henkilötietojen käsittelijän toimintamenettelyjä, jotka liittyvät henkilötietojen suojaan
- Henkilötietojen käsittelyä koskeva suunnittelu- ja kehittämistoiminta, tietoturva- ja tietosuojaryhmän jäsenenä
- Osallistuu rekisterinpitäjän hyväksymiä tietosuoja- ja tietoturvaohjeita koskevaan valmisteluun ja ylläpitoon
- Antaa pyydettäessä neuvoja tietosuojaa koskevasta vaikutustenarvioinnista ja valvoo sen toteutusta
- Tekee yhteistyötä valvontaviranomaisen kanssa ja toimii yhteyspisteenä käsittelyyn liittyvissä kysymyksissä
- Raportoi suoraan organisaation johdolle tietosuojan (ja tietoturvallisuuden) tilasta ja kehittämistarpeista (sisäiset auditoinnit ja käytönvalvonta)

Toimialojen johto

- Tietoturvallisuuden toteuttaminen ja toteutumisen valvonta oma toimialansa osalta
- Tietoturva- ja tietosuojavastuiden toteuttaminen vastuullaan olevissa tytäryhtiöissä
- Tietoturvaa ja tietosuojaa säätelevien lakien, säädösten, direktiivien ja määräysten huomioiminen omassa organisaatiossaan
- Sisäisen valvonnan raportin tuottaminen vuosittain toimialaansa koskien

Esimies

- vastaavat oman yksikkönsä osalta annettujen määräysten ja ohjeistusten noudattamisesta. Tähän sisältyy niin työntekijöiden perehdyttäminen kuin toteutumisen seuranta.
- raportoi mahdollisista poikkeamista toimialan tietosuojavastaavalle
- tietojärjestelmien käyttöoikeuksien hyväksyminen

Tietotekniikan tukihenkilöstö

- Tietoturva- ja tietosuojapolitiikan soveltaminen ja toteuttaminen omaa erikoisasiantuntemusta hyödyntäen
- Tietoturvatoimenpiteiden huomioiminen omalla vastuualueellaan
- Teknisen valvonnan toteuttaminen tietoturvapäällikön ohjauksessa ja valvonnassa

Tietojärjestelmän pää- ja varapääkäyttäjä

- Tiedon tai tietojärjestelmän suojaamistarpeen määrittäminen ja toteuttaminen
- Tietojärjestelmäkuvauksien ja tietojärjestelmä- sekä tietosuojaselosteiden ylläpito
- Käyttöoikeuksien hallinta tietojärjestelmissä

Henkilöstö

- Käsittelevät tietoja annettujen ohjeiden ja määräysten mukaisesti
- Havaitsemiensa tietoturvaan ja tietosuojaan liittyvien ongelmien, uhkien, poikkeamien tai ohjeiden vastaisen menettelyn raportointi

Rekisteröidyt

- ovat tietoisia oikeuksistaan sekä vastuussa antamiensa tietojen oikeellisuudesta

Ulkoiset palveluntuottajat

- Sitoutuvat noudattamaan kunnan tietoturva- ja tietosuojapolitiikkaa
- Palveluntuottajien vastuut henkilötietojen käsittelyssä sovitaan palvelukohtaisissa sopimuksissa
- Palveluntuottajien tulee nimetä tietoturva- ja tietosuoja-asioihin yhteyshenkilö