TIETOTURVA- JA TIETOSUOJAPOLITIIKKA

Hyväksytty valtuustossa 11.12.2023

Sisällysluettelo

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 henkilöstön saatavilla intranetissä. Julkinen versio julkaistaan kunnan verkkosivuilla.

2 TIETOTURVA- JA TIETOSUOJAPOLITIIKAN TARKOITUS JA RAKENNE

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 ja asetusten vaatimuksiin.

Tietoturvakäytännöt ovat tietoturvapolitiikan alaisia ohjeistusdokumentteja. Tietoturvakäytäntöjen on tarkoitus ohjata tietoturvan ja tietoturvaratkaisujen toteuttamista käytännönläheisesti ja konkreettisesti. Tietoturvakäytännöt ja niihin liittyvän dokumentaation hyväksyy tietohallinnon johtoryhmä ja vie kunnan johtoryhmälle tiedoksi.

Tietoturvapolitiikkaa toteutetaan seuraavilla tietoturvakäytännöillä:

- ICT Varautumissuunnitelma
- Pääsynhallintakäytäntö
- Työasemien ja oheislaitteiden käytäntö
- Tietoverkon- ja palvelinympäristön ylläpitokäytäntö
- Opas sähköiseen työympäristöön

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 (tuottaminen, kerääminen, säilytys, siirto, luovuttaminen, hävittäminen) ja kaikissa muodoissa (mm. paperi, sähköinen, optinen, puhuttu) olevaa tietoa.

4 TIEDONHALLINTA

Vuoden 2020 alussa voimaan tullut tiedonhallintalaki asettaa julkiselle hallinnolle tiedon hallintaan liittyviä vaatimuksia. Joroisten kunta noudattaa nykyisiä lakien ja asetusten mukaisia vaatimuksia.

Joroisten kunta on laatinut tiedonhallintamallin, jota katselmoidaan vuosittain tietohallinnon johtoryhmässä. Tiedonhallintalain edellyttämä asiakirjajulkisuuskuvaus on julkaistu kunnan verkkosivuilla.

Virka- tai työsuhteen, työharjoittelun tai luottamustehtävän päättyessä tehtävää hoitaneen henkilön tulee luovuttaa kaikki haltuunsa annetut Joroisten kuntaa, sen tytäryhtiöitä tai asiakkaita koskevat, liike- ja ammattisalaisuuksia ja/tai muuta taloudellista arvoa sisältävät dokumentit (pöytäkirjat, muistiot, piirustukset, tietovälineet ja –ohjelmat, suunnitelmat, keskeneräiset dokumentit yms.) takaisin kunnalle.

5 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, saatavuus ja käytettävyys kyetään varmistamaan.

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

Tietoturvallisuuden toteutumiselle asetetaan seuraavat käytännön tavoitteet:

- **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 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 voimassa olevia lakeja 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. Pääsynvalvontaa ohjataan pääsynhallintakäytännöillä (tarkemmin dokumentissa Pääsynhallintakäytäntö).
- **Saatavuus:** Tieto ja tietojärjestelmät ovat käytettävissä ja käyttökelpoisia valtuutetuille käyttäjille ja tietojärjestelmille, sovituilla tavoilla ja sovittuun aikaan.

Kunnan tietoturvatyön periaatteet ja toteutukset perustuvat voimassa olevan lainsäädännön lisäksi julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) ohjeisiin, tiedonhallintalautakunnan ohjeisiin ja suosituksiin (mm. julkisen hallinnon tietoturvallisuuden arviointikriteeristö), sekä tietosuojavaltuutetun toimiston antamiin ohjeisiin.

6 TIETOSUOJA

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)).

Henkilötietoja kerätään vain siinä laajuudessa 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 eikä tietoja luovuteta muihin tarkoituksiin ilman asiakkaalta pyydettyä käyttötarvekohtaista lupaa.

Toiminnassa muodostuvista henkilörekistereistä on julkisesti tarjolla tietosuojaselosteet, joista käy ilmi rekistereiden sisältämät tiedot ja käyttötarkoitus. Rekisterinpitäjänä on se toimija, jonka käyttötarkoitusta varten henkilötiedot on kerätty.

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.

Joroisten kunta tekee sopimuksen kumppaneiden ja palveluntarjoajien kanssa henkilötietojen käsittelystä tietohallinnon johtoryhmän suositusten mukaisesti. Uudet tietojärjestelmähankkeet käsitellään tietohallinnon johtoryhmässä.

Joroisten kunta edellyttää, että henkilöstö on osallistunut tietoturva- ja tietosuojakoulutuksiin ja todentaa osaamisen vuosittain verkko-oppimisympäristössä suoritetun testin avulla. Lisäksi henkilöstö allekirjoittaa tietoturva- ja tietosuojasitoumuksen työsuhteen alussa, jossa jokainen sitoutuu noudattamaan kunnan tietoturvasääntöjä.

Joroisten kunta rekisterinpitäjänä vastaa siitä, että henkilötietojen käsittelyä koskevia periaatteita on noudatettu (asetuksen mukainen osoitusvelvollisuus):

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

7 KOKONAISTURVALLISUUS

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

8 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.

Erilaisiin uhkatilanteisiin ennalta varautuminen pienentää mahdollisuutta riskien toteutumiselle. Riskienhallinnan tulee olla kiinteä osa tiedon hallinnan prosesseja. Riskiarviointien tekeminen tulee myös olla säännöllistä ja toistuvaa toimintaa.

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 ennen käsittelyn aloittamista, kun henkilötietojen käsittelyyn todennäköisesti kohdistuu korkea riski. Vaikutustenarvioinnin tarkoituksena on auttaa rekisterinpitäjää tietosuoja-asetuksen vaatimusten noudattamisessa ja noudattamisen osoittamisessa.

9 VARAUTUMINEN JA JATKUVUUDENHALLINTA

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

- ICT Valmiussuunnitelma kuuluu Joroisten kunnan valmiussuunnitelman yleisen osan alaisuuteen sekä saman sisältöisenä tietoturvapolitiikan käytäntöihin. Valmiussuunnitelma kuvaa varautumistoimenpiteet palveluiden ja järjestelmien hallintaan häiriö- ja poikkeusoloissa.
- Jatkuvuudenhallintakäytäntö on sisällytetty ICT valmiussuunnitelmaan. Käytäntö kuvaa hallintatoimet toiminnan kannalta kriittisten tietojärjestelmien ja tietoverkkojen jatkuvuuden turvaamiseksi normaaliolojen häiriötilanteissa. Toipumissuunnitelmat mahdollisimman nopean toipumisen, toiminnan uudelleenaloittamisen ja jatkamisen varmistamiseksi ovat osa jatkuvuudenhallintakäytäntöä.

9.1 MENETTELY TIETOSUOJAN TAI TIETOTURVAN VAARANTUESSA

Tietosuoja-/tietoturvaloukkaukseksi katsotaan kaikki henkilötietojen käsittelyä koskevien lakien ja asetusten, tämän politiikan sekä kunnan tarkempien periaatteiden ja ohjeistuksien vastainen toiminta.

Jokaisella työntekijällä on velvollisuus ilmoittaa huomatessaan mahdollisen tietoturva- tai tietosuojaloukkauksen. Ilmoitus tehdään tietohallintoon ja tietosuojavastaavalle. Jo pelkkä epäily tietosuoja- tai tietoturvaloukkauksesta johtaa asian selvittämiseen.

Jos henkilötietojen tietosuojaloukkauksesta todennäköisesti aiheutuu rekisteröidyn oikeuksiin ja vapauksiin kohdistuva korkea riski, rekisterinpitäjän on ilmoitettava siitä rekisteröidyille ja valvontaviranomaiselle ilman aiheetonta viivytystä (72 h). Joroisten kunnan tietosuojavastaava toimii yhteyshenkilönä valvontaviranomaiselle sekä rekisteröidyille, joita tietosuojaloukkaus koskee.

Tietoturvarikkomuksista ja tietosuojaloukkauksista voi olla seurauksena käyttöoikeuksien rajoituksia, palvelussuhteeseen vaikuttavia toimenpiteitä sekä laissa ja asetuksissa määriteltyjä seuraamuksia. Palvelussuhteeseen vaikuttavista seuraamuksista on säädetty ensi sijassa työsopimuslaissa ja viranhaltijalaissa. Jos tietosuojaloukkaus arvioidaan lainsäädännön perusteella rangaistavaksi toiminnaksi tai rangaistavuudesta on olemassa riittävä epäilys, asian käsittely annetaan viranomaiselle. Seuraamuksia arvioitaessa moitittava toiminta, sen vaikutukset ja seuraukset käsitellään kokonaisuutena.

10 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.

11 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 ’Roolit ja vastuut’.

12 TIETOJÄRJESTELMIEN KÄYTTÖ

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

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

13 TIETOTURVAN JA TIETOSUOJAN SEURANTA, YLLÄPITO JA KEHITTÄMINEN

Kunnan tietoturva- ja tietosuojatavoitteiden toteutumista seurataan säännöllisesti tietohallinnon johtoryhmässä. 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 sisällytetään koko kunnan henkilöstön perehdytysprosessiin.

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: ROOLIT JA VASTUUT

Luottamushenkilöstö

- Vastaa tietoturvallisuuden toteuttamisesta omissa luottamustehtävissään

Kunnanhallitus

- Päättää kunnan tietoturvapolitiikasta
- Vastaa tietoturvapolitiikan toteutumisesta

Talous- ja hallintojohtaja yhdessä tietohallinnon johtoryhmän kanssa

- Päättää käytännön tietoturvan toteuttamistavoista
- Raportoi ja tekee kehittämisehdotukset johtoryhmälle tietoturvapolitiikkaan liittyen, josta kunnanjohtaja vie esitykset kunnanhallitukselle.
- Tietoriskien ja tietoturvapoikkeamien hallinnan koordinointi

Tietohallinnon johtoryhmä

- Valmistelee tietoturva- ja tietosuojapolitiikan kehittämiseen ja käytäntöön viemiseen liittyvät asiat
- Edistää tietoturva- ja tietosuojatietoisuutta
- Hyväksyy yhteiset periaatteet ja käytännöt, mm. tietoturvakäytäntö-dokumentaation
- Käsittelee, kommentoi, antaa lausuntoja ja kannanottoja tietosuojaan, tietoturvaan ja kyberturvallisuuteen liittyen
- Tarkastaa henkilötietoja sisältävien sopimusten tietoturvan ja tietosuojan
- Käsittelee tietosuojaan ja tietoturvaan liittyvät merkittävät poikkeamat
- Käsittelee ja hyväksyy osaltaan projektit sovituissa tarkastuspisteissä
- Kehittää ja edistää organisaation tietoturvan ja tietosuojan toteutumista
- Valmistelee tietoturvan ja tietosuojan tekniset linjaukset

Tietoturvapäällikkö (tietohallintojohtaja)

- Valmistelee tietoturva- ja tietosuojapolitiikan 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
- Antaa pyydettäessä neuvoja tietosuojaa koskevasta vaikutustenarvioinnista ja valvoo sen toteutusta
- Tekee yhteistyötä valvontaviranomaisen kanssa ja toimii yhteyspisteenä käsittelyyn liittyvissä kysymyksissä
- Osallistuu henkilötietojen käsittelyä koskeva suunnittelu- ja kehittämistoimintaan tietohallinnon johtoryhmän jäsenenä
- Osallistuu rekisterinpitäjän hyväksymiä tietosuoja- ja tietoturvaohjeita koskevaan valmisteluun ja ylläpitoon
- Seuraa ja valvoo henkilötietojen käsittelyä ja niiden suojausmenetelmiä
- 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

Esihenkilö

- vastaa oman yksikkönsä osalta annettujen määräysten ja ohjeistusten noudattamisesta sisältäen niin työntekijöiden perehdyttämisen kuin toteutumisen seurannan
- raportoi mahdollisista poikkeamista tietosuojavastaavalle
- tietojärjestelmien käyttöoikeuksien hakeminen, hyväksyminen, muuttaminen ja poisto- ja passivointipyyntöjen tekeminen

Asiakirjahallinnosta vastaava

- Osallistuu asiakirjallisen tietoaineiston käsittelyn kehittämiseen ja tietoturvallisuuden toteuttamiseen
- Ohjaa toimialoja asiakirjahallinnon hoidossa, jotta arkistolain 7§ toteutuu oikeusturva ja tietosuoja huomioiden
- Hyväksyy asiakirjallisten tietoaineistojen hallinnan edellyttämät arkistonmuodostus- ja tiedonohjaussuunnitelmat
- Vastaa päätearkistoon luovutetusta pysyvästi säilytettävästä tietoaineistosta ja niiden tietoturvallisuudesta ja tietosuojasta

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, yhdessä tiedon tai tietojärjestelmän omistajan kanssa
- Tietojärjestelmäkuvauksien ylläpito, yhdessä tiedon tai tietojärjestelmän omistajan kanssa (tiedonhallintamalli ja tietosuojaselosteet)
- Käyttöoikeuksien hallinta tietojärjestelmän omistajan valtuuttamana

Henkilöstö

- Käsittelee tietoja annettujen ohjeiden ja määräysten mukaisesti
- Havaitsemiensa tietoturvaan ja tietosuojaan liittyvien ongelmien, uhkien, poikkeamien tai ohjeiden vastaisen menettelyn raportointi tietosuojavastaavalle tai IT tukihenkilöstölle
- Noudattaa kaikkia tietoturvakäytäntöjä ja tietosuojaohjeita

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

MUUT LIITTEET

Seuraavat liitteet eivät ole julkisia:

- ICT Varautumissuunnitelma
- Pääsynhallintakäytäntö
- Työasemien ja oheislaitteiden hallintakäytäntö
- Tietoverkon- sekä palvelinympäristön hallintakäytäntö
- Opas sähköiseen työympäristöön