8.2.2021

# Sulkavan kunnan

# tietoturva- ja tietosuojapolitiikka

ATK-tuki ja tietosuojavastaava 11.11.2020
Johtoryhmä 11.1.2021
Yhteistyötoimikunta 29.1.2021
Kunnanhallitus 8.2.2021

# SISÄLLYS



# 1 JOHDANTO

Tiedonhallinta, tietoturvallisuus ja tietosuoja perustuvat lainsäädäntöön, ohjaukseen ja sopimuksiin.


Kuva 1. Kunnan tiedonhallintaa ohjaava lainsäädäntö

Tämä asiakirja ”Sulkavan kunnan tietoturva- ja tietosuojapolitiikka” määrittää vastuut, periaatteet ja toimintatavat tietojen käsittelyyn ja suojaamiseen sekä varmistaa yhdenmukaiset käytännöt tietoturva- ja tietosuojatoimenpiteiden toteuttamiseksi. Tietoturva- ja tietosuojapolitiikkaa täydennetään ja tarkennetaan dokumentin liitteenä olevilla erillisillä tietoturvaa ja henkilötiedon käsittelyä koskevilla ohjeilla ja ohjeistuksilla.

Tietoturva- ja tietosuojapolitiikan soveltaminen ei ole sidoksissa tiedon muotoon, käsittely- tai esitystapaan ja sitä tulee soveltaa kaikkiin tiedon elinkaaren eri vaiheisiin (suunnittelusta arkistointiin/hävittämiseen). Tiedonhallinta on tiedon keräämistä, käsittelyä ja tallentamista niin, että tieto saadaan käyttöön tarkoituksenmukaisesti ja hallitusti sekä hävitetään tietoturvallisesti.

Tietoturvallisuus täydentää myös riskienhallintaa ja on osa turvallisuustoimintaa. Tietoturvallisuudella tarkoitetaan sekä lakisääteistä että omista tarpeista lähtevää tietojen, järjestelmien ja palveluiden asianmukaista suojaamista. Tietoturvallisuudella pyritään

varmistamaan myös, etteivät mahdolliset tietojenkäsittelyhäiriöt aiheuta hallitsematonta maksuvalmius-, kannattavuus- tai vakavaraisuusongelmaa tai muuta merkittävää vahinkoa. Tietojen luottamuksellisuutta, eheyttä ja käytettävyyttä suojataan laitteisto- ja ohjelmistovikojen sekä inhimillisten tekojen aiheuttamilta uhilta ja vahingoilta. Jokainen tietoja käsittelevä henkilö vastaa tietoturvasta omalta osaltaan riippumatta tiedon ilmenemismuodosta (puhuttu, kirjoitettu, koneellinen ja tulostettu tieto). Tietoturvallisuus edellyttää aina työntekijöiden riskitietoisuutta.

Tietoturva- ja tietosuojapolitiikka velvoittaa kunnan henkilöstöä, johtoa, luottamushenkilöitä, viranhaltijoita sekä muita kunnan tietoja käsitteleviä henkilöitä, kuten konsultteja, alihankkijoita, sidosryhmiä riippumatta siitä, missä muodossa käsiteltävä tieto on. Se tulee huomioida myös kunnan käyttämien palvelutuottajien ja sidosryhmien toiminnassa.

Tietosuoja- ja tietoturvapolitiikan hyväksyy kunnanhallitus. Tietosuojaa ja tietoturvaa koskeva dokumentaatio tarkistetaan vuosittain sekä päivitetään ja edelleen hyväksytetään hallituksessa tarvittaessa.

# 2 KESKEISET KÄSITTEET

- **Tietosuojalla** tarkoitetaan yksilön (rekisteröidyn) yksityisyyden suojaamista. Tietosuojalla turvataan rekisteröidyn oikeuksia, yksilön tietoja ja luottamusta. Sisäänrakennettu ja oletusarvoinen tietosuoja tarkoittaa sitä, että henkilötietojen suoja otetaan huomioon jo suunniteltaessa toimintaa tai hankittaessa tietojärjestelmiä, jossa käsitellään henkilötietoja.

- **Tietoturvalla** tarkoitetaan niitä hallinnollisia ja teknisiä toimenpiteitä, joilla varmistetaan tiedon luottamuksellisuus ja eheys, käytettävyys sekä rekisteröidyn oikeuksien toteutuminen. Tietojen luottamuksellisuutta, eheyttä ja käytettävyyttä turvataan laitteisto- ja ohjelmistovikojen, luonnontapahtumien sekä tahallisten, tuottamuksellisten tai tapaturmaisten tekojen aiheuttamilta uhilta ja vahingoilta.

- **Kyberturvallisuus** on tietoturvallisuuden alalaji, jolla pyritään sähköisen ja verkotetun yhteiskunnan turvallisuuteen. Kunnan kyberturvallisuuteen varautuminen tarkoittaa sitä, että keskeisten toimintojen osalta on tehty varautumis- ja riskienhallintasuunnitelma. Kyberturvallisuuden varautumisen toimilla on tarkoitus varmistaa organisaatioiden sisäistä turvallisuutta sekä sitä, että esimerkiksi kunnan tietojärjestelmiä/ -verkkoja ei käytetä kyberiskujen / hakkerointien suunnittelussa.

- **Digiturvallisuus** puolestaan koostuu tietosuojasta, tietoturvasta ja kyberturvallisuudesta sekä jatkuvuudenhallinnasta ja riskienhallinnasta. Digiturvan avulla kehitämme turvallisuutta ja ylläpidämme luottamusta omaan ja organisaatiomme toimintaan. Sen avulla ylläpidämme ja kehitämme luottamusta myös kansalaisiin, asiakkaisiin ja muihin sidosryhmiin.

# 3 TIETOTURVA – JA TIETOSUOJAPERIAATTEET

Tietoturva- ja tietosuojaperiaatteilla ohjataan tietojen suojaamista. Tiedon suojaaminen on oleellinen osa organisaation kokonaisturvaa ja päivittäistä toimintaa sekä tärkeä osa toiminnan ja palveluiden laatua ja varmentamista. Tiedon suojaamisen käytänteet ovat edellytys uuden teknologian turvalliseen käyttämiseen.

Tietoturvalla suojataan kunnassa säilytettäviä manuaalisia ja sähköisiä tietoja sekä rekisteröityjen ja henkilöstön oikeuksia. Tietosuoja kattaa myös vaitiolovelvollisuuden piiriin kuuluvan ja muunkin puhutun tiedon käsittelyn.

Tietoturva- ja tietosuojaperiaatteita noudatetaan kaikissa tietojen käsittelyn elinkaaren eri vaiheissa ja tätä edistetään tuomalla tietoturva- ja tietosuojasuojaperiaatteet osaksi henkilöstön perehdytystä ja koulutusta. Tiedon elinkaarella tarkoitetaan kaikkia tiedon käsittelyn vaiheita alkaen tiedon keräämisestä tiedon hävittämiseen. Näiden väliin kuuluu esimerkiksi tietojen tallentaminen, järjestäminen, käyttö, siirtäminen, luovuttaminen, säilyttäminen, muuttaminen, yhdistäminen, suojaaminen, poistaminen ja tuhoaminen. Teknisillä ja organisatorisilla ratkaisuilla varmistetaan, että oletusarvoisesti käsitellään vain käsittelyn kannalta tarpeellisia tietoja.

## 3.1 TIETOTURVAPERIAATTEET

Tietoturvalla varmistetaan tiedon luottamuksellisuus, eheys, saatavuus ja käytettävyys ja tätä kautta kunnan palvelutuotannon, prosessien ja muiden toimintojen luotettavuus, laatu sekä jatkuvuus. Tietoturvallisuudesta huolehtiminen on edellytys tietosuojaperiaatteiden toteutumiselle.

### 3.1.1 Hallinnollinen tietoturvallisuus - johtaminen

Hallinnollisella tietoturvallisuudella tarkoitetaan tietoturvallisuustoiminnan järjestelyjen, henkilöstön tehtävien ja vastuiden sekä ohjeistuksen, koulutuksen ja valvonnan muodostamaa kokonaisuutta. Sen tarkoituksena on luoda organisaatioon tietoturvalliset toimintatavat luonnolliseksi osaksi kaikkea toimintaa. Toiminnasta vastaavat henkilöt huolehtivat resurssien riittävyydestä ja oikeasta kohdistamisesta sekä menettelytavoista.

Hallinnollinen tietoturvallisuus on kaikkien muiden tietoturvallisuuden osa-alueiden toteutuksen ja määrittelyn perusta. Sen avulla määritellään tietoturvallisuuden suuntaviivat ja turvallisuutta

parantavat toimenpiteet. Tietoturvan kehittäminen ja ylläpito ovat osa organisaation yleistä turvallisuustoimintaa, riskien hallintaa ja sisäistä valvontaa.

Tietoturvan hallinnassa otetaan huomioon lainsäädännölliset vaatimukset ja vaikutukset. Palveluja ulkoistettaessa palveluntuottajia vaaditaan noudattamaan kunnan tietosuoja- ja tietoturvapolitiikkaa ja tähän liittyviä käytäntöjä sekä ohjeita.

**Hallinnollisen tietoturvan periaatteet:**

- Tietoriskit ennakoidaan ja niiden vaikutuksia hallitaan.
- Tiedon luotettavuus, virheettömyys ja laatu varmistetaan johtamisessa, päätöksenteossa, toiminnassa ja viestinnässä.
- Tiedon saatavuus ja käytettävyys varmistetaan riittävillä toimilla.
- Estetään tiedon tahaton tai tahallinen tuhoutuminen ja vääristyminen.
- Kunnan tietoturva- ja tietosuojapolitikka viedään käytäntöön ohjeistamalla, kouluttamalla ja tiedottamalla, ja sen toteutuminen näkyy tietojärjestelmien käytössä ja tietojen käsittelyssä.

### 3.1.2 Henkilöstöturvallisuus

Henkilöstöön liittyvien riskien hallintaa kutsutaan henkilöstöturvallisuudeksi. Sen tavoitteena on ehkäistä henkilökuntaan suuntautuvia ja henkilökunnasta tulevia uhkia.

Näitä riskejä voidaan torjua

- turvakartoituksilla
- vastuun ja velvollisuuden selkeällä määrittämisellä
- selkeillä ohjeilla toimenpiteistä, kun työsuhde päättyy ja
- sitouttamalla henkilö tietoturvalliseen toimintaan.

Henkilöstön mitoituksessa on huolehdittava siitä, että varmistetaan turvalliselle tietojenkäsittelylle välttämättömien henkilöresurssien riittävyys. Avainhenkilöille nimetään varahenkilöt, joiden osaaminen on sillä tasolla, että avainhenkilön puuttuminen (sairaus, tapaturma, vuosiloma, irtisanoutuminen) ei estä päivittäisiä toimintoja eikä vaaranna tietoturvaa. Oikealla henkilöiden valinnalla, töiden mitoittamisella ja niiden jakamisella sekä koulutuksella huolehditaan työtehtävien vaatiman osaamisen ja siihen liittyvän tietotekniikan osaamisen tasosta.

Lain yhteistoimintamenettelystä yrityksissä (334/2007) tavoitteena on edistää työnantajan ja henkilöstön välistä vuorovaikutusta. Yhteistyötoimikunta muodostuu työntekijöiden ja työnantajan edustajista. Tietoturvaan liittyvät ohjeet, sopimukset ja sanktiosäännökset on hyvä saattaa yhteistyötoimikunnan tiedoksi ja myös hyväksyttää ne siellä.

Sulkavan kunnan henkilöstöturvallisuus edellyttää, että kaikkien henkilökuntaan kuuluvien tulee suorittaa tietosuoja- ja tietoturvakoulutus joka toinen vuosi ja aina uuden työsuhteen alkaessa. Koulutuksesta tulee tulostaa todistus esimiehelle näytettäväksi.

### 3.1.3 Tietoaineistoturvallisuus

Tietoaineistoturvallisuudella tarkoitetaan eri tallennusmuodoissa olevien tietojen suojaamista. Se koskee sekä paperiasiakirjoja että digitaalisessa muodossa olevia tallenteita, optisia ja magneettisia muistivälineitä, mikrofilmiä, äänitteitä tai muita vastaavia teknisiä laitteita.

Tietoaineistoturvallisuudella varmistetaan asiakirja- ja tietoaineistojen käytettävyys, oikeellisuus, eheys, luottamuksellisuus ja salassapito elinkaaren kaikissa vaiheissa.

Tietoaineistoturvallisuuteen kuuluvat ne ulkoiset normit, jotka rajoittavat tai ohjaavat tietosisällön perusteella tehtävää tietojenkäsittelyä, kuten yleiset ja/tai erityisalan lait, asetukset, viranomaismääräykset ja kansallisarkiston päätökset. Lisäksi tietoaineiston käsittelystä tarvitaan organisaatiokohtaiset ohjeet, johon kuuluvat tietojärjestelmien käsittelysäännöt sekä tietojen ja asiakirjojen luokittelu julkisuus- ja salassapitosäännösten mukaisesti.

Kunnassa otetaan käyttöön vuonna 2021, kaikki tietoaineistot kattava arkistonmuodostus- tai tiedonohjaussuunnitelma, josta ilmenee tietoaineiston käsittelysäännöt tietojen synnystä niiden tuhoamiseen asti, turvaluokitus sekä eheyden ja käytettävyyden varmistaminen aineiston elinkaaren kaikissa vaiheissa.

Organisaation johto vastaa henkilöstön perehdyttämisestä tietoaineistojen käsittelyohjeisiin. Tietoaineistojen tietoturvallisuuden varmistaminen koskee koko henkilöstöä ja tietoaineiston koko elinkaarta. Organisaation tietoaineistoturvallisuuden perustason edellytyksenä on, että henkilöstö tuntee ja noudattaa toiminnassaan.

**Tietoaineistoturvallisuuden periaatteet:**

- tietoaineistojen luettelointi ja luokitus
- tietoaineistojen käsittelyn ohjeistus
- pääsynhallinta ja käyttöoikeusprosessit

- lukittavat säilytystilat
- tietoaineiston turvallinen hävitys
- salassapitosopimukset
- salaustekniikka
- dokumenttien tunnistetiedot
- tietosuojaohjeet
- tietovälineiden ohjeistettu hallinta, käsittely, säilytys ja hävittäminen

Riippumatta tiedon olomuodosta tietoturvallisilla toimilla tähdätään tietoaineistojen käytettävyyteen, eheyteen ja luottamuksellisuuden ylläpitämiseen. Edellä mainitut toimet kattavat tiedon koko elinkaaren alkaen tiedon syntymisestä tiedon hävittämiseen.

**Tietoja käsiteltäessä on huolehdittava**

- luottamuksellisen tiedon salassapidosta
- tiedon oikeellisuudesta siten, että käsiteltävä tieto on oikeaa ilmenemismuodostaan riippumatta
- tiedon käytettävyydestä siten, että tieto on sitä tarvitsevan ja siihen oikeutetun ihmisen tai järjestelmän käytettävissä

Tietoaineisto on suojattava virheiltä, tahattomalta menetykseltä, luvattomalta tai tahalliselta tuhoamiselta, käyttämiseltä, muuttamiselta tai joutumiselta ulkopuolisten käyttöön. Turvallisuusmenettelyt kohdistetaan tiedon käyttöön sen luomisesta käsittelyyn, säilytykseen, arkistointiin ja tietojen hävittämiseen asti.

Henkilöstöllä ja luottamushenkilöstöllä on tietojenkäsittelyn ja asiakirjaturvallisuuden osalta vain heidän työtehtäviensä suorittamisen kannalta välttämättömät käyttö- ja käsittelyoikeudet koskien syöttö-, käsittely- ja tulostusmateriaalia sekä muita asiakirjoja.

### 3.1.4 Ohjelmistoturvallisuus

Ohjelmistoturvallisuudella tarkoitetaan käyttöjärjestelmien, varus- ja työkaluohjelmistojen sekä muiden ohjelmistojen ja sovellusten tunnistautumis- ja suojausominaisuuksia, valvonta- ja lokimenettelyjä sekä ohjelmistojen määrittelyyn, suunnitteluun, kehittämiseen ja hankintaan sekä ylläpitoon ja päivitykseen liittyviä turvallisuustoimenpiteitä (mm. versiointi, lisensointi ja muutoksenhallinta).

Ohjelmistoturvallisuudella varmistetaan ohjelmistojen toimivuus sekä käsiteltävien tietojen eheyden ja luotettavuuden säilyminen. Ohjelmistojen vastuuhenkilöt huolehtivat siitä, että ohjelmistoilla on riittävät suojausominaisuudet. ATK-tuki ja ict -palvelujen ylläpitäjät huolehtivat palvelimille asennettujen ohjelmistojen varmistuksista, palvelinten suojauksen teknisestä toteutuksesta, ylläpidosta ja valvonnasta.

- Pääsynhallinnan suunnittelulla estetään ohjelmien ja järjestelmien luvaton käyttö.
- Käyttäjätunnukset ja salasanat ovat henkilökohtaisia.
- Ohjelmistojen ja järjestelmien käyttöön tulee aina saada perehdytys.
- Ohjelmiston tietoturvallisuuteen ja tietosuojaan kiinnitetään huomioita jo hankintavaiheessa.
- Ohjelmistoista tulee olla olemassa varmuuskopiot.

Muita huomioitavia asioita:

- asianmukaiset päivitykset
- lisenssien hallinta
- arkkitehtuuriyhteensopivuus
- tietoturvalliset asennukset
- huolellinen ylläpito
- käyttäjien hallinta pääsyoikeudet, käyttäjien todennus
- tukipalvelut
- varmistukset
- jäljitettävyys
- haittaohjelmien torjunta

Keskeisimmät tietojärjestelmät ja verkkosovellukset sekä niiden vastuuhenkilöt on kuvattu pääkäyttäjien/vastuuhenkilöiden ylläpitämässä tietojärjestelmäluettelossa. (Liite 3)

### 3.1.5 Laitteistoturvallisuus

Laitteistoturvallisuudella tarkoitetaan ict-laitteistojen (ml. mobiililaitteet) rakenteeseen, käyttöjärjestelmiin, ohjelmistoihin, laite- ja ohjelmistohuoltoon, keskitettyyn operointiin, varmistuksiin ja ict-laitteisiin pääsyn suojaukseen liittyvää turvallisuutta. Laitteistoturvallisuudella turvataan myös kunnan laitteiston elinkaarta.

Laitteistoista on huolehdittava niin, että ne ovat niihin oikeutettujen henkilöiden käytettävissä sovittujen periaatteiden mukaisesti.  Vierailijoilta on evätty pääsy henkilökunnan käytössä oleville laitteille. Laitteistohankinnassa kiinnitetään huomiota niiden yhteensopivuuteen, ylläpitoon ja saatavuuteen.

Laitteistoturvallisuuteen kuuluvat laitteiston suojauksen, asennuksen, takuun ja ylläpidon lisäksi erilaiset tukipalvelut ja -sopimukset sekä laitteiston turvallinen poisto elinkaaren lopussa.

Lisäksi:

- Huolehditaan laitteiston elinkaareen liittyvistä palvelusopimuksista (esimerkiksi, että laitteistojen poistossa tietojen tuhoaminen hoidetaan lopullisesti).
- Huolehditaan sopimuksilla erityisesti tilanteita, joissa koko palvelu sijaitsee palveluntarjoajalla tai osa organisaation laitteista sijaitsee fyysisesti kunnan tilojen ulkopuolella (ja vaaditaan selvityksiä).
- Huolehditaan, että järjestelmien tietoturvapäivityksiä varten on selkeät suunnitelmat ja ohjeet.
- Huolehditaan hankinnoissa ja sopimuksissa tietojärjestelmätoimittajien ja tietoinfrastruktuurin ylläpitäjän vastuut laitteistoturvallisuuden osalta.

### 3.1.6 Tietoliikenneturvallisuus

Tietoliikenneturvallisuus käsittää tiedonsiirtoyhteyksien käytettävyyteen, tiedonsiirron suojaamiseen ja salaamiseen, käyttäjän tunnistamiseen ja verkon varmistamiseen liittyvät turvallisuustoimenpiteet. Tavoitteena on estää luvaton tunkeutuminen järjestelmiin tietoverkon kautta, paljastaa tunkeutumisyritykset, estää siirrettävän tiedon joutuminen sivullisten haltuun ja tarvittaessa estää sen käyttö sekä estää väärän tiedon syöttö tietojärjestelmiin.

### 3.1.7 Käyttöturvallisuus

Käyttöturvallisuus koostuu

- järjestelmien turvallisista käyttöperiaatteista
- tiedonkäytön valvonnasta sekä
- jatkuvuuden turvaamisesta.

Käyttöturvallisuuden avulla luodaan ja ylläpidetään tietotekniikan turvallisen käytön vaatimat olosuhteet huolehtimalla

- tekniikan toimivuuden valvonnasta
- käyttöoikeuksista
- käytön ja lokien valvonnasta
- ohjelmistotukeen, ylläpito-, kehittämis- ja huoltotoimintoihin liittyvistä turvallisuustoimenpiteistä
- varmuus- ja suojauskopioinnista sekä
- häiriöraportoinnista.

Periaatteena on luoda sellaiset menettelytavat, joilla päivittäisessä toiminnassa säilytetään tietojärjestelmien käytössä tietoturvallisuuden taso mahdollisimman hyvänä sekä asiakkaan että työntekijän kannalta.

- Tietojärjestelmän käyttövaltuudet on määritelty ja dokumentoitu asianmukaisesti.
- Haittaohjelmien torjunnassa noudatetaan annettuja ohjeita.
- Tietojen sisällön käyttökelpoisuus ja saatavuus sekä atk-ohjelmien ylläpidon ja huollon saatavuus on varmistettu.
- Palvelimilla olevat ohjelmistot varmistetaan päivittäin ja viikoittain atk-tuen ja ict-palveluntuottajan toimesta. Ict-laitteiden käyttötiedostojen varmistuksista huolehtivat asianomaiset sovellusten käyttäjät.

Käytännössä pääkäyttäjät, projektin vetäjät ja esimiehet huolehtivat sovellusten käyttötuen hankkimisesta ja tarvittavien kehitys- ja ylläpitotoimenpiteiden tekemisestä ohjelmistotoimittajien kanssa.

Käyttäjät vastaavat käyttöturvallisuudesta omalta osaltaan huolehtimalla, ettei työasema ole ulkopuolisen käytössä eikä muut käyttäjät tai ulkopuoliset henkilöt saa tietoonsa käyttäjän henkilökohtaisia salasanoja.

ATK-tuki ja ict-palveluntuottaja vastaa laitteistojen huollosta ja korjauksista.

Käyttöturvallisuuden osa-aluetta tarkennetaan erillisellä tietoturvaa koskevalla ohjeistuksella. (Liite 1 Yleiset tietoturvaohjeet).

Tietoturvapoikkeamiin kuten salasanojen ja käyttäjätunnusten kalasteluun, haittaohjelmiin ja muuhun sellaiseen tulee suhtautua vakavasti. Varautuminen tietoturvapoikkeamiin on kuvattu tarkemmin ei-julkisessa liitteessä (Liite 4 Tietoturvapoikkeamiin varautuminen).

### 3.1.8 Fyysinen turvallisuus

Fyysisen turvallisuuden tavoitteena on tietojenkäsittelyn käyttöympäristön ja sen tilojen suojaaminen fyysisiltä vahingoilta ja häiriöiltä sekä luvattomalta pääsyltä tiloihin, laitteille ja tietoihin sekä ympärystekniikan toiminnan varmistaminen. Fyysinen turvallisuus käsittää kiinteistöjen rakenteellisen turvallisuuden, valvontatekniikan kuten kulunvalvonta-, paloilmoitus-, rikosilmoitus- ja kameravalvontajärjestelmät sekä valvonnan ja vartioinnin.

Käyttöympäristöllä tarkoitetaan niitä tiloja, joissa sijaitsevat

- palvelimet
- mikrotietokoneet
- lähiverkot
- tietoliikennelaitteet
- suunnittelu-, kehitys-, tulostus- ja jälkikäsittelytilat
- tietojenkäsittelyn toimistotilat ja
- teletilat.

Ympärystekniikka käsittää toimintaa tukevat ja sitä varmistavat tekniset järjestelmät kuten

- sähkönsyötön
- ilmastoinnin ja
- lämmityksen.

## 3.2 TIETOSUOJAPERIAATTEET

Tietosuojan lähtökohdat tulevat yksilön perusoikeuksien ja –vapauksien suojaamisesta, erityisesti henkilön ja hänen perheensä yksityisyyden suojasta. Kunnassa noudatetaan asiakkaiden ja henkilöstön sekä muiden sidosryhmien henkilötietojen käsittelyssä voimassa olevaa lainsäädäntöä.

Toukokuusta 2018 lähtien EU:n yleinen tietosuoja-asetus velvoittaa rekisterinpitäjää osoittamaan, että henkilötietojen käsittelyssä noudatetaan lakia ja rekisterinpitäjän omia erillisiä ohjeita. Tietosuojalla turvataan henkilötietojen asianmukainen käsittely koko organisaation toiminnassa, varmistetaan tietojen oikeellisuus ja ennalta ehkäistään henkilötietojen käyttöön liittyviä loukkauksia.

### 3.2.1 Henkilötiedon kerääminen ja käsittelyn periaatteet

Käyttötarkoitus

- Henkilötiedon käsittelylle tulee määritellä käyttötarkoitus, ja tietoa saa jatkossa käsitellä vain sitä tarkoitusta varten (ellei laki tai rekisteröidyn suostumus muuta mahdollista).
- Käsittelytoimet määritellään tiedon elinkaari huomioiden.
- Henkilötietojen käsitteleminen on aina suunniteltava uutta palvelua tai tietojärjestelmää käyttöönotettaessa.
- Henkilötietoja kerätään ja käsitellään vain siltä osin, kun se on kyseisen palvelun/tehtävän kannalta tarpeellista.
- Tietoja ei käytetä tarkoituksen kannalta yhteen sopimattomalla tavalla.

Lainmukaisuus

- Henkilötietoja käsitellään lainmukaisesti ja asianmukaisesti.
- Henkilötiedon käsittelylle tulee aina olla tietosuoja-asetuksen mukainen oikeusperuste.
- Tietoja käsitellään siten, että varmistetaan niiden asianmukainen turvallisuus.

Säilytettävyys

- Henkilötietoja säilytetään organisaatiossa asian käsittelyn kannalta tarpeellisen ajan, ellei näistä ole erikseen toisin säädetty, ja hävitetään säilytysajan päätyttyä kunnan arkistonmuodostus-suunnitelman tai erillisen ohjeistuksen mukaisesti.
- Henkilötietojen säilytys ja hävittäminen toteutetaan suunnitellusti ja yhdenmukaisesti. Henkilötietoja ei voida hävittää suunnittelemattomasti ilman perusteita.
- Henkilötiedon säilytystä ohjaa kunnan arkistonmuodostussuunnitelma.

Tietojen käsittelyn rajoittaminen

- Henkilötietoja saa käsitellä vain ne henkilöt, joilla työtehtävän mukainen oikeutus käsitellä asianomaisia tietoja.
- Henkilötietojen saatavuus organisaatiossa on aina oletusarvoisesti rajoitettua.
- Tietojärjestelmien käyttö on rajattu työtehtävien mukaisin käyttöoikeuksin.

Luottamuksellisuus ja eheys

- Henkilöiden oikeus omien tietojensa tarkastamiseen, korjaamiseen, poistamiseen tai siirtämiseen toteutetaan rekisterinpitäjän hallinnollisilla ja teknisillä toimenpiteillä.

- Henkilötietojen käsittelyssä huolehditaan tietojen virheettömyydestä ja siitä, että tarvittavat tiedot ovat saatavilla.
- Henkilötiedot kulkeutuvat tietoturvallisesti niille, joille ne on tarkoitettu. Tämä huomioidaan mm. siten, että henkilötiedot suojataan asianmukaisesti tilanteesta riippuen.

### 3.2.2 Henkilörekisterit ja niiden tietoryhmät

Kunnan henkilörekisterit koostuvat tiettyä käyttötarkoitusta varten olemassa olevista henkilötiedoista ja muista tietoryhmistä. Rekisteröidyt henkilöt ja niiden tietoryhmä kuvataan henkilörekistereiden tietosuojaselosteissa. Tietosuojaselosteesta rekisteröity saa tiedon hänen tietoihinsa kohdistuvista toimista ja tämä tieto tulee olla rekisteröidyn saatavilla. Tietosuojaselosteet julkaistaan kunnan kotisivuilla/internet-sivuilla ja ylläpidetään rekistereiden vastuuhenkilöiden ja tietosuojavastaavan toimesta.

Henkilörekisteritietoja luovutettaessa huomioidaan tietosuoja-asetuksen, julkisuuslain ja erityslain-säädännön vaatimukset. Rekisteröidyn tietoja käsiteltäessä huomioidaan avoimuuden ja läpinäkyvyyden periaatteet. Rekisteröityä informoidaan hänen tietojensa käsittelystä ja hänen oikeuksiansa kunnioitetaan.

### 3.2.3 Yhteistyö eri sidosryhmien kanssa

Tietosuoja huomioidaan kunnan ja eri osapuolten välisissä sopimuksissa. Henkilötiedon käsittelyä sisältävissä palvelu-/tietojärjestelmäsopimuksissa huolehditaan, että sopimusehdoissa varmistutaan tietosuojasäädöksien vaatimuksista. Hankinta- ja ulkoistussopimuksia tekevät vastaavat siitä, että tietoturvan ja tietosuojan taso vastaa myös ostopalveluissa kunnan määräyksiä ja ohjeita sekä voimassa olevia säännöksiä sopimuksen tekohetkellä sekä toimeksiannon aikana. Sopimuksiin tulee tietosuojaliite ja kuvaus henkilötiedon käsittelystä.

Sopimuksia tehdessä tulee varmistua siitä, voiko henkilötietojen käsittelyä rajoittaa EU-alueelle ja ETA-alueella. Tarvittaessa käytetään hyväksi tietosuojavaltuutetun listausta muista hyväksytyistä maista. Henkilötiedon käsittely muiden viranomaistahojen kanssa on yleensä lakisääteistä tai rekisteröidyn suostumuksella tapahtuvaa.

### 3.2.4 Tietosuojaa valvova viranomainen ja tietosuojaloukkaukset

Suomessa tietosuojavaltuutettu on viranomainen, joka ohjaa, neuvoo ja valvoo henkilötietojen käsittelyä tietosuojalainsäädännön mukaisesti. Tietosuojavaltuutettu käyttää päätösvaltaa tarkastusoikeuden toteuttamista ja tiedon korjaamista koskevissa asioissa sekä antaa ratkaisuja rekisterinpidon lainmukaisuudesta ja rekisteröityjen oikeuksien toteutumisesta. Kunnan tietosuojavastaava on yhdyshenkilö valvovaan tietosuojaviranomaiseen.

Tietosuoja-asetuksen (GDPR) mukaisesta henkilötiedon käsittelystä on kunnassa erillinen, tarkemman tason ohjeistus. (Liite 2)

# 4 TIETOTURVAN JA TIETOSUOJAN VASTUUT JA ORGANISOINTI

Jokainen viranhaltija ja työntekijä, luottamushenkilö sekä sopimus- ja yhteistyötaho

- vastaa omalta osaltaan tietoturvan ja tietosuojan toteutumisesta omissa työtehtävissään
- raportoi tai tekee poikkeamailmoituksen havaitsemistaan tietoturvaan tai tietosuojaan liittyvien uhkista, riskeistä tai rikkomuksista viipymättä esimiehelleen tai tietosuojavastaavalle.

Esimiehet

- vastaavat yksiköidensä tietoturvallisuudesta ja siitä, että henkilöstö tuntee tietoturvallisuuden perusasiat
- mahdollistavat henkilökunnan (myös määräaikaisten ja sijaisten) osallistumisen tietoturva-koulutuksiin (ml. verkkokoulutus)
- tukevat tietoturvan jatkuvaa ylläpitämistä ja kehittämistä
- toteuttavat ja organisoivat tietoturvallisuus- ja tietosuojatoimenpiteet yksikössään
- suunnittelevat, budjetoivat ja organisoivat yksikkönsä tietoturvallisuustoimenpiteet
- huolehtivat, että keskeisille järjestelmille on nimetty vastuuhenkilöt/pääkäyttäjät (minimissää kaksi)
- hoitavat yksikkönsä yleiset tietoturvallisuusasiat, tiedottamisen ja toimintaohjeiden ylläpitämisen käyttäen asiantuntija-apuna tietosuojavastaavaa
- raportoivat tietoturvallisuusongelmista ja tietosuojarikkomuksista johdolle ja tietosuojavastaavalle

Hallintojohtaja

- varmistaa, että organisaatiossa tunnistetaan keskeinen tietosuoja- ja turvallisuuden lainsäädäntö
- määrittää tietoturvallisuusperiaatteet
- määrittää tietoturvallisuuteen liittyvät roolit ja vastuut sekä tietoturvallisuuden tarvitsemat resurssit
- varmistaa, että organisaatiolla on edellytykset toimia poikkeama-, erityis- ja kriisitilanteissa
- viestii organisaatiolle tietoturvallisuustavoitteiden ja tietoturvapolitiikan lakisääteisten velvoitteiden noudattamisen ja jatkuvan parantamisen tärkeydestä
- huolehtii riittävistä resursseista tietoturvallisuuden toteuttamiseen, ylläpitoon ja kehittämiseen
- valvoo, että tietoturvallisuusasiat on organisoitu kunnan toimipaikoissa ja yksiköissä

- huomioi tietosuojan ja tietoturvan osana muuta riskienhallintaa ja päättää hyväksyttävästä riskitasosta
- raportoi tietoturvallisuudesta osana sisäistä valvontaa
- ryhtyy toimenpiteisiin väärinkäytöstapauksissa

Kunnanhallitus

- hyväksyy riskienhallinta- ja tietoturvapolitiikan sekä niihin liittyvät periaatteet
- vahvistaa tietoturvallisuuden ja riskienhallinnan päälinjaukset
- vastaa tietoturvallisuuden ja riskienhallinnan toteutumisesta
- luo edellytykset taata tietoturvallisuuden ja riskienhallinnan tarvitsemat resurssit
- asettaa vaatimukset raportoinnille sekä
- asettaa vaatimukset tietoturvallisuuden ja riskienhallinnan huomioon ottamisesta toiminnoissa.

Tietosuojavastaava

Erityisasiantuntija, jonka tehtävä on toimia ensisijaisesti rekisterinpitäjän tukena ja auttaa rekisterinpitäjää lakisääteisten velvoitteiden toteuttamisessa.

- vastaa tietoturva- ja tietosuojaohjeiden olemassaolosta ja noudattamisesta sekä huolehtii niiden ajan tasalle saattamisesta ja hyväksyttämisestä
- toimii tietoturvallisuuden ja tietosuojan erityisasiantuntijana kunnassa
- tukee, ohjaa ja opastaa henkilökuntaa ja rekisteröityjä tietosuoja-asioissa
- kehittää ja edistää tietoturvallisuutta organisaatiossa
- ohjeistaa tietoturvallisuusasiat ja huolehtii, että niistä tiedotetaan ja koulutetaan
- seuraa ja valvoo henkilötietojen käsittelyä, suojaamista ja suojausmenetelmiä sekä raportoi niihin liittyvistä epäkohdista organisaation johdolle
- toteuttaa tietojärjestelmien lokiseurantaa
- osallistuu organisaation henkilötietojen käsittelyä koskevaan suunnittelutoimintaan
- osallistuu henkilöstölle annettavan tietosuojakoulutuksen toteuttamiseen
- toimii yhdyssiteenä valvontaviranomaisiin.
- raportoi organisaation johdolle tietosuojan tilasta ja kehittämistarpeista sekä tietosuojavastaavan toiminnasta
- toteuttaa organisaation johdon osoittamia muita tietosuojaa tukevia tehtäviä

Tietojärjestelmän omistaja on palvelualue kunnassa ja siitä on vastuussa palvelualueen johtaja.

# 5 OSAAMISEN VARMISTAMINEN JA OHJEISTUS

Kunnan tulee osoittaa, että henkilöstön tietoturva- ja tietosuojaosaaminen on ajantasaista. Tietosuojaosaaminen tulee osoittaa toteutetulla perehdytyksellä, koulutuksiin osallistumalla ja osaamista seuraamalla.

Johtajien, päälliköiden ja esimiesten tulee huolehtia alaistensa ja ulkopuolisten konsulttien tietosuoja- ja tietoturvaosaamisesta mm. seuraavien asioiden osalta:

- sitouttaminen kunnan salassa pidettävän tiedon ja henkilötietojen asianmukaiseen suojaamiseen, perehdyttäminen tietoturva- ja tietosuoja-asioihin,
- annettujen tietoturva- ja tietosuojamääräysten ja -ohjeiden noudattaminen,
- pääsy tarpeelliseen tietoon työsuhteen tai yhteistyön aikana (käyttöoikeudet).
- työtehtävien muuttuessa valtuuksien muutokset sekä
- työsuhteen tai yhteistyön päättyessä tietoon pääsyn ja valtuuksien poistaminen sekä tietojen siirtäminen työnantajalle.

Tietoturvaan ja tietosuojaan liittyvää koko kuntaa ohjaavaa ohjeistusta laaditaan hallinnollisessa yhteistyössä. Lisäksi tietoturvaan ja tietosuojaan liittyvää ohjeistusta tulee sisällyttää kunnan muihin ohjeistuksiin ja prosessien eri vaiheisiin.

Henkilötietojen käsittelyyn liittyvä ohjeistus tarvitaan niihin työvaiheisiin, joissa henkilötietoja käsitellään.

Tietoturvaohjeita tulee liittää erityisesti tietojärjestelmien käyttämiseen. Ohjeistuksen laatimista toteutetaan tämän politiikan periaatteet huomioiden.

ATK-tukihenkilö ja tietosuojavastaava koordinoivat tietoturvan ja tietosuojan ohjeistusta yhteistyössä hallintojohtajan kanssa. ATK-tukihenkilö ja tietosuojavastaava raportoivat tietoturvan toteutumisesta organisaation johdolle. He myös valvovat tietoturvan toteutumista sekä sitä, että tietoturvaloukkaukset kirjataan ja selvitetään viipymättä ja havaitut riskit saatetaan hallintaan.

# 6 LIITTEET

Liite 1: Yleiset tietoturvaohjeet

Liite 2: Henkilötiedon käsittelyn yleisohje

Liite 3: Tietojärjestelmäluettelo (SALAINEN, JulkL 621/1999, § 24, k 7)

Liite 4: Tietoturvapoikkeamiin varautuminen (SALAINEN, JulkL 621/1999, § 24, k 7)

# Elä ihmeessä!

Kauppatie 1, PL 25
58700 Sulkava

Puh. 015-527 5200
kirjaamo@sulkava.fi

sulkava.fi