

Janakkalan kunta

# Tietoturvapolitiikka

Kunnanhallitus 13.4.2015 § 81

## Sisällys

|   |    |
|---|----|
| Johdanto .....  | 3  |
| Tietoturvapolitiikan kattavuus ja sen soveltaminen .....  | 3  |
| Tietoturvallisuus .....   | 3  |
| Tietoturvaluustavoitteet .....  | 5  |
| Roolit ja vastuut .....   | 5  |
| Tietojärjestelmien käyttö .....   | 7  |
| Tietoturvallisuuden seuranta, ylläpito ja kehittäminen.....   | 8  |
| Riskienhallinta.....  | 8  |
| Jatkuvuudenhallinta ja varautuminen.....  | 8  |
| LIITE 1: TIETOTURVALLISUUDEN PERUSTASON TOTEUTTAMINEN (Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa: 5 §)..... | 9  |
| LIITE 2: LAIT, ASETUKSET JA MÄÄRÄYKSET .....  | 10 |

## 1. Johdanto

Janakkalan kunnan toiminnan ja palvelutuotannon keskeisimpiä resursseja on tieto. Kunnan tiloissa ja niiden ulkopuolella tietoa käsittelevät kunnan henkilöstön lisäksi ulkoiset sidosryhmät ja asiakkaat. Tietoa esiintyy muiden muassa paperille tulostettuna, tallennettuna tietojärjestelmiin, kannettaviin laitteisiin ja muistivälineille sekä käyttäjien muistiin tallentuneena. Tiedon sijainnista ja olomuodosta riippuen, sitä pyritään turvaamaan hallinnollisin ja/tai teknisin menetelmin.

Kunnanhallitus on hyväksynyt kunnan johtoryhmän tässä tietoturvapoliitikassa kuvaamat, kunnan strategian mukaiset periaatteet, tavoitteet ja vastuut. Tietoturvapoliitikan onnistuneen käyttöönoton edellytyksenä on, että kunnan ylin johto sitoutuu toteuttamaan tätä politiikkaa yhdessä osaavan ja tietoturvaluuteen perehdytetyn henkilöstön sekä sidosryhmien kanssa.

## 2. Tietoturvapoliitikan kattavuus ja sen soveltaminen

Tämä tietoturvapoliitikka kattaa kaiken kunnan käyttämän tiedon riippumatta esitystavasta tai elinkaaren vaiheesta ja toimii perustana muille tietoturvaan liittyville ohjeille ja määräyksille.

Lisäksi politiikka koskee jokaista kunnan kanssa palvelussuhteessa olevaa viranhaltijaa, työntekijää ja määräaikaista henkilöä, harjoittelijaa sekä luottamushenkilöä ja tarvittavilta osin yhteistyökumppania.

Politiikka saatetaan koko henkilöstön tietoon kunnan perehdytys- ja koulutuskäytäntöjen avulla. Yhteistyökumppanien ohjeistamisesta vastaa tilaaja. Periaatteena on, että kaikki jotka käsittelevät kunnan tietoa, ovat saaneet riittävän perehdytyksen tiedon turvallisen käsittelyn varmistamiseksi.

## 3. Tietoturvallisuus

Kunnassa tietoturvallisuudella tarkoitetaan tiedon, tietojärjestelmien, tietoliikenteen ja palveluiden, sekä niiden käyttöympäristöjen ja käyttäjän itsensä turvaamista siten, että niihin kohdistuvat uhat eivät aiheuta merkittävää riskiä tiedon elinkaaren missään vaiheessa.

Periaatteena on, että tietoturvallisuus on luonnollinen, sisäänrakennettu osa kunnan palveluita ja toimintaa sekä jokaisen käyttäjän työtapoja. Tietoturvallisuuteen liittyvillä käytännöillä pyritään varmistamaan, että kunnan käyttämä tieto on:

- oikeaa ja eheää, eikä muuttunut tahallisen tai tahattoman teknisen tai inhimillisen toiminnan seurauksena
- vain siihen oikeutettujen saatavilla
- saatavilla aina sitä tarvittaessa.

Lisäksi tietoon sen käsittelyn eri vaiheissa tehdyt muutokset on tarvittaessa kyettävä todentamaan.

Kunnan tietoturvallisuuteen liittyvää toimintaa johdetaan ja kehitetään osana kunnan hallintojärjestelmää ja se liittyy kiinteästi kunnan kokonaisturvallisuuteen, joka muodostuu seuraavista osa-alueista:

**Turvallisuusjohtaminen** on turvallisuuden toteutumisen ohjaamista ja valvomista kaikilla turvallisuuden osa-alueilla, mukaan lukien riskienhallinta ja varautuminen.

**Henkilöstöturvallisuus** on henkilöstöön kohdistuvien ja henkilöstöstä aiheutuvien riskien hallintaa. Henkilöstöturvallisuuden perustana on osaava ja sitoutunut henkilöstö, jolle tietoturvastuut ja -tehtävät on selkeästi perehdytetty. Henkilöstöturvallisuuteen pyritään vaikuttamaan palvelussuhteen kaikissa vaiheissa – rekrytointivaiheessa, työsuhteen aikana ja työsuhteen päätyttyä tehtävillä toimenpiteillä.

**Fyysinen turvallisuus** käsittää toimenpiteet, järjestelmät ja rakenteet, joiden avulla kunnan tiloja, ja siellä olevia ihmisiä, tietoa ja muuta omaisuutta, suojataan fyysisiltä vahingoilta, vahingoittamisyrityksiltä, oikeudettomilta henkilöiltä ja erilaisilta kiinteistövahingoilta. Fyysistä turvallisuutta toteutetaan mm. vartiointilla, kameravalvonnalla, kulunvalvonnalla ja turvallisilla rakenteilla.

**Tietosuoja** tarkoittaa henkilön yksityisyyden ja henkilötietojen suojaamista niin, että henkilön yksilöiviä tietoja ei paljastu asiattomille käsittelyprosessin missään vaiheessa. Kuntalaisia

koskevat yksilöivät henkilötiedot ovat kunnan keskeisimpiä suojattavia tietoja ja vaativat siten käsittelijöiltä erityistä huomiota.

**Työturvallisuus ja -suojelu** kattavat sekä henkilöstöön kohdistuvien että henkilöstön aiheuttamien, tahallisten ja tahattomien, vahingontekojen estämiseen tähtäävät toimenpiteet.

Perustana kunnan tietoturvatyössä käytetään ensisijassa Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) suosituksia ja Tietoturvasojen kuvaaman Perustason vaatimuksia (LIITE 1: Valtioneuvoston asetus tietoturvallisuudesta valtioneuvostossa 681/2010).

#### 4. Tietoturvaluustavoitteet

Kunnan tietoturvaluustavoitteet ovat tärkeysjärjestyksessä seuraavat:

1. Kunnan henkilökunnalla on vähintään Tietoturvasojen Perustason tietoturva- ja tietosuojasaaminen tehtäviensä suorittamiseksi.
2. Tekniset ja hallinnolliset tietoturvajärjestelyt täyttävät keskeisiltä osin Perustason vaatimukset.
3. Kunnan käyttämää tietoa ei paljastu tietoon oikeudettomille tahoille.

#### 5. Roolit ja vastuut

Kunnan tietoturvaluuteen liittyvät roolit ja vastuut ovat:

##### Kunnanhallitus

- Tietoturvapoliitiikan hyväksyminen

##### Kunnanjohtaja

- Tietoturvan ja tietosuojan järjestäminen ja toimintaedellytysten luominen
- Poikkeusolojen viestinnän johtaminen
- Varautuminen ja jatkuvuudenhallinta yhdessä kunnan johtoryhmän kanssa
- Tietoturvaohjeiden ja muiden vastaavien ohjeiden vahvistaminen

##### Toimialajohtajat

- Omistajan nimeäminen tietojärjestelmille
- Tietoturvaluuden toteutuminen omalla toimialallaan

### Tietohallinto

- Tietoturvallisuuden suunnittelu, ohjaus, seuranta ja kehittäminen
- Teknisen tietoturvallisuuden minimivaatimusten määrittely, toteutus, ohjaus ja valvonta kunnan tietojärjestelmäympäristössä
- Tietoturvallisuuden teknisen valvonnan toteutuminen tietojärjestelmäympäristössä, lain sallimin ja yhteistoimintamenettelyn valtuuttamin menetelmin
- Tietoturvariskien ja -poikkeamien hallinnan koordinointi
- Tietoturvallisuuden tilan raportointi kunnanjohtajalle

### Konsernipalvelut

- Kunnan tietouden ylläpitäminen koskien tietoturvallisuuteen vaikuttavia lakeja, säädöksiä ja määräyksiä, sekä huolehtiminen niiden huomioimisesta tietoturvaluustoiminnassa
- Henkilöstöturvallisuuden ja henkilöstötietojen käytön ohjaus ja koordinointi työntekijän palvelussuhteen kaikissa vaiheissa

### Tietosuojavastaavat

- Auttaa rekisterinpitäjää saavuttamaan hyvän henkilötietojen käsittelytavan ja mahdollisten erityislakien edellyttämän tietosuojan tason

### Tietojärjestelmän, tiedon tai prosessin omistaja

- Omistamaansa tai hallinnoimaansa järjestelmään, tietoon tai prosessiin liittyvä:
  - Pääkäyttäjän nimeäminen ko. järjestelmän osalta
  - Käyttäjien ja käyttöoikeuksien hyväksyntä ko. järjestelmään
  - Riskien- ja jatkuvuudenhallintatoimenpiteiden toteuttaminen omalta osaltaan
  - Tiedon oikeellisuuden ja oikeiden käsittelytapojen varmistaminen
  - Tietojen julkisuuden ja salassapidon määrittely mukaan lukien arkistonmuodostus

### Pääkäyttäjä

- Tietoturvan toteutumisen valvonta omalla vastualueellaan
- Sovelluksen ylläpitotoiminnoista huolehtiminen ja varmistaminen, että järjestelmää käytetään lakien, säädösten ja ohjeiden mukaisesti
- Tietosuojavastaavien avustaminen, henkilöstön neuvonta ja kouluttaminen
- Käyttäjien ja käyttöoikeuksien toteuttaminen

### Esimies

- Tietoturvallisuuden toteutuminen alaisessaan toiminnassa

**Tiedon ja tietojärjestelmien käyttäjä**

- Määräysten ja ohjeiden noudattaminen sekä tietoturvaan liittyvien poikkeuksien, uhkien ja riskien välitön ilmoittaminen joko esimiehelle, tietohallintoon tai tietosuojavastaaville

**Asianhallintasihteeri**

- Yksiköiden arkistonmuodostuksen ohjaaminen ja neuvonta
- Kunnanarkistoon siirretyistä asiakirjoista huolehtiminen ja niistä tietojen antaminen

**6. Tietojärjestelmien käyttö**

Kunnan käytössä olevat ICT-palvelut, -järjestelmät, -laitteet ja -ohjelmistot, on tarkoitettu työtehtävien hoitamista varten. Kunnan tietojärjestelmiä ei tule käyttää toimintaan mikä saattaa, välittömästi tai välillisesti, vaarantaa kunnan vastuulla olevan tiedon ja/tai järjestelmien turvallisuuden ja aiheuttaa haittaa kunnalle, sen toiminnalle tai käyttäjälle itselleen.

Tietojärjestelmien vähäinen käyttö henkilökohtaisiin tarkoituksiin on sallittu omalla ajalla. Henkilökohtainen käyttö ei kuitenkaan saa aiheuttaa ylimääräisiä kustannuksia kunnalle, eikä vaarantaa kunnan tietoa tai tietojärjestelmiä.

Tietojärjestelmiä, laitteita ja ohjelmistoja kunnan tietoverkkoon saa asentaa vain tietohallinto tai sen valtuuttama taho.

Käyttöoikeudet kunnan tietojärjestelmiin ja tietoon myönnetään vain kunnan tehtävien hoitoon liittyen. Pääsääntöisesti tarvittavat oikeudet määrittelee esimies.

Tietojärjestelmien turvallinen käyttäminen etätöitä tehdessä vaati etätöyöntekijältä erityistä huolellisuutta ja sitoutumista tietoturvaohjeiden noudattamiseen.

Väärinkäyttöihin puututaan välittömästi kunnan normaalein kurinpitomenettelyin.

Kunnan tietoverkkojen toimintaa valvotaan erityisillä valvontamenetelmillä ja -ohjelmistoilla. Toiminnan ja turvallisuuden takaamiseksi tietoliikenteestä suodatetaan palomuurijärjestelmän

avulla haittaohjelmat ja muu asiaton sisältö sekä estetään pääsy haitalliseksi luokitelluille sivustoille.

## 7. Tietoturvallisuuden seuranta, ylläpito ja kehittäminen

Kunnan tietoturvallisuustavoitteiden toteutumista ja järjestelyjen riittävyyttä seurataan säännöllisesti hallintojärjestelmän mukaisesti.

Tietoturvallisuuden ylläpito ja kehittäminen sovitetaan yhteen palveluiden, toimintatapojen ja teknisten ratkaisujen kehittämisen kanssa. Lisäksi säännöllinen tiedottaminen, osaamisen ylläpito ja koulutus ovat olennaisessa roolissa tietoturvallisuuden kehittämisessä.

## 8. Riskienhallinta

Tietoturvallisuus on kiinteä osa kunnan säännöllisiä ja koko organisaation laajuisia riskienhallintakäytäntöjä ja kuuluu jokaisen työntekijän vastuulle. Riskienhallinnan avulla palveluihin, toimintaan ja tietoon kohdistuvia riskejä kartoitetaan, analysoidaan ja hallitaan järjestelmällisesti.

Riskienhallintakäytäntöjen tavoitteena on riskien rajoittaminen hyväksyttävälle tasolle niin, että käytetyt keinot ovat suhteessa suojattavan kohteen kriittisyyteen ja riskin suuruuteen.

## 9. Jatkuvuudenhallinta ja varautuminen

Kunta pyrkii varmistamaan toimintansa ja palveluidensa jatkuvuuden normaalioloissa, normaaliolojen häiriötilanteissa sekä poikkeusoloissa. Poikkeusoloja varten kunta ylläpitää valmiussuunnitelmaa.



## LIITE 1: TIETOTURVALLISUUDEN PERUSTASON TOTEUTTAMINEN (Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa: 5 §)

**Tietoturvallisuuden toteuttamiseksi valtionhallinnon viranomaisen on huolehdittava että:**

1. viranomaisen toimintaan liittyvät tietoturvallisuusriskit kartoitetaan;
2. viranomaisen käytössä on riittävä asiantuntemus tietoturvallisuuden varmistamiseksi ja että tietoturvallisuuden hoitamista koskevat tehtävät ja vastuu määritellään;
3. asiakirjojen käsittelyä koskevat tehtävät ja vastuut määritellään;
4. tietojen saanti ja käytettävyys eri tilanteissa turvataan ja luodaan menettelytavat poikkeuksellisten tilanteiden selvittämiseksi;
5. asiakirjojen ja niihin sisältyvien tietojen salassapito ja muu suoja varmistetaan antamalla pääsy asiakirjoihin vain niille, jotka tarvitsevat salassa pidettäviä tietoja tai henkilörekisteriin talletettuja henkilötietoja työtehtäviensä hoitamiseksi;
6. tietojen luvaton muuttaminen ja muu luvaton tai asiaton käsittely estetään käyttöoikeushallinnan, käytön valvonnan sekä tietoverkkojen, tietojärjestelmien ja tietopalvelujen asianmukaisilla ja riittävillä turvallisuusjärjestelyillä ja muilla toimenpiteillä;
7. asiakirjojen tietojenkäsittely- ja säilytystilat ovat riittävästi valvottuja ja suojattuja;
8. henkilöstön ja muiden asiakirjojen käsittelyyn liittyviä tehtäviä hoitavien luotettavuus varmistetaan tarvittaessa turvallisuusselvitysmenettelyn ja muiden lain perusteella käytettävissä olevien keinojen avulla;
9. henkilöstölle ja muille asiakirjojen käsittelyyn liittyviä tehtäviä hoitaville annetaan ohjeet ja koulutusta asiakirjojen ja niihin sisältyvien tietojen asianmukaisesta käsittelystä;
10. annettujen ohjeiden noudattamista valvotaan ja niiden muutostarpeita arvioidaan säännöllisesti.

Valtionhallinnon viranomaisen velvollisuudesta huolehtia tietojen suojaamisesta annettaessa salassa pidettäviä tietoja toimeksiantotehtävän suorittamista varten säädetään viranomaisten toiminnan julkisuudesta annetun lain 26 §:n 2 momentissa. Henkilörekisteriin talletettujen henkilötietojen antamisesta säädetään lisäksi henkilötietolain 32 §:n 2 momentissa.

## LIITE 2: LAIT, ASETUKSET JA MÄÄRÄYKSET

### Arkistolaki (831/1994)

Arkistointia on hoidettava siten, että se tukee arkistonmuodostajan tehtävien suorittamista sekä yksityisten ja yhteisöjen oikeutta saada tietoja julkisista asiakirjoista, että yksityisten ja yhteisöjen oikeusturva samoin kuin tietosuojaa on otettu asianmukaisesti huomioon ja että yksityisten ja yhteisöjen oikeusturvaan liittyvien asiakirjojen saatavuus on varmistettu sekä että asiakirjat palvelevat tutkimuksen tiedon lähteinä.

### Hallintolaki (434/2003)

Tarkoituksena on toteuttaa ja edistää hyvää hallintoa sekä oikeusturvaa hallintoasioissa. Lain tarkoituksena on myös edistää hallinnon palvelujen laatua ja tuloksellisuutta.

### Henkilötietolaki (523/1999)

Tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista (1§). Sovelletaan henkilötietojen automaattiseen käsittelyyn. Myös muuhun henkilötietojen käsittelyyn sovelletaan tätä lakia silloin, kun henkilötiedot muodostavat tai niiden on tarkoitus muodostaa henkilörekisteri tai sen osa (2 §).

### Laki eräiden suojauksen purkujärjestelmien kieltämisestä (1117/2001)

Lakia sovelletaan televerkon avulla tarjottavien tietoyhteiskunnan palvelujen suojaamiseen niiden suojauksen purkujärjestelmien oikeudetonta käyttöä vastaan.

## **Laki julkisen hallinnon tietohallinnon ohjauksesta (634/2011)**

Tarkoitus tehostaa julkisen hallinnon toimintaa sekä parantaa julkisia palveluja ja niiden saatavuutta säätämällä julkisen hallinnon tietohallinnon ohjauksesta ja tietojärjestelmien yhteen toimivuuden edistämisestä ja varmistamisesta (1 §).

## **Laki julkisista hankinnoista (1505/1992)**

Lain tavoitteena on tehostaa julkisten varojen käyttöä, edistää laadukkaiden hankintojen tekemistä sekä turvata yritysten ja muiden yhteisöjen tasapuolisia mahdollisuuksia tarjota tavaroita, palveluita ja rakennusurakointia julkisten hankintojen tarjouskilpailuissa. Valtion ja kuntien viranomaisten sekä muiden hankintayksiköiden on kilpailutettava hankintansa siten kuin tässä laissa säädetään.

## **Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004)**

Laissa säädetään viranomaisten toimenpiteistä kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseksi. Lakia sovelletaan myös elinkeinonharjoittajaan ja tämän palveluksessa olevaan silloin, kun elinkeinonharjoittaja on sopimusosapuolena turvallisuusluokitellussa sopimuksessa tai osallistuu tällaista sopimusta edeltävään hankintakilpailuun tai toimii tällaisen elinkeinonharjoittajan alihankkijana.

## **Laki lasten kanssa työskentelevien rikostaustan selvittämisestä (504/2002)**

Lain tarkoituksena on suojella alaikäisten henkilökohtaista koskemattomuutta ja edistää heidän henkilökohtaista turvallisuuttaan. Laissa säädetään menettelystä, jolla alaikäisten kanssa työskentelemään valittavien henkilöiden rikostaustaa selvitetään.

## **Laki potilaan asemasta ja oikeuksista (785/1992)**

Jollei muussa laissa toisin säädetä, sovelletaan tätä lakia Potilaan asemaan ja oikeuksiin terveyden- ja sairaanhoitoa järjestettäessä.

## **Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (2000/812)**

Edistää asiakaslähtöisyyttä ja asiakassuhteen luottamuksellisuutta sekä asiakkaan oikeutta hyvään palveluun ja kohteluun sosiaalihuollossa.

## **Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007)**

Lain tarkoituksena on edistää sosiaali- ja terveydenhuollon asiakastietojen tietoturvallista sähköistä käsittelyä. Lailla toteutetaan yhtenäinen sähköinen potilastietojen käsittely- ja arkistointijärjestelmä terveydenhuollon palvelujen tuottamiseksi potilasturvallisesti ja tehokkaasti sekä potilaan tiedonsaantimahdollisuuksien edistämiseksi.

## **Laki sähköisistä allekirjoituksista (14/2003)**

Laissa säädetään vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista sekä niihin liittyvien palveluiden tarjoamisesta niitä käyttäville palveluntarjoajille ja yleisölle.

## **Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)**

Tarkoituksena on lisätä asioinnin sujuvuutta ja joutuisuutta samoin kuin tietoturvallisuutta hallinnossa, tuomioistuimissa ja muissa lainkäyttöelimissä sekä ulosotossa edistämällä sähköisten tiedonsiirtomenetelmien käyttöä. Laissa säädetään viranomaisten ja näiden asiakkaiden oikeuksista, velvollisuuksista ja vastuista sähköisessä asioinnissa (1 §).

## **Laki sähköisestä lääkemääräyksestä 61/2007**

Jollei tästä laista muuta johdu, sähköistä lääkemääräystä laadittaessa, toimitettaessa ja käsiteltäessä on noudatettava, mitä muualla säädetään potilaan asemasta ja oikeuksista, lääkkeen määräämisestä ja toimittamisesta, henkilötietojen käsittelystä, viranomaisten toiminnan julkisuudesta, sähköisestä viestinnästä ja asioinnista sekä sähköisistä allekirjoituksista (2 §, 3. kappale).

## **Laki tietoyhteiskunnan palvelujen tarjoamisesta (458/2002)**

Säädetään tietoyhteiskunnan palvelujen tarjoamiseen liittyvistä seikoista, erityisesti palvelujen tarjoamisen vapaudesta, palvelun tarjoajien velvollisuudesta antaa tietoja, sopimusta koskevien muotovaatimusten täyttämisestä sähköisesti sekä välittäjänä toimivien palvelun tarjoajien vastuuvapaudesta (1 §).

## **Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista 617/2009**

Säädetään vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista sekä niihin liittyvien palveluiden tarjoamisesta niitä käyttäville palveluntarjoajille ja yleisölle (1 §).

## **Laki turvallisuusselvityksistä (177/2002)**

Säätää turvallisuusselvityksestä, joka voidaan tehdä suppeana, perusmuotoisena tai laajana. Voidaan tehdä virkaan tai tehtävään hakeutuvasta, tehtävään tai koulutukseen otettavasta taikka virkaa tai tehtävää hoitavasta henkilöstä.

## **Laki viranomaisten toiminnan julkisuudesta (621/1999)**

Säädettyjen tiedonsaantioikeuksien ja viranomaisten velvollisuuksien tarkoituksena on toteuttaa avoimuutta ja hyvää tiedonhallintatapaa viranomaisten toiminnassa sekä antaa yksilöille ja yhteisöille mahdollisuus valvoa julkisen vallan ja julkisten varojen käyttöä, muodostaa vapaasti mielipiteensä sekä vaikuttaa julkisen vallan käyttöön ja valvoa oikeuksiaan ja etujaan (3 §).

## **Asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintotavasta (1030/1999)**

Viranomaisen on viranomaisten toiminnan julkisuudesta annetun lain (621/1999) 18 §:n 1 momentin 4 kohdassa tarkoitettujen toimenpiteiden suunnittelua ja toteuttamista varten arkistolaisissa (831/1994) tarkoitettua arkistonmuodostussuunnitelmaa hyväksi käyttäen

selvitettävä ja arvioitava asiakirjansa ja tietojärjestelmänsä sekä niihin talletettujen tietojen merkitys samoin kuin asiakirja- ja tietohallintonsa.

## **Laki yksityisyyden suojasta työelämässä (759/2004)**

Tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia työelämässä (1 §). Säädetään työntekijää koskevien henkilötietojen käsittelystä, työntekijälle tehtävistä testeistä ja tarkastuksista sekä niitä koskevista vaatimuksista, teknisestä valvonnasta työpaikalla sekä työntekijän sähköpostiviestin hakemisesta ja avaamisesta. Mitä tässä laissa säädetään työntekijästä, sovelletaan myös virkamieheen, virkasuhteessa olevaan ja näihin verrattavassa julkisoikeudellisessa palvelussuhteessa olevaan sekä soveltuvin osin työnhakijaan (2 §).

## **Rikoslaki (39/1889)**

Laissa säädetään mm. seuraavat kokonaisuudet:

- Virkarikokset
- Aineettomien oikeuksien loukkaaminen
- Tieto- ja viestintärikokset
- Yleisvaaralliset rikokset (Vaaran aiheuttamiseen tietojenkäsittelylle)
- Yksityisyyden, rauhan ja kunnian loukkaaminen

## **Sosiaali- ja terveystieteiden ministeriön asetus potilasasiakirjoista (2009/298)**

Sovelletaan potilaan hoidon järjestämisessä ja toteuttamisessa käytettävien asiakirjojen laatimiseen sekä niiden ja muun hoitoon liittyvän materiaalin säilyttämiseen (2 §).

## **Suomen perustuslaki (731/1999) 10 §**

Jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla. Kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton.

## **Sähköisen viestinnän tietosuojalaki (516/2004)**

Tarkoituksena on turvata sähköisen viestinnän luottamuksellisuuden ja yksityisyyden suojan toteutuminen sekä edistää sähköisen viestinnän tietoturvaa ja monipuolisten sähköisen viestinnän palvelujen tasapainoista kehittymistä (1 §).

## **Terveydenhuoltolaki (1326/2010)**

Käytettäessä toisen terveydenhuollon toimintayksikön tietoja tietojärjestelmien välityksellä, on potilastietojen käyttöä seurattava sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain (159/2007) 5 §:n edellyttämällä tavalla. Hoitosuhde potilaan ja luovutuspyynnön tekijän välillä on varmistettava tietoteknisesti. Sairaanhoidopiirin kuntayhtymän on vastattava yhteisen potilastietorekisterin edellyttämistä koordinoitavista sekä huolehdittava siitä, että tietojärjestelmien välityksellä tapahtuvissa tietojen luovutuksissa noudatetaan 2 ja 3 momentissa säädettyjä velvoitteita. Kukin terveydenhuollon toimintayksikkö vastaa omassa toiminnassaan syntyneiden potilasasiakirjojen rekisterinpidosta.

## **Valmiuslaki (1080/1991)**

Lain tarkoituksena on poikkeusoloissa suojata väestöä sekä turvata sen toimeentulo ja maan talouselämä, ylläpitää oikeusjärjestystä, perusoikeuksia ja ihmisoikeuksia sekä turvata valtakunnan alueellinen koskemattomuus ja itsenäisyys.

## **Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (2010/681)**

Asetuksessa säädetään valtionhallinnon viranomaisten asiakirjojen käsittelyä koskevista yleisistä tietoturvallisuusvaatimuksista sekä asiakirjojen luokittelun perusteista ja luokittelua vastaavista asiakirjojen käsittelyssä noudatettavista tietoturvallisuusvaatimuksista (1 §).

## **Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuudesta (VM0024:00/02/99/1998), VAHTI 7/2009**

Periaatepäätöksellä ohjataan valtionhallintoa kehittämään tietoturvallisuutta tärkeänä osana johtamista, osaamista, riskienhallintaa sekä hallinnon kehittämistä ja toimintaa.

### **Viestintäviraston määräyksiä**

- Viestintävirasto 9 B/2004 M, määräys tietoturvaloukkausten sekä vika- ja häiriötilanteiden ilmoittamisvelvollisuudesta yleisessä teletoiminnassa
- Viestintävirasto 11/2004 M, määräys sähköpostipalvelujen tietoturvasta ja toimivuudesta
- Viestintävirasto 47 B/2004 M, määräys teleyritysten tietoturvasta
- Viestintävirasto 48 B/2004 M, määräys viestintäverkon fyysisestä suojaamisesta