Tuusulan kunta
Tietoturvapolitiikka

Hyväksyntä	
Julkisuusluokka	
Sijainti	
Versio	

Sisällys

1 Johdanto

Tuusulan kunnan toiminta ja palvelut perustuvat enenevässä määrin tietoon. Ollakseen tehokkaasti hyödynnettävissä, tietoa tukevien järjestelyjen tulee toimia asianmukaisesti kaikissa tilanteissa. Tämä edellyttää tehokasta johtamista luotettavien toteutusten ja osaavan henkilöstön tueksi.

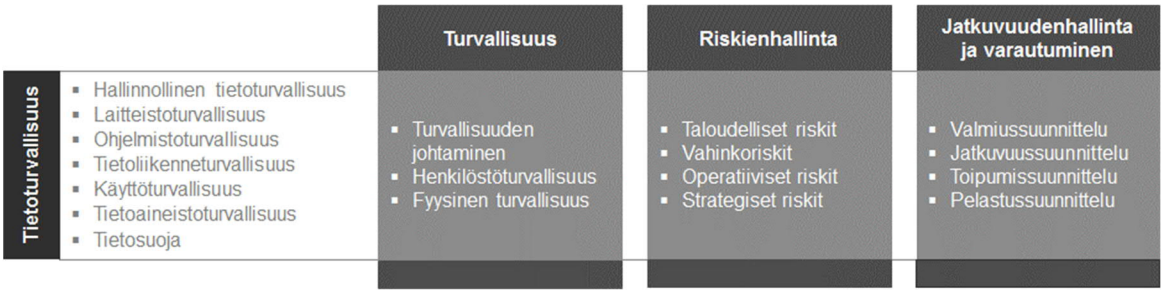
Kunnan johto määrittelee tässä Tuusulan kunnan tietoturvapolitiikassa tietoturvallisuutta koskevat periaatteet, vastuut ja tavoitteet. Politiikka toimii perustana kunnan tietoturvallisuutta koskeville ohjeille, joiden tehtävänä on tarkentaa politiikassa annettuja määräyksiä ja ohjeistaa niiden käytäntöön soveltamisessa. Tietoturvapolitiikka ja sen soveltamisohjeet pidetään käyttäjien saatavilla intranetissä.

Tietoturvapolitiikka koskee koko kuntaorganisaatiota sekä kaikkia sen sidosryhmien edustajia, jotka toimeksiantojensa puitteissa käsittelevät kunnan omistamaa tai hallinnoimaa tietoa. Politiikka kattaa kunnan käyttämän, omistaman ja hallinnoiman tiedon riippumatta tiedon esitystavasta, muodosta, suojaustasosta tai elinkaaren vaiheesta.

2 Mitä tietoturvallisuus on?

Tietoturvallisuus on kiinteä osa kunnan johtamista, palveluita ja toimintoja. Lisäksi tietoturvallisuus liittyy jokaisen työntekijän arkipäivän työtehtäviin ja työtapoihin.

Tietoturvallisuus integroituu kuvan 1 mukaisesti kaikkiin kokonaisturvallisuuden osa-alueisiin: turvallisuus, riskienhallinta sekä jatkuvuudenhallinta ja varautuminen.



Kuva 1. Kunnan kokonaisturvallisuus

Tietoturvallisuuteen liittyvillä vastuilla ja käytännöillä pyritään varmistamaan, että kunnan omistama ja hallinnoima:

- tieto on oikeaa ja eheää, eikä muuttunut tahallisen tai tahattoman teknisen tai inhimillisen toiminnan seurauksena
- tieto on vain siihen oikeutettujen saatavilla
- tieto on saatavilla aina sitä tarvittaessa
- tietoon tehdyt muutokset sen käsittelyn eri vaiheissa on tarvittaessa kyettävä todentamaan.

2.1 Tietoturvallisuuden hallinta

Kunnan tietoturvallisuuteen liittyvää toimintaa johdetaan ja kehitetään osana kunnan johtamisjärjestelmää. Tietoturvallisuuden osalta kokonaisuus sisältää suunnitteluun, toteutukseen, seurantaan ja ohjaukseen liittyvät prosessit, asiakirjat, kontrollit ja vastuut.

Kunnan tietoturvatyötä ohjaavat, soveltuvilta osin, seuraavat viitekehykset:

- Kuntaa velvoittavat lait ja asetukset
- Julkisen hallinnon tietohallinnon neuvottelukunnan (JUHTA) suositukset
- Kunnan omat strategiat ja niistä johdetut vaatimukset
- Valtionhallinnon Tietoturvallisuuden johtoryhmän (VAHTI) ohjeet
- Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010).

2.2 Riskienhallinta sekä jatkuvuuden hallinta ja varautuminen

Kunnanvaltuuston hyväksymä ja kunnan johtoryhmän organisoima riskienhallintaprosessi toimii kunnan turvallisuusjärjestelyiden ja varautumisen perustana.

Riskienhallinnan tavoitteena on riskien rajoittaminen hyväksyttävälle tasolle niin, että riskienhallintakeinot ovat suhteessa suojattavan kohteen kriittisyyteen ja riskin suuruuteen. Riskienhallinta kattaa kaikki riskit, mukaan lukien tietoon kohdistuvat ja tiedosta aiheutuvat riskit.

Kunnan tulee varautua turvaamaan sen toiminnan ja palveluiden jatkuvuus normaalioloissa, normaaliolojen häiriötilanteissa sekä poikkeusoloissa. Tätä varten kunta voi tarvittaessa laatia erillisiä suunnitelmia prosessien ja tietojärjestelmien tueksi.

3 Tietoturvallisuustavoitteet

Kunnan tavoitteena on saavuttaa Tietoturvallisuusasetuksen (681/2010) kuvaaman tietoturvallisuuden perustason vaatimukset koko kunnan laajuisesti ja korotetun tason vaatimukset lainsäädännön edellyttämissä toiminnoissa tai toiminnan tarpeiden niin vaatiessa.

4 Organisointi ja vastuut

Kunnan keskeisimmät tietoturvallisuuteen liittyvät toimijat ja roolit vastuineen on määritelty alla. Mikäli kunnan hallinto- tai muissa säännöissä ei ole määritelty kenelle roolin vastuu kuuluu, on kunnanjohtaja vastuussa sopivimman henkilön nimeämisestä kyseiseen rooliin. Kaikki roolit ja vastuut kuvataan liitteessä 1.

Kunnanhallitus hyväksyy kunnassa noudatettavan tietoturvapolitiikan (ja valvoo tietoturvapolitiikan toteutumista).

Kunnanjohtaja toimii tietoturvallisuuden ja tietosuojan omistajana kunnassa luoden edellytykset niiden asianmukaiselle toteuttamiselle. Tarvittaessa kunnanjohtaja nimeää vastuuhenkilöitä seuraamaan tietoturvan ja tietosuojan toteutumista, tekemään kehitysehdotuksia sekä toimimaan tietosuojavastaavien sekä järjestelmien pääkäyttäjien tukena.

Toimialajohtaja vastaa tietoturvallisuuden ja tietosuojan toteutuksesta johtamansa toiminnan osalta ja siitä, että järjestelmien omistajat sekä pääkäyttäjät on nimetty.

Tietojärjestelmän **omistaja** vastaa omistukseensa liittyvästä:

- Käyttäjien ja käyttöoikeuksien määrittelystä ja hyväksynnästä
- Riskienhallinnan toteuttamisesta, sisältäen riittävän dokumentaation varmistamisen järjestelmästä
- Tiedon eheyden varmistamisesta
- Tietojen luokittelusta (julkisuuden ja salassapidon määrittely, arkistonmuodostus).
- Rekisteriselosteen tai tietoturvaselosteen laadinnasta ja nimeää rekisterin yhteyshenkilön

ICT-johtoryhmä tukee toimialoja tietoturvapolitiikan toteuttamisessa mm. antamalla uusista järjestelmähankinnoista lausunnon tietoturvaan ja kokonaisarkkitehtuuriin liittyen.

Järjestelmän **pääkäyttäjä** valvoo tietoturvan ja käyttöoikeuspolitiikan toteutumista omalla vastuualueellaan. Pääkäyttäjä huolehtii sovelluksen ylläpitotoiminnoista ja toimii yhdyshenkilönä järjestelmätoimittajaan. Pääkäyttäjä tiedottaa käyttäjiä vikatilanteista ja käyttökatkoista ja huolehtii käyttökatkojen aikataulutuksista.

Esimies vastaa tietoturvallisuuden ja tietosuojan toteutumisesta alaisessaan toiminnassa sekä erityisesti alaisten ja muun henkilökunnan riittävästä perehdyttämisestä tietoturvapolitiikkaan ja siihen liittyviin tietoturvaohjeisiin.

Tiedon ja tietojärjestelmien **käyttäjä** vastaa omalta osaltaan määräysten ja ohjeiden noudattamisesta. Jokaisen käyttäjän vastuulla on lisäksi tietoturvaan ja tietosuojaan liittyvien poikkeamien, uhkien ja riskien ilmoittaminen viipymättä joko esimiehelle tai Tietojärjestelmäpalveluiden Helpdeskiin tai muuten virallisesti sovitulla tavalla.

Tietoturvapäällikkö vastaa tietoturvallisuuden toteutumisesta ja integroitumisesta muihin kokonaisturvallisuuden osa-alueisiin. Vastuuseen sisältyy tarvittava suunnittelu, ohjaus, seuranta ja kehittäminen, sekä tietoturvariskien ja -poikkeamien hallinnan koordinointi. Tietoturvapäällikkö raportoi kunnanjohtajalle.

Tietojärjestelmäpalvelut vastaa tietoturvallisuuden ja teknisen valvonnan toteutumisesta tietojärjestelmäympäristössä, lain sallimin ja yhteistoimintamenettelyn valtuuttamin menetelmin.

Tietosuojavastaava toimii kunnan erityisasiantuntijana henkilötietojen käsittelyyn liittyvissä asioissa. Tietosuojavastaava antaa asiantuntija-apua sekä kunnan henkilöstölle että ennen kaikkea johdolle, jolla on rekisterinpitäjän vastuu henkilötietojen käsittelystä. Tietosuojavastaava raportoi kunnanjohtajalle. Kunnassa on erillinen ohjeistus tietosuoja-asioista. Tarvittaessa toimialoilla nimetään toimialakohtainen tietosuojavastaava, jos lainsäädäntö tai toiminnan tarpeet niin edellyttävät.

5 Tiedon ja tietojärjestelmien käyttö

Kunnassa noudatetaan lainsäädännön tarkoittamaa hyvää tietojenkäsittelyn ja –hallinnan tapaa. Kunnan tietoja ja tietojärjestelmiä käytettäessä tulee noudattaa seuraavia tietoturvallisuutta edistäviä periaatteita ja sääntöjä.

1. Kunnan käytössä oleva tieto sekä tietojärjestelmät, laitteet ja ohjelmistot on tarkoitettu ensisijaisesti työtehtäviä varten.
2. Kunnan tietojärjestelmäympäristössä saa käyttää ainoastaan tietohallinnon hyväksymiä tietojärjestelmiä, laitteita ja ohjelmistoja.
3. Asennustyön saa suorittaa vain tietohallinto tai sen valtuuttama taho.
4. Kunnan toimintaa ja palveluita tukevat tietojärjestelmät tunnistetaan, luokitellaan kriittisyyden perusteella ja niille nimetään omistaja.
5. Käyttöoikeudet kunnan tietoon ja tietojärjestelmiin myönnetään työtehtävien hoitoon tarvittavassa laajuudessa. Toteutuksesta riippuen käyttöoikeudet hyväksyy käyttäjän esimiehen hakemuksen perusteella tietojärjestelmän omistaja tai hänen valtuuttamansa taho.
6. Laiminlyönteihin ja väärinkäytöksiin puututaan välittömästi kunnan normaalein kurinpidollisin keinoin tai lainsäädännön edellyttämällä tavalla.
7. Tiedon turvalliset käsittelytavat ja tietoturvapoikkeamien hallintakäytännöt kuvataan erillisissä ohjeissa.

Tietoturvarikkomuksista voi olla seurauksena käyttöoikeuksien rajoituksia, työsuhteeseen vaikuttavia toimenpiteitä sekä laissa ja asetuksissa määriteltyjä seuraamuksia. Työsuhteeseen vaikuttavista seuraamuksista on säädetty ensisijassa työsopimuslaissa ja viranhaltijalaissa. Sovellettavaksi voivat tulla myös rikos- ja vahingonkorvauslainsäädäntö. Tietoturvarikkomuksista ilmoitetaan aina esimiehelle.

6 Tietoturvaosaamisen ja -tietoisuuden ylläpito

Jokainen uudessa tehtävässä aloittava työntekijä perehdytetään kunnan perehdytyskäytäntöjen mukaisesti tietoturvan perusteisiin ja tietoturvan toteuttamiseen hänen omissa työtehtävissään. Lisäksi tietoturvallisuuden peruskoulutusta on tarjolla säännöllisesti ja tietoturvaohjeet ovat kaikkien työntekijöiden saatavilla.

Tietoturvallisuuden ja tietosuojan ylläpidosta, kehittämisestä ja johtamisesta vastaaville tarjotaan riittävä hallinnollinen ja tekninen koulutus.

7 Tietoturvallisuuden seuranta, ylläpito ja kehittäminen

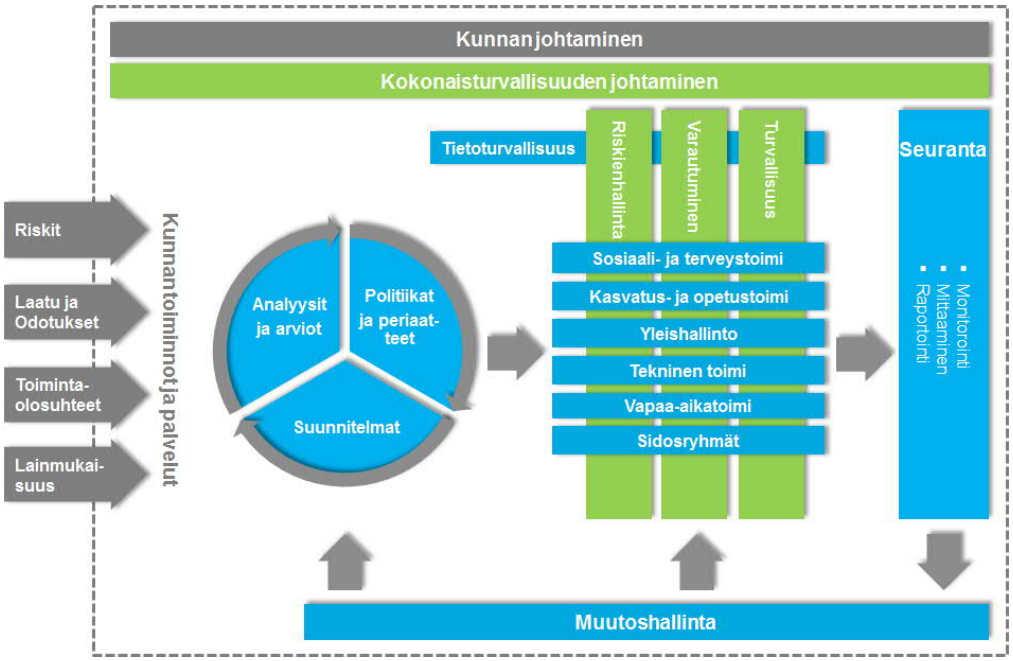
Kunnan tietoturvallisuustyö perustuu toiminnan, teknologian ja osaamisen jatkuvaan kehittämiseen seuraavassa kokonaisturvallisuusprosessissa kuvattujen vaiheiden mukaisesti:

SUUNNITTELU -vaiheessa tuotetaan analyysien ja arvioiden perusteella politiikkoja, periaatteita ja suunnitelmia. Tässä vaiheessa vaatimuksia asettavat mm. lainmukaisuus, riskienhallinnan tulokset, vaatimukset (asukkaat, asiakkaat, henkilökunta, sidosryhmät) ja toimintaolosuhteet.

TOTEUTUS -vaiheessa edellisen vaiheen tuotokset otetaan käyttöön kunnan toiminnassa.

SEURANTA -vaiheessa suoritetaan teknistä valvontaa ja hallinnollista seurantaa.

MUUTOSHALLINTA -vaiheessa seurantavaiheen tuloksista opitun perusteella toteutetaan muutoshallintaa kunnan normaalin muutoshallintaprosessin mukaisesti.



Kuva 2. Kunnan kokonaisturvallisuusprosessi

Tämä tietoturvapolitiikka katselmoidaan vuosittain ja päivitetään tarvittaessa.

8 Liitteet

- LIITE 1: Käsitteet ja roolit
- LIITE 2: Lait, asetukset ja direktiivit
- LIITE 3: Tietoturvallisuuden perustason toteuttaminen (Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa)

LIITE 1: KÄSITTEET JA ROOLIT

Tässä liitteessä kuvataan kunnan toiminnan kannalta keskeisimmät käsitteet, ensisijassa VAHTI-ohjeisiin perustuen (Kappale 1) sekä roolit ja vastuut (Kappale 2).

1 Käsitteet ja termit

Arkaluonteinen tieto
Yksilöä tai organisaatiota koskeva tieto, jonka rekisteröintiä ja käyttöä on rajoitettu lain tai asianomaisen vaatimuksesta. Suomen henkilötietolain mukaan arkaluonteisia ovat henkilötiedot, jotka kuvaavat tai on tarkoitettu kuvaamaan:

- rotua tai etnistä alkuperää
- henkilön yhteiskunnallista, poliittista tai uskonnollista vakaumusta tai ammattiliittoon kuulumista
- rikollista tekoa, rangaistusta tai muuta rikoksen seuraamusta
- henkilön terveydentilaa, sairautta tai vammaisuutta taikka häneen kohdistettuja hoitotoimenpiteitä tai niihin verrattavia toimia
- henkilön seksuaalista suuntautumista tai käyttäytymistä
- henkilön sosiaalihuollon tarvetta tai hänen saamiaan sosiaalihuollon palveluja, tukitoimia ja muita sosiaalihuollon etuuksia.

Arkisto
Säilytettävien dokumenttien tai tallenteiden kokoelma tai paikka, jossa sitä on tarkoitus säilyttää.

Asiakirjallinen tieto
Organisaation tai henkilön toiminnasta todisteena oleva tieto, jolla on oikeudellista tai tutkimuksellista merkitystä.

Eheys
Tietojen tai tietojärjestelmän sisäinen ristiriidattomuus, kattavuus, ajantasaisuus, oikeellisuus ja käyttökelpoisuus. Ominaisuus, joka ilmentää, että tietoa tai viestiä ei ole valtuudettomasti muutettu, ja että mahdolliset muutokset voidaan todentaa kirjausketjusta.

Ei-julkinen tieto
Tieto, jonka viranomainen voi harkintansa mukaan julkaista, vaikka ei olisi siihen velvoitettu. Ei-julkisia ovat muun muassa valmisteltavana olevat asiakirjat ja sisäiset viranomaisselvitykset.

Erityissuojattava tieto
Asiakirja tai tieto, jonka käsittelylle on asetettu erityisiä tietoturvavaatimuksia luottamuksellisuuden (salassa-pito, tietosuoja), eheyden tai käytettävyyden suhteen.

Fyysinen turvallisuus (tai Toimitilaturvallisuus)
Henkilöiden, laitteiden, aineistojen, postilähetysten, toimitilojen ja varastojen suojaaminen tuhoja ja vahinkoja vastaan. Fyysinen turvallisuus sisältää muun muassa kulun- ja tilojen valvonnan, vartioinnin, palo-, vesi-, sähkö-, ilmastointi- ja murtovahinkojen torjunnan sekä kuriirien ja tietoaineistoja sisältävien lähetysten turvallisuuden.

Haittaohjelma
Ohjelma, joka tarkoituksellisesti aiheuttaa koneen käyttäjän kannalta ei-toivottuja tapahtumia tietojärjestelmässä tai sen osassa. Haittaohjelmia ovat esimerkiksi virukset, madot ja troijanhevoset sekä näiden yhdistelmät.

Hallinnollinen tietoturvallisuus
Tietoturvallisuuteen tähtäävät hallinnolliset keinot, kuten organisaatiojärjestelyt, tehtävien ja vastuiden määrittely sekä henkilöstön ohjeistus, koulutus ja valvonta.

Henkilökortti
Kortti, jota käytetään haltijansa tunnistamiseen, esimerkiksi osoituksena henkilöllisyydestä tai valtuudesta.

Henkilörekisteri
Käyttötarkoituksensa vuoksi yhteenkuuluvista merkinnöistä muodostuva henkilötietoja sisältävä tietojoukko, jota käsitellään osin tai kokonaan tietojärjestelmällä tai joka on teknisesti järjestetty niin, että tiettyä henkilöä koskevat tiedot voidaan löytää helposti ja ilman kohtuuttomia kustannuksia.

Henkilörekisteriseloste
Henkilötietolain edellyttämällä tavalla laadittu ja saatavilla pidettävä määrämuotoinen kuvaus henkilörekisterin sisällöstä, käytöstä ja suojauksesta.

Henkilöstöturvallisuus
Henkilöstön luotettavuuteen ja soveltuvuuteen, oikeuksien hallintaan, sijaisjärjestelyihin, henkilöstön suojaamiseen ja työsuhteen sekä työyhdistelmien järjestelyihin liittyvien turvallisuustekijöiden toteuttaminen. Henkilöstöturvallisuuteen kiinnitetään huomiota työsuhteen kaikissa vaiheissa.

Henkilötieto
Luonnollista henkilöä tai hänen ominaisuuksiaan tai elinolojaan kuvaava merkintä, joka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa elävää koskevaksi.

Hyvä tiedonhallintatapa
Huolehtiminen asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen asianmukaisesta saatavuudesta, käytettävyydestä, suojaamisesta, eheydestä ja muista tietojen laatuun vaikuttavista tekijöistä. Julkisuuslain mukaan hyvään tiedonhallintatapaan sisältyy diaarin ja rekisteriselosteiden huolellinen ylläpito, asiakirjajulkisuuden vaatimat järjestelyt, asianmukainen tietosuoja ja tietoturvallisuus, henkilökunnan koulutus ja informointi näistä

seikoista, niitä koskevien ohjeiden noudattamisen valvonta, sekä varautuminen suunniteltujen hallintouudistusten vaikutuksiin asiakirjain julkisuuteen, salassapitoon ja suojaan sekä tietojen laatuun.

Hyvä tietojenkäsittelytapa
Tietojenkäsittelyä koskevaa lainsäädäntöä ja sen soveltamisohjeita noudattavat menettelyt. Hyvällä tietojenkäsittelytavalla tarkoitetaan rekisterinpitäjän velvollisuutta huolehtia hyvän tietojenkäsittelyn toteutumisesta henkilötietojen käsittelyssä. Henkilötietolaki kertoo, milloin voi kerätä ja muutoin käsitellä henkilötietoja. Hyvän tietojenkäsittelytavan kannalta tärkeimmät yleiset periaatteet ovat tällöin suunnittelu-, tarpeellisuus-, huolellisuus- ja suojaamisvelvoitteet sekä rekisteröityjen henkilöiden oikeuksien huomioon ottaminen.

Hyvä turvallisuuskulttuuri
Muodostuu kunnan johdon sitoutumisesta, osaavasta, ammattitaitoisesta ja motivoituneesta henkilöstöstä, ajantasaisesta normistosta sekä vaatimukset täyttävästä teknologiasta.

Jatkuvuuden hallinta
Toimenpiteet toiminnan jatkuvuuden turvaamiseksi.

Jatkuvuussuunnittelu
Varautuminen toiminnan häiriöihin ja keskeytyksiin niin, että toimintaa voidaan jatkaa ja häiriöiden haittavaikutuksia rajoittaa. Jatkuvuussuunnittelu on jatkuva prosessi ja osa riskienhallintaa. Työnä jatkuvuussuunnittelu on kriittisen toiminnon (esim. palvelun tai toiminnon omistajan) vastuulla olevaa työtä. Jatkuvuussuunnittelun tuotoksena syntyy kriittisten ja tärkeimpien toimintaprosessien jatkuvuussuunnitelma, jossa kuvataan toimintojen ja niitä mahdollistavan tietojenkäsittelyn ja tiedonsiirron turvaaminen niin, että ne voivat jatkua kriisien, katastrofien, onnettomuuksien, toimintaolosuhteiden merkittävien muutosten ja häiriöiden aikana sekä niiden jälkeen. Kaikki ne toimenpiteet, jotka tulee tehdä kriittisen toimintaprosessin jatkuvuuden turvaamiseksi.

Jäljitettävyys
Mahdollisuus jälkeenpäin saada yksityiskohtaisesti selville, mitä toiminnassa, esimerkiksi tietojenkäsittelyprosessissa tapahtui.

Järjestelmän omistaja
Nimetty taho, jolla on valta tai valtuudet sekä vastuu päättää järjestelmästä.

Kansalaisvarmenne
Henkilöllisyyden todistamiseen käytettävä sähköinen varmenne, joka pohjautuu väestörekisterijärjestelmään. Kansalaisvarmenne sisältää mm. varmentajan nimen, varmenteen haltijan nimen, haltijan sähköisen asiointitunnuksen (SATU), varmenteen voimassaoloajan, varmenteen käyttötarkoituksen, sekä muita tietoja, kuten tietoja varmentajan käyttämistä, laskentamenetelmistä ja varmennepolitiikasta.

Kiistämättömyys

Tietoverkossa eri menetelmin saatava näyttö siitä, että tietty henkilö on lähettänyt tietyn viestin (alkuperän kiistämättömyys), vastaanottanut tietyn viestin (luovutuksen kiistämättömyys), tai että tietty viesti tai tapahtuma on jätetty käsiteltäväksi. Luovutukseen tai käsiteltäväksi jättämiseen voidaan liittää aikaleima, joka todistaa viestin saapumisajankohdan.

Käyttäjätunnus
Tunnistamista varten annettu käyttäjätilin yksilöivä tunniste.

Käyttöturvallisuus
Sisältää kunnan päivittäisten toimintojen ja rutiinien turvaamiseksi tehtävät suojaustoimenpiteet, kuten salasanojen hallinnoinnin ja tietojärjestelmien valvonnan.

Laitteistoturvallisuus
Laitteistojen käytettävyyden, toiminnan, ylläpidon sekä laitteiden ja tarvikkeiden saatavuuden turvaavat toimenpiteet. Laitteiston elinkaarta turvataan laitteistoturvallisuudella, johon kuuluvat asennuksen, takuun ja ylläpidon lisäksi erilaiset tukipalvelut ja -sopimukset sekä laitteiston turvallinen poisto elinkaaren lopussa.

Luottamuksellisuus
Tietojen säilyminen luottamuksellisina (ettei kukaan sivullinen saa tietoa) ja tietoihin, tietojenkäsittelyyn ja tietoliikenteeseen kohdistuvien oikeuksien säilyminen vaarantumiselta ja loukkaukselta.

Ohjelmistoturvallisuus
Käyttöjärjestelmiin, varus- ja työkaluohjelmistoihin sekä muihin ohjelmistoihin kohdistuvat turvatoimet. Näitä ovat esim. ohjelmistojen tunnistamis-, eristämis-, pääsynvalvonta- ja varmistusmenettelyt, tarkkailu- ja paljastustoimet, lokimenettelyt ja laadunvarmistus.

Oikeellisuus
Virheettömyys, yhtäpitävyys todellisen asiaintilan kanssa.

Pelastussuunnittelu
Pelastussuunnitelman laatimiseksi ja ylläpitämiseksi tehtävät toimenpiteet. Lakisääteisessä pelastussuunnitelmassa kuvataan toimenpiteet ja järjestelyt onnettomuuksien ennaltaehkäisemiseksi ja vaaratilanteissa toimimiseksi. Tarkemmin pelastuslaki (379/2011) ja valtioneuvoston asetus pelastustoimesta (407/2011).

Poikkeusolot
Kansainvälisestä tilanteesta tai suuronnettomuudesta johtuva vakava vaara Suomen väestön toimeentulolle, talouselämälle, oikeusjärjestykselle, kansalaisten perusoikeuksille, maan alueelliselle koskemattomuudelle tai itsenäisyydelle.

Potilastiedot
Henkilön terveyttä ja hoitoa koskevat tiedot, joiden käsittelyssä on noudatettava potilaslain ja lain potilastietojen sähköisestä käsittelystä antamia määräyksiä.

Rekisterinpitäjä

Rekisterinpitäjällä tarkoitetaan yhtä tai useampaa henkilöä, yhteisöä. laitosta tai säätiötä, jonka käyttöä varten henkilörekisteri perustetaan ja jolla on oikeus määrätä sen käytöstä, tai jonka tehtäväksi rekisterinpito on lailla säädetty.

Riski
Todennäköisyys, että uhka toteutuu aiheuttaen tietyn menetyksen tai vahingon. Uhkaan liittyvän vahingon rahallinen arvo tai odotusarvo.
Riski voi olla myös mahdollisuus menettää päämääräksi asetettu seikka.

Riskienhallinta
Järjestelmällinen toiminta riskien rajoittamiseksi niin, että ne ovat optimisuhteessa riskien rajoittamisen kustannuksiin samalla kun organisaation toiminnalle asetetut tavoitteet voidaan saavuttaa. Riskien hallinta on jokaisen hallinnon tehtävää suorittavan henkilön vastuulla. Erikseen organisoitu riskienhallintatoiminto tukee hallinnon johtamista. Riskienhallinnan vaiheita ovat riskianalyysi, riskienhallintamenetelmän valinta, päätös riskien poistamisesta, alentamisesta tai pitämisestä omalla vastuulla, sekä riskienhallinnan organisointi.

Roskaposti
Vastaanottajan kannalta ei-toivottu keskusteluryhmä- tai sähköpostiviesti, joka usein lähetetään mainostarkoituksessa suurelle vastaanottajajoukolle yhdellä kertaa. Roskapostia saatetaan lähettää myös häirintätarkoituksessa.

Saatavuus
Ominaisuus, että tieto, tietojärjestelmä tai palvelu on siihen oikeutetuille saatavilla ja hyödynnettävissä haluttuna aikana ja vaaditulla tavalla.

Salasana
Vain käyttäjän tiedossa oleva merkkijono, jonka avulla tietojärjestelmä voi todentaa annettua käyttäjätunnusta vastaavan käyttäjäidentiteetin.

Salassa pidettävä tieto
Laissa salassa pidettäväksi säädetty asiakirja tai tieto. Suomessa salassapitoa koskevia säädöksiä on muun muassa julkisuuslain 22 ja 24 §:ssä.

Salaus
Tiedon, esimerkiksi toiselle henkilölle lähetettävän viestin käsittely niin, että ulkopuolinen ei saisi haltuunsa tietoa, viestiä tai sen sisältämää informaatiota. Salakirjoittaa: Käyttää menetelmää tiedon esityksen muuttamiseksi sellaiseksi, että tiedon alkuperäinen sisältö on mahdollista saada selville vain samaa tai soveltuvaa käänteistä menetelmää käyttäen. Salakirjoittaminen tapahtuu salausavainta käyttäen tietyn salausalgoritmin mukaisesti.

Sosiaalinen tiedustelu
Ihmisten väliseen toimintaan perustuvaa tiedustelua, esimerkiksi esiintymistä puhelimessa jonain toisena henkilönä kuin itsenään tai valheellisesti jonkun organisaation edustajana luottamuksellisten tietojen hankkimiseksi. Vrt. käyttäjän manipulointi, toiseksi tekeytyminen.

Tietoaineistoturvallisuus

Tietoturvallisuuteen tähtäävät toimet asiakirjojen, tiedostojen ja muiden tietoaineistojen käytettävyyden, eheyden ja luottamuksellisuuden ylläpitämiseksi keinoina muun muassa tietoaineistojen luettelointi ja luokitus sekä tietovälineiden ohjeistettu hallinta, käsittely, säilytys ja hävittäminen.

Tietojen luokitus
Tietojen jakaminen luokkiin kunnan määrittelemän mallin ja tietojen omistajan asettamien perusteiden mukaisesti.

Tietoliikenneturvallisuus
Tiedonsiirtoyhteyksien saavuuden, tiedonsiirron turvaamisen, suojaamisen ja salaamisen, käyttäjän tunnistamisen ja verkon varmistamisen turvallisuustoimenpiteet sekä lainsäädäntö, normit ja toimet, joilla pyritään aikaansaamaan tietoliikenteen turvallisuus.

Tietoriski
Tietoon kohdistuva tai tiedosta aiheutuva riski.

Tietosuoja
Ihmisen yksityisyyden suoja ja muut sitä turvaavat oikeudet henkilötietoja käsiteltäessä.

Näitä ovat muun muassa:

- Tietojen valtuudettoman saannin estäminen ja tietojen luottamuksellisuuden säilyttäminen
- Henkilötietojen suojaaminen valtuudettomalta tai henkilöä vahingoittavalta käytöltä.

Tietoturva
Tietoturvalla tarkoitetaan niitä hallinnollisia ja teknisiä toimenpiteitä, joilla varmistetaan tiedon luottamuksellisuus ja eheys, järjestelmien käytettävyys sekä rekisteröidyn oikeuksien toteutuminen.

Tietoturvajohtaminen
Kokonaisturvallisuuden hallinta kunnassa.

Tietoturvallisuuden johtamis- ja hallintajärjestelmä
Osa yleistä toimintajärjestelmää, joka luodaan ja toteutetaan toimintariskien arviointiin perustuen, ja jota käytetään, valvotaan, katselmoidaan, ylläpidetään ja parannetaan tavoitteena hyvä tietoturvallisuus. Sisältää kunnan organisaatiorakenteen, politiikat, suunnittelu- ja kehittämistoimenpiteet, vastuut, menettelytavat, menetelmät, prosessit, mittarit ja resurssit.

Tietoturvallisuuden kehittämissuunnitelma (tai Tietoturvasuunnitelma)
Riskianalyysiin perustuva tietoturvallisuuden arvioinnin tulos, joka on perusta tulevalle kehittämistyölle. Kehittämissuunnitelma toimii toteutuksen ohjaajana toimenpiteille, joilla korjataan tietoturvallisuuden arvioinnissa havaitut puutteet ja joiden avulla pyritään hallitusti kehittämään tietoturvallisuuden kypsyystasoa tavoitetasolle.

Tietoturvallisuus
Järjestelyt, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus. Tietoturvallisuus on riskienhallintaa ja osa kunnan kokonaisturvallisuutta.

Tietoturvapoikkeama
Haitallinen tapahtuma, tahallinen tai tahaton tapahtuma tai olotila, jonka seurauksena kunnan vastuulla olevien tietojen ja palvelujen eheys, luottamuksellisuus tai tarkoituksenmukainen käytettävyystaso on tai saattaa olla vaarantunut.

Toipumissuunnittelu
Toipumissuunnitelman laatimiseksi ja ylläpitämiseksi tehtävät toimenpiteet. Toipumissuunnitelma on jatkuvuussuunnitelman tai varautumissuunnitelman osa, joka sisältää ohjeet katastrofista toipumiseen, toiminnan jatkamisesta ja paluusta normaaliin toimintaan. Määrittelee tärkeille tietojärjestelmille varajärjestelyvaatimukset, vastuut ja toimet valmiuden luomiseksi sekä antaa ohjeet toiminnasta poikkeustilanteissa. Suunnitelma ei sisällä vain vaatimuksia vaan konkreettisia sovittuja toimenpiteitä / menettelytapoja / teknisiä vararatkaisuja.

Turvallisuuden johtaminen
Kokonaisvaltaista, suunnitelmallista ja tavoitehakuista toimintaa kunnan kokonaisturvallisuuden johtamiseksi. Johtamisen keskeisin tehtävä on asianmukaisten toimintaedellytysten luominen ja ylläpitäminen.

Troijanhevonen
Hyödyllinen tai harmiton tai sellaiseksi naamioitu ohjelma, johon on piilotettu haittaohjelma. Troijanhevonen voi olla naamioitu hyödylliseksi esimerkiksi käyttämällä sopivaa nimeä tai sisällyttämällä ohjelmaan myös hyödyllisiä ominaisuuksia.

Uhka
Haitallinen tapahtuma, joka voi mahdollisesti toteutua, tai useampi mahdollinen häiriö, joka tapahtuessaan voi aiheuttaa sen että tiedoille, muulle omaisuudelle tai toiminnalle tapahtuu ei-toivottua.

Vahva salaus
Salakirjoitus, joka ei ole väsytystekniikalla avattavissa tavanomaisella laskentakapasiteetilla ja käytettävissä olevassa ajassa.

Valmiussuunnittelu
Varautuminen ja toimenpiteiden suunnittelu poikkeusolojen tai muun vakavan häiriön varalta ja siitä toipumiseksi. Valmiussuunnittelun konkreettinen tuotos on valmiussuunnitelma, jossa määritellään toiminnan ja sitä tukevan tietojenkäsittelyn toimivuusvaatimukset valmiuslain astuttua voimaan, toiminnan ja palvelujen sekä niitä tukevan teknologian hallitun supistamisen vaiheet sekä toipumistoimenpiteet normaalioloihin palaamiseksi.

Varautuminen

Toiminta, jonka tarkoituksena on luoda ja ylläpitää kunnan riittävä valmius oman toiminnan jatkumiseen normaaliolojen vakavien häiriötilanteiden ja poikkeusolojen varalta. Varautuminen käsittää suunnittelun sekä tarvittavat etukäteisvalmistelut.

Verkkourkinta
Käyttäjän manipuloinnin muoto, jossa pyritään sähköpostin tai WWW-sivun välityksellä saamaan luottamuksellista tietoa.

Virus
Ohjelmaan tai dataan kätketty haittaohjelma, joka leviää tietokoneessa muihin ohjelmiin ja tietoverkossa muihin tietokoneisiin monistamalla itseään siten, että monistetut virukset edelleen monistuvat. Virus voi levitä esimerkiksi tiedoston, sähköpostin, pikaviestiohjelman tai WWW-sivun välityksellä. Osa viruksista on muuntautumiskykyisiä.

2 Roolit ja vastuut

Kunnan **arkisto** ohjaa ja neuvoo yksiköiden arkistonmuodostusta sekä huolehtii ja antaa tietoja kunnan arkistoon siirretyistä asiakirjoista.

Esimies vastaa tietoturvallisuuden ja tietosuojan toteutumisesta alaisessaan toiminnassa.

Hankintoja ja sopimuksia tekevät vastaavat siitä, että tietoturvallisuuden taso vastaa hankittavien tuotteiden, palveluiden ja kumppanuus- ja ulkoistusratkaisujen osalta kunnan vaatimuksia, määräyksiä ja ohjeita.

Henkilöstöosasto ohjaa ja koordinoi henkilöstöturvallisuutta sekä henkilötietojen käyttöä työsuhteen kaikissa vaiheissa (kuten työsuhteen solmiminen, perehdytys, työsuhteen päättäminen).

Kunnan **lakiasioista vastaava** ylläpitää kunnan tietoutta tietoturvallisuuteen ja tietosuojaan vaikuttavista laeista, säädöksistä ja määräyksistä, sekä huolehtii niiden huomioimisesta tietoturvallisuus- ja tietosuojatyössä.

Kunnanhallitus on kunnan ylin kokonaisturvallisuudesta päättävä taho. Kunnanhallitus hyväksyy tähän tietoturvapolitiikkaan ehdotetut muutokset.

Kunnanjohtaja toimii tietoturvallisuuden ja tietosuojan omistajana kunnassa luoden edellytykset niiden asianmukaiselle toteuttamiselle. Tarvittaessa kunnanjohtaja nimeää vastuuhenkilöitä seuraamaan tietoturvan ja tietosuojan toteutumista, tekemään kehitysehdotuksia sekä toimimaan toimialojen tietoturva- ja tietosuojavastaavien sekä järjestelmien pääkäyttäjien tukena.

Tiedon ja tietojärjestelmien **käyttäjä** vastaa omalta osaltaan määräysten ja ohjeiden noudattamisesta. Jokaisen käyttäjän vastuulla on lisäksi tietoturvaan ja tietosuojaan liittyvien poikkeamien, uhkien ja riskien ilmoittaminen viipymättä joko esimiehelle tai Tietojärjestelmäpalveluiden Helpdeskiin tai muuten virallisesti sovitulla tavalla.

Tietojärjestelmän **omistaja** vastaa omistukseensa liittyvästä:

- Käyttäjien ja käyttöoikeuksien määrittelystä ja hyväksynnästä
- Riskienhallinnan toteuttamisesta, sisältäen riittävän dokumentaation varmistamisen järjestelmästä
- Tiedon eheyden varmistamisesta
- Tietojen luokittelusta (julkisuuden ja salassapidon määrittely, arkistonmuodostus).
- Rekisteriselosteen tai tietoturvaselosteen laadinnasta ja nimeää rekisterin yhteyshenkilön

Järjestelmän **pääkäyttäjä** valvoo tietoturvan ja käyttöoikeuspolitiikan toteutumista omalla vastuualueellaan. Pääkäyttäjä huolehtii sovelluksen ylläpitotoiminnoista ja toimii yhdyshenkilönä järjestelmätoimittajaan. Pääkäyttäjä tiedottaa käyttäjiä vikatilanteista ja käyttökatkoista ja huolehtii käyttökatkojen aikataulutuksista.

Tietojärjestelmäpalvelut vastaa tietoturvallisuuden ja teknisen valvonnan toteutumisesta tietojärjestelmäympäristössä, lain sallimin ja yhteistoimintamenettelyn valtuuttamin menetelmin.

Tietosuojavastaava toimii kunnan erityisasiantuntijana henkilötietojen käsittelyyn liittyvissä asioissa. Tietosuojavastaava antaa asiantuntija-apua sekä kunnan henkilöstölle että ennen kaikkea johdolle, jolla on rekisterinpitäjän vastuu henkilötietojen käsittelystä. Tietosuojavastaava raportoi kunnanjohtajalle. Kunnassa on erillinen ohjeistus tietosuoja-asioista. Tarvittaessa toimialoilla nimetään toimialakohtainen tietosuojavastaava, jos lainsäädäntö tai toiminnan tarpeet niin edellyttävät.

Tietoturvapäällikkö vastaa tietoturvallisuuden toteutumisesta ja integroitumisesta muihin kokonaisturvallisuuden osa-alueisiin. Vastuuseen sisältyy tarvittava suunnittelu, ohjaus, seuranta ja kehittäminen, sekä tietoturvariskien ja -poikkeamien hallinnan koordinointi. Tietoturvapäällikkö raportoi kunnanjohtajalle.

Toimialajohtaja vastaa tietoturvallisuuden ja tietosuojan toteutuksesta johtamansa toiminnan osalta ja siitä, että järjestelmien omistajat sekä pääkäyttäjät on nimetty.

Viestinnästä vastaava tukee tietoturvallisuuteen ja tietosuojaan liittyvästä viestinnästä vastaavia toimijoita.

LIITE 2: LAIT, ASETUKSET JA MÄÄRÄYKSET

1 Arkistolaki (831/1994)

Arkistotointa 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 tietosuoja on otettu asianmukaisesti huomioon ja että yksityisten ja yhteisöjen oikeusturvaan liittyvien asiakirjojen saatavuus on varmistettu sekä että asiakirjat palvelevat tutkimuksen tiedon lähteinä.

- Arkistotoimi ja sen järjestäminen
  - Tehtävänä varmistaa asiakirjojen käytettävyys ja säilyminen, huolehtia asiakirjoihin liittyvästä tietopalvelusta, määritellä asiakirjojen säilytysarvo ja hävittää tarpeeton aineisto
- Asiakirjojen laatiminen, säilyttäminen ja käyttö
  - Säilytystavat ja -materiaalit
  - Turvassa tuhoutumiselta, vahingoittumiselta ja asiattomalta käytöltä
  - Hävittäminen määrätyn säilytysajan jälkeen siten, että tietosuoja on varmistettu

2 Hallintolaki (434/2003)

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

- Hyvän hallinnon perusteet
- Asiamiehen ja avustajan salassapitovelvollisuus
- Hallintoasian vireille tulo ja asian käsittely viranomaisessa
  - Asiakirjan lähettäjän vastuu
  - Käsittelyn julkisuus
  - Esteellisyys

3 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 §).

- Henkilötietojen käsittelyä koskevat yleiset periaatteet

- Arkaluonteiset tiedot ja henkilötunnus
- Henkilötietojen käsittely erityisiä tarkoituksia varten
- Henkilötietojen siirto Euroopan unionin ulkopuolelle
- Rekisteröidyn oikeudet
- Tietoturvallisuus ja tietojen säilytys
- Vahingonkorvausvelvollisuus ja rangaistussäännökset

4 Laki eräiden suojauksen purkujärjestelmien kieltämisestä (1117/2001)

- Suojauksen purkujärjestelmää koskeva kielto
  - Suojauksen purkujärjestelmän oikeudeton hallussapito, käyttö, valmistus, maahantuonti, kaupanpito, vuokraus, levittäminen, myynninedistäminen, asentaminen ja huolto on kielletty
- Rangaistussäännös

5 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 §). Tässä laissa tarkoitetaan:

- Julkisen hallinnon tietohallinnolla tukitoimintoa, jolla turvataan julkisten hallintotehtävien hoitaminen tieto- ja viestintäteknisiä menetelmiä ja keinoja hyväksikäyttäen.
- Tietojärjestelmällä tiettyä käyttötarkoitusta varten kerätyistä tiedoista muodostettua automaattisen tietojenkäsittelyn avulla pidettyä tiedostoa tai tietovarantoa, jonka avulla käyttäjä voi tuottaa palveluja tai suorittaa muita tehtäviä järjestelmän käyttötarkoituksen ja tietojen käsittelyä koskevien vaatimusten mukaisesti.
- Tietohallinnon kokonaisarkkitehtuurilla kuvausta julkisen hallinnon organisaatioiden, palvelujen, toimintaprosessien, käsiteltävien tietojen sekä käytettyjen tietojärjestelmien ja teknologian muodostaman tietohallinnon kokonaisuuden rakenteesta ja sen osien välisistä suhteista.
- Tietojärjestelmien yhteen toimivuudella tietojärjestelmien teknistä ja tietosisällöllistä, yhteen toimivuutta muiden julkisen hallinnon viranomaisten tietojärjestelmien kanssa silloin, kun järjestelmät käyttävät samoja tietoja (3 §).

6 Laki julkisista hankinnoista (1505/1992)

- Hankinnan tekeminen
- Vahingonkorvaus ja markkinaoikeuden määräämät seuraamukset
- Tietojenanto

- Tiedonsaantioikeus ja vaitiolovelvollisuus
- Rangaistussäännös

7 Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004)

- Salassapitovelvollisuus ja tietojen käyttö
- Vaitiolovelvollisuus ja hyväksikäyttökielto
- Turvallisuusluokan merkitseminen
- Turvallisuusluokkaa vastaavat käsittelyvaatimukset
- Tiloihin liittyvät turvallisuusvaatimukset
- Henkilöturvallisuusselvitykset ja arviot
- Yhteisöturvallisuusselvitykset ja arviot
- Turvallisuustodistus
- Rangaistussäännökset

8 Laki lasten kanssa työskentelevien rikostaustan selvittämisestä (504/2002)

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

9 Laki potilaan asemasta ja oikeuksista (785/1992)

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

10 Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (2000/812)

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

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

- Tarkoituksena on edistää sosiaali- ja terveydenhuollon asiakastietojen tietoturvallista sähköistä käsittelyä.

- Toteutetaan yhtenäinen sähköinen potilastietojen käsittely- ja arkistointijärjestelmä terveydenhuollon palvelujen tuottamiseksi potilasturvallisesti ja tehokkaasti sekä potilaan tiedonsaantimahdollisuuksien edistämiseksi (1§).
- Säädetään sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä. Sovelletaan julkisten ja yksityisten sosiaalihuollon ja terveydenhuollon palvelujen antajien järjestäessä taikka toteuttaessa sosiaalihuoltoa tai terveydenhuoltoa (2 §).

12 Laki sähköisistä allekirjoituksista (14/2003)

- Sähköisiin allekirjoituksiin liittyvien palvelujen ja tuotteiden vapaa liikkuvuus
- Turvallinen allekirjoituksen luomisväline
- Laatuvarmenne
- Vastuu allekirjoituksen luomistietojen oikeudettomasta käytöstä
- Sähköisen allekirjoituksen oikeusvaikutus ja henkilötietojen käsittely

13 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 §).
- Sähköisten asiointipalvelujen järjestäminen
- Viranomaisen saavutettavuuden turvaaminen ja yhteystiedoista ilmoittaminen
- Sähköisen viestin lähettäminen
    - Vastuu sähköisen viestin perillemenosta
    - Kirjallisen muodon ja allekirjoitusvaatimuksen täyttyminen
    - Sähköisen viestin saapumisajankohta
    - Sähköisen asiakirjan kirjaaminen tai rekisteröiminen
    - Sähköisen viestin tekninen muokkaaminen
    - Päätösasiakirjan sähköinen allekirjoittaminen ja sähköinen tiedoksianto

14 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).

15 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 §).

- Tietoyhteiskunnan palvelujen tarjoamisen vapaus
- Tiedonantovelvollisuus sekä sähköiset tilaukset ja sopimukset

16 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 §).

17 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.

- Suppea turvallisuusselvitys
- Perusmuotoinen turvallisuusselvitys
  - Haetaan kirjallisesti
  - Etukäteen kirjallinen suostumus
  - Tekemisestä päättää suojelupoliisi
  - Annetaan hakijalle kirjallisesti
  - Ei sido selvityksen hakijaa
  - Selvityksen turvallinen säilyttäminen ja salassapitovelvollisuus
- Turvallisuusluokitus ja laaja turvallisuusselvitys
- Rangaistussäännökset

18 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 §).

- Julkisuusperiaate
- Asiakirjan julkiseksi tuleminen
- Oikeus saada tieto asiakirjasta

- Tiedon antaminen asiakirjasta
- Viranomaisen velvollisuudet edistää tiedonsaantia ja hyvää tiedonhallintatapaa
- Salassapitovelvoitteet
  - Asiakirjasalaisuus
  - Vaitiolovelvollisuus ja hyväksikäyttökielto
  - Salassa pidettävät viranomaisen asiakirjat
  - Salassapito- ja luokitusmerkintä
- Rangaistussäännökset

19 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 arkistolaissa (831/1994) tarkoitettua arkistonmuodostussuunnitelmaa hyväksi käyttäen selvitettävä ja arvioitava asiakirjansa ja tietojärjestelmänsä sekä niihin talletettujen tietojen merkitys samoin kuin asiakirja- ja tietohallintonsa.

- Hyvän tiedonhallintatavan toteuttaminen
  - Selvitykset hyvän tiedonhallintatavan toteuttamiseksi
  - Erityissuojattavan tietoaineiston luokitus
  - Erityissuojattavaa tietoaineistoa koskevat yleiset tietoturvallisuustoimenpiteet
  - Ohjeet, valvonta ja seuranta
- Tiedonsaantioikeuksien toteuttaminen ja edistäminen
- Valtionhallinnon viestintä

20 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 §).

- Henkilötietojen käsittelyn yleiset edellytykset
- Huumausaineiden käyttöä koskevien tietojen käsittely
- Testien ja tarkastusten suorittamista koskevat vaatimukset
- Kameravalvonta työpaikalla
- Työnantajalle kuuluvien sähköpostiviestien hakeminen ja avaaminen

- YT-menettely teknisin menetelmin toteutetun valvonnan ja tietoverkon käytön järjestämisessä
- Rangaistussäännös

21 Rikoslaki (39/1889)

- Yksityisyyden, rauhan ja kunnian loukkaaminen
  - Salakuuntelu ja -katselu
  - Elinkeinorikokset (Yritysvakoilu, yrityssalaisuuden rikkominen, yrityssalaisuuden väärinkäyttö)
- Yleisvaaralliset rikokset
  - Vaaran aiheuttaminen tietojenkäsittelylle
- Tieto- ja viestintärikokset
  - Salassapitorikos
  - Salassapitorikkomus
  - Tietoliikenteen häirintä
  - Suojauksen purkujärjestelmärikos
  - Henkilörekisteririkos
  - Viestintäsalaisuuden loukkaus**,** Törkeä viestintäsalaisuuden loukkaus
  - Tietomurto**,** Törkeä tietomurto
- Virkarikos
  - Virkasalaisuuden rikkominen
  - Virkavelvollisuuden rikkominen
- Aineettomien oikeuksien loukkaaminen
  - Tekijänoikeusrikos
  - Teknisen suojauksen kiertäminen
  - Oikeuksien sähköisten hallinnointitietojen loukkaus

22 Sosiaali- ja terveysministeriön asetus potilasasiakirjoista (2009/298)

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

23 Suomen perustuslaki (731/1999) 10 § ja 12 §

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

Perustuslain 12.2§:n mukaan viranomaisten asiakirjat ja muut tallenteet ovat julkisia, jollei niiden julkisuutta ole välttämättömien syiden vuoksi lailla erikseen rajoitettu. Viranomaisen

asiakirjojen julkisuudesta säädetään tavallisen lain tasolla julkisuuslaissa, Jokaisella on oikeus saada tieto julkisesta asiakirjasta.

24 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 §).

- Yksityisyyden ja luottamuksellisen viestin suoja
- Viestien ja tunnistamistietojen käsittely
- Paikkatiedot
- Viestinnän tietoturva
- Puhelupalvelut
- Suoramarkkinointi
- Rangaistussäännökset

25 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. Sairaanhoitopiirin kuntayhtymän on vastattava yhteisen potilastietorekisterin edellyttämistä koordinointitehtävistä 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.

26 Valmiuslaki (1080/1991)

- Päätöksentekomenettely
- Yleiset periaatteet
- Toimivaltuudet
- Varautuminen
    - Valtioneuvoston, valtion hallintoviranomaisten, valtion liikelaitosten ja muiden valtion viranomaisten sekä kuntien tulee valmiussuunnitelmin ja poikkeusoloissa tapahtuvan toiminnan etukäteisvalmisteluin sekä muina toimenpiteinä varmistaa tehtäviensä mahdollisimman häiriötön hoitaminen myös poikkeusoloissa. Poikkeusoloihin varautumista johtaa, valvoo ja yhteen sovittaa valtioneuvosto sekä kukin ministeriö hallinnon alallansa.
- Tiedonantovelvollisuus ja salassapitosäännökset

- Rangaistussäännökset

27 Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (2010/681)

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

28 Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuudesta (VM0024:00/02/99/1998)

- Tietoturvallisuuden ja sen kehittämisen merkitys
- Tietoturvallisuus ja sen osa-alueet
- Tietoturvallisuuden hallinta ja tietoturvallisuustyö viranomaisessa
  - Kukin viranomainen on velvollinen huolehtimaan omasta tietoturvallisuudestaan
    - Viranomaisilla tulee olla ajantasainen tiedonkäsittelyn turvaamissuunnitelma, toipumissuunnitelma ja tiedonkäsittelyn valmiussuunnitelma
    - Ylin johto hyväksyy ja vahvistaa organisaatiossaan noudatettavat turvallisuus- ja varautumisperiaatteet sekä määrittelee asiaa hoitavan sisäisen organisaation
- Tietoturvallisuuden ohjaus ja seuranta valtionhallinnossa

29 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

30 Laki sosiaalihuollon asiakasasiakirjoista (254/2015)

Tämän lain tarkoituksena on toteuttaa yhdenmukaisia menettelytapoja käsiteltäessä sosiaalihuollon asiakasta koskevia tietoja ja siten edistää sosiaalihuollon tehtävien asianmukaista hoitamista.

Tässä laissa säädetään asiakastietojen kirjaamisesta ja siihen liittyvistä velvoitteista sosiaalihuollossa.

Tätä lakia sovelletaan sosiaalihuollon henkilötietolaissa (523/1999) tarkoitettujen asiakastietojen käsittelyyn sekä julkisessa että yksityisessä sosiaalihuollossa.

Asiakastietojen käsittelyyn sovelletaan lisäksi, mitä säädetään sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetussa laissa (159/2007), jäljempänä *asiakastietolaki*, sosiaalihuollon asiakkaan asemasta ja oikeuksista annetussa laissa (812/2000), jäljempänä*asiakaslaki*, viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999), jäljempänä*julkisuuslaki*, hallintolaissa (434/2003), henkilötietolaissa, sähköisestä asioinnista viranomaistoiminnassa annetussa laissa (13/2003), vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetussa laissa (617/2009), väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annetussa laissa (661/2009), arkistolaissa (831/1994) sekä laissa potilaan asemasta ja oikeuksista (785/1992).

31 Tietoyhteiskuntakaari (917/2014)

Lain tavoitteena on edistää sähköisen viestinnän palvelujen tarjontaa ja käyttöä sekä varmistaa, että viestintäverkkoja ja viestintäpalveluja on kohtuullisin ehdoin jokaisen saatavilla koko maassa. Lain tavoitteena on lisäksi turvata radiotaajuuksien tehokas ja häiriötön käyttö sekä edistää kilpailua ja varmistaa, että viestintäverkot ja -palvelut ovat teknisesti kehittyneitä, laadultaan hyviä, toimintavarmoja ja turvallisia sekä hinnaltaan edullisia. Lain tavoitteena on myös turvata sähköisen viestinnän luottamuksellisuuden ja yksityisyyden suojan toteutuminen.

LIITE 3: TIETOTURVALLISUUDEN PERUSTASON TOTEUTTAMINEN (Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa: 5 §)

Tietoturvallisuuden toteuttamiseksi valtionhallinnon viranomaisen on huolehdittava siitä, 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.