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.

Henkilötunnus rinnastuu arkaluonteiseen tietoon.

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 ker-

too, 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).

Tietosuojavastaava ylläpitää kunnan tietoutta tietoturvallisuuteen ja tietosuojaan vaikuttavista laeista, säädöksistä ja määräyksistä, sekä huolehtii niiden huomioimisesta tietoturvallisuus- ja tietosuojatyössä.

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

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

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. Lisäksi tietosuojavastaava neuvoo ja ohjaa rekisteröityjä heidän oikeuksiensa totuttamisessa. Tietosuojavastaava raportoi kansliapäällikölle. 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 kansliapäällikölle.

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.