

## Lapinlahden kunta

### Henkilöstön tietoturvaohje

#### Johdanto

Vastuu tietoturvallisuudesta ja siihen liittyvästä osaamisesta kuuluu omalta osaltaan jokaiselle työntekijälle. Tätä tietoturvaohjetta tulee noudattaa koko kuntaorganisaatiossa. Osassa työyksiköitä on omia tarkempia ammattialakohtaisia ohjeita, joita noudatetaan rinnan tämän ohjeen kanssa. Osassa yksiköitä on toiminnan luonteesta johtuen tarve noudattaa tiukempaa ohjeistusta. Tässä ohjeessa on asetettu kuntaorganisaation minimitaso tietoturvassa, jota voidaan yksiköiden omissa ohjeissa tiukentaa. Oman toiminnan ohella tätä ohjetta tulee noudattaa kunnan toimeksiannosta tehtävässä työssä (esim. palvelutoimittajat). Ohjetta tulee noudattaa myös esim. harjoittelijoiden ja opiskelijoiden osalta.

#### Tiedottaminen ja koulutus

- Seuraa tietoturvallisuuteen liittyviä organisaatiosi tiedotteita, tutustu ohjeisiin ja osallistu tietoturvakoulutukseen.
- Noudata organisaatiosi tietoturvaohjeita.

#### Toimitilaturvallisuus

- Noudata organisaatiosi kulunvalvontaohjetta.
- Mikäli epäilet, että ulkopuolinen henkilö oleskelee kunnan tiloissa ilman asiallista syytä, tarkista henkilön kulkuoikeus kyseiseen tilaan ja huolehdi, että henkilö poistuu tarvittaessa tilasta.
- Älä jätä työvälineitä valvomatta neuvottelutiloihin.
- Älä jätä vieraita yksin neuvottelu- tai työtiloihin. Saata vieraat aulaan tai ulos kokouksen jälkeen.
- Asiakaspalvelupisteessä tai -tilanteessa päätelaitteen näyttö ei saa näkyä asioijalle.
- Älä jätä vierasta yksin tai ilman valvontaa työhuoneeseen tai henkilökunnan tiloihin.
- Huolehdi, ettei neuvottelutiloissa ole esillä asiaan liittymätöntä materiaalia. Huolehdi neuvottelun päättyessä, ettei pöydille, tauluihin, roskakoreihin tai muualle jää käsiteltyä salassa pidettäviä aineistoja tai muistiinpanoja.
- Säilytä tieto ja laitteet turvallisessa paikassa, tarpeen mukaan lukitussa kaapissa ja huoneessa.
- Älä jätä kannettavaa päätelaitetta ilman valvontaa. Huolehdi myös muistitikkujen, CD-/DVD-levyjen, paperitulosteiden ym. asianmukaisesta säilyttämisestä.
- Noudata "puhtaan pöydän" periaatetta. Työpöydällä ei saa säilyttää salassa pidettävää tietoa.
- Lukitse työhuoneesi ovi työpäivän päättyessä tai poistuessasi pidemmäksi aikaa työpisteestäsi. Huolehdi myös siitä, että toimitilan ulko-ovi lukittuu poistuessasi.
- Ohjaa vieraat tai "eksyneet" henkilöt oikeisiin paikkoihin, tarvittaessa saata henkilö aulaan tai ulos. Älä päästä asiattomia henkilöitä toimitiloihin esim. töistä lähtiessäsi.
- Älä jätä auki kulunvalvonnassa olevia tai ovia, jotka on muuten tarkoitettu pidettäväksi suljettuina.

#### Päätelaitteet

- Päätelaitetta (kannettava tietokone, pöytäkone, älypuhelin, tabletti jne.) käytetään yhä useammin maksu- ja tunnistautumisvälineenä. Suojele sitä kuten lompakkoasi.
- Älä anna ulkopuolisen henkilön, edes tutun, käyttää päätelaitettasi.

- Estä päätelaitteesi, esimerkiksi puhelimen, luvaton käyttö asettamalla siihen laitteen käyttöohjeen mukaiset automaattiset lukitukset.

### **Tietoaineistojen käsittely**

- Merkitse salassa pidettäviin asiakirjoihin sen salassapidosta kertova tunniste. Laatiessasi salassa pidettävää asiakirjaa, vastaat sen luokittelusta ja luokittelun merkitsemisestä.
- Käsittele (mm. tallenna, siirrä, tulosta, lähetä, kopioi, kuljeta, säilytä, arkistoi, hävitä) salassa pidettäviä tietoja annettujen ohjeiden mukaan.
- Muista, että voit käyttää ja käsitellä käyttöösi saamiasi salassa pidettäviä ja arkaluonteisia tietoja vain työtehtäviesi hoitamisessa. Esimerkiksi henkilörekisterin tietojen käyttötarkoituksen vastainen käyttö on lainvastaista. Huomioi myös, että tietojärjestelmien käyttöä valvotaan.
- Telekopiota (faxia) voi poikkeustapauksissa käyttää salassa pidettävän aineiston lähettämiseen. Varmistu tällöin, että vastaanottaja on paikalla.
- Salassa pidettävää tietoa voidaan tallentaa, siirtää ja arkistoida usealla eri tallennusvälineellä ja tavalla. Noudata tietoaineistojen ja tallennusvälineiden hävittämisessä annettuja ohjeita. Selvitä, missä sijaitsevat lähimmät salassa pidettävän materiaalin hävittämiseen tarkoitetut tietoturvalliset säiliöt tai tuhoajat.
- Noudata tulostamisessa ja tulosteiden noutamisessa huolellisuutta ja annettuja ohjeita, jotta tulosteet eivät joudu muiden tahojen luettaviksi.
- Ole erityisen varovainen työskennellessäsi julkisissa tiloissa ja huomioi, että joku voi nähdä syöttämiäsi tunnuksia tai muita tietoja huomaamattasi tai salakuunnella keskusteluitasi.
- Julkista tietoa voi välittää internetin kautta tavallisella salaamattomalla sähköpostilla. Salassa pidettävän tiedon välittämisessä internetin kautta on käytettävä turvasähköpostia.
- Älä anna ulkopuolisten nähdä tietokoneesi näyttöruutua, kun käsittelet salassa pidettävää tietoa, tai näppäimistöä, kun syötät käyttäjätunnuksia ja salasanoja. Pyri käyttämään päätelaitteissasi tietoturvakalvoa.

### **Tunnukset ja salasanat**

- Älä luovuta henkilökohtaisia käyttäjätunnuksiasi tai salasanojasi toisen henkilön käyttöön. Älä edes tietohallintohenkilöstölle, koska he eivät tarvitse niitä työtehtäviensä hoitamiseen.
- Käytä eri salasanaa eri palveluissa – työkäyttöön liittyviä tunnuksia tai salasanoja ei saa koskaan käyttää vapaa-ajan palveluissa.
- Huolehdi salasanasi laadusta käyttämällä vain vahvoja salasanoja, jotka ovat mahdollisimman pitkiä. Vaihda salasanasi silloin kun sitä edellytetään tai kun epäilet sen paljastuneen. Vahvassa salasanassa on pieniä ja isoja kirjaimia, numeroita ja erikoismerkkejä. Se on helppo muistaa, mutta vaikea arvata.
- Älä kirjoita salasanoja muistiin tai säilytä sellaisessa paikassa, mistä ne ovat helposti löydettävissä.

### **Työvälineiden ja internetin käyttö**

- Käytä työhösi liittyviä tietoaineistoja ja organisaatiosi antamia työvälineitä vain työtehtäviesi hoitamiseen.
- Kunnan internet yhteys on tarkoitettu työasioiden hoitamiseen. Omia yksityisasioita voi hoitaa vain vähäisessä määrin (esim. pankin sivujen kautta tapahtuva laskujen maksaminen). Älä selaa sellaisia epäilyttäviä www-sivustoja, jotka eivät liity työtehtäviisi. Sivujen kautta saatetaan yrittää siirtää päätelaitteeseesi haitta- tai vakoiluohjelmia.

- Ole varovainen – valitse tarvittaessa ”Peruuta”, jos www-sivu ei vaikuta luotettavalta ja sivusto ehdottaa tai edellyttää tiedoston lataamista tietokoneellasi.
- Älä asenna ohjelmistoja tai tee niiden asetusmuutoksia, ellei se kuulu työtehtäviisi. Peruskäyttäjänä sinulla näitä oikeuksia ei tulisi olla. Jos huomaat, että sinulla on johonkin palveluun tai toimintoon liikaa oikeuksia, velvollisuutesi on pyytää niiden korjaamista.
- Salaamaton muistitikku soveltuu vain julkisen tiedon siirtämiseen. Salatulla muistitikulla voit siirtää salassa pidettäviä tietoaineistoja.
- Lahjaksi saatuja tai löydettyjä muistitikkuja ei saa liittää päätelaitteeseen.
- Huolehdi käytöstä poistetun muistitikun asianmukaisesta hävittämisestä.
- Tallenna laatimasi asiakirjat N tai K-asemalle, josta tiedot varmistetaan keskitetysti. Tietokoneen paikallista muistia (C asema) ei tule käyttää asiakirjojen tallennukseen.
- Omia henkilökohtaisia tiedostoja ei saa tarpeettomasti tallentaa työnantajan päätelaitteisiin tai palvelimille.
- Jos käytät julkisia päätelaitteita tai tilapäisesti toisen henkilön hallussa olevaa tietokonetta, muista tyhjentää Internet-selaimen välimuisti ja evästeet (cookies).
- Säilytä tieto ja laitteet turvallisessa paikassa. Älä jätä kannettavaa tietokonetta tai puhelinta ilman valvontaa. Muista myös tietovälineiden, paperitulosteiden ym. asianmukainen säilyttäminen. Kannettavia tietokoneita tai puhelimia ei saa jättää autoon näkyvälle paikalle, eikä niitä saa säilyttää autossa yön yli.
- Vältä julkisten päätteiden (esim. nettikahvilat, kirjastot) käyttöä työasioihin. Et voi vaikuttaa siihen, mitä tietoja käytöstäsi kerätään ja mitä tiedoilla tehdään. Yleensä sinulla ei myöskään ole mahdollisuutta poistaa näitä tietoja laitteelta.

### **Sosiaalinen media ja sähköposti**

- Muista, että aina kun käytät oman työorganisaatiosi laitteita, verkkoa tai sähköpostia, esiinnyt tietoverkossa organisaatiosi edustajana.
- Huomioi, että palvelun ylläpitäjät pääsevät käsiksi kaikkeen palvelussa käsiteltävään tietoon, myös kahdenvälisiin keskusteluihin. Internetverkkoon päätynyttä tietoa voi olla mahdotonta poistaa jälkikäteen.
- Käsittele palveluissa vain sellaista tietoa, jonka käyttöön palvelu on hyväksytty (huomioi mikä tieto on julkista, mikä salassa pidettävää).
- Älä keskustele työasioista tai jaa työhön liittyviä kuvia muissa kuin työtehtäviin hyväksytyissä palveluissa tai järjestelmissä. Tämä koskee myös sosiaalisen median käyttöä.
- Käytä työ sähköpostia vain työtehtäviesi hoitamiseen. Käytä muuhun kuin työtehtävien hoitamiseen vapaa-ajan sähköpostiasi. Työnantajan sähköpostiosoitteen saa luovuttaa vain sellaiseen internetpalveluun rekisteröidytessä, jolla on selkeä yhteys työtehtäviin.
- Ole erityisen varovainen, jos saat vieraskielisen tai huonolla suomen kielellä kirjoitetun sähköpostiviestin, jonka mukana on liitetiedosto tai linkki ulkoiselle www-sivustolle, vaikka lähettäjä olisi hyvin tuntemasi henkilö, vaikka viestin asiasisältö vaikuttaa tai liitetiedoston nimi ja tyyppi vaikuttavat työtehtäviisi liittyviltä.
- Pyydä tarvittaessa kunnan tietohallintoa tutkimaan saamasi epäilyttävä liitetiedosto ennen sen avaamista.
- Poista epäilyttävät sähköpostit, älä avaa niitä.
- Kunnan sähköpostijärjestelmä ei lähetä automaattisesti kuittausta viestin lähettäjälle. Huolehdi sähköisen asiakirjan vastaanottamisesta ilmoittamisesta.
- Työtehtävien keskeytymättömän hoitamisen vuoksi työntekijällä on velvollisuus käyttää sähköpostijärjestelmän automaattista vastaustoimintoa ilmoittaakseen poissaolostaan, sen kestosta ja siitä kuka hoitaa hänen tehtäviään poissaolon aikana.

- Jos saat toiselle henkilölle kuuluvan sähköpostin, ohjaa viesti oikealle vastaanottajalle ja ilmoita lähettäjälle vastaanottajan oikea sähköpostiosoite. Jos oikea osoite ei ole tiedossa, ilmoita virheellisestä lähetyksestä lähettäjälle. Muista, että sinulla on vaitiolovelvollisuus saamastasi viestistä.
- Jakelulista on henkilöluettelo (sähköpostiosoitteita), jonka jokainen vastaanottaja saa tietoonsa. Se voi olla henkilökisteritieto tai salassa pidettävä tieto, jonka luovuttamisesta on erikseen säädetty. Voit käyttää sähköpostin piilokopiointoa, jos haluat estää sähköpostin jakelussa olevien osoitteiden näkymisen vastaanottajille.
- Huolehdi, että lähettämäsi sähköpostiviesti on kohdistettu oikeille henkilöille ja oikeisiin osoitteisiin, myös valmiita jakelulistoja käyttäessäsi. Vältä turhien sähköpostien lähettämistä jakelulistojen kautta.
- Työsuhteen päättyessä sähköpostiosoite ja -laatikko poistetaan. Siirrä käsittelyä edellyttävä virkapostisi työnantajan käyttöön.

### **Haastattelut, kyselyt, tutkimukset ja tietojen luovutus**

- Ohjaa haastattelu- ja kyselypyynnöt asian vastuuhenkilölle ja toimi organisaation viestintäpolitiikan mukaisesti. Pyydä tarvittaessa apua esimieheltäsi.
- Varo antamasta viattomankin oloisten keskustelujen yhteydessä tietoa salassa pidettävistä tai yksityisyyden suojan piiriin kuuluvista tiedoista. Ole tarkka etenkin erilaisissa internetissä toimivissa sosiaalisen median palveluissa.
- Ohjaa tietojen luovutus- ja tutkimuspyynnöt vastuuhenkilölle, jonka tehtävänä on varmistua tietojen luovutuksen perusteista ja mahdollisesta korvattavuudesta sekä päättää luovutuksesta. Ellet tiedä oikeaa tahoa, ota yhteys esimieheesi.

### **Havaitsitko ongelman?**

- Jos huomaat tietoturvaongelman, velvollisuutesi on tarttua asiaan ja ilmoittaa siitä välittömästi esimiehelle ellet itse pysty korjaamaan ongelmaa.
- Ilmoita tietoturvallisuuteen liittyvistä ongelmista, uhkista tai suojauspuutteista organisaatiosi tietosuojavastaavalle tai esimiehellesi.

# Lapinlahden kunnan tietoturvapoliittikka

## 1. Johdanto

Tietoturvapoliittikka on kunnan ylimmän johdon hyväksymä strateginen asiakirja, joka on kannanotto tietoturvan kehittämiseen. Tietoturvapoliittikan tavoitteena on luoda yhdenmukaiset toimintaperiaatteet ja käytännöt hyvän tietoturvatason toteuttamiseksi. Tietoturvapoliittikassa määritellään tietoturvatyön tavoitteet, vastuut, organisointi ja toteutuskeinot. Poliittikan toteuttamisella luodaan edellytykset tietoturvallisen toiminnan pitkäjänteiseen kehittämiseen. Kunnanhallitus on hyväksynyt kunnan johtoryhmän tässä tietoturvapoliittikassa kuvaamat periaatteet, tavoitteet ja vastuut. Työssä onnistuminen edellyttää johdon sitoutumista tietoturvatyön tukemiseen.

## 2. Tietoturvapoliittikan tavoite

Tietoturvallisuuden käsite ja merkitys

Tiedon turvaaminen on merkittävä osa kunnan toiminnan ja sen järjestämien palvelujen laatua, ICT-riskienhallintaa ja kokonaisturvallisuutta. Riskienhallinnan keskeisenä tavoitteena on tunnistaa toimintaan kohdentuvat riskitekijät, arvioida niitä ja ryhtyä tarvittaviin toimenpiteisiin. Tietoturvan hyvä hallinta edellyttää toiminnan pitkäjänteistä suunnittelua, jatkuvaa kehittämistä, seuranta ja erilaisiin uhkatilanteisiin varautumista. Tietoturvan toteuttaminen vaatii koko henkilöstön tietoturvatietoisuuden parantamista, sovittujen ohjeiden ja toimintatapojen noudattamista, koulutusta ja monikanavaista viestintää.

### Määritelmät

Tieto eri muodoissaan on tärkeä perusta kaikelle kunnan toiminnalle. Tietoturvalla tarkoitetaan eri muodoissa olevien tietojen (mm. sähköisesti tallennettu, välitetty tai rekisteröity tieto, suullinen puhuttu, postin kuljettama tai paperilla oleva tieto) suojaamista erilaisilta uhkatekijöiltä varmistaen palvelutoiminnan jatkuvuus minimoiden toimintaan tai asiakkaiden tietoihin liittyvät riskitekijät. Tietosuoja on myös osa tietoturvaa ja se tarkoittaa ihmisten yksityisyyden kunnioittamista ja suojelemista oikeudellisia säännöksiä noudattavien periaattein ja käytännöin.

Tietoturva määritellään kolmen peruskäsitteen kautta seuraavasti:

- 1) Tietojen luottamuksellisuus: tieto on vain niiden tahojen käytettävissä, joilla on siihen oikeudet.
- 2) Tietojen eheys: tiedon oikeellisuus ja suojaus on järjestetty niin, että tietoa ei voi tahallisesti tai tahattomasti muuttaa vaarantaen toiminnan luotettavuutta. Lisäksi tietoon sen käsittelyn eri vaiheissa tehdyt muutokset on tarvittaessa kyettävä todentamaan.
- 3) Palveluiden ja tietojen saatavuus: tieto on saatavissa ja käytettävissä silloin, kun sitä palvelutoiminnassa tarvitaan.

Hyvä tietoturvaso saavutetaan tietoturvapoliittikan ja ohjeiden mukaisilla tietoturvaisilla toimintaperiaatteilla ja erilaisilla turvamekanismeilla, joita hallitaan ja katselmoidaan jatkuvan kehittämisen periaatteita noudattaen.

## 3. Tietoturvatoimintaa ohjaavat tekijät

Organisaation tietoturvallisuutta velvoittavat ja ohjaavat kansalliset ja kansainväliset yleiset lainsäädäntövelvoitteet sekä toimialakohtaiset erityislainsäädäntövelvoitteet. Lisäksi muut

tietoturvallisuutta ohjaavat velvoitteet, määräykset ja ohjeet. Jokaisen kuntakonsernin viranhaltijan, työntekijän ja luottamushenkilön sekä muun kunnan tietojen ja tietojärjestelmien käyttäjän on tunnettava tämä tietoturvapoliittikka ja noudatettava sen perusteella annettuja ohjeita ja määräyksiä.

#### 4. Tietoriskien hallinta

Tietohallinto ja eri hallintokunnat seuraavat tietohallinto- ja ict-riskien ja uhkien toteutumista osana kunnan sisäistä valvontaa. Tarvittaessa suurimpien riskien vaikutuksia pyritään pienentämään tai ehkäisemään. Tietoriskien hallinta on jatkuvaa aktiivista toimintaa.

#### 5. Tietoturvallisuuden merkitys organisaatiolle

Tietoturvatyön tavoitteena on turvata tietojärjestelmien, tietoverkkojen ja tietojenkäsittelylaitteiden keskeytymätön toiminta, havaita ja estää tietojen luvaton käyttö, tiedon tahaton tai tahallinen tuhoaminen tai vääristäminen ja minimoida niistä aiheutuvat vahingot. Keskeinen tavoite on suojata elintärkeitä toiminnot kaikissa häiriötilanteissa varmistuen palveluiden käytettävyyden mahdollisimman lyhyellä toipumisajalla.

Toiminnan kannalta kriittiset palvelut on kartoitettu ja arvioitu keskeytysten vaikutukset toimintaan. Tietohallinnon varautumissuunnitelmassa käsitellään nämä asiat tarkemmin.

#### 6. Turvatoimien priorisointi

Turvatoimien priorisoinnissa nojaututaan samaan priorisointiin kun palvelupyynnöjä koskevassa priorisoinnissa. Korkeimmalle prioriteetille asetetaan toiminnoista terveydenhuolto, palkkojen maksu, maksuliikenne ja laskutukset sekä teknisesti suuria käyttäjämääriä koskevat verkon työt kuten palvelimiin ja kytkimiin liittyvät toimenpiteet.

#### 7. Tietoturvavastuut

Kunnan tietoturvallisuuteen liittyvät roolit ja vastuut ovat:

##### Kunnanhallitus

- Tietoturvapoliittikan ja muiden koko kuntaa koskevien ohjeiden hyväksyminen
- Seuraa tietoturvan tilaa osana sisäistä valvontaa ja riskienhallintaa.

##### Kunnanjohtaja

- Tietoturvan ja tietosuojan järjestäminen ja toimintaedellytysten luominen sekä seuranta.
- Poikkeusolojen viestinnän johtaminen
- Varautuminen ja jatkuvuudenhallinta yhdessä kunnan johtoryhmän kanssa

##### 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 osana sisäisen valvonnan selontekoa

##### Tietosuojavastaavat

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

Osastopäällikkö ja yksiköiden päälliköt

- Osastopäällikkö nimeää jokaiselle rekisterille rekisterin pitäjän edustajan (rekisteriasioista vastaavan henkilön) sekä jokaiselle tietojärjestelmälle vastuuhenkilön/omistajan.
- Tietoturvallisuuden toteutuminen omalla toimialallaan

Tietojärjestelmän vastuuhenkilö/omistaja

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

Pääkäyttäjä

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

Jokaiselle henkilötietorekisterille on nimettävä rekisteriasioista vastaava henkilö. Tämän henkilön vastuulla on laatia rekisteristä asianmukainen seloste.

Jokaisella tietojärjestelmällä tulee olla yksilöity omistaja, joka vastaa koko järjestelmän elinkaaren hallinnasta, tietosuojasta ja tietoturvan toteuttamisesta. Järjestelmän omistajuuteen liittyvät tiedot dokumentoidaan keskitetysti rekisteri- ja tietojärjestelmäselosteisiin sekä tietohallinnon ylläpitämään tietojärjestelmäluetteloon.

Tietojärjestelmän omistajan on huolehdittava tietojenkäsittelyn luottamuksellisuudesta, tietojen oikeellisuudesta ja pääsynvalvonnasta sekä tuottamaan lakisääteiset seurantaraportit. Jokaiselle tietojärjestelmälle on nimettävä pääkäyttäjä, jonka vastuulla on huolehtia järjestelmän käyttöoikeuksista.

Pääkäyttäjältä vaaditaan hyvää tietoturva- ja tietosuojaosaaamista. Lisäksi tiedon omistajien ja pääkäyttäjien on huolehdittava tiedon koko elinkaaren hallinnasta ja ICT-varautumissuunnitelmista, missä kuvataan vastuuhenkilöt, roolit ja toimintamallit riskien toteutumisen varalta. Tietohallinnon vastuulla on järjestää tukitoimintoja ja tarvittavia koulutuksia edellisten toteuttamiseksi.

Esimiesten vastuulla on huolehtia ja noudattaa työnantajaa koskevien lakisääteisten tietoturva ja tietosuoja velvoitteiden toteutumista. Esimiehet ja tietojärjestelmien pääkäyttäjät vastaavat työntekijöiden käyttöoikeuksista tietojärjestelmiin ja niiden tietosisältöihin työtehtävien edellyttämässä laajuudessa. Lisäksi he huolehtivat loppukäyttäjän riittävästä perehdytyksestä konsernin tietoturvakäytänteisiin varmistaen,

että jokainen ymmärtää niiden merkityksen työtehtävissään. Esimiesten ja pääkäyttäjien vastuulla on myös huolehtia, että työtehtävien muutokset huomioidaan järjestelmien käyttöoikeuksissa ja työsuhteen päättyessä työntekijät palauttavat kaiken työnantajalle kuuluvan omaisuuden sekä käyttöoikeudet tietojärjestelmistä poistetaan.

Esimiehiltä odotetaan esimerkillistä sekä vastuullista tietoturvakäyttäytymistä ja heillä on raportointivelvollisuus tietoturvaepoikkeamista tietohallinnon vastuuhenkilölle.

Kunnan työntekijän velvollisuus on allekirjoittaa tietoturva- ja käyttäjäsitoumus. Työntekijällä on vastuu noudattaa hyväksytyjä tietoturvaohjeita ja huolehtia päivittäisissä työtehtävissä hyvän tiedonhallintatavan käytänteistä. Työntekijän vastuulla on myös huolehtia käsittelemänsä tiedon oikeellisuudesta, saatavuudesta ja luokittelusta sekä huolehtia, että organisaation tiedot ovat asianmukaisesti käytettävissä. Tietojen säilytys- tai arkistointiajan päätyttyä ne on hävitettävä ohjeiden mukaisesti.

Työntekijällä on velvollisuus raportoida tietoturvaongelmista oman organisaation tietosuojavastaavalle, esimiehelle tai suoraan tietohallinnon vastuuhenkilölle.

Ostopalveluna hankitun ICT-palvelun operatiivisesta ja teknisestä tietoturvasta ja sen ohjeistamisesta vastaavat palveluntuottajat, joille palvelun toteutus on sopimus pohjaisesti luovutettu. ICT-palveluiden tuottajien tehtävänä on laatia ja ylläpitää keskitetysti tietohallinnon hyväksymien palvelukonseptien mukaisia käytännön tietoturvaohjeita.

Tilaajan tulee huolehtia, että kaikkiin tarjouspyyntöihin ja palvelusopimukseen sisällytetään tietohallinnon ylläpitämät yleiset tietoturva vaatimukset täydennettynä kyseisen palvelun erityisvaatimuksilla sekä häiriötilanteiden toimintamallit ja selkeä vastuunjako läpi koko palveluketjun. Tilaajan tehtävä on huolehtia ja vaatia palveluntuottajaa raportoimaan ja tiedottamaan merkittävistä tietoturvaan kohdistuvista poikkeustilanteista, riskitekijöistä sekä uhkatilanteista välittömästi palvelusopimuksessa määritellyille yhteyshenkilöille.

## 8. 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 etätyötä tehdessä vaatii etätyöntekijältä erityistä huolellisuutta ja sitoutumista tietoturvaohjeiden noudattamiseen.

Väärinkäyttöksiin 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.

#### 9. Tietoturvakoulutus ja -ohjeet sekä selosteet

Esimiehen vastuulla on huolehtia, että kaikilla työntekijöillä on riittävä koulutus tietoturvasta. Mikäli henkilön työtehtäviin kuuluu olennaisena osana henkilötietojen käsittely, niin osastopäällikön tulee edellyttää, että työntekijä suorittaa hyväksytysti kulloinkin voimassa oleva tietoturva- tai tietosuojakoulutuksen säännöllisin väliajoin.

Tietoturvallisuuteen liittyvät oppaat, säännöt ja materiaalit ovat työntekijöiden luettavissa sisäverkossa sekä kunnan kotisivuilla. Hyvällä perehdyttämällä luodaan työviihtyvyyttä ja -turvallisuutta. Uuden henkilön perehdyttämisestä huolehtii lähin esimies.

Tietojärjestelmien ja henkilörekistereiden selosteet on toimitettava asianhallintasihteerille. Selosteet on nähtävissä kunnan sisäisessä verkossa.

#### 10. Tietoturvallisuudesta tiedottaminen ja sen toteutumisen valvonta

Ennalta tiedetyistä palvelukatkoksista tiedotetaan hyvissä ajoin ennen katkosta.

Havaitusta väärinkäytöksestä tai pistokokeena havaitusta väärinkäytöksestä raportoidaan ja tiedotetaan lähintä esimiestä.

Tietoturvallisuuden toteutumista valvotaan osana sisäistä valvontaa.

#### 11. Henkilötietojen tietoturvaloukkaus

Henkilötietojen tietoturvaloukkauksella tarkoitetaan tietoturvaloukkausta, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvottomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta. Henkilötietojen tietoturvaloukkauksia voivat olla esimerkiksi hävinnyt USB-tikku, varastettu tietokone, hakkerointi, haittaohjelmatartunta, kyberhyökkäys, tulipalo datakeskuksessa tai tiliotteen postitus väärälle henkilölle.

Tietoturvaloukkaus edellyttää rekisterinpitäjän edustajalta kykyä arvioida, minkä tasoinen riski tietoturvaloukkauksesta aiheutuu tietoturvaloukkauksen kohteena olleille henkilöille. Arvion johtopäätös voi olla esimerkiksi se, että tietoturvaloukkauksesta ei aiheudu riskiä, aiheutuu riski tai aiheutuu korkea riski. Riskin taso määrittää ne toimenpiteet, joihin rekisterinpitäjän on ryhdyttävä (esimerkiksi tietoturvaloukkauksen dokumentointi, ilmoitus valvontaviranomaiselle tai ilmoitus rekisteröidylle).

Rekisterinpitäjän edustajan on dokumentoitava kaikki henkilötietojen tietoturvaloukkaukset sekä niiden vaikutukset ja toteutetut korjaavat toimet riippumatta siitä, mitä toimenpiteitä tietoturvaloukkauksesta lopulta seuraa.

Rekisterinpitäjän edustajan on ilmoitettava henkilötietojen tietoturvaloukkauksesta valvontaviranomaiselle, jos siitä voi aiheutua riski luonnollisten henkilöiden oikeuksille ja vapauksille.

Henkilötietojen tietoturvaloukkauksesta on ilmoitettava valvontaviranomaiselle ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa siitä, kun rekisterinpitäjä on tullut tietoiseksi tietoturvaloukkauksesta. Henkilötietojen käsittelijän tulee ilmoittaa tietoturvaloukkauksesta rekisterinpitäjälle, jollei ole erikseen sovittu, että käsittelijä voi ilmoittaa tietoturvaloukkauksista suoraan valvontaviranomaiselle asetuksen edellyttämällä tavalla. Vastuu ilmoitusvelvollisuuden toteuttamisesta on rekisterin vastuuhenkilöllä.

Henkilötietojen tietoturvaloukkauksesta on ilmoitettava rekisteröidylle, jos se todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille. Rekisterin vastuuhenkilön on ilmoitettava asiasta silloin ilman aiheetonta viivytystä, jotta rekisteröidyllä on mahdollisuus suojata itseään esimerkiksi sulkemalla luottokorttinsa.

#### 12. Toiminta normaaliolojen häiriötilanteissa, poikkeustilanteissa ja -oloissa

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

Normaaliolojen häiriötilanteita pyritään ennaltaehkäisemään ja toipumisaikoja lyhentämään pitämällä järjestelmiä ja laitteita mahdollisimman ajantasaisina. Kriittisille laitteille hankitaan varalaitteita.

Poikkeustilanteessa varautumista johtaa ja valvoo valtioneuvosto sekä kukin ministeriö toimialallaan. Tietohallinnon osalta poikkeusolojen valmiussuunnitelmaa päivitetään säännön mukaisesti.