Luhangan kunta

Tietoturvaperiaatteet

Luhangan kunnanhallitus
9.12.2024 §182

Sisällys

Johdanto

Tieto on keskeisessä roolissa organisaatioiden toiminnassa ja palvelutuotannossa. Tiedon tulee olla hyödynnettävissä tarpeen mukaisesti ja tiedon hallinta- ja käsittelykäytäntöjen tulee toimia asianmukaisesti kaikissa tilanteissa. Tietojenkäsittelyn turvallisuus, luotettavuus ja virheettömyys ovat tärkeitä toiminnan jatkuvuuden sekä palveluiden laadun ja tehokkuuden kannalta.

Tietosuoja suojaa ihmisten yksityisyyttä. Inhimillisenä toimintana tietojenkäsittelyyn liittyy aina riskejä, joita pyritään minimoimaan ohjeistuksilla, koulutuksella ja teknisillä ratkaisuilla. Tietoturvariskeistä pystytään minimoimaan teknisin ratkaisuin vain osa, tärkeintä ovat päivittäisessä tietojenkäsittelyssä tehdyt ratkaisut ja toimenpiteet.

Tietoturva suojaa henkilötietoja ja muita tietoja luvattomalta käytöltä. Se käsittää keskeisiin toimintoihin kohdistuvat toimenpiteet, joiden tavoitteena on saavuttaa kyky hallita ennakoivasti uhkia ja tarvittaessa sietää niiden vaikutuksia. Riskien tunnistamisen ja hallinnan sekä vaikutusten minimointi on osa organisaation aktiivista tietoturvan toteuttamista.

Poikkeamatilanteisiin varautumisen ensisijainen vastuu on organisaation ylimmällä johdolla, jonka on varmistettava tietoturvatyön riittävä resursointi ja seuranta. Panostaminen tietoturvaan sekä yleisellä että tekniikan tasolla ovat strategisia päätöksiä, joilla vaikutetaan myös organisaation toimintakykyyn. Lisäksi lainsäädäntö edellyttää tietoturvan asianmukaista hoitamista. Edut ovat häiriötön toiminta, toiminnan laatu ja positiivisen julkisuuskuvan säilyminen. Tietoturvan ja tietotekniikan ammattilaisilla on keskeinen merkitys johdon neuvon antajina.

Tiedonhallintalaki (906/2019) ja tiedonhallintamalli

Tiedonhallintalaki on yleislaki, minkä tarkoituksena on säädellä ja yhdenmukaistaa tiedonhallintaa digitalisoituvassa toimintaympäristössä. Lain tavoitteena on toteuttaa hyvää hallintoa ja julkisuusperiaatetta sekä edistää julkishallinnon tietojen ja tietovarantojen digiturvallisuutta, yhteentoimivuutta, tiedon jakamista ja hyödyntämistä. Kunta muodostaa oman tiedonhallintalain mukaisen tiedonhallintayksikkönsä, johon kuuluu useita viranomaisia. Tiedonhallintalaissa säädetään tiedonhallinnan järjestämisestä, mikä kuvataan lain edellyttämällä tiedonhallintamallilla.

Luhangan kunnan tiedonhallintaa ja tietoturvallisuustyötä ohjaa 2023-2024 laaditut tiedonohjaussuunnitelma, tiedonhallintaohje sekä toimialakohtaiset ohjeet. Lisäksi ”Tietoturvaperiaatteet” tulee olemaan olennainen osa tiedonhallintalain edellyttämää dokumentointia ja vastuiden määrittelyä. Tiedonhallintalain vaatimuksiin kunnassa vastattu siirtymällä 1.1.2024 alkaen sähköiseen asianhallintajärjestelmään, jonka tiedonohjaussuunnitelma sisältää lain vaatimat tiedot eikä erillistä tiedonhallintamallia ole vielä laadittu. Samalla on tarkennettu käytännön toimintatapoja, jotta lain asettamat tietoturvallisuutta koskevat vaatimukset saavutetaan.

Tietoturvallisuuden seuranta, ylläpito ja kehittäminen

Toiminnan jatkosuunnittelussa ja kehittämisessä otetaan huomioon uhkien ja haasteiden lisäksi päivittyvä lainsäädäntö ja suositukset sekä muu kansallinen julkishallinnon tietoturvaa koskeva ohjeistus. Kunta päivittää tietoturvaa koskevia tavoitteita ja tähän liittyviä toimintaprosesseja osana tietoturvan kokonaissuunnittelua. Ohjeistuksen ja käytännön toteutusten tulee olla yhteneväiset ja vastata niin toiminnan tarpeisiin kuin lainsäädännön vaatimuksiin ja riskienhallinnan muihin tavoitteisiin. Seurannalla varmistetaan, että tietoturvallisuuteen liittyvät kokemukset ja ohjeistus eivät ole ristiriidassa, palaute ja muutokset vaatimuksissa tai olosuhteissa tulevat jatkossa huomioitua ja niihin pystytään varautumaan tarpeeksi ajoissa. Luhangan tietoturvaperiaatteita tarkastellaan uudelleen samassa yhteydessä kun kunnalle laaditaan riskienhallinnan – ja sisäisen valvonnan ohjeistusta. Jatkossa tietoturvaperiaatteet katselmoidaan vähintään kerran valtuustokaudessa ja päivitetään tarvittaessa ainakin lainsäädännön tai muiden ohjeistusten muuttuessa.

1. Tietoturvan ja tietosuojan periaatteet

Tietoturvaperiaatteet sisältää toimintatavat, vastuut ja toimivallat, joita noudatetaan tietoturvan ja tietosuojan toteuttamiseksi ja kehittämiseksi. Periaatteilla tarkennetaan mm. hallintosäännön määräyksiä. Tietoturvallisuuskäytännöt kattavat kaikki kunnan tietojenkäsittelytehtävät, ottaen huomioon toimialojen ja tulosalueiden tietoturvatarpeet.

Tietoturvaperiaatteita sovelletaan kaikessa toiminnassa ja koko henkilöstöön sekä sidosryhmiin. Sitä noudatetaan kaikissa tiedon elinkaaren vaiheissa ja tämän edistämiseksi tietoturva- ja tietosuojaperiaatteet ovat osa henkilöstön perehdytystä ja koulutusta. Teknisin ratkaisuin varmistetaan toiminnan ja työtehtävän kannalta tarpeellisten tietojen käsittely.

Kunnalle palveluja tuottavat kolmannet osapuolet velvoitetaan noudattamaan kunnan ja lakien määrittelemiä tietoturvaperiaatteita ja sopimuksiin tehdään tarvittaessa velvoittavat kirjaukset. Kunnan tietoturva- ja tietosuojaperiaatteita ja ohjeita sovelletaan myös hankkeisiin ja pilotteihin.

Tietoturvatyö on osa yleistä turvallisuustoimintaa, riskien hallintaa ja sisäistä valvontaa. Tietoturvan ja tietosuojan toteutuminen varmennetaan vuosittain raportoinnilla kunnanjohtajalle.

Tietoturvaperiaatteet on julkinen asiakirja.

1.1. Tietoturva- ja tietosuoja hankinnoissa ja sopimuksissa

Hankinnoissa tulee noudattaa hankintalainsäädäntöä, kunnan hankintaohjeistusta sekä julkishallinnon yleisiä suosituksia ICT-hankintojen ja hankinnan kohteiden tietoturvan huomioimisesta. Tieto- ja viestintäteknisissä hankinnoissa tulee hankintalainsäädännön asettamissa puitteissa pyrkiä mahdollisimman yhdenmukaisiin, olemassa olevaa osaamista hyödyntäviin hankintoihin kokonaistaloudellisuus ja riskit huomioon ottaen.

Hankintoja suunniteltaessa tulee määritellä tarvittavat asianmukaiset tietoturvajärjestelyt ja tietoturvan toteutumisen valvonta sekä varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan. Vaadittavien tietoturvajärjestelyiden tulee perustua käsiteltävien tietojen laatuun ja kriittisyyteen kunnan palveluiden jatkuvuuden hallinnan sekä tietosuojan näkökulmista. Tiedon elinkaari, normaaliolojen häiriötilanteisiin ja poikkeusoloihin varautumiseen liittyvät vaatimukset sekä muu asiaa sääntelevä lainsäädäntö tulee ottaa huomioon.

Hankintasopimuksissa määritellään, kuinka tietoturva huomioidaan palvelutuotannossa mukaan lukien se, minkä tasoinen häiriönhallintakyky palveluntuottajalta ostetaan. Lähtökohtaisesti kunnan sopimuksissa ja hankinnoissa sopimukseen tulee lisäksi liittää kunnan tietoturva- ja tietosuojaliitteet. jolloin asetuksen vaatimukset täyttävät ehdot sisällytetään kaikkiin uusiin sopimuksiin, joiden perusteella käsittelijä käsittelee henkilötietoja kunnan lukuun. Kyseisten sopimusvelvoitteiden lisäksi hankinnassa tulee huomioida tietoturvavaatimukset tarkemmalla tasolla tämän tietoturva- ja tietosuojapolitiikan mukaisesti.

Hankintojen ja sopimusten asiakirjat saattavat sisältää hankinnan tai sopimuksen osapuolen merkintöjä luottamuksellisuudesta, jolloin niiden salassapitomerkintöjä tulee kuitenkin arvioida huomioiden lainsäädännön vaatimukset viranomaisen asiakirjojen julkisuudesta. Laki viranomaisten toiminnan

julkisuudesta (21.5.1999/621) antaa mahdollisuuden tarvittaessa salata asiakirjat, jos ne sisältävät liike- tai ammattisalaisuuksia. Ellei lain perustetta asiakirjan salaamiselle kokonaisuudessaan ole voidaan asiakirja merkitä osittain salaiseksi. Kun vain osa asiakirjasta on salassa pidettävä, tieto on annettava asiakirjan julkisesta osasta, jos se on mahdollista niin, ettei salassa pidettävä osa tule tietoon.

Tietosuojan osalta tietosuoja-asetus edellyttää, että kunta saa käyttää ainoastaan sellaisia palvelutuottajia tai muita henkilötietojen käsittelijöitä, jotka toteuttavat riittävät tekniset ja organisatoriset suojatoimet. Käsittelyn on täytettävä tietosuoja-asetuksen vaatimukset ja varmistettava rekisteröidyn oikeuksien suojelu. Tietosuojalainsäädännön asettamia ehtoja ja niiden toteutumista tulee valvoa.

2. Tietoturva ja sen tavoitteet

Tietoturva huomioidaan Luhangan kunnassa jo toiminnan suunnitteluvaiheessa. Tietoturvallisuustoimien tulee vastata vaatimuksiin, joita toiminta ja palvelut asettavat tietojenkäsittelyn varmuudelle, käytettävyydelle, salassapidolle ja laadulle.

Toimilla varmistetaan, että palveluiden jatkuvuus ja rekisteröityjen laissa määrätyt oikeudet on turvattu. Toimenpiteet koskevat sekä sähköistä että manuaalista tietojenkäsittelyä. Tietoturvalliseen toimintatapaan ohjeistetaan ja sen tulee olla jokapäiväistä niin työpaikalla kuin sen ulkopuolella.

Tietoturvatoiminnassa tulee arvioida tietoaineistoihin /- järjestelmiin kohdistuvia sekä tiedosta aiheutuvia erityyppisiä riskejä osana kokonaisturvallisuutta ja suunnittelua, jotta ne ovat oikein mitoitettuja niin tiedon kuin toiminnankin näkökulmasta. Riskit pyritään rajoittamaan hyväksyttävälle tasolle niin, että riskienhallintakeinot ovat suhteessa suojattavan kohteen kriittisyyteen ja riskin suuruuteen. Esimerkiksi suojaustoimet tulee suhteuttaa suojattavaan tietoon; julkisen tiedon suojaamiseksi ei tarvita samanlaisia toimenpiteitä kuin salassa pidettävien tietojen suojaamiseksi.

Ostopalveluna tai yhteistyönä toteuttavien palveluiden tietojärjestelmien ja ohjelmistojen riskienhallinasta vastaavat omalta osaltaan myös palveluntuottajat.

Henkilötietojen käsittelyn periaatteet käydään läpi tarkemmin ohjeen osuudessa tietosuojasta (4 Tietosuoja)

2.1. Seuranta, raportointi ja valvonta

Tietoturvan ylläpito ja kehittäminen vaativat jatkuvaa seurantaa. Tähän kuuluvat tietoturvan valvonta sekä poikkeamien raportointi ja tilastointi. Seurannan toteuttaminen ja valvonta kuuluvat toimialojen osalta toimialajohtajille ja esihenkilöiden työhön, kuntatason valvonnasta vastaa kunnanjohtaja. Lisäksi valvontaa tehdään rekisteröidyn pyynnöstä tai työntekijän ilmoituksen perusteella.

Seurantaa toteutetaan sekä tietojärjestelmien että fyysisen turvallisuuden osalta. Jokaisen työntekijän ja luottamushenkilön on seurattava tietoturvaa aktiivisesti myös arjessa ja epäilyttäviin toimintoihin on reagoitava välittömästi. Valvonta- ja selvitystyötä tekeville on mahdollistettava pääsy suoritettavan tehtävän edellyttämään tietoon. Näin varmistetaan että tietoturvaperiaatteiden tavoitteet saavutetaan. Varautumista erilaisiin tietoturvapoikkeamiin käsitellään omassa kappaleessaan.

Seurannan ja valvonnan toteuttamiseksi kunnassa on kiinnitettävä huomioita myös hallinnolliseen turvallisuuteen. Se tarkoittaa, että sovellettavien lakien ja asetusten lisäksi kunnassa on vahvistettu tai vahvistetaan viipymättä tietoturvallisuusvaatimuksiin vastaavat linjaukset ja ohjeet sekä seurannan organisointi.

2.2. Tietoturvaosaamisen varmistaminen

Tietoturvatietoisuus ja -osaaminen on merkittävä osa kunnan luotettavuutta tiedonkäsittelijänä. Henkilökunta ja luottamushenkilöt on koulutettava ja ohjeistettava myös tunnistamaan tietoturvauhat ja toimimaan niiden mukaisesti. Myös osaamisen ylläpidosta on huolehdittava niin, että se vastaa kulloinkin vallitsevia tilanteita ja toimintaympäristön vaatimuksia.

Esihenkilö huolehtii uudessa tehtävässä aloittavan työtekijän perehdyttämisestä tietoturva- ja tietosuojaohjeisiin ja siihen, miten tietoturvallisuus tulee huomioida hänen omissa työtehtävissään.

Tietoturvallisuuden peruskoulutusta tarjotaan säännöllisesti, ja tietoturva- ja tietosuojaohjeet pidetään kaikkien työntekijöiden saatavilla.
Kunnan työntekijät suorittavat omatoimisen tietoturva- ja tietosuojakoulutuksen kunnanjohtajan antamien ohjeiden mukaisesti.

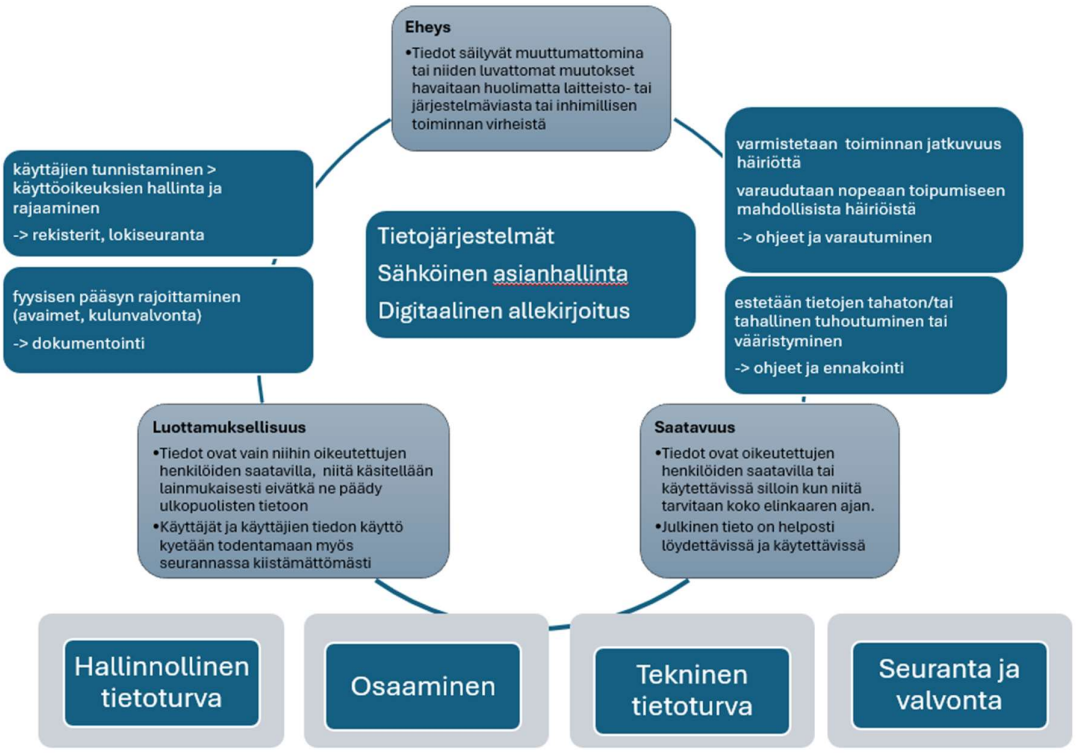
3. Tietoturvallisuus

Tietoturvallisuus on tietojen, tietojärjestelmien ja tietoverkkojen suojaamista luvattomalta käytöltä ja muilta tietoturvariskeiltä. Varmistamalla hyvä tietoturvallisuus vaikutetaan suoraan tietojen luottamuksellisuuteen, eheyteen ja saatavuuteen.
Tietoturvallisessa ympäristössä tiedon käyttö on järjestetty ja resurssit mitoitettu oikeassa suhteessa niin, että toiminta edistää tietoturvan ja -suojan toteutumista.

Tietoturvan perusperiaatteet luottamuksellisuus, eheys ja saatavuus toteutuvat kunnan käytännön toiminnassa muun muassa seuraavasti:

1. Luottamuksellisuus:
Tiedot ovat vain niihin oikeutettujen henkilöiden saatavilla, niitä käsitellään lainmukaisesti eivätkä ne päädy ulkopuolisten tietoon.
Käyttäjät ja käyttäjien tiedon käyttö kyetään todentamaan myös seurannassa kiistämättömästi.
2. Eheys:
Tiedot säilyvät muuttumattomina tai niiden luvattomat muutokset havaitaan huolimatta laitteisto- tai järjestelmäviasta tai inhimillisen toiminnan virheistä.
3. Saatavuus:
Tiedot ovat oikeutettujen henkilöiden saatavilla tai käytettävissä silloin kun niitä tarvitaan koko elinkaaren ajan.

Kuvassa (A) on koottu yhteen käytännön toimia ja niiden suhdetta perusperiaatteisiin ja tietoturvan osa-alueisiin.



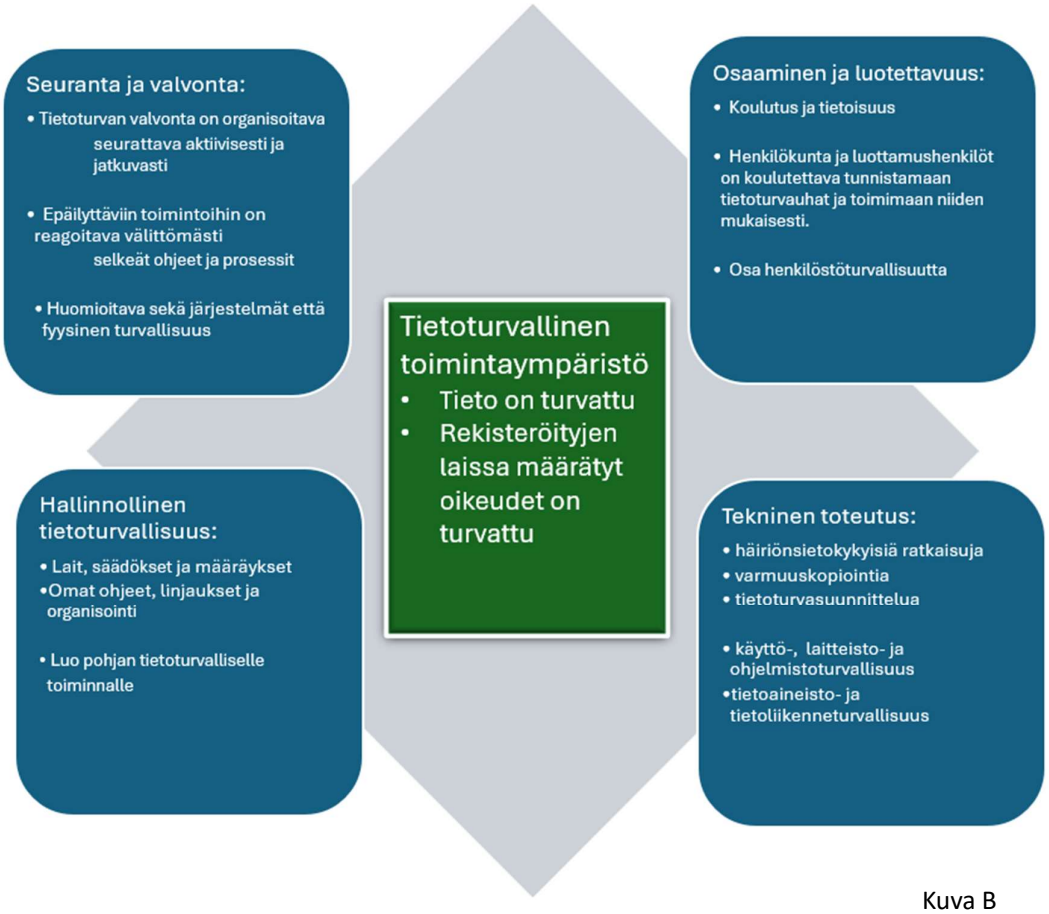
Kuva A

Tietojärjestelmien, sähköisen asianhallinnan ja digitaalisen allekirjoituksen käytöllä on merkittävä rooli jotta kunnassa pystytään toteuttamaan tietoturvaperiaatteita ja dokumentoimaan tietojenkäsittely ja tietoturvatoimet lainmukaisesti. Henkilökunnan ja toimielimien riittävä osaaminen on perusta järjestelmien käytölle, mikä on varmistettava tietoturvan toteutumiseksi.

Käytännön toimenpiteinä myös prosessi digitaalisten tietojärjestelmien käyttöön on tärkeätä hallita esim. käyttäjien henkilökohtaisesta tunnistamisesta alkaen käyttöoikeuksia luovutettaessa.

Yhtä tärkeätä on myös tunnistaa riskit, joita digitaalisten ratkaisujen käyttö tuo mukanaan perusperiaatteiden toteutumiselle ja kiinnittää huomiota tietojen suojaukseen ja toisaalta saavutettavuuteen sekä vähentää toimintojen häiriöherkkyyttä.

Toisessa kuvassa (B) on kerrottu muutamalla lauseella miten tietoturvan eri osa-alueet vaikuttavat tietoturvallisen toimintaympäristön muodostumiseen.



Kuva B

3.1. Tieto ja tietojärjestelmät

Tiedolla on aina omistaja ja omistaja vastaa tiedon luokittelusta ja oikeasta käsittelystä ohjeiden mukaisesti. Henkilötietojen käsittelyssä noudatetaan voimassa olevaa lakia ja tietosuojaa ohjaavia periaatteita (4 Tietosuoja)

Tietojärjestelmä on kokonaisuus, joka koostuu tietovarannoista, niitä käsittelevistä sovelluksista ja laitteista sekä tietoverkoista, tietojen käyttöä määrittävistä ohjeista, käyttäjistä sekä liittymistä toisiin tietojärjestelmiin. Myös tietojärjestelmällä on nimetty omistaja, jonka vastuut on kuvattu (5.7 *Tietojärjestelmän omistaja*). Tietojärjestelmään kuuluu oleellisena osana käsiteltävien tietojen turvallisuus ja tietoturvan yleinen hallinta ja valvonta. Poikkeama missä tahansa kokonaisuuden osassa merkitsee häiriötä järjestelmän toiminnassa.

Kunta pitää yllä luetteloa käytössä olevista tietojärjestelmistä ja sen sisältöä kehitetään jatkuvasti osana parempaa riskienhallintaa ja dokumentointia.

Kunnan tietojärjestelmäympäristössä käytetään toimialan hyväksymiä ja hallinnoimia tietojärjestelmiä, laitteita ja ohjelmistoja, jotka on tarkoitettu työtehtävien hoitamista varten. Uusien ratkaisujen käyttöönoton yhteydessä tulee varmistua, että ne ovat toimialan tiedossa ja hyväksymiä.

Käytettävät tietojärjestelmät ja laitteet on tarkoitettu työtehtävien hoitamiseen. Niitä ei saa käyttää siten, että kunnan omistama tai hallinnoima tieto vaarantuu. Kunnalle tai sen toiminnalle mahdollisesti aiheutetun haitan korvausvastuussa on ensi sijassa vaarantumisen aiheuttaja. Mahdollisiin laiminlyönteihin ja väärinkäytöksiin sovelletaan lakien lisäksi kunnan omaa sisäisen valvonnan ohjeistusta.

3.2. Käyttöoikeudet

Kunnan omistamaan ja hallinnoimaan tietoliikenneverkkoon, työasemaan, tietoon sekä tietojärjestelmiin myönnetään käyttäjälle henkilökohtainen käyttöoikeus työ- tai luottamustehtävien hoitoon tarvittavassa laajuudessa. Tietojärjestelmät edellyttävät yleensä sekä kunnan että järjestelmän tuottajan määrittämiä ja hallinnoimia käyttöoikeuksia. Järjestelmille nimetään omistaja ja pääkäyttäjä/t, minkä lisäksi niiden kriittisyys ja riskit arvioidaan.

Käyttöoikeudet toteutetaan käyttäjän tehtäviin liittyvien käyttötarpeiden mukaan ja niiden myöntämisestä päättää kunnanjohtaja. Käyttäjätunnuksiin ja käyttövaltuuksiin tehdyt muutokset dokumentoidaan sähköisesti ja niitä valvotaan, jotta varmistetaan niiden elinkaaren hallinta. Kunnan toimielimien ja toimihenkilöiden vastuut ja valtuudet on kuvattu erikseen omassa kappaleessaan (5 Roolit ja vastuut)

3.3. Lokitietojen kerääminen

Silloin kun tieto- ja viestintäjärjestelmän toiminta tai todennetun käyttäjän toimet pitää osoittaa kiistämättömästi, tulee tarvittava tapahtumakirjanpito toteuttaa tietojen eheyden säilyttävillä teknisillä ratkaisuilla (lokijärjestelmät). Lokitietojen kerääminen edellyttää, että käyttöoikeudet ovat henkilökohtaisia.

Lokien keräämiselle tulee olla peruste ja määritelynä lokien käsittelytavat sekä vastuut. Lokeihin tallentuvien tietojen tyypit ja suojaustarpeet tulee tunnistaa ja määritellä. Pääsyä lokitietoihin tulee kontrolloida pääsyoikeushallinnalla ja lähtökohtaisesti käyttäjien pääsy tulee olla evätty, silloin kun henkilön työtehtävät eivät pääsyä edellytä. Luottamuksen säilyttämiseksi lokeja ei tule oikeudettomasti muuttaa tai tuhota.

Kun tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista, tulee tietojärjestelmien käytöstä ja niistä tehtävistä tietojen luovutuksista kerätä tarpeelliset lokitiedot.

Lokitietoja käytetään seuraamaan tietojärjestelmissä olevien tietojen käyttöä ja luovuttamista sekä selvittämään tietojärjestelmien teknisiä virheitä. Lokitietojen käsittelyssä tulee huomioida tiedonhallintalainsäädännön mukainen tarpeellisuusarviointi sekä tietosuojalainsäädäntö. Käytännössä lokitietojen edellytyksistä ja vaatimuksista vastaa tietojärjestelmän toimittaja joten ennen uuden tiedojärjestelmän käyttöönottoa kunnan tehtävänä on varmistua, että järjestelmän toimittaja on huomioinut vaatimukset.

3.4. Fyysinen tietoturva

Fyysinen tietoturvan keinoin pyritään suojaamaan organisaation hallussa olevia tietoja ja tietovarantoja fyysisten uhkien, kuten rakenteiden ja niiden vikojen aiheuttamilta vahingoilta ja luvattomien tai rikollisten toimien seurauksilta. Se on osa kunnan riskien hallintaa ja tulee huomioida riskienhallinnan ja sisäisen valvonnan ohjeistuksessa. Fyysisen tietoturvan suunnittelussa kartoitetaan ja huomioidaan tärkeimmät suojattavat kohteet ja varmistetaan teknisten järjestelmien toiminta mahdollisimman hyvin myös häiriötilanteissa.

3.5. Laitteistoturvallisuus

Laitteistoturvallisuudella suojataan organisaation laitteistojen elinkaarta ja turvallista käyttöä, siihen kuuluvat laitteiston asennuksen, suojauksen, takuun ja ylläpidon lisäksi erilaiset tukipalvelut ja sopimukset sekä laitteistojen turvallinen poisto niiden elinkaaren lopussa.
Laitteiden elinkaareen liittyvät palvelusopimukset pidetään ajan tasalla ja laitteiston elinkaaren päättyessä huolehditaan tietojen asianmukaisesta tuhoamisesta. Tietojärjestelmätoimittajilla ja tietoinfrastruktuurin ylläpitäjällä on omat vastuunsa laitteistoturvallisuuden osalta ja nämä huomioidaan hankinnoissa ja sopimuksissa.
Kunnanjohtaja hyväksyy yhteistyössä toimialajohtajien kanssa suunnitellut ict-laitehankinnat ja laitteiden hankinnasta, ohjelmistoasennuksista, suojauksesta ja ylläpidosta vastaa kunnanjohtaja.

3.6. Tietoliikenneturvallisuus

Tietoliikenneturvallisuudella varmistetaan viestinnän häiriöttömyys, tiedonsiirtoyhteyksien käytettävyys, tiedonsiirron suojaaminen ja salaus sekä käyttäjien tunnistaminen.
Tietoliikenneturvallisuus kattaa tietoverkon ja sen laitteiden kokoonpanon, ylläpidon ja muutosten hallinnan, jonka tuloksena ovat turvatut ja luotettavat tiedonsiirtoyhteydet.
Tietoliikenneturvallisuuden ylläpito on keskitetty palveluntuottajalle palvelusopimuksen mukaisesti.

3.7. Liikkuva työ

Liikkuva työ tarkoittaa kaikkea kunnan omien toimitilojen ulkopuolella tehtävää työtä ja tällöin työntekijän on myös itse arvioitava aktiivisesti työympäristön turvallisuutta. Työntekijän tulee kiinnittää erityistä huomiota laitteiden huolelliseen säilytykseen ja tilaturvallisuuteen sekä tietoturvavaatimusten noudattamiseen.
Etätyötä tehtäessä työntekijän ja työnantajan välillä tehdään etätyösopimus. Etätyötä tehtäessä huolehditaan puhelinten ja muiden mobiililaitteiden käytön turvallisuudesta sekä tietojen salassa pidon toteutumisesta.

4. Tietosuoja

Tietosuoja on oleellinen osa tietoturvallisuutta, sillä turvataan oikeuksia, tietoja ja luottamusta. Tietosuojalla tarkoitetaan henkilötietojen käsittelyä koskevien vaatimusten huomioon ottamista yksityisten ihmisten yksityisyyden, oikeuksien ja oikeusturvan varmistamiseksi. Tietosuojalainsäädäntö edellyttää, että henkilötietojen käsittely on turvattava ja henkilötiedot on suojattava asiattomalta käsittelyltä.

Tietosuojaa ohjaavina periaatteina ovat lainmukaisuus, kohtuullisuus ja läpinäkyvyys, tietojen minimointi, täsmällisyys, säilytyksen rajoittaminen sekä tietojen eheys ja luottamuksellisuus.

Kunnan toiminnassa toteutetaan sisäänrakennetun ja oletusarvoisen tietosuojan periaatteita. Tietosuoja otetaan huomioon monipuolisesti perustoiminnan yhteydessä mm. johtamisessa, hankinnoissa, kehitystyössä sekä toimintaprosesseissa. Henkilöstön tietosuojaosaamisesta huolehditaan koulutuksilla sekä työroolin mukaisilla ohjeistuksilla. Kunta mahdollistaa asiakkaille tiedonsaannin omiin henkilötietoihinsa sekä informoi henkilötietojen käsittelystä kunnan verkkosivuilla. Kunnan henkilörekistereitä käsittelevät sopimuskumppanit velvoitetaan noudattamaan vähintään lainsäädännön mukaisia tietosuojaperiaatteita.

Tietosuojaa ja sen vaatimuksia määrittelee EU:n yleinen tietosuoja-asetus sekä kansallinen lainsäädäntö, joka velvoittaa rekisterinpitäjän suunnittelemaan ja osoittamaan henkilötietojen käsittelyn lainmukaisuuden. Suojaamistoimet kattavat kaiken tiedon käsittelyn, siirron ja säilytyksen, riippumatta niiden tallennusmuodosta tai niihin kohdistuvan uhan luonteesta. Uhat voivat olla tahallisia tai tahattomia, kuten tietojen urkinta, huolimattomuus, järjestelmäviat, tapaturmat tai luonnonkatastrofit.

Kunnan tulee seurata tietosuojan toteutumista ja puuttua havaitsemaansa asiattomaan käyttöön, myös työntekijällä on velvollisuus ilmoittaa havaitsemistaan tietoturvaongelmista. Tietojen luvattomasta käytöstä saattaa seurauksena olla oikeudellisia seurauksia tai erilaisia työnantajan menettelyjä, riippuen tilanteen vakavuudesta (6.4 Tietoturvarikkomusten seuraamukset)

4.1. Henkilötietojen kerääminen ja käsittely

Kunta käsittelee henkilötietoja vain perustellun käyttötarkoituksen vuoksi ja vain siinä määrin ja niin kauan, kun se on käyttötarkoituksen kannalta tarpeellista. Henkilötietojen käyttö on sallittua vain lainsäädännön nojalla tai henkilön suostumuksen perusteella ja niihin pääsy on rajattu työtehtävän mukaiseksi eikä ulkopuolisten ole mahdollista saada niitä tietoonsa. Henkilötietoja säilytetään ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten.

Mikäli Luhangan kunta dokumentoi asiakastietoja henkilörekisteriin säädetään rekisteröidyn oikeuksista EU:n yleisellä tietosuoja-asetuksella (GDPR) sekä kansallisella tietosuojalailla. Rekisteröidylle kerrotaan hänen henkilötietojensa käsittelystä henkilötietoja kerättäessä. Samassa yhteydessä luovutetaan rekisterikohtainen tietosuojaseloste, jossa on yksityiskohtaisempaa tietoa henkilötietojen käsittelystä tiettyä tarkoitusta varten.

Luhangan kunta käsittelee henkilötunnusta tai dokumentoi sen ainoastaan silloin jos se on välttämätöntä asian luonteesta johtuen. Jos henkilötunnus tallennetaan asianhallintajärjestelmään kirjataan ko.asian/asiakirjan julkisuusluokaksi osittain salassapidettävä ja salassapitoperusteeksi Tietosuojalain (TSL) 29§.

Julkisuuslain salassapitosäädoksen mukaan henkilötunnus ei ole asiakirjan salassapidon peruste, mutta ellei lain perustetta asiakirjan salaamiselle kokonaisuudessaan ole voidaan asiakirja merkitä osittain

salaiseksi. Kun vain osa asiakirjasta on salassa pidettävä, tieto on annettava asiakirjan julkisesta osasta, jos se on mahdollista niin, ettei salassa pidettävä osa tule tietoon

Henkilötietojen tulee säilyä virheettöminä ja niiden tulee olla saatavilla tarpeen mukaisesti. Sähköinen asianhallintajärjestelmä mahdollistaa esim. henkilö-tai muun arkaluontoisen tiedon peittämisen muuten julkisista asiakirjoista. Peittämistoiminnon käyttäminen on osa arkistonmuodostajan säilytyspäätöstä. Mikäli henkilötietoja luovutetaan, tulee siirron olla tietoturvallinen ja luovutus on dokumentoitava. Tietoja voidaan luovuttaa lakien ja asetusten nojalla tai rekisteröidyn suostumuksella. Rekisteröidyllä on EU:n yleisen tietosuoja-asetuksen mukainen oikeus tarkistaa itseään koskevat tiedot.

Henkilötietojen tarkastuspyyntöjen/ korjauspyyntöjen tekemiseen tarkoitetut lomakkeet löytyvät Luhangan verkkosivuston Kuntainfo- välilehdeltä. Pyynnön voi halutessaan tulostaa ja toimittaa kirjaamoon myös postitse tai henkilökohtaisesti. Tietoaineistot lukuunottamatta julkista päätöksentekoa eivät ole saatavissa avoimesti teknisen rajapinnan avulla.

Suomessa henkilötietojen käsittelyä ohjaa ja valvoo tietosuojavaltuutettu, joka käyttää päätösvaltaa tarkastusoikeuden toteuttamista ja tiedon korjaamista koskevissa asioissa sekä antaa ratkaisuja rekisterinpidon lainmukaisuudesta ja rekisteröidyn oikeuksien toteutumisesta. Yhteyshenkilönä organisaation ja tietosuojavaltuutetun välillä toimii tietosuojavastaava.

5. Roolit ja vastuut

Tietoturvan ja tietosuojan toteuttaminen on jatkuvaa ja kuuluu kaikille. Sen toteuttamiseen osallistuvat luottamushenkilöt, kunnan henkilöstö ja sidosryhmät. Tämä tarkoittaa yhteisten ohjeiden noudattamista sekä tietoturvan ja tietosuojan huomioimista kaikessa tekemisessä.

5.1. Kunnanhallitus

hyväksyy kunnan tietoturvaperiaatteet, asiakirjallisten tietoaineistojen hallinnan edellyttämät tiedonohjaussuunnitelmat/ tiedonhallintaohjeen sekä vastaa tietoturvan ja tietosuojan toteuttamisen edellytyksien luomisesta asetettujen tavoitteiden saavuttamiseksi.
Kunnanhallitus seuraa roolissaan tietoturvallisuuden toteutumista kunnassa (HS §62-63) .
Kunnanhallituksella on vastuu kunnan sisäisen valvonnan ja riskienhallinnan järjestämisestä. (HS §86)

5.2. Kunnanjohtaja

vastaa yhteistyössä toimialajohtajien kanssa tietoturva- ja tietosuojamääräysten toteuttamisesta hallinnollisella tasolla sekä tietoturvan ja tietosuojan integroimisesta kunnan kokonaistoimintastrategiaan. Kunnanjohtaja nimeää tietosuojavastaavan ja myöntää pääkäyttäjän/käyttäjän oikeudet kunnan käyttämiin tietojärjestelmiin. Kunnanjohtaja hyväksyy HS §64 mukaisena viranhaltijana kuntatasoiset asiakirjahallinnon, tiedonkäsittelyn ja säilytyksen ohjeet. Kunnanjohtaja vastaa myös lähi- ja pääarkistoihin luovutetusta pysyvästi säilytettävästä tietoaineistosta ja sen tietoturvallisuudesta ja tietosuojasta.

5.3. Toimialojen johtajat

vastaavat toimialansa riskienhallinnasta ja varautumisesta sekä tietoturvallisuuden ja tietosuojan toteutumisesta. Esihenkilöinä toimivia toimialajohtajia koskevat myös esihenkilön vastuut.

5.4. Esihenkilöt

vastaavat siitä, että työntekijät perehdytetään tietoturva- ja tietosuoja-asioihin ja – ohjeistuksiin. Esihenkilöiden tehtäviin kuuluu havainnoida ja reagoida tietoturva- ja tietosuojaongelmiin. Esihenkilö vastaa tietoturvallisuuden toteutumisesta omalla vastuualueellaan.

Esihenkilöt

- perehdyttävät työntekijän kunnan tietoturvaohjeisiin ja ko. työtehtäviin liittyviin tietoturvavastuisiin
- vastaavat työntekijän palvelussuhteen muutostilanteissa vaadittavista toimista mm. käyttöoikeuksien ja -valtuuksien muutokset/poistot, kunnan tiedon/ omaisuuden palauttaminen

5.5. Jokainen kunnan työntekijä ja luottamushenkilö

on vastuussa tietoturvan ja tietosuojan toteuttamisesta omalta osaltaan.

Jokaisella on henkilötietoja käsitellessään velvollisuus

- noudattaa niitä koskevia lakeja ja annettua ohjeistusta
- pyytää apua niitä koskevissa kysymyksissä sitä tarvitessaan
- tuoda esille mahdolliset turvallisuuspoikkeamat, epäkohdat sekä havaitsemansa uhkat ja riskit ja raportoida niistä välittömästi omalle esihenkilölleen tai kunnanjohtajalle

5.6. Tiedon omistaja

on se, joka tiedon tuottaa ja joka vastaa sen oikeellisuudesta. Hän vastaa tiedon elinkaaren hallinnasta, tiedon luokittelusta (julkisuuden ja salassapidon määrittely), eheyden varmistamisesta sekä tallentamisesta luokituksen edellyttämään ympäristöön.

5.7. Tietojärjestelmän omistaja

on tietojärjestelmästä vastaava toimialan johtaja tai esihenkilö. Hän vastaa tietojärjestelmänsä ja sen sisältämän tiedon riskienhallinnasta ja varautumisesta sekä tietoturvallisuuden toteutumisesta. Käyttöoikeudet tietojärjestelmiin käsitellään omassa kappaleessaan (viittaus)

5.8. Prosessin omistaja

vastaa prosessinsa riskienhallinnasta ja varautumisesta sekä tietoturvallisuuden toteutumisesta. Lisäksi hän vastaa prosessin riippuvaisuuksien tunnistamisesta ja kriittisyyden arvioinnista.

5.9. Palveluntuottajat

vastaavat tietoturvallisuuden ja teknisen valvonnan toteutumisesta ICT-ympäristössä ja tietojärjestelmissä lain sallimin ja yhteistoimintamenettelyn valtuuttamin menetelmin. Milloin tietosuojalainsäädäntö edellyttää tietosuojan vaikutustenarvioinnin (dpia) tekemistä, vastaa palveluntuottaja vaikutustenarviointiprosessiin osallistumisesta omalta osaltaan. Palveluntuottajat noudattavat kunnan tietoturvapolitiikkaa sekä sopimusten tietoturva- ja tietosuojaliitteitä.

5.10. Tietosuojavastaava

valvoo ja seuraa tietosuojan toteutumista ja raportoi havaitsemistaan puutteista ja esittää parannusehdotuksia niihin kunnanjohtajalle. Tietosuojavaltuutettu osallistuu myös aktiivisesti tietoturvapoikkieamien selvittämiseen ja dokumentointiin (6.2 Tietoturvapoikkeamat)

5.11. Asiakirjahallinnosta vastaava (HS §18kohta 21, §64)

kehittää asiakirjahallintoa osana koko kunnan tiedonhallintaa sekä ohjaa toimialoja asiakirjahallinnon hoidossa oikeusturva ja tietosuoja huomioiden.

5.12. Tietotekniikan henkilöstö

Tietotekniikan tukipalvelut on toteutettu ostopalveluna. Kunnanjohtaja vastaa tietoturvallisuuden ja teknisen valvonnan toteutumisesta tietojärjestelmäympäristössä lain sallimien ja yhteistoimintamenettelyn valtuuttamin menetelmin.

5.13. Tietojärjestelmän pääkäyttäjä

vastaa käyttöoikeuksien hallinnasta saamansa toimeksiannon mukaisesti sekä huolehtii sovelluksen ylläpitotoiminnoista ja toimii yhdyshenkilönä järjestelmätoimittajaan. Hän tiedottaa käyttäjiä, tietotekniikkayksikköä ja kunnanjohtajaa vikatilanteista ja käyttökatkoista.

5.14. Hankintoja ja sopimuksia tekevät

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

Kunnan toteuttaessa palvelua yhteistyönä tai ostopalveluna/ulkoiset palveluntuottajat vastuut henkilötietojen käsittelyssä sovitaan palvelukohtaisissa sopimuksissa. Tällöin palveluntuottajien tulee nimetä tietoturva- ja tietosuoja-asioihin yhteyshenkilö. Palveluiden tietojärjestelmien ja ohjelmistojen riskienhallinasta ja tietosuojasta vastaavat omalta osaltaan myös palveluntuottajat.

6. Tietoturvariskeihin varautuminen

Riskienhallinnassa olennaista on tunnistaa riskit ja niiden kriittisyys tietoturvan toteutumiselle. Tietoturvariskejä tulee arvioida ja suurimmat/kriittisimmät riskit tulee sisällyttää jatkossa kunnan riskienhallintasuunnitelmaan. Riskejä syntyy aina tietojen käsittelyssä, etenkin kun tietoja on tarpeen siirtää. Myös tietojen vahingossa tapahtuva tai tarkoituksellinen tuhoaminen, muuttaminen, luvaton luovuttaminen tai tietoihin oikeudettomasti pääseminen on tunnistettu riski.

Tietoturvariskejä on arvioitava säännöllisesti ja niihin on varauduttava ennalta. Uhkia aiheuttavat mm. tietoisesti tehdyt väärinkäytökset, tietomurrot, virheellisesti toimivat ohjelmistot ja laitteet, virukset ja haittaohjelmat, palvelunestohyökkäykset sekä tekniset ongelmat. Tietoturvaan kohdistuvat uhat voivat aiheuttaa riskin tietojen, tietojärjestelmien tai tietoliikenteen luottamuksellisuudelle, eheydelle ja käytettävyydelle.

Laitetason ratkaisuilla voidaan vaikuttaa tietoturvan toteutumiseen vain rajallisesti, henkilöstön osaaminen ja tietoisuus ovat suuressa roolissa tietoturvan toteutumisessa. Kouluttaminen sekä tietoisuuden lisääminen tietoturvasta ovat merkittävä tekijä uhkien pienentämisessä. Esihenkilöiden vastuulla on huolehtia henkilöstön perehdyttämisestä.

6.1. Tietoturvallisuuden vaarantuminen

Tietoturvallisuuden vaarantuminen voi aiheuttaa vakavia seurauksia, minkä vuoksi on tärkeää, että kunta ja sen työntekijät ottavat tietoturvan vakavasti.

Tavallisimpia ja helposti toteuttavia keinoja tietoturvallisuuden parantamiseksi ovat mm:

- vahvojen salasanojen käyttö
- tietojen varmuuskopioiminen
- ohjelmistojen / laitteistojen päivittäminen
- tietoturvakoulutukset

Tietoturva- ja tietosuojaohjeiden noudattamista valvotaan sekä säännöllisin rutiinein tai automaattisesti että pistokokein. Väärinkäytöksiin puututaan.

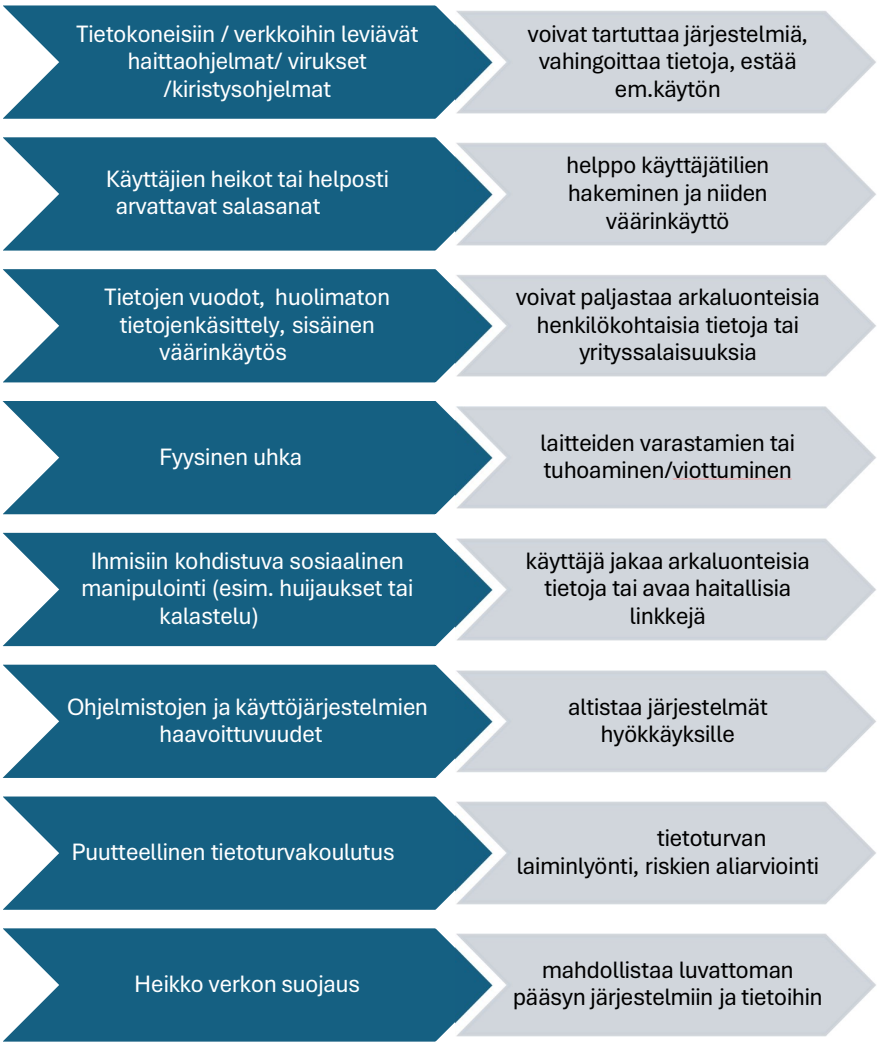
Sekä odottamattomista että ennalta tiedetyistä palvelukatkoksista ja muista tietojärjestelmien käytön häiriöistä tiedotetaan kunnan tavanomaisia tiedotuskanavia hyödyntäen. Järjestelmän omistaja tiedottaa käyttöhäiriöistä niiden edellyttämässä laajuudessa.

Tietoturvapoikkeamat käsitellään ja niistä raportoidaan kunnanjohtajalle erikseen ohjeistetulla tavalla. Muulle organisaatiolle havaituista poikkeamista tiedotetaan niiden luonteen ja laajuuden edellyttämällä tavalla.

Tietoturvaloukkauksissa noudatetaan EU:n yleisen tietosuoja-asetuksen määräyksiä henkilötietojen tietoturvaloukkauksen ilmoittamisesta valvontaviranomaiselle ja rekisteröidylle artiklojen 33 ja 34 mukaisesti.

Tietoturvallisuuden vaarantuminen tarkoittaa tilannetta, jossa tietoja, järjestelmiä tai verkkoja uhkaa erilaiset riskit ja haavoittuvuudet, jotka voivat johtaa tietoturvaloukkauksiin.

Tietoturvallisuuden vaarantumisen voivat aiheuttaa mm.:



6.2. Tietoturvapoikkeamat

Jokaisen henkilön vastuulla on ilmoittaa, mikäli havaitsee tietoturvaan kohdistuvia uhkia tai ohjeistuksen vastaista toimintaa. Poikkeamista on raportoitava sähköpostitse esihenkilölle, kunnanjohtajalle tai tietosuojavastaavalle.

Kunnan tietosuojavastaava osallistuu tietoturva- ja tietosuojapoikkeamien, väärinkäytösten sekä nykytilan arviointiin oman työroolinsa rajoissa. Valvonta- ja selvitystehtävien suorittamiseksi tietosuojavastaavalle mahdollistetaan pääsy tehtävän edellyttämään tietoon.

Tietoturvapoikkeama on tahallinen tai tahaton tapahtuma tai olotila, jonka seurauksena kunnan tietovarantoihin ja palveluihin kohdistuu uhka, joka vaarantaa tiedon ja palvelun eheyden, luottamuksellisuuden tai saatavuuden.

Tietoturvarikkomukset ja tietoturvapoikkeamat käsitellään johtoryhmässä, jossa esitetään jatkotoimet kunnanjohtajalle. Tietoturvarikkomusten ja väärinkäytösten rangaistusta määritettäessä sovelletaan niistä säädettyjä lakeja ja asetuksia tapauskohtaisen vakavuuden mukaisesti, jolloin seuraamuksena voi olla käyttöoikeuteen kohdistuvista rajoituksista aina rikoslaissa määriteltyihin rangaistuksiin. Näitä käsitellään erikseen luvussa Tietoturvarikkomusten seuraamukset .

Työntekijän velvollisuus on viedä asia eteenpäin, mikäli esimerkiksi asiakas siitä hänelle ilmoittaa.

Toimintatapa tietoturvallisuuden vaarantuessa riippuu siitä, koskeeko tapahtuma henkilötietoja vai ei.
Tietoturvan/ tietosuojan vaarantumisepäilyn ilmetessä:

1 Ilmoitus omalle esihenkilölle. (Jokaisella on velvollisuus ilmoittaa mahdollisesta tietoturva- ja tietosuojaloukkauksesta.)
2 Esihenkilö vie epäilyn eteenpäin tietosuojavastaavalle
3 Tietosuojavastaava käynnistää tietoturva- ja tietosuojaloukkauksen selvitysprosessin.

6.3. Henkilötietojen tietoturvaloukkaus

Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvattomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta.

Henkilötietojen tietoturvaloukkauksia voivat olla esimerkiksi:

- hävinnyt tiedonsiirtoväline, kuten USB-tikku
- varastettu tietokone
- hakkerointi
- haittaohjelmatartunta
- kyberhyökkäys
- tulipalo datakeskuksessa
- tiliotteen postitus väärälle henkilölle.

Tietoturvaloukkauksesta voi seurata esimerkiksi henkilötietojen valvomiskyvyn menettäminen, identiteettivarkaus tai petos, maineen vahingoittuminen tai salassapitovelvollisuuden alaisten henkilötietojen paljastuminen.

Jos loukkauksesta voi aiheutua riski luonnollisten henkilöiden oikeuksille ja vapauksille, on kyseessä henkilötietojen tietoturvaloukkaus.
Kaikki henkilötietojen tietoturvaloukkaukset sekä niiden vaikutukset ja toteutetut korjaavat toimet dokumentoidaan asianhallintajärjestelmään riippumatta siitä, mitä toimenpiteitä tietoturvaloukkauksesta lopulta seuraa.
Dokumentointivelvollisuuden piiriin kuuluvat myös tietojärjestelmään kohdistuneen tietoturvaloukkauksen osalta tapahtuma-ajan lokitiedot.

Käsittelyvaiheet:

1 Henkilötietojen käsittelijä ilmoittaa vaarantumisepäilystä tai havaitusta tietoturvaloukkauksesta omalle esihenkilölle, joka vie asian eteenpäin tietosuojavastaavalle.
2 Tietosuojavastaava ilmoittaa asiasta valvontaviranomaiselle (Suomessa tietosuojavaltuutetun toimisto).
3 Tietosuojavastaava vastaa tarvittaessa tietoturvaloukkauksen ilmoittamisesta rekisteröidylle
4 Tietosuojavastaava vastaa asian riittävästä dokumentoinnista

Henkilötietojen tietoturvaloukkaus tunnistettu:

- ilmoitettava tietosuojavaltuutetun toimistolle ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa siitä, kun rekisterinpitäjä on tullut tietoiseksi tietoturvaloukkauksesta
- ilmoitettava rekisteröidylle, jos se todennäköisesti aiheuttaa korkean riskin tämän oikeuksille ja vapauksille em. tapahduttava ilman aiheetonta viivytystä, jotta rekisteröidyllä on mahdollisuus suojautua esimerkiksi sulkemalla luottokorttinsa
- vastuu ilmoitusten tekemisestä on rekisterinpitäjällä eli Luhangan kunnalla

6.4. Tietoturvarikkomusten seuraamukset

Tietoturvarikkomuksista säädetään työsopimuslaissa ja viranhaltijalaissa. Henkilötietoihin kohdistuvien rikkomusten osalta asiaa säätää lisäksi EU:n yleinen tietosuoja-asetus sekä kansalliset lait ja asetukset.

Seurauksena rikkomuksista, niiden tapauskohtaisen vakavuuden mukaisesti, voi olla käyttöoikeuteen kohdistuvia rajoituksia, palvelusuhteeseen vaikuttavia seuraamuksia sekä rikoslaissa määriteltyjä seuraamuksia. Mikäli rikkomuksesta aiheutuu välittömästi tai välillisesti taloudellisia menetyksiä, voidaan päätyä vahingonkorvausvaatimuksiin.

Vakava rikkomus / Lain mukaan rikkomuksena tai rikoksena tuomittava teko.

- salassa pidettävien tietojen oikeudeton käsittely ja luovuttaminen (esim. henkilötietojen katsominen ilman oikeudellista perustetta)
- tietojen luvaton käyttö (esim. tekijänoikeuden loukkaus tai rikoslain alaisen materiaalin oikeudeton käsittely ja hallussapito, kuten mm. rasistinen aineisto tai lapsiporno)
- Hakkerointi ja tunkeutuminen tietojärjestelmiin
- vahingonteko (esim. virusten tahallinen levittäminen tai palvelun tahallinen estäminen)
- vakoilu
- virka-aseman väärinkäyttö
- hyötymistarkoitus

Rikkomus / Vakava väärinkäyttö tai turvallisuuden rikkominen.

- ohjeiden vastainen laitteistojen tai ohjelmien käyttö
- tunnuksen luovuttaminen (esim. oman salasanan kertominen toiselle käyttäjälle, avoimen työaseman luovuttaminen toisen käytettäväksi omalla tunnuksella)
- tiedon luottamuksellisuuden vaarantaminen (esim. avoimen työaseman jättäminen valvomatta, henkilötiedon luovuttaminen henkilölle, jolla ei ole oikeutta saada sitä)
- ylläpito-oikeuksien luvaton hallussapito

- ohjelmien ja pelien luvaton kopiointi
- luvattomien ohjelmien asentaminen
- luvattomien laitteiden lisääminen verkkoon

Lievä rikkomus / Asiaton toiminta tai väärinkäytös.

- henkilökohtaisen tietoturvan/tietosuojan laiminlyönti (esim. käyttäjätunnuksen huolimaton käyttö, salasanan jättäminen näkyviin, salassa pidettävien asiakirjojen jättäminen näkyviin)
- haitan aiheuttaminen (esim. laitteiden/ohjelmien lukitseminen ja toisten oikeutetun pääsyn estäminen)
- resurssien tuhlaus (esim. työajan väärinkäyttö, kuten asiaton surffailu internetissä)
- luvaton kaupallinen tai poliittinen toiminta (esim. sähköpostin käyttäminen henkilökohtaiseen markkinointiin)
- kulunvalvontaohjeiden rikkominen (esim. avainten luovuttaminen toisen käyttöön)

7. Lainsäädäntöä ja ohjeita

- Tietoturvaperiaatteet pohjautuu kansalliseen lainsäädäntöön ja EU:n
- yleiseen tietosuoja-asetukseen.
- Lainsäädäntöä ja ohjeita:
- Arkistolaki (831/1994)
- Tietosuojalaki (1050/2018)
- EU:n yleinen tietosuoja-asetus (679/2016)
- Hallintolaki (434/2003)
- Julkisuuslaki (621/1999)
- Julkisuusasetus (1030/1999)
- Tiedonhallintalaki (906/2019)
- Digipalvelulaki (306/2019)
- Asiointilaki (13/2003): Tietoturvallisuus asioinnissa ja viranomaisten keskinäisessä
- tietojenvaihdossa
- Tunnistuslaki (617/2009)
- Työelämän tietosuojalaki (759/2004): työntekijää koskevien henkilötietojen käsittely
- Tiedonhallintalautakunnan suositukset ja ohjeet https://vm.fi/tiedonhallintalautakunta
- Luhangan kunnan tietoturvaperiaatteet
- Luhangan kunnan tiedonhallinnanohje
- Luhangan kunnan hallintosääntö
- Dynasty 10 (Innofactor Oy) tiedonohjaussuunnitelma
- Lupapiste (Cloudpermit Oy) tiedonohjaussuunnitelma

Lisäksi on toimialakohtaisia erityislainsäädäntöjä, jossa käsitellään tietosuojaan ja tietoturvaan liittyviä asioita.
Ajantasainen lainsäädäntö löytyy Finlex-palvelusta osoitteesta www.finlex.fi

Lisätietoja

- Tietosuoja-asetuksen 5 artikla https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32016R0679&qid=1637319193404
- Liikenne- ja viestintävirasto Traficom Kyperturvallisuuskeskus https://www.kyberturvallisuuskeskus.fi/fi/
- Tietosuojavaltuutetun toimisto www.tietosuoja.fi
- Kuntaliitto https://www.kuntaliitto.fi/laki/tietosuoja
- Työelämän tietosuojalain 24 §:n rangaistussäännökset https://www.kt.fi/palvelussuhde/tyoelaman-kaytannot/tietosuoja/rangaistukset