|  |
| --- |
|  |
| Siikaisten kunnan tietoturva- ja tietosuojapolitiikka |
| Siikaisten kunnanhallitus 23.4.2018 |
|  |
|  |
|  |

|  |
| --- |
|  |

Sisällysluettelo

[1.Johdanto 2](#_Toc511730963)

[2. Tietoturvapolitiikan tavoite 2](#_Toc511730964)

[2.1. Tietoturvallisuuden käsite ja merkitys 2](#_Toc511730965)

[2.2. Tietosuojan käsite ja merkitys 3](#_Toc511730966)

[2.3. Määritelmät 3](#_Toc511730967)

[3. Tietoturvallisuuteen keskeisesti liittyvät säädökset 3](#_Toc511730968)

[4. Tietoturvallisuuteen kohdistuvat uhat 4](#_Toc511730969)

[5. Tietoturvallisuuden merkitys ja toteuttaminen 5](#_Toc511730970)

[5.1. Turvattavat kohteet 5](#_Toc511730971)

[5.2 Siikaisten kunnassa noudatettavat tietoturvaperiaatteet 5](#_Toc511730972)

[5.3 Tietoturvallisuuden toteutumista tukevia käytäntöjä 5](#_Toc511730973)

[6. Turvatoimien priorisointi 6](#_Toc511730974)

[7. Tietoturvallisuuden hallintajärjestelmä 6](#_Toc511730975)

[8. Tietoturvavastuut 6](#_Toc511730976)

[8.1. Organisaation tietoturvavastuut 6](#_Toc511730977)

[8.2. Kunnan yhteistyökumppaneiden vastuut 7](#_Toc511730978)

[9. Tietoturva- ja tietosuojakoulutus ja –ohjeet 7](#_Toc511730979)

[10. Tietoturvallisuudesta tiedottaminen 7](#_Toc511730980)

[11. Tietoturvallisuuden toteutumisen valvonta 7](#_Toc511730981)

[12.Toiminta häiriötilanteissa ja poikkeusoloissa 7](#_Toc511730982)

SIIKAISTEN KUNNAN TIETOTURVA- JA TIETOSUOJAPOLITIIKKA

# 1.Johdanto

Yhteiskunta ja kuntien toiminnot ovat jatkuvasti entistä riippuvaisempia ICT-teknologiasta ja - palveluista sekä niiden toimintavarmuudesta. Tietojen käsittelyyn ja tietotekniikkaan liittyviä   
riskejä pitää tunnistaa ja hallita aktiivisesti. Riskien negatiivisia vaikutuksia pitää minimoida   
teknisillä ja hallinnollisilla keinoilla. Euroopan unionin yleinen tietosuoja-asetus entisestään korostaa tietosuojan vaatimuksia.

Tietoturvan tärkeyttä lisäävät myös kansalaisille suunnattujen sähköisten palvelujen   
laajentuminen, tietojärjestelmien etä- ja mobiilikäytön lisääntyminen, kuntien yhteistyö   
palvelujen järjestämisessä, laaja palveluntuottajien verkosto (monituottajamallissa myös   
ostopalvelu- ja palvelusetelituottajat käyttävät kuntien järjestelmiä) sekä palvelutuotannon   
uudet menetelmät (erityisesti pilvipalvelut, jotka hämärtävät maiden rajat ja tietojen sijainnin).

Siikaisten kunnan tietoturvapolitiikka on laadittu ja tarkoitettu kunnan henkilöstölle, luottamushenkilöille  
sekä kunnan tietoja ja tietojärjestelmiä tai toimitiloja käyttäville muille henkilöille.

Tietoturvapolitiikka on sisäinen määräys, joka jaetaan tiedoksi ja noudatettavaksi.   
Siikaisten kunnan tietoturvapolitiikkaan sisältyvät erikseen hyväksytyt tietoturvaan ja tietosuojaan   
liittyvät määräykset ja ohjeet.

# 2. Tietoturvapolitiikan tavoite

Tietoturvallisuuden ensisijaisena päämääränä on organisaatioiden vastuulla olevienpalvelujen jatkuvuuden turvaaminen kaikissa olosuhteissa eli tietotekniikkanäkökulmasta mahdollistaa organisaation palveluihin liittyvien ICT-ratkaisujen käytettävyys sekä prosesseissa, rekistereissä ja palveluissa käytettävien tietojen eheys ja luottamuksellisuus kaikissa olosuhteissa.

Toimintalähtöisesti painottuvalla tietoturva- ja tietosuoja-asioiden hoidolla tuetaan oman organisaation toiminnalle asetettuja vaatimuksia ja varmistetaan tietojen ja tietojärjestelmien huolellinen käsittely varmistaen samalla kansalaisten yksityisyyden suoja.

## 2.1. Tietoturvallisuuden käsite ja merkitys

Tietoturvallisuus kattaa järjestelyt, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus. Se edellyttää tietojen, järjestelmien, palvelujen ja tietoliikenteen asianmukaista suojaamista sekä normaali- että poikkeusoloissa hallinnollisilla, teknisillä ja muilla toimenpiteillä. Tietojen luottamuksellisuutta, eheyttä ja käytettävyyttä turvataan laitteisto- ja ohjelmistovikojen, luonnontapahtumien sekä tahallisten, tuottamuksellisten tai tapaturmaisten tekojen aiheuttamilta uhkilta ja vahingoilta.

Tietoturvallisuus on toimintatapa, jonka tavoitteena on tietojärjestelmien ja toiminnan jatkuvuutta uhkaavien riskien hallinta. Se on edellytys toiminnan luotettavalle hoitamiselle.

## 2.2. Tietosuojan käsite ja merkitys

Tietosuojalla tarkoitetaan henkilötietojen käsittelyä koskevien vaatimusten huomioon ottamista yksityisten henkilöiden yksityisyyden ja oikeusturvan varmistamiseksi. Tietosuojan tarkoituksena on näin ollen turvata tiedon kohteen yksityisyys sekä edut ja oikeusturva. Tietosuoja on Suomessa yksilön perustuslaillinen oikeus ja osa palvelujen laatua.

## 2.3. Määritelmät

Tietoturvallisuuden keskeisillä käsitteillä tarkoitetaan seuraavaa (lyhyt ja tarkempi kuvaus):

**Luottamuksellisuus**; kukaan sivullinen ei saa tietoa

 tietojen säilyminen luottamuksellisina ja tietoihin, tietojenkäsittelyyn sekä   
tietoliikenteeseen kohdistuvien oikeuksien säilyminen vaarantumiselta ja loukkauksilta.

**Eheys**; tiedon yhtäpitävyys alkuperäisen tiedon kanssa

 tietojen tai tietojärjestelmän aitous, väärentämättömyys, sisäinen ristiriidattomuus, kattavuus, ajantasaisuus, oikeellisuus ja käyttökelpoisuus sekä ominaisuus, että tietoa tai viestiä ei ole valtuudettomasti muutettu, ja että mahdolliset muutokset voidaan todentaa kirjausketjusta.

**Käytettävyys**; tieto on siihen oikeutettujen hyödynnettävissä haluttuna aikana

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

**Todentaminen** (autentikointi); varmistuminen kohteen todenmukaisuudesta, oikeellisuudesta, alkuperästä tai varmistuminen käyttäjän aitoudesta halutulla luottamustasolla.

**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.

Tietosuojaan liittyvät käsitteet **henkilötieto**, **henkilötietojen käsittely**, **henkilörekisteri**,   
**rekisterinpitäjä**, **rekisteröity**, **sivullinen** ja **suostumus** määritellään henkilötietolaissa sekä EU:n tietosuoja-asetuksessa.

# 3. Tietoturvallisuuteen keskeisesti liittyvät säädökset

Tietoturvatoimintaa ohjataan säädöksin, määräyksin, ohjein ja suosituksin. Näistä tärkeimpiä ovat:

* + - Euroopan unionin yleinen tietosuoja-asetus (velvoittaa 5/2018-)
    - Suomen perustuslaki (731/1999) 2. luku 10 §: Yksityiselämän suoja ja luottamuksellisen viestin salaisuus
    - Suomen perustuslaki (731/1999) 2. luku 12 §: Viranomaisten hallussa olevien asiakirjojen ja tallenteiden julkisuus
    - Laki viranomaisten toiminnan julkisuudesta (621/1999)
    - Henkilötietolaki (523/1999): Henkilötietojen käsittelyä koskevat yleiset periaatteet
    - Asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999)
    - Laki kunnallisesta viranhaltijasta (304/2003)
    - Työsopimuslaki (55/2001)
    - Arkistolaki (831/1994): Asiakirjojen laatiminen, säilyttäminen ja käyttö
    - Turvallisuusselvityslaki (726/2014)
    - Laki yksityisyyden suojasta työelämässä (759/2004): Työntekijää koskevien henkilötietojen käsittely
    - Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003): Tietoturvallisuus asioinnissa ja viranomaisten keskinäisessä tietojenvaihdossa
    - Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007)
    - Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (617/2009)
    - Sähköisen viestinnän tietosuojalaki (516/2004): Sähköisen viestinnän luottamuksellisuus ja yksityisyyden suoja
    - Rikoslaki (39/1889) 34. luku 9a §: Vaaran aiheuttaminen tietojenkäsittelylle
    - Rikoslaki (39/1889) 38. luku 8 §: Tietomurto
    - Rikoslaki (39/1889) 38. luku 9 § 1. kohta: Henkilötietorikos
    - Henkilötietolaki (523/1999) 48 §: Henkilörekisteririkkomus
    - Vahingonkorvauslaki (41/1974)

Lainsäädännön lisäksi tulee noudattaa muita omalle organisaatiolle hyväksyttyjä tietoturvaan ja tietosuojaan liittyviä ohjeita ja määräyksiä. Organisaation omat päätökset, määräykset ja ohjeet eivät saa olla ristiriidassa tämän tietoturvapolitiikan tai organisaation ylemmän tason määräysten kanssa siten, että tietoturva tai tietosuoja heikkenee.

# 4. Tietoturvallisuuteen kohdistuvat uhat

Tietoturvallisuuteen kohdistuvat uhat aiheuttavat riskin tietojen, tietojärjestelmien tai tietoliikenteen luottamuksellisuudelle, eheydelle ja käytettävyydelle.

Henkilöiden mahdollinen osaamattomuus, huolimattomuus ja välinpitämättömyys aiheuttavat merkittävimmän uhan organisaation tietoturvallisuudelle. Lisäksi uhkia aiheuttavat tietoisesti tehty tietojen väärinkäyttö, tietomurrot, virheellisesti toimivat ohjelmistot ja laitteet, virukset, haittaohjelmat, palvelunestohyökkäykset sekä tekniset ongelmat. Merkittäviä uhkia voi liittyä myös ulkopuolisten palvelujen tuottamiseen, mikäli palveluntuottajien kanssa ei ole tehty sopimuksia, joissa huomioidaan tietoturvaan, tietosuojaan ja varautumiseen liittyvät asiat sekä rikkomuksiin liittyvät sanktiot.

Jokaisessa organisaatiossa, prosessissa, projektissa ja tietojärjestelmässä tulee huolehtia tietoturvaan ja tietosuojaan sekä laajemminkin tietotekniikkaan liittyvien riskien hallinnasta.

# 5. Tietoturvallisuuden merkitys ja toteuttaminen

## 5.1. Turvattavat kohteet

Toiminnan tietoturvallisuuden kannalta tärkeimmät turvattavat kohteet ovat henkilöt, tilat,   
laitteet, tietoliikenne, tietojärjestelmät, palvelut sekä tiedot ja tietoaineistot kaikissa   
olomuodoissaan.

Näiden kohteiden turvaamisen tavoitteena on operatiivisten järjestelmien ja sisäisen   
tietoverkon toiminnan turvaaminen sekä palvelujen tuottaminen normaali- ja poikkeusoloissa.

## 5.2 Siikaisten kunnassa noudatettavat tietoturvaperiaatteet

* 1. Tietoturva ja tietosuoja ovat Suomen lainsäädännön mukaisesti osa organisaation päivittäistä toimintaa ja koskevat koko toimintaa ja henkilöstöä.
  2. Asiat pitää tehdä tietoturvallisesti, millä tarkoitetaan tiedon suojaamista monenlaisilta uhkilta. Tarkoituksena on varmistaa toiminnan jatkuvuus, minimoida toiminnalliset riskit sekä maksimoida investoinneista ja toiminnan mahdollisuuksista saatu tuotto.
  3. Tietoturvaan liittyvät ongelmat tulee mieluummin ennaltaehkäistä kuin hoitaa jälkikäteen.
  4. Tietoturva- ja tietosuoja-asiat pitää huomioida välineestä riippumatta eli ne eivät liity vain tietotekniikkaan.
  5. Paperiset asiakirjat, sähköiset tietovarannot, tietojärjestelmät, tietotekniset laitteet, tietoverkot ja niihin liittyvät palvelut on pidettävä asianmukaisesti suojattuina sekä normaali- että poikkeusoloissa.
  6. Tietoturvallisuuden saavuttamiseksi pitää toteuttaa sopivia turvamekanismeja, jotka muodostuvat toimintaperiaatteista, prosesseista, organisaatiorakenteista ja ohjelmisto- ja laitteistotoiminnoista.
  7. On varmistettava, että luottamukselliset, arkaluonteiset ja muut salassa pidettävät asiat kuuluvat vaitiolovelvollisuuden piiriin riippumatta siitä, miten tai mihin niitä on tallennettu tai millä tavalla tiedot on saatu.
  8. Jokaisen esimiehen on huolehdittava, että tietoturva- ja tietosuojamääräykset ja ohjeet koulutetaan ja perehdytetään henkilöstölle.
  9. Tietoturvaan liittyvä ohjaus, valvonta ja seuranta tulee organisoida.
  10. Tietoturvan toteutumista tulee seurata ja kehittää.

## 5.3 Tietoturvallisuuden toteutumista tukevia käytäntöjä

Jokaisen kunnan tulee nimetä oma tietoturvasta ja tietosuojasta vastaava henkilö:tietosuojavastaava.

Uusien tietojärjestelmien, prosessien sekä tilojen tietoturva-asiat tulee huomioida ja testata jo ennen niiden käyttöön ottamista. Tietojärjestelmien toimintaa ja käyttöä tulee valvoa.

Sisäisten tietojärjestelmien tietojen käyttö tulee pääsääntöisesti sallia vain työtehtävien tai niihin rinnastettavien tehtävien hoitamiseen sekä yhteistyökumppaneilla vastaavasti sopimusten ja lupien mukaisten tehtävien hoitamiseen.

Tietoturvan ja tietosuojan toteuttamisessa tulee käyttää tarvittaessa ulkopuolisten asiantuntijoiden apua.

Palvelujen hankintaan ja ulkoistuksiin liittyvissä sopimuksissa pitää huomioida turvallisuuteen ja varautumiseen liittyvät asiat.

Tietojärjestelmiin ja tietojen käsittelyyn liittyvissä suunnitelmissa, järjestelyissä sekä ohjeissa   
varaudutaan tietoturvallisuutta ja tietosuojaa koskevien laiminlyöntien, vahinkojen tai virheiden jälkikäteisselvittämiseen. Tässä on hyvä pitää periaatteena kustannusten kohtuullisuus saatuun hyötyyn nähden.

# 6. Turvatoimien priorisointi

Turvatoimien järjestys tilanteissa, joissa joudutaan toteuttamaan priorisointia:

 henkilön hengen tai terveyden turvaaminen

 arkaluonteisen tai muuten erittäin merkittävän tiedon luottamuksellisuuden turvaaminen

 tietojärjestelmien ja rekistereiden eheyden turvaaminen

 käyttö- ja toimintaympäristön käytettävyyden turvaaminen

# 7. Tietoturvallisuuden hallintajärjestelmä

Hallintajärjestelmän avulla toteutetaan tietoturvan hallintaa ja seurantaa sekä arvioidaan tietoturvatoimien tehokkuutta ja tarkoituksenmukaisuutta. Järjestelmän jatkuva kehittäminen parantaa valmiuksia hallita tietoturvallisuutta järjestelmällisesti. Tietoturvallisuuden hallintajärjestelmä on luonteeltaan viitekehys, joka koostuu toimintamalleista ja dokumenteista.

Toimintamalleja ovat esim. tietosuojan vastuuhenkilöiden yhteistoiminta muiden kuntien kanssa, tietojärjestelmien ja henkilörekisterien omistajuuden hallinta, poikkeamien ja selvitysten käsittely sekä tietoturvaan ja tietosuojaan liittyvä riskienhallinta.

Dokumentteina on mm. kunnan tietoturva- ja tietosuojapolitiikka (tämä dokumentti), tietoturvallisuuteen liittyvä ohjeistus (mm. henkilöstön tietoturva- ja tietosuojaopas) sekä tietosuojaselosteet.

# 8. Tietoturvavastuut

## 8.1. Organisaation tietoturvavastuut

Tietoturvapolitiikan ja tietosuojan järjestämisestä vastaa kunnanhallitus ja toimiva johto. Johtamansa toiminnan tietosuojan valvonnasta vastaa kukin toimielin ja vastuuhenkilö.  Tietoturvapolitiikkaa ja tietosuojaa ei eriytetä muusta tavoitteiden saavuttamiseen tähtäävästä toiminnasta, vaan se on jatkuva osa päivittäistä johtamista, ohjaamista ja työn toteuttamista. Kunnan hallintosäännössä on määrätty tietosuojavastaavaksi kunnansihteeri. Kunnanhallitus määrää tarvittaessa sijaisen.

## 8.2. Kunnan yhteistyökumppaneiden vastuut

Kunnalle palveluja tuottavat tahot tulee velvoittaa nimeämään tietoturva- sekä tietosuoja-asioihin yhteyshenkilö, joka heillä vastaa sovitun tietoturva- ja tietosuojatason noudattamisesta. Kumppanien tulee viipymättä ilmoittaa omista kuntaan vaikuttavista tietoturvapoikkeamistaan ilmoitetuille kunnan yhteyshenkilöille.

# 9. Tietoturva- ja tietosuojakoulutus ja –ohjeet

Tietoturvallisuus tulee olla sisällytettynä perehdytysprosessiin. Koulutusta järjestetään ja mahdollistetaan kaikille työntekijöille määräajoin. Henkilöstön tietoturva- ja tietosuojaopas pidetään ajan tasalla ja siitä kerrotaan työntekijöille sekä kaikille organisaation tietoja ja tietojärjestelmiä käyttäville muille henkilöille.

Tietojärjestelmien käyttäjiltä edellytetään käyttö- ja salassapitositoumuksen hyväksyminen. Tietoturvaan ja tietosuojaan liittyvien ohjeiden sisällöstä ja ajantasaisuudesta vastaavat nimetyt tietoturvan ja tietosuojan vastuuhenkilöt.

Esimiesten tulee varmistaa, että henkilöstö hallitsee tietoturvan ja tietosuojan perusteet. Varmistaminen onnistuu esim. tarkastamalla kehityskeskusteluissa, että jokainen tietojärjestelmiä käyttävä henkilö on tutustunut henkilöstön tietoturva- ja tietosuojaoppaaseen ja mahdollisesti suorittanut tietoturvaan liittyviä kursseja.

# 10. Tietoturvallisuudesta tiedottaminen

Tietoturva- ja tietosuoja-asioista tiedotetaan tarpeen mukaan. Tietoturva-asioiden sisäisestä tiedottamisesta vastaavat tietoturvan ja tietosuojan vastuuhenkilö yhdessä viestinnästä vastaavan tahon kanssa.

Tietoturva- ja tietosuoja-asioista ei aktiivisesti tiedoteta ulkopuolisille, mutta jos tiedottamistarvetta ilmenee, sen hoitavat tietoturvasta tai tietosuojasta vastaava henkilö yhteistyössä viestinnästä vastaavan tahon kanssa.

# 11. Tietoturvallisuuden toteutumisen valvonta

Jokainen organisaation tietoja ja tietojärjestelmiä käyttävä on velvollinen ilmoittamaan havaitsemistaan tietoturvallisuuden puutteista, uhkista tai menettelyvirheistä kunnan tietoturvavastaavalle tai omalle esimiehelleen.

Esimiesten tulee valvoa, että henkilöstö noudattaa tietoturvasta ja tietosuojasta annettuja määräyksiä ja ohjeita.

# 12.Toiminta häiriötilanteissa ja poikkeusoloissa

Erilaisissa häiriötilanteissa toimitaan tarvittaessa riskienhallintaan ja varautumiseen liittyvien suunnitelmien mukaisesti. Poikkeusolojen toiminnan suunnittelua koordinoi alueellinen pelastuslaitos.