Tampereen seudun tietoturvapolitiikka

Sisällys

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.

Tietoturvan tärkeyttä lisäävät myös asiakkaille suunnattujen sähköisten palvelujen laajentuminen, tietojärjestelmien etä- ja mobiilikäyttö, kuntien yhteistyö palvelujen järjestämisessä, laaja palveluntuottajien verkosto sekä palvelutuotannon ja tietojenkäsittelyn nykyaikaiset menetelmät.

Tampereen seudun tietoturvapolitiikka on laadittu ja tarkoitettu Tampereen seudun tietohallintoyhteistyössä mukana olevien kuntien (Hämeenkyrö, Kangasala, Lempäälä, Nokia, Orivesi, Pirkkala, Tampere, Vesilahti ja Ylöjärvi) henkilöstölle sekä kuntien tietoja ja tietojärjestelmiä tai toimitiloja käyttäville yrityksille tai muille yhteistyökumppaneille.

Tämä tietoturvapolitiikka on sisäinen velvoittava määräys, joka on tarkoitettu seudun kuntien sisäiseen käyttöön. Politiikka on hyväksytty kunkin kunnan kaupunginhallituksessa tai kunnanhallituksessa. Seudun tietoturvapolitiikkaa täydennetään erikseen hyväksyttävillä tietoturvaan ja tietosuojaan liittyvillä määräyksillä ja ohjeilla.

2 Tietoturvapolitiikan tavoite

Tietoturvallisuuden ensisijaisena päämääränä on organisaatioiden vastuulla olevien tietojen ja palvelujen jatkuvuuden turvaaminen kaikissa olosuhteissa eli tietotekniikkanäkökulmasta mahdollistaa organisaation tietojen ja ICT-ratkaisujen käytettävissä oleminen (saatavuus) sekä 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 asiakkaiden, työntekijöiden ja muiden osallisten yksityisyyden suoja.

Tiedonhallintalain mukaisesti kuntien on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan.

Toiminnan tietoturvallisuuden kannalta tärkeitä turvattavia kohteita ovat mm. henkilöt, tilat, laitteet, tietoliikenne, tietojärjestelmät, palvelut sekä tiedot ja tietoaineistot kaikissa olomuodoissaan.

Tavoitteena on operatiivisten järjestelmien ja tietoverkon toiminnan turvaaminen sekä palvelujen tuottamisen turvaaminen normaali- ja poikkeusoloissa.

3 Määritelmät

3.1 Tietohallinto

Tietohallinnolla (organisaatiolla) tarkoitetaan tässä tietoturvapolitiikassa ensisijaisesti Tampereen kaupungin tietohallinnon johtamaa seudullista tietohallintoa, mutta mikäli käsiteltävästä asiasta ei ole seudullista päätöstä tai ratkaisua, niin myös kunkin kunnan omaa tietohallintoa.

3.2 Tietoturvallisuus, tietosuoja ja muut termit

Tietoturvallisuus, tietosuoja ja näihin liittyvät muut termit määritellään liitteessä 2.

4 Tietoturvatoimintaa ja tietosuojaa ohjaavat tekijät

Tietoturvatoimintaa ja tietosuojaa ohjataan säädöksin, määräyksin, ohjein ja suosituksin. Näihin liittyviä päätöksiä tehdään sekä omassa organisaatiossa että sen ulkopuolella. Esimerkkejä toimintaa tietoturvallisuuden ja tietosuojan näkökulmasta ohjaavista säädöksistä on liitteessä 3.

Lainsäädännön lisäksi tulee noudattaa muita omalle organisaatiolle hyväksyttyjä ja velvoittavia tietoturvaan ja tietosuojaan liittyviä ohjeita ja määräyksiä. Organisaation omat päätökset, määräykset ja ohjeet eivät saa olla ristiriidassa tämän tietoturvapolitiikan tai organisaation ylemmän tason muiden määräysten kanssa. Organisaation osa voi kuitenkin tehdä omaan toimintaansa tiukempiakin ohjeita tai linjauksia, mikäli se on heidän toimintansa kannalta perusteltu ratkaisu.

5 Tietoturvallisuuteen kohdistuvat uhat

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

Henkilöiden kouluttaminen ja tietoturvakulttuurin ylläpitäminen on tärkeää, jotta voidaan välttää osaamattomuuden, huolimattomuuden ja välinpitämättömyyden aiheuttavat merkittävät uhat organisaation tietoturvallisuudelle. Uhkia aiheuttavat myös tietoisesti tehty tietojen väärinkäyttö, tietomurrot, virheellisesti toimivat ohjelmistot ja laitteet, haittaohjelmat, kyberhyökkäykset, palvelunestohyökkäykset, tietojen kalastelut 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. Tehtyjen sopimusten noudattamisen valvominen on myös olennainen osa toimittajien hallintaa.

Tiedonhallintalaki velvoittaa selvittämään olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoittamaan tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti. Jokaisessa kunnassa, organisaatiossa, prosessissa, projektissa ja tietojärjestelmässä tulee

huolehtia tietoturvaan ja tietosuojaan liittyvien riskien hallinnasta. Merkittäville riskeille tulee määritellä hallintakeinot ja tällaiset riskit tulee tuoda tiedoksi kunnan tietoturvasta vastaavalle sekä seudun tietoturvaryhmälle.

6 Tietoturvallisuuden merkitys ja toteuttaminen

6.1 Tietoturvaperiaatteet

Seudullisesti on sovittu yhteisesti noudatettaviksi tietoturvaperiaatteiksi seuraavat:

1. Tietoturva ja tietosuoja ovat osa organisaation päivittäistä toimintaa ja riskienhallintaa.
2. Asiat pitää tehdä tietoturvallisesti, millä tarkoitetaan tiedon suojaamista monenlaisilta uhkilta. Tarkoituksena on varmistaa (liike)toiminnan jatkuvuus ja minimoida (liike)toiminnalliset riskit.
3. Tietoturvaan ja tietosuojaan liittyvät ongelmat tulee mieluummin ennaltaehkäistä kuin hoitaa jälkikäteen.
4. Tietoturva- ja tietosuoja-asiat pitää huomioida välineestä riippumatta eli ne liittyvät muuhunkin kuin vain tietotekniikkaan ja koskevat kaikkia henkilöitä.
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 esihenkilön on huolehdittava, että tietoturva- ja tietosuojamääräykset ja ohjeet koulutetaan ja perehdytetään henkilöstölle.
9. Tietoturvaan liittyvä ohjaus, valvonta, raportointi ja seuranta tulee organisoida.
10. Tietoturvan toteutumista tulee seurata ja kehittää.
11. Tietoturvaan ja tietosuojaan liittyvät asiat pitää huomioida tarkasti sopimuksissa.
12. Työntekijöiden ja yhteistyökumppaneiden taustat tulee tarkistaa voimassa olevan lainsäädännön mukaisesti.

Nämä periaatteet tulee jokaisen huomioida mm. valintoja, suunnitelmia ja päätöksiä tehdessään.

6.2 Tietosuojaperiaatteet

Henkilötietojen käsittelyssä noudatetaan seuraavia tietosuoja-asetuksen (GDPR) mukaisia henkilötietojen käsittelyä koskevia periaatteita:

- lainmukaisuus, kohtuullisuus ja läpinäkyvyys

- käyttötarkoitussidonnaisuus
- tietojen minimointi
- täsmällisyys
- säilytyksen rajoittaminen
- eheys ja luottamuksellisuus
- osoitusvelvollisuus.

Kaikessa henkilötietojen käsittelyssä tulee lisäksi noudattaa kulloinkin voimassa olevaa soveltuvaa lainsäädäntöä. Kunnat voivat antaa erillisiä tarkentavia ohjeistuksia ja määräyksiä vaatimustenmukaisen henkilötietojen käsittelyn varmistamiseksi.

6.3 Tietoturvallisuuden ja tietosuojan toteutumista tukevia käytäntöjä

Jokaisen kunnan tulee nimetä oma **tietoturvasta vastaava henkilö**.

Lainsäädäntö edellyttää, että jokainen kunta nimeää **tietosuojavastaava**n, jonka asemasta ja tehtävistä säädetään tietosuoja-asetuksessa.

Myös kuntien sisällä palvelualueilla tai muissa isommissa kokonaisuuksissa tulee nimetä henkilöt, jotka kyseisessä organisaatiossa vastaavat tai ainakin toimivat **yhteyshenkilö**inä tietoturvaan ja tietosuojaan liittyvissä asioissa.

Kunnissa tulee huolehtia tietoturvaan ja tietosuojaan kohdistuvasta uskottavasta ja riittävästä resursoinnista. Tietoturvan ja tietosuojan toteuttamisessa tulee käyttää tarvittaessa ulkopuolisten asiantuntijoiden apua.

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

Organisaatioille ja tietojenkäsittely-ympäristöille voidaan asettaa eritasoisia teknisiä ja hallinnollisia vaatimuksia (tietoturvallisuustasoja) muun muassa sen mukaan, millaisia tietoja kohteessa käsitellään. Tiedonhallintalaki ja siihen liittyvät tiedonhallintalautakunnan suositukset asettavat kunnille ja muulle julkiselle hallinnolle sekä näiden lukuun toimiville tietoturva-asioiden minimitason, johon tulee kaikessa toiminnassa päästä.

Uusien tietojärjestelmien, prosessien sekä tilojen tietoturva ja tietosuoja tulee huomioida ja testata jo ennen käyttöönottoa. Erityisesti tärkeissä/kriittisissä tietojärjestelmissä ja projekteissa on hyvä tarkastaa eli auditoida ulkopuolisella asiantuntijataholla tai sisäisesti jo määrittelyvaiheessa, mutta erityisen tärkeää se on ennen kuin uusi tietojärjestelmä voidaan ottaa tuotantokäyttöön.

Tietojärjestelmien toimintaa ja käyttöä tulee valvoa.

Henkilötietojen käsittelyn ulkoistuksiin liittyvissä sopimuksissa pitää laatia henkilötietojen käsittelysopimus tai liite.

Mikäli henkilötietojen käsittely todennäköisesti aiheuttaa korkean riskin rekisteröityjen oikeuksille ja vapauksille, tulee käsittelystä laatia tietosuojaa koskeva vaikutustenarviointi (DPIA) ennen käsittelytoimien aloittamista.

Toiminnan jatkuvuus tulee turvata toipumissuunnittelulla, joka sisältää häiriöiden ennalta ehkäisemisen ja mahdollistaa niistä nopean toipumisen. Toipumissuunnittelussa tulee erityisesti huomioida toiminnan riskit ja prioriteetit.

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

7 Turvatoimien priorisointi

Turvatoimien järjestys tilanteissa, joissa joudutaan toteuttamaan priorisointia:

- henkilön hengen tai terveyden turvaaminen
- merkittävän omaisuuden turvaaminen
- arkaluonteisen tai muuten salassa pidettävän tai erittäin merkittävän tiedon luottamuksellisuuden turvaaminen
- tietojärjestelmien ja rekistereiden eheyden turvaaminen
- käyttö- ja toimintaympäristön saatavuuden turvaaminen.

8 Tietoturvallisuuden hallintajärjestelmä

Tietoturvapolitiikka on osa Tampereen seudun kuntien tietoturvallisuuden ja tietosuojan hallintajärjestelmää. Hallintajärjestelmään kuuluvat kaikki tietoturvallisuuden ja tietosuojan hallintaan tarvittavat toimintatavat, hallintakeinot ja dokumentit.

Hallintajärjestelmän avulla toteutetaan tietoturvan hallintaa ja seurantaa sekä arvioidaan tietoturvatoimien tehokkuutta ja tarkoituksenmukaisuutta. Tavoitteena on järjestelmän jatkuva kehittäminen ja sen myötä riittävän tietoturvatason ylläpitäminen.

Liitteessä 4 on lueteltu esimerkkejä tärkeimmistä hallintajärjestelmään kuuluvista toimintamalleista sekä dokumenteista.

Kaikki tietoturvallisuuden ja tietosuojan hallintajärjestelmään liittyvät politiikat ja muut velvoittavat dokumentit katselmoidaan vähintään kahden vuoden välein. Tampereen seudun yhteisten dokumenttien katselmoinnista vastaa seudun tietoturvaryhmä. Muiden osalta katselmoinnista vastaa dokumentin omistaja.

9 Vastuut ja valtuudet

9.1 Yleiset vastuut

Vastuu omassa organisaatiossa ja toiminnassa tietoturvan ja tietosuojan toteuttamisesta sekä tietoturvapolitiikan noudattamisesta on **jokaisella** työntekijällä, vaikka **tietohallinto** vastaa yleisestä tietoturvan ja tietosuojan hallinnan kehittämisestä sekä koordinoinnista. Tietoturvaan ja tietosuojaan liittyvissä asioissa **jokainen** henkilö on vastuussa riskeistä, jotka liittyvät hänen päätöksentekovaltaansa tai päätöksiin.

Jokainen seudun **kunta** vastaa tämän tietoturvapolitiikan mukaisesta tietoturvan ja tietosuojan toteuttamisesta. **Organisaation eri osat** vastaavat tietoturvallisuuden ja tietosuojan toteutumisesta omalla vastuualueellaan.

Jokainen organisaation tietoja ja tietojärjestelmiä käyttävä on velvollinen ilmoittamaan havaitsemistaan tietoturvallisuuden puutteista, uhkista tai menettelyvirheistä eteenpäin tietohallinnon ohjeistamalla tavalla. Henkilötietoihin kohdistuvat tietoturvaloukkaukset tulee käsitellä sovellettavan tietosuojalainsäädännön edellyttämällä (mm. GDPR:n 72 tunnin sääntö) ja tietohallinnon ohjeistamalla tavalla.

Kunnan virallisille henkilörekistereille pitää nimetä **vastaava viranhaltija**, joka vastaa kyseisen henkilörekisterin osalta hyvän henkilötietojen käsittelytavan ja lainsäädännön edellyttämän korkean tietoturvan ja tietosuojan tasosta sekä rekisterin tietojen käsittelyyn liittyvistä linjauksista sekä rekisteröidyn oikeuksien toteuttamisesta. Erityisesti palvelu- ja alihankintasopimuksissa on rekisterinpitoon, tietosuojaan ja tietoturvaan liittyvät asiat huomioitava tarkasti. Yksityisyyden suoja on ihmisten perusoikeus, jonka varmistamisesta on vastuuhenkilöiden lisäksi myös kaikkien esihenkilöiden ja tietoja käsittelevien henkilöiden huolehdittava.

Henkilörekistereiden vastuuhenkilöiden, **toimintayksiköiden** ja **prosessien omistajien** vastuulla on rekistereissä, toiminnassa ja prosesseissa tuotettavien sekä käsiteltävien tietojen ajantasaisuuden, oikeellisuuden, saatavuuden ja eheyden varmistaminen sekä tietoihin liittyvien käyttövaltuuksien määrittely. **Tietohallinto** vastaa yleisistä käyttövaltuusperiaatteista.

Kunkin **tietojärjestelmän omistajalla** on vastuu tietojärjestelmän toimintavarmuudesta ja dokumentoinnista mukaan lukien riskien hallinta ja tarvittaessa jatkuvuus- ja toipumissuunnitelman laatiminen. Jokainen **sovellusta tai ICT-palvelua käyttävä organisaatio**, **rekisterinpitäjä** tai **prosessin omistaja** on kuitenkin itse vastuussa toimintansa riskien hallinnasta ja varautumisesta muun muassa sen varalta, että sovelluksen tai ICT-palvelun toiminnassa on häiriöitä. Riskienhallinta ja varautuminen tulee tehdä kunnan sekä oman toiminnan lähtökohdista ja laatia suunnitelmat siitä, miten toimitaan häiriöiden aikana ja miten toiminta palautetaan normaaliksi häiriöiden jälkeen. **Tietohallinto** turvaa ja priorisoi omistamansa järjestelmät asiakkaidensa toi-

minnan prioriteettien ja riskien pohjalta. Tietojärjestelmien ylläpitoon liittyvät tietoturva-asiat tietohallinto määrittelee tarkemmin sitä asiaa käsittelevissä erillisissä määräyksissä ja ohjeissa.

9.2 Tietoturvan hallinnan vastuut ja -valtuudet

Tietoturvatoiminnan ja tietoturvallisuuden hallintajärjestelmän ylläpidosta ja kehittämisestä vastaa **tietohallinto tietoturvapäällikön** johdolla. Kukin **kunta** laatii itse tarkemman oman kunnan tarpeisiin liittyvän tietoturvasuunnitelman, jonka toteutumista pitää seurata ja valvoa. Lisäksi kuntien pitää laatia tietoturva- ja tietosuojapoikkeamiin liittyvä viestintä- ja selvityssuunnitelma sekä kyseisiin poikkeamiin liittyvä seuraamustaulukko, joka pitää käsitellä kunnan yhteistoimintaryhmässä.

Seudun tietoturvaryhmä tekee **Tampereen kaupungin tietoturvapäällikön** johdolla tietoturvaan liittyviä seudullisia linjauksia ja esityksiä. Mikäli ne edellyttävät aiemmin hyväksymättömiä kustannuksia tai muuten vaikuttavat merkittävästi tietojärjestelmien käyttäjiin, kuntalaisiin tai palvelutuotantoon, niin ne lisäksi käsitellään ja vahvistetaan **tietohallinnon seudullisessa johtoryhmässä**. Seudun tietoturvaryhmä käsittelee ja ottaa kantaa myös seudun ICT-palveluntuottajien palveluihin liittyviin tietoturva-asioihin.

Akuuteissa yksittäistä kuntaa koskevissa uhka- tai ongelmatilanteissa päätöksen turvaamistoimenpiteistä (estää, sulkea tai avata jokin yhteys, järjestelmä, tunnus tms.) voi tehdä kyseisen **kunnan tietoturvasta vastaava** henkilö. Laajemmissa tai koko seutua koskevissa akuuteissa uhka- tai ongelmatilanteissa päätöksen turvaamistoimenpiteistä voi tehdä **Tampereen kaupungin tietoturvapäällikkö tai tietohallintojohtaja**.

Kunkin kunnan **tietoturvasta vastaavalla** henkilöllä on valtuus muiden päätösten estämättä tarkastaa ja muuttaa oman kunnan tietojärjestelmien käyttöoikeuksia ja tehdä niihin liittyviä päätöksiä. **Tampereen kaupungin tietoturvapäälliköllä** on vastaava oikeus Tampereen järjestelmien lisäksi myös seudun yhteisiin järjestelmiin.

Tampereen seudun tietoturvaryhmällä ja **Tampereen kaupungin tietoturvapäälliköllä** on valtuudet tarvittaessa sallia perusteltuja poikkeuksia tietoturvalinjauksiin.

Kunkin **kunnan tietoturvasta vastaavalla** henkilöllä sekä **kunnan tietosuojavastaavalla** on oikeus suorittaa käytönvalvontaa sekä tarkastaa ja auditoida toimintatapoja, tietojärjestelmiä ja tietoja liittyen oman kunnan tietoturvan tai tietosuojan sääntöjen ja ohjeiden noudattamiseen ja toteuttamiseen tai väärinkäytösepäilyjen selvittämiseen. **Tampereen kaupungin tietoturvapäälliköllä** on vastaava oikeus Tampereen lisäksi myös seudun yhteisiin järjestelmiin ja toimintatapoihin.

Tietoturvapolitiikka päivitetään tarvittaessa. Päivitystarvetta seuraa **tietohallinto** ja **tietoturvapäällikkö**. Organisaatiomuutoksista, laeista tai muista määräyksistä sekä hallintaympäristön uusista hyväksytyistä toimintamalleista ja dokumenteista johtuvia

teknisiä korjauksia tähän dokumenttiin ja sen liitteisiin voidaan tehdä seudun tietoturvaryhmän käsittelyn pohjalta ilman erillistä hyväksyntäkäsittelyä kuntien hallituksissa.

9.3 Organisaation yhteistyökumppaneiden vastuut

Organisaatiolle palveluja tuottavat tahot tulee velvoittaa nimeämään tietoturva- sekä tietosuoja-asioihin yhteyshenkilö, joka heillä huolehtii sovitun tietoturva- ja tietosuojatason noudattamisesta. Kumppanit tulee velvoittaa ilmoittamaan ja raportoimaan viipymättä omista seudulle vaikuttavista tietoturvapoikkeamista, henkilötietoihin kohdistuneista tietoturvaloukkauksista ja muista läheltä piti -tilanteista sovituille yhteyshenkilöille tai suoraan tietoturvasta ja tietosuojasta vastaaville. Kumppaneille asetettavat vaatimukset (mm. varautumisesta, henkilöstön kouluttamisesta ja henkilötietojen käsittelystä) tulee kuvata sopimuksessa tai sen erillisessä liitteessä.

Yhteistyökumppaneiden ne henkilöt, joilla on pääsy Tampereen seudun tietojärjestelmiin tai luottamukselliseen tietoon, tulee velvoittaa noudattamaan tilaajan tietoturva- ja tietosuojaohjeistusta ja heille tulee järjestää tilaajan edellyttämä yhteistyön kannalta välttämätön koulutus.

10 Tietoturva- ja tietosuojakoulutus sekä -ohjeet

Tietoturvallisuuden ja tietosuojan tulee olla sisällytettynä perehdytysprosessiin. Koulutusta järjestetään ja mahdollistetaan kaikille työntekijöille määräajoin. Kohdennettua koulutusta järjestetään työntekijän roolin asettamien vaatimusten mukaisesti tarpeen mukaan. Seudullinen Henkilöstön tietoturva- ja tietosuojaopas pidetään ajan tasalla ja siitä kerrotaan työntekijöille sekä kaikille organisaation tietoja ja tietojärjestelmiä käyttäville muiden organisaatioiden henkilöille.

Tietojärjestelmien käyttäjiltä edellytetään tietojen ja tietojärjestelmien käyttö- ja salassapitositoumuksen hyväksymistä ennen pääsyn myöntämistä tietojärjestelmiin.

Tietoturvaan ja tietosuojaan liittyvien ohjeiden sisällöstä ja ajantasaisuudesta vastaavat nimetyt **tietoturvan ja tietosuojan vastuuhenkilöt**.

Esihenkilöiden 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 sekä mahdollisesti suorittanut tietoturvaan liittyviä kursseja.

11 Tietoturvallisuudesta tiedottaminen

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

Tietoturva- ja tietosuoja-asioista ei aktiivisesti tiedoteta ulkopuolisille, mutta jos tiedottamistarvetta ilmenee, sen hoitaa tietohallintojohtaja, viestintä tai muu sovittu henkilö yhteistyössä tietoturvasta ja/tai tietosuojasta vastaavien henkilöiden kanssa.

12 Tietoturvallisuuden toteutumisen valvonta

Tietoturvallisuudesta annettujen vaatimusten toteutumisesta vastaa kukin toimintayksikkö tai organisaatiolle palveluja tuottava yritys omalla vastuualueellaan. Esihenkilöiden tulee valvoa, että henkilöstö noudattaa tietoturvasta ja tietosuojasta annettuja määräyksiä ja ohjeita.

Tampereen seudun tietoturvapolitiikan ja siihen liittyvien ohjeistuksien toteutumista ja noudattamista seuraavat seudun tietoturvaryhmä sekä nimetyt tietoturvan ja tietosuojan vastuuhenkilöt, joiden velvollisuus on raportoida oman organisaationsa johdolle.

13 Toiminta häiriötilanteissa ja poikkeusoloissa

Erilaisissa häiriötilanteissa toimitaan tarvittaessa riskienhallintaan ja varautumiseen liittyvien suunnitelmien mukaisesti. Mikäli organisaatiolla on oma valmiussuunnitelma, toimitaan poikkeusoloissa sen menettelytapojen mukaisesti. Valmiussuunnitelmien sisällön tulee olla yhteneväinen jatkuvuuteen ja toipumiseen liittyvien suunnitelmien kanssa.

Koko seudun näkökulmasta poikkeusolojen toiminnan suunnittelua koordinoi alueellinen pelastuslaitos, mutta siitä vastaa kunkin kunnan johto.

14 Liite 1 – Versiohistoria ja hyväksynnät

Tampereen seudun tietoturvapolitiikka on hyväksytty kuntien hallituksessa seuraavissa kokouksissa:

Kaupunki / kunta	Kokouspäivämäärä	Edellinen hyväksyntä
Hämeenkyrö		21.1.2013
Kangasala		17.12.2012
Lempäälä		17.12.2012
Nokia		17.12.2012
Orivesi		19.11.2012
Pirkkala		26.11.2012
Tampere		26.11.2012
Vesilahti		3.12.2012
Ylöjärvi		17.12.2012

Dokumentin versiohistoria:

Versio (päivämäärä)	Päivittäjä tai hyväksyjä	Tehdyt muutokset
1.1.2013	Kuntien hallitukset	Tampereen seudun ensimmäinen yhteinen tietoturvapolitiikka
27.5.2022	Tampereen seudun tietoturvaryhmä	Uusi 2022 versio seudun tietoturvapolitiikasta
31.5.2022	Tietohallinnon seudullinen johtoryhmä	Käsittely ja hyväksyntä eteenpäin kuntien hallitusten käsittelyyn.
1.8.2022	Juha Koivisto	Tietohallinnon seudullisen johtoryhmän kommenttien perusteella tehty pienet muutokset lukuihin 7, 9.2 ja 15.1.

15 Liite 2 – Määritelmät ja sanasto

15.1 Tietoturvallisuus

Tietoturvallisuus kattaa järjestelyt, joilla pyritään varmistamaan tiedon saatavuus, 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 saatavuutta turvataan laitteisto- ja ohjelmistovikojen, luonnontapahtumien, häiriö- ja kriisitilanteiden 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 ja sille, että toiminnan johdolla säilyy näkyvyys heidän vastuullaan oleviin palveluprosesseihin.

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; tietoa ei ole muutettu luvatta tai se ei ole muuttunut vahingossa ja mahdolliset muutokset voidaan todentaa

- 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.

Saatavuus; tieto, tietojärjestelmä tai palvelu on hyödynnettävissä vaaditulla tavalla

- ominaisuus, että tieto, tietojärjestelmä tai palvelu on siihen oikeutetuille saatavilla ja hyödynnettävissä haluttuna aikana ja vaaditulla tavalla. Saatavuus termin sijasta käytetään usein myös termiä käytettävyys.

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

Kiistämättömyys; 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.

15.2 Tietosuoja

Tietosuoja on perusoikeus, joka turvaa rekisteröidyn (henkilön, jonka henkilötietoja käsitellään) oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä. Tietosuojan tarkoituksena on osoittaa, milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä.
Henkilötietoja tulee käsitellä aina lainmukaisesti. Riippumaton viranomainen (tietosuojavaltuutettu) valvoo henkilötietojen suojaa koskevien säännösten noudattamista.
Tietosuojaan liittyvät keskeiset käsitteet kuten **henkilötieto**, **erityiset henkilötietoryhmät**, **henkilötietojen käsittely**, **rekisterinpitäjä**, **henkilötietojen käsittelijä, tietosuojavastaava** ja **rekisteröity** määritellään EU:n yleisessä tietosuoja-asetuksessa (GDPR).

Tietoturva on yksi tietosuojan toteuttamisen keino.

15.3 Kyberturvallisuus

Kyberturvallisuus on tavoitetila, jossa kybertoimintaympäristöstä yhteiskunnan elintärkeille toiminnoille tai muille kybertoimintaympäristöstä riippuvaisille toiminnoille koituvat uhkat ja riskit ovat hallinnassa, myös häiriötilanteissa.

15.4 Digiturvallisuus

Digiturvallisuus (Digitaalinen turvallisuus) on

- tavoitetila, jossa digitaaliseen toimintaympäristöön voidaan luottaa ja toiminta sekä siellä että siihen liittyen on turvallista ja hallittua, myös häiriötilanteissa.
- Digiturvallisuus on laaja kokonaisuus, johon katsotaan kuuluvaksi tietoturvallisuus, tietosuoja, kyberturvallisuus sekä niihin liittyvät riskienhallinta, toiminnan jatkuvuus ja varautuminen.

16 Liite 3 – Tietoturvaa ja tietosuojaa ohjaavia säädöksiä / lakeja

Esimerkkejä toimintaa tietoturvallisuuden ja tietosuojan näkökulmasta ohjaavista säädöksistä ovat:

- EU:n yleinen tietosuoja-asetus (GDPR)
- Suomen perustuslaki
- tietosuojalaki
- laki viranomaisten toiminnan julkisuudesta
- laki julkisen hallinnon tiedonhallinnasta
- laki yksityisyyden suojasta työelämässä
- laki sähköisen viestinnän palveluista
- laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista
- vahingonkorvauslaki
- turvallisuusselvityslaki
- rikoslaki
- kuntalaki
- yhteistoimintalaki

sekä muut eri toimialueiden toimintaa ohjaavat erityislait.

17 Liite 4 – Tietoturvan ja tietosuojan hallintajärjestelmä

Tampereen seudun kuntien tietoturvallisuuden ja tietosuojan hallintajärjestelmään kuuluvat kaikki tietoturvallisuuden ja tietosuojan hallintaan tarvittavat toimintatavat, hallintakeinot ja dokumentit.

Hallintajärjestelmään kuuluvia toimintamalleja ovat muun muassa:

- Seudun tietoturvaryhmän toiminta.
- ICT-palveluiden toimittajien tietoturvaan liittyvät toimintamallit ja raportointi.
- Tietoturvapoikkeamien käsittely.
- Henkilötietojen tietosuojapoikkeamien ja –selvitysten käsittely.
- Poikkeamien lakisääteinen ilmoittaminen valvontaviranomaisille.
- Tietoturvan ja tietosuojan varhaisessa vaiheessa huomioiminen sopimuksissa, prosesseissa ja projekteissa.
- Tietoturvaan ja tietosuojaan liittyvien vaatimusten määrittely ICT-hankinnoissa.
- Tietoturva- ja tietosuojakoulutus.
- Tietoturvaan ja tietosuojaan liittyvien asioiden huomioiminen projektien, toimittajahallinnan ja organisaatioiden riskienhallinnassa.
- Omistajien ja/tai vastuuhenkilöiden määrittäminen tiedoille, tietojärjestelmille ja henkilörekistereille.
- Tietoturvan ja tilannekuvan kannalta tärkeiden lokitietojen kerääminen SIEM järjestelmään ja automatiikalla havaittujen poikkeamien selvittely (SOC ja Tukikeskuspalvelut).
- Tietojärjestelmien ylläpidossa huomioidaan tiedonhallintalain vaatimukset ja niihin liittyvät tiedonhallintalautakunnan suositukset.
- Tampereen seudun käyttövaltuusperiaatteiden noudattaminen tietojärjestelmien käyttövaltuuksien hallinnassa.

Hallintajärjestelmään liittyviä dokumentteja ovat muun muassa:

- Tampereen seudun tietoturvapolitiikka (tämä dokumentti)
- Tietojen ja tietojärjestelmien käyttö- ja salassapitositoumus
- Muut tietoturvaan ja tietosuojaan liittyvät määräykset, linjaukset, suunnitelmat sekä ohjeistus esimerkiksi seudulliset:
    - Henkilöstön tietoturvaopas
    - Mobiilipolitiikka
    - Sähköisten viestintävälineiden käyttösäännöt
    - Tietojenkäsittely pilvipalveluissa
    - Tiedon sijainti ja tiedon siirron edellytykset
- Tietosuojaa koskevat vaikutustenarvioinnit.

18 Liite 5 – Digiturvallisuuteen liittyviä uhkia / riskejä

Tähän kuvaan on kerätty erilaisia tietoturvaan ja tietosuojaan liittyviä uhkia eri riskinäkökulmista helpottamaan digiturvallisuuteen liittyvien riskien kartoitusta: