



PÄIJÄT-HÄMEEN SOSIAALI- JA TERVEYDENHUOLLON KUNTAYHTYMÄ

---

# PÄIJÄT-HÄMEEN SOSIAALI- JA TERVEYSYHTYMÄN TIETOTURVAPOLITIIKKA

*Kuntayhtymän hallitus 30.3.2009 § 42*

*Kuntayhtymän johtoryhmä 19.3.2009*

*Tietoturvallisuuden ja tietosuojan ohjaus- ja kehittämisryhmä 2.3.2009*

Versio 1.00 – 19.3.2009

# Sisällys

|                                                                                 |    |
|---------------------------------------------------------------------------------|----|
| 1. Johdanto .....                                                               | 3  |
| 1.1 Säädösten ja muiden vaatimusten täyttäminen .....                           | 3  |
| 1.2 Tarkoitus .....                                                             | 3  |
| 1.3 Tavoite .....                                                               | 4  |
| 2. Tietoturvallisuuden perustason määrittely.....                               | 5  |
| 2.1 Tärkeimmät hallinnolliset tietoturvatoimet .....                            | 5  |
| 2.1.1 Tietoturvallisuus osana kaikkea toimintaa .....                           | 5  |
| 2.1.2 Säädökset ohjaavat tietoturvallisuuden kehittämistä .....                 | 5  |
| 2.1.3 Tietojen turvallinen käsittely tietojärjestelmissä ja tietoverkoissa..... | 6  |
| 2.1.4 Tietoturvariskien hallinta .....                                          | 6  |
| 2.1.5 Kriittiset tilanteet ja toiminnan jatkuvuuden turvaaminen .....           | 6  |
| 2.1.6 Tietoturvallisuusasioiden tiedottaminen .....                             | 6  |
| 2.2 Tärkeimmät teknisluontoiset tietoturvatoimet .....                          | 7  |
| 2.2.1 Tietoturvapäivitykset ja käyttöturvallisuus.....                          | 7  |
| 2.2.2 Käyttäjähallinta .....                                                    | 7  |
| 2.2.3 Lokitiedot ja poikkeamaraportointi .....                                  | 7  |
| 2.2.4 Viestien ja dokumenttien välittäminen.....                                | 7  |
| 2.3 Fyysiset turvallisuustoimenpiteet.....                                      | 8  |
| 3. Valtuudet ja vastuut .....                                                   | 9  |
| 3.1 Tietoturvatyön organisointi ja tehtävät.....                                | 10 |
| 3.2 Tarkemmat ohjeet .....                                                      | 11 |
| 3.3 Soveltaminen .....                                                          | 11 |

## 1. Johdanto

Tietojen turvaaminen on olennainen osa Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän, (Päijät-Hämeen sosiaali- ja terveysyhtymä, PHSOTEY) toiminnan turvallisuutta. Tietojärjestelmät tukevat merkittävässä määrin yhtymän toimintaa sen tuottaessa toiminta-ajatuksensa mukaisia erikoissairaanhoidon, perusterveydenhuollon, sosiaalitoimen ja ympäristöterveydenhuollon palveluja. PHSOTEY:n tietoturvalähtöisyyden tarkoituksena on vahvistaa tietojenkäsittelyn perusturvasäädöksiä eli periaatteet, jotka luovat perustan tietoturvallisuuden kehittämistoimille.

Turvattavia tietoja ovat sekä manuaalisessa että sähköisessä muodossa olevat tiedot. Erityistä huomiota kiinnitetään sosiaali- ja terveysyhtymän toiminnan kannalta kriittisiin tietojärjestelmiin sekä niiden sisältämiin tietoihin.

### 1.1 Säästöjen ja muiden vaatimusten täyttäminen

PHSOTEY:ssä tietojenkäsittelyn ja sen turvaamisen periaatteet noudattavat kansallisia ja kansainvälisiä tietoturvallisuutta koskevia säädöksiä, standardeja, terveydenhuollon (sertifiointi)vaatimuksia ja suosituksia. Kaikessa toiminnassa noudatetaan hyvää tietojenkäsittelytapaa, velvoitteita ja sopimuksia. Tietoturvaratkaisujen tulee noudattaa myös taloudellisia realiteetteja, eivätkä ne saa vaikeuttaa merkittävästi tietojärjestelmien hyötykäyttöä ja asiakaspalvelua.

### 1.2 Tarkoitus

Tietoturvatavoimilla estetään tietojen luvaton käyttö ja haltuunotto. Suurin osa sosiaali- ja terveysyhtymässä käsiteltävästä tiedosta on luottamuksellista, arkaluonteista sekä salassa pidettävää ja voi paljastuttuaan rikkoa yksityisyyden suojaa. Tietoturvatavoiminnan tavoitteena on vastata siitä, että tieto on oikeaan aikaan, oikeassa paikassa ja oikean muotoisena niiden henkilöiden käytettävissä, joilla on siihen laillinen tai työtehtävänsä vaatima valtuutus.

Tiedon saatavuudella ja käytettävyydellä tarkoitetaan, että tieto on tallennettu sellaisessa muodossa, että se on luettavissa, ymmärrettävissä ja tulkittavissa oikein. Lisäksi tiedon on oltava kattavaa, ajantasaista, oikeellista ja helposti käytettävissä ilman tulkinta- ja väärinkäyttömahdollisuutta.

Tietoturvatavoimilla vähennetään ja ennaltaehkäistään tietoturvariskien syntyminen, varmistetaan tietojen saatavuus poikkeuksellisissa olosuhteissa, toiminnan jatkuvuus, asiakkaiden ja potilaiden oikeusturva ja yksityisyyden suoja lainsäädännön ja muiden määräysten edellyttämällä tavalla. Lisäksi varmistetaan tietojen oikeellisuus ja luotettavuus sekä se, että asianosaiset ovat tiedostaneet tietoturvan merkityksen.

### 1.3 Tavoite

PHSOTEY on tietoturvallinen organisaatio, joka mahdollistaa tiedon luotettavan ja turvallisen hallinnan sekä välityksen kaikille osapuolille. Tietoturvallista organisaatiota rakennetaan eri toimijoiden välisessä yhteistyössä tietoturvariskienhallintaprosessin ohjaamana. Tämän päämäärän saavuttamiseksi:

- Käyttäjien, ylläpitäjien ja johdon tietoturvatietoisuus on oltava hyvä. Kaikki ymmärtävät oman merkityksensä sekä tehtävänsä ja velvollisuutensa tietoturvallisuuden ylläpidossa.
- Tietoturvallisuutta toteutetaan kaikilla tasoilla siten, että se on mukana kaikessa toiminnassa.
- Tietojen luottamuksellisuuden, eheyden ja saatavuuden vaatimus toteutuu kaikessa tietojenkäsittelyssä, mikä mahdollistaa tietoturvallisen asiointin ja tietojen käytön.
- Varsinaisen toiminnan lisäksi sekä arkistotoimella että tietohallinnolla on yhteisenä tavoitteena tietojen saatavuuden ja käytettävyyden turvaaminen.

## 2. Tietoturvallisuuden perustason määrittely

Tietoturvallisuus on laaja toiminnallinen kokonaisuus, jonka keskeisimmät turvallisuustekijät liittyvät ihmisten toimintaan. Tietoturvallisuuden vaikutukset ulottuvat koko organisaatioon. Tietoturvallisuuden ylläpitäminen on jatkuva prosessi, jota toteutetaan hallinnollisten, fyysisten ja teknisten ratkaisujen avulla. Toimenpiteet kuvataan käyttöympäristöille ja yksiköille laadituissa tietoturvallisuuden kehittämissuunnitelmissa ja turvallisuussuunnitelmissa. Käyttäjien toimintaa ohjataan tietoturvaratkaisuihin sisältyvillä käytösäännöillä ja toimintaohjeilla sekä koulutuksella.

### 2.1 Tärkeimmät hallinnolliset tietoturvatoimet

#### 2.1.1 Tietoturvallisuus osana kaikkea toimintaa

Hyväksytyn tietoturvapoliittikan mukaiset tietoturvatoimet sisällytetään luonnollisena osana kaikkeen toimintaan. Tietoturvan kehittäminen ja ylläpito ovat osa sosiaali- ja terveysyhtymän yleistä turvallisuustoimintaa, riskien hallintaa ja sisäistä valvontaa.

Tietoturva on sosiaali- ja terveydenhuollon kriittinen tekijä, koska asiakkaan ja potilaan on luotettava ehdottomasti tietojensa tietosuojaan. Tämä luottamus on palvelun kulmakivi.

Sosiaali- ja terveysyhtymän tietoturvallisuustyön tulee luoda asiakkaille, potilaille ja henkilöstölle luottamus siitä, että salassapito- ja vaitiolovelvollisuus sekä yksityisyyden suoja toteutuvat säädösten mukaisesti. Lisäksi tietoja tulee käsitellä kaikissa vaiheissa huolella ja asianmukaisesti.

#### 2.1.2 Säädökset ohjaavat tietoturvallisuuden kehittämistä

Sosiaali- ja terveysyhtymän tietoturvallisuuden kehittäminen tapahtuu kansallisten ja kansainvälisten tietoturvallisuutta koskevien lakien ja asetusten pohjalta sekä erilaisia tietoturvallisuudesta annettuja ohjeita ja suosituksia noudattaen. Sosiaali- ja terveysyhtymän toimintaa ohjaavat mm. tietosuojasäädökset sekä joukko muita lakeja, säädöksiä, ohjeita ja standardeja. Tietoturvallisuutta koskevat määräykset ovat keskeisiä ja velvoittavia. Velvoitteissa korostetaan salassapidon, vaitiolovelvollisuuden ja yksityisyyden suojan toteutumista sekä tietoturvallisuuden, tietosuojan, hyvän tietojenkäsittelytavan ja laadun merkitystä.

Voimassa olevat velvoittavat säädökset on luetteloitu ja niiden vaikutukset tietoturvajärjestelyihin on selvitetty. Lainsäädäntöä ja ohjeistusta seurataan jatkuvasti. Muutosten vaikutus otetaan huomioon sosiaali- ja terveysyhtymän tietoturvallisuuden kehittämisessä.

### 2.1.3 Tietojen turvallinen käsittely tietojärjestelmissä ja tietoverkoissa

Sosiaali- ja terveystyöryhmän tiedot, tietojenkäsittelyjärjestelmät ja -palvelut pidetään asianmukaisesti suojattuina sekä normaali- että poikkeusoloissa hallinnollisten, teknisten sekä fyysisten toimenpiteiden avulla.

Sosiaali- ja terveystyöryhmän toiminnalle tärkeiden tietojärjestelmien ja tietoverkkojen keskeytymätön toiminta turvataan, estetään tietojen ja tietojärjestelmien joutuminen väärin käsiin, estetään valtuudeton käyttö, tahaton tai tahallinen tiedon tuhoutuminen tai vääristyminen. Mahdollisesti aiheutuvat vahingot minimoidaan ja suhteutetaan niistä aiheutuviin kustannuksiin. Yhtä lailla varaudutaan normaaliajan toiminnan tietojenkäsittelyn turvaamisen lisäksi toiminnan keskeytyksiin ja niistä toipumiseen.

Potilaiden sekä asiakkaiden informointi tietojen käytöstä ja laadinnasta hoidetaan lakien, asetusten ja viranomaisohjeiden mukaisesti. Informoinnista ja sen kieltämisestä tehdään merkintä asiakirjoihin. Informointia voidaan antaa sekä yleisenä että asiayhteyteen liittyvänä informaationa.

### 2.1.4 Tietoturvariskien hallinta

Tietoturvariskejä hallitaan erikseen määriteltävän ja kuvattavan tietoturvariskienhallintaprosessin avulla. Hyväksyttävän riskitason määrittelee työryhmän johtoryhmä riskianalyysin tulosten perusteella yhteisesti valmisteltujen vertailuperusteiden ja mittarien avulla.

Sosiaali- ja terveystyöryhmässä on käytössä tietojärjestelmien kriittisyysluokitus. Tietoaineiston luokitteluvastuu on aineiston laatijalla, ellei lainsäädännöstä muuta johdu. Jokaisella tietojärjestelmällä tai sen osalla on oltava yksikäsitteinen omistaja/haltija. Tietoturvallisuuden toteuttamista ohjaavat dokumentit ovat vahvistettuja ja asianomaisten kohderyhmien saatavilla.

### 2.1.5 Kriittiset tilanteet ja toiminnan jatkuvuuden turvaaminen

Toiminnan jatkuvuuden hallintaan sisältyy turvamekanismit riskien havaitsemiseen ja vähentämiseen. Toiminnan jatkuvuuden hallinta vähentää onnettomuuksien ja turvallisuushäiriöiden (esim. luonnonmullistukset, onnettomuudet, laiteviat ja ilkivalta) aiheuttamia keskeytyksiä.

Jatkuvuussuunnitelmat varmistavat sen, että normaalit toimintaprosessit saadaan palautettua takaisin vaaditussa ajassa. Suunnitelmia ylläpidetään ja harjoitellaan säännöllisesti, jotta niistä tulee muiden hallinnollisten prosessien rinnalla osa toimintaa. Säännöllisillä arvioinneilla ja suunnitelmien päivityksillä varmistetaan jatkuvuussuunnitelmien tehokkuus.

### 2.1.6 Tietoturvallisuusasioiden tiedottaminen

Sosiaali- ja terveystyöryhmän toiminnasta vastuussa oleville tahoille, kuntayhtymän johtajalle ja työryhmän tulosryhmien johtajille kuuluu vastuu tiedottamisesta, myös tietoturvallisuutta koskevista asioista. Tietosuoja-asioihin liittyvässä tiedottamisessa rekisterinpitäjä on ensisijaisesti yhteydessä tietosuojavastaavaan.

## 2.2 Tärkeimmät tekniluontoiset tietoturvatimet

### 2.2.1 Tietoturvapäivitykset ja käyttöturvallisuus

Kriittisten komponenttien, palvelinten, työasemien, käyttöjärjestelmien sekä ohjelmistojen tietoturvapäivityksiä varten on oma toimintasuunnitelmansa. Käyttöturvallisuudella luodaan ja ylläpidetään tietotekniikan turvallisen käytön vaatimat toimintaolosuhteet huolehtimalla tekniikan toimivuuden valvonnasta, käyttöoikeuksista, käytön ja lokien valvonnasta, ohjelmistotukeen, ylläpito-, kehittämis- ja huoltotoimintoihin liittyvistä turvallisuustoimenpiteistä, varmuus- ja suojakopiointista sekä häiriöraportoinnista.

### 2.2.2 Käyttäjähallinta

Tietojärjestelmien käyttäjähallinta rakentuu henkilötietojen hallinnasta, käyttöoikeuksien ja pääsynhallinnasta, tunnistamisesta, käyttöoikeuksien jakamisesta sekä käyttöoikeuksien seurannasta. Käyttäjähallintaan kuuluvat organisaatiossa yhteisesti sovitut toimintatavat, joiden perusteella tietojärjestelmien käyttöoikeuksia määritellään, luodaan, ylläpidetään ja hyödynnetään.

Käyttäjähallinta perustuu henkilön asemaan organisaatiossa, roolimäärityksiin, lupiin ja kieltoihin. Tietojärjestelmän käyttäjälle myönnetään tehtävän vaatimat oikeudet tietojärjestelmiin. Esimies vastaa henkilöstönsä käyttöoikeuksien hallinnoinnista, niiden myöntämisestä, muuttamisesta ja poistamisesta.

### 2.2.3 Lokitiedot ja poikkeamaraportointi

Julkisuuslainmukaisen valitusprosessin aikana lokitietoja ei saa tuhota säilytysajan päättyessä. Tietoturvapoikkeamista, haitallisista ja toimintaa vaarantavista tapahtumista raportoidaan kaikilla tasoilla viivytyksettä poikkeamien hallintaprosessin mukaisesti. Kaikki merkittävät haitalliset tapahtumat kirjataan tulevien kehittämistoimien perustaksi. Myös ns. ”läheltä piti” -tapaukset rekisteröidään.

Onnettomuuksien, turvallisuusrikkomusten ja palvelujen keskeytysten seuraukset analysoidaan. Haitallisista tietoturva- ja suojatapahtumista kerätään jatkuvasti ajan tasalla olevaa tietoa yhdyshenkilöverkoston ja teknisten valvontatietojen avulla. Tietojen pohjalta muodostettu tilannekuva havainnollistaa tietoturva-poikkeamatilanteen ja niiden aiheuttamat vaikutukset. Se toimii yhtenä perustana riskianalyseissä tulevien tietoturvatimien suunnittelussa ja priorisoinnissa.

### 2.2.4 Viestien ja dokumenttien välittäminen

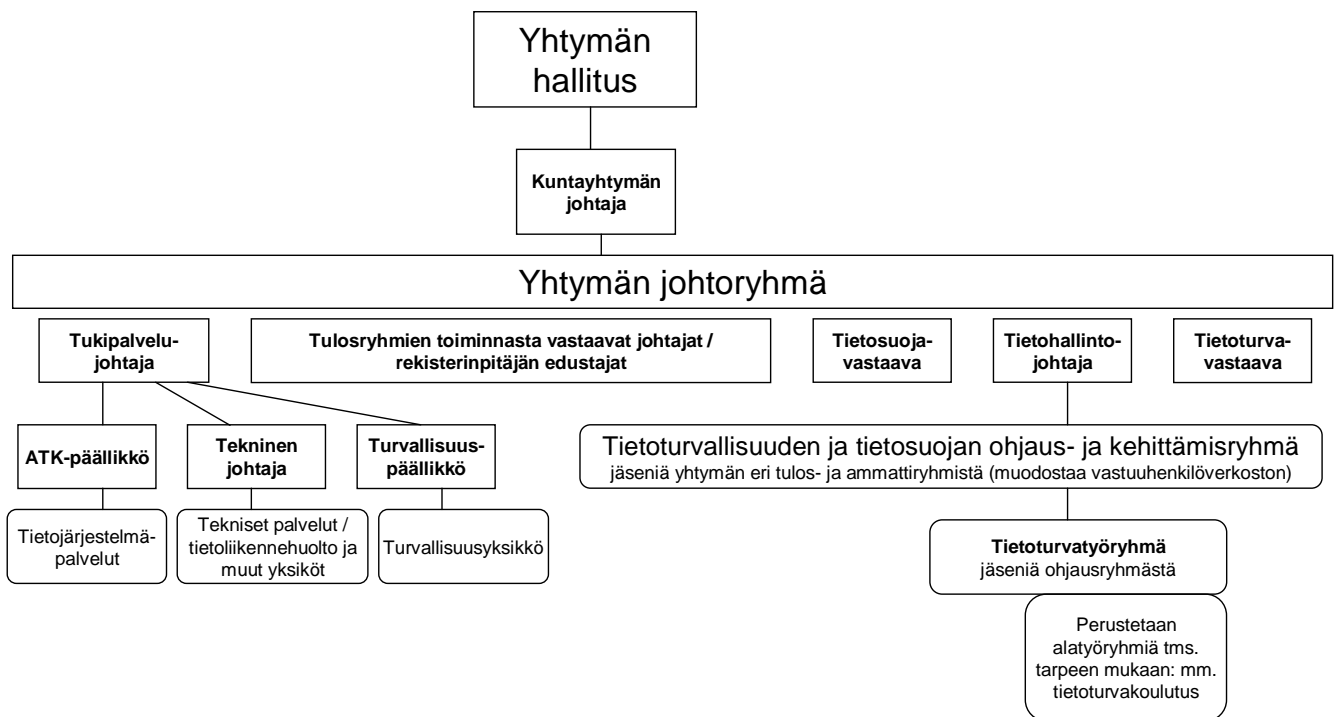
Viestit ja dokumentit välitetään tarvittavin salaustenmenettelyin. Viestinvälityksen tietosuojaa koskevat vaatimukset ja vastuut on määritelty sopimuksissa.

## **2.3 Fyysiset turvallisuustoimenpiteet**

Fyysisin turvallisuustoimenpitein luodaan ja ylläpidetään tietotekniikan vaatiman käyttöympäristön (tilat, laitteet, tiedonsiirto ja käyttö) toimintaolosuhteet, joilla varmistetaan tietoteknisten järjestelmien toiminta. Lisäksi suojataan ja valvotaan yhtymän kiinteistöjä, niiden erikoistiloja ja laite- yms. tiloja luvattomia tai rikollisia toimia vastaan sekä onnettomuuksilta että luonnontuhoilta.

### 3. Valtuudet ja vastuut

Tietojen turvaaminen ja tietosuojan toteuttaminen ovat osa johtamistoimintaa. Käytännön tietoturvatyöitä hallinnoi ja hoitaa nimetty Päijät-Hämeen sosiaali- ja terveysyhtymän tietoturvallisuusorganisaatio, ks. kuva alla. Toimintaan kuuluvat päivittäisten toimien ohella tietojen turvaamisen menettelyjen määrittely ja ylläpito, työhön osoitettujen riittävien resurssien turvaaminen sekä välineistön ja toimenpiteiden turvallisuudesta ja tietoturvaominaisuuksista huolehtiminen.



### 3.1 Tietoturvatyön organisointi ja tehtävät

Kuntayhtymän hallitus hyväksyy tietoturvapoliitikan. Kuntayhtymän johtaja vastaa tietoturvallisuuden yleisestä järjestämisestä. Tulosryhmän toiminnasta vastaavat sekä tulosalueiden ja -yksiköiden esimiehet vastaavat osaltaan tietoturvan toteuttamisesta omissa yksiköissään. Henkilörekisterilain mukaisesta rekisterihallinnosta on annettu ohje. Rekisterinpitäjien edustajat (tietojärjestelmien omistajat rekistereineen) vastaavat tietoturvan ja tietosuojan toteutumisesta jokaisen rekisterin osalta.

Tietohallintojohtaja vastaa yhtymän tietoturvallisuuden ja tietosuojan kehittämisen johtamisesta ja koordinoinnista.

Tietosuojavastaava auttaa rekisterinpitäjää saavuttamaan hyvän henkilötietojen käsittelytavan ja korkean tietosuojan tason, on kuntayhtymän tietosuojan erityisasiantuntija ja antaa asiantuntija-apua sekä henkilöstölle että johdolle.

Tietoturvavastaavan tehtävänä on ohjata ja valvoa yhtymän tietoturvapoliitikan toteutumista. Tietoturvavastaava toimii aktiivisessa yhteistyössä tietosuojavastaavan kanssa.

Turvallisuuspalveluita tuottaa yhtymän turvallisuusyksikkö turvallisuuspäällikön johdolla. Turvallisuusyksikkö vastaa fyysisten turvallisuustoimenpiteiden (luku 2.3) toteutumisesta.

Tietoturvallisuuden ja tietosuojan ohjaus- ja kehittämisryhmän päätehtävänä on ohjata ja koordinoita tietoturvallisuuteen ja tietosuojaan liittyvien asioiden seuranta ja kehittämistä. Keskeisenä näkökulmana on henkilöstön opastaminen ja ohjaaminen kohti tietoturvallisempia toimintatapoja. Ryhmässä on jäseniä eri tulosryhmistä ja ammattiryhmistä. Työryhmän alaisuuteen perustetaan tarpeen mukaan alatyöryhmiä.

Tietoturvatyöryhmä on tietoturvallisuusasioita valmisteleva taho tietoturvallisuuden ja tietosuojan ohjaus- ja kehittämisryhmän alaisuudessa.

Atk-päällikkö tietojärjestelmäpalveluiden esimiehenä vastaa tietojärjestelmien operatiivisesta toiminnasta tietoturvallisella tavalla.

Tekninen johtaja teknisten palveluiden esimiehenä vastaa tietoliikennehuollon ja muun tekniikan järjestämisestä tietoturvallisella tavalla.

### 3.2 Tarkemmat ohjeet

Tietoturvapoliitikassa esitetään yleiset periaatteet, joita sosiaali- ja terveisyhtymässä tulee noudattaa kaikessa tietojen käsittelyssä. Tarkempi kuvaus tietoturvasta ja sen toteuttamisesta on dokumentissa Tietoturvallisuuskäytännöt ja -periaatteet sekä tietoturvaohjeissa, jatkuvuussuunnitelmissa, tiedonohjaussuunnitelmassa ja arkistotoimen ohjeissa. Näistä mainituista dokumenteista julkisia ovat tiedonohjaussuunnitelma ja arkistotoimen ohjeet.

### 3.3 Soveltaminen

Sosiaali- ja terveisyhtymän hallituksen hyväksymä kirjallinen tietoturvapoliittikka (tämä asiakirja) saatetaan tiedoksi jokaiselle sosiaali- ja terveisyhtymän työntekijälle ja tietojärjestelmien käyttäjälle. Poliittikan toimeenpano perustuu tietoturvallisuuden kehittämissuunnitelmaan. Tietoturvallisuuden toteutuminen varmennetaan vuosittain toimintakertomukseen tulevilla maininnalla suoritetuista toimenpiteistä.

Tietoturvapoliittikkaa, tietoturvallisuuskäytäntöjä ja -periaatteita sekä ohjeita noudatetaan kaikessa toiminnassa ja ne koskevat kaikkia sosiaali- ja terveisyhtymän palveluksessa olevia henkilöitä ja luottamushenkilöstöä. Niitä noudatetaan myös kaikessa toiminnassa sosiaali- ja terveisyhtymän ulkopuolisten yhteistyökumppaneiden kanssa. Tietoturvallisuuteen liittyviä määräyksiä tarkistetaan ja arvioidaan vähintään vuosittain tai suurten muutosten yhteydessä.

Kuntayhtymän hallitus hyväksyy sosiaali- ja terveisyhtymän tietoturvapoliittikan. Tietoturvallisuuskäytännöt ja -periaatteet sekä tietoturvallisuuden kehittämissuunnitelma käsitellään tietoturvallisuuden ja tietosuojan ohjaus- ja kehittämisryhmässä sekä yhtymän johtoryhmässä. Tarvittaessa informoidaan yhtymän hallitusta. Tietoturvallisuuden kehittämistoimenpiteet ovat osa normaalia toiminnan ja talouden suunnittelua. Mikäli tietoturvallisuusdokumenttien muuttamisesta aiheutuu muutoksia politiikkaan, viedään tällöin asia kuntayhtymän hallituksen käsittelyyn. Tietoturvapoliittikka on voimassa toistaiseksi.