# TIETOTURVA- JA TIETOSUOJAPOLITIIKKA

Hyväksytty: Kunnanhallitus 10.5.2021 § 78
4.11.2019 § 160

Muutokset:

## Sisällys

# 1. JOHDANTO

Tietoaineistot ovat keskeisessä roolissa tietoyhteiskunnassa. Tietojen 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.

Tietoturva- ja tietosuojapolitiikka määrittää tietoturvaa ja tietosuojaa, joista käytetään tässä politiikassa myös nimitystä tietoturvallisuus, koskevat periaatteet ja linjaukset, se toimii perustana tietoturvaa ja tietosuojaa koskeville ohjeille. Tietoturva- ja tietosuojapolitiikka koskee jokaista työntekijää, viranhaltijaa, luottamushenkilöä ja sidosryhmän edustajaa, joka työnsä tai toimeksiantonsa puitteissa käsittelee tietoaineistoja. Tätä politiikkaa sovelletaan kaikkeen tietoon, riippumatta sen esitystavasta, muodosta, elinkaaren vaiheesta, tallennusympäristöstä tai siirtotiestä.

Ensisijainen vastuu tietoturvan ja tietosuojan toteutumisesta on organisaation ylimmällä johdolla, joka varmistaa tietoturva- ja tietosuojatyön riittävän resursoinnin ja seurannan. Tietoturvan ja tietotekniikan ammattilaisilla on keskeinen merkitys johdon neuvonantajina.

Tietoturva- ja tietosuojapolitiikka on julkinen asiakirja ja se on voimassa toistaiseksi, sitä täydennetään tai päivitetään tarpeen mukaan, kuten lainsäädännön tai muiden ohjeistusten muuttuessa.

# 2. TIETOTURVA- JA TIETOSUOJAPERIAATTEET

Tietoturva- ja tietosuojatyö ovat osa yleistä turvallisuustoimintaa, riskien hallintaa ja sisäistä valvontaa. Tietoturvan ja tietosuojan toteutumista seurataan vuosittain tietoturvaorganisaation raportoinnilla johdolle.

Tietoturva- ja tietosuojapolitiikka määrittää periaatteet, toimintatavat, vastuut, toimivallat, valvonnan ja seuraamusjärjestelmän, joita noudatetaan tietoturvan toteuttamiseksi ja kehittämiseksi.

Henkilöstön tietoturva- ja tietosuojaoppaasta löytyvät käytännön ohjeet tietosuojan ja tietoturvan toteuttamiseksi. Alakohtaisia lisäohjeita ja määräyksiä annetaan tarpeen mukaisesti. Nämä ohjeet annetaan tiedoksi jokaiselle työntekijälle ja tietojärjestelmän käyttäjälle.

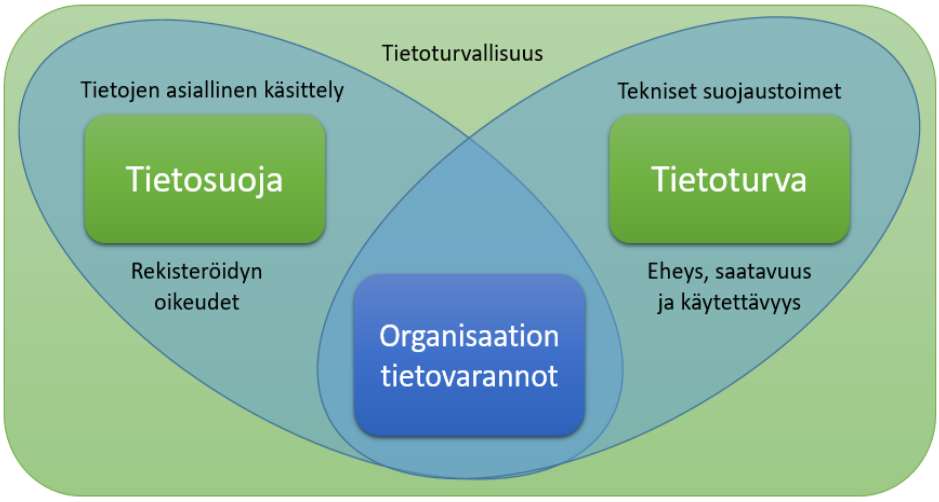
Tietoturvaperiaatteita noudatetaan kaikissa tiedon elinkaaren vaiheissa ja tämän edistämiseksi tietoturva- ja tietosuojaperiaatteet ovat osa henkilöstön perehdytystä ja koulutusta. Teknisin ratkaisuin varmistetaan toiminnan ja työtehtävän kannalta tarpeellisten tietojen käsittely ja rajoitetaan työn kannalta tarpeettomaan tietoon pääsyä.

# 3. TIETOTURVA

Tietoturvan toteuttaminen on tietojen, tietojärjestelmien, tiedonvälityksen ja niitä käyttävien palveluiden turvaamista ja suojaamista siten, että tietojen olemassaolo, oikeellisuus, käytettävyys, luottamuksellisuus ja palveluiden jatkuvuus eivät vaarannu. Tietoturvatoimenpiteet koskevat sekä sähköistä että manuaalista tietojenkäsittelyä. Tietoturvan toteuttamiseen liittyvät oleellisena henkilöstölle ja luottamushenkilöille suunnatut ohjeet, yleiset ohjeet ovat henkilöstön tietoturva- ja tietosuojaoppaassa, lisäksi alakohtaisia, tarkentavia, ohjeita annetaan tarpeen mukaan.

**Tietoturva koostuu:**

- *Tiedon luottamuksellisuudesta,* eli siitä, että tiedot ovat vain niihin oikeutettujen henkilöiden saatavilla eivätkä ne päädy ulkopuolisten tietoon.
- *Tiedon eheydestä,* joka tarkoittaa tietojen muuttumattomuutta tai muutoksen havaitsemista ja säilyvyyttä huolimatta laitteisto- tai järjestelmäviasta tai inhimillisen toiminnan virheistä.
- *Tiedon saatavuudesta,* eli tieto on oikeutettujen henkilöiden saatavilla tai käytettävissä silloin kun niitä tarvitaan.
- *Todentamisesta ja kiistämättömyydestä,* joilla tarkoitetaan käyttäjän todentamista ja käyttäjien tietojen käytön kiistämätöntä todistamista.

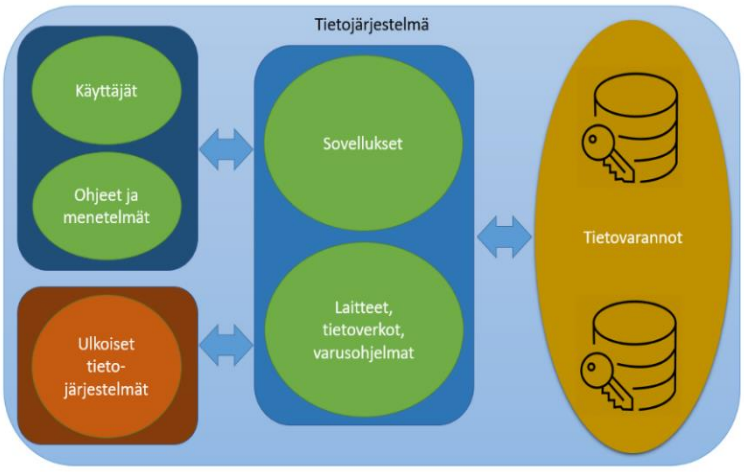



*Kuva 1: Tietoturva ja tietosuoja*

Tietojärjestelmien teknisen ympäristön ja laitteiden ylläpidon toteuttaa Suupohjan seutupalvelukeskus Oy, joka vastaa sopimusten mukaisesti tietoturvan toteutumisesta. Johdon vastuulla on huolehtia sopimusten ajantasaisuudesta ja vaatimustenmukaisuudesta. Lainsäädännön tai viranomaismääräysten muuttuessa on tarkistettava vastaako sopimus muuttuneeseen tilanteeseen.

## 3.1. Tietojärjestelmä

Tietojärjestelmä on kokonaisuus, joka koostuu tietovarannoista, niitä käsittelevistä sovelluksista ja laitteista sekä tietoverkoista, tietojen käyttöä määrittävistä ohjeista, käyttäjistä sekä liittymistä toisiin tietojärjestelmiin. Tietojärjestelmän oleellinen vaatimus on käsiteltävien tietojen turvallisuus ja tietoturvan yleinen hallinta ja valvonta. Poikkeama missä tahansa kokonaisuuden osassa merkitsee häiriötä järjestelmän toiminnassa.




*Kuva 2: Tietojärjestelmä*

Tietojärjestelmistä ylläpidetään tietojärjestelmäluetteloa yhteistyössä Suupohjan Seutupalvelukeskus Oy:n ICT-palveluiden kanssa.

## 3.2. Tietoturvan hallinnolliset periaatteet

Hallinnollinen tietoturva on tietoturvatoimintojen johtamista ja organisointia, ja sillä tarkoitetaan tietoturvatoimintojen, henkilöstön tehtävien ja vastuiden sekä ohjeistuksen, koulutuksen ja valvonnan muodostamaa kokonaisuutta. Hallinnollinen tietoturva pyrkii ennakoimaan riskejä sekä arvioimaan ja hallitsemaan riskien mahdollisia vaikutuksia. Tavoitteena on sekä tietoturvan tekninen toteutuminen että johdon ja henkilöstön sitoutuminen sen suunnitelmalliseen hoitamiseen ja kehittämiseen.

Palveluiden hankinnoissa edellytetään tiedon käsittelyyn liittyvien suojatoimien, vastuiden ja teknisten tietoturvavastuiden sisältyvän palvelusopimuksiin, lisäksi henkilötietojen käsittelystä sovitaan EU:n yleisen tietosuoja-asetuksen mukaisesti.

Tietoturvaan liittyvillä tehtävillä on omat vastuuhenkilöt. Vastuuhenkilöillä järjestetään resurssit ja toimivalta toteuttaa vastuulleen annetut tehtävät. Tarkemmin tästä on kerrottu luvussa Vastuut ja organisointi.

Tietoturvaperiaatteet viedään käytäntöön ohjeistuksin, koulutuksin ja tiedottein.

## 3.3. Henkilöstöturvallisuus

Henkilöstöturvallisuus on henkilöiden toimista johtuvia ja heihin kohdistuvien tietoturvauhkien hallintaa. Tavoitteena on luotettava ja tehtäväänsä soveltuva henkilöstö, joka tuntee oman roolinsa mukaisesti asetetut tietoturvavaatimukset. Henkilöstö, opiskelijat, harjoittelijat ja organisaatiolle ostopalveluita tuottavat henkilöt ja toimijat velvoitetaan noudattamaan tietoturvallisia toimintatapoja tehtävässään.

Henkilöstöturvallisuuden tietoturvaperiaatteiden toteutumiseksi haavoittuvat työyhdistelmät eliminoidaan, tämä tarkoittaa mm. sitä, että ei synny työtehtävää, jossa valvontaa suorittava henkilö valvoo myös omaa toimintaansa.

Työtehtävän mukainen käyttöoikeus järjestelmiin ja ohjelmistoihin annetaan käyttölupahakemus ja vaitiolo-/salassapitositoumus täyttämällä ja esimiehen allekirjoituksella varmentaen (Liite 1 - malli salassapitositoumuksesta). Esimies vastaa käyttölupahakemuksen tekemisestä ja työtehtävän määrittelystä tehtäväkuvauksessa.

Henkilökunnan koulutus, valmennus ja perehdyttäminen ovat tärkeä osa henkilökunnan tietoturvatietoisuuden ylläpidossa. Henkilöstö perehdytetään ja koulutetaan tehtäväänsä, perehdytyksessä käydään läpi tietoturva- ja tietosuojaohjeet. Osallistumista koulutuksiin ja tietoturvaosaamista seurataan esimiesten, tietosuojavastaavan ja johdon toimesta.

Tietoturvaohjeiden noudattamisen seuranta on säännöllistä ja osa sisäistä valvontaa. Tietoturvarikkomukset ja tietoturvapoikkeamat käsitellään tietoturvan vaarantumisepäilyn selvitysprosessin (Liite 2) mukaisesti. Tietoturvarikkomusten ja väärinkäytösten rangaistusta määritettäessä sovelletaan tietosuojarikkomusten seuraamustaulukkoa (Liite 3).

## 3.4. Fyysinen tietoturva

Fyysisen tietoturvan keinoin suojataan organisaation hallussa olevia tietoja ja tietovarantoja fyysisten uhkien, kuten rakenteiden ja niiden vikojen aiheuttamilta vahingoilta ja luvattomien tai rikollisten toimien seurauksilta. Fyysisen tietoturvan suunnittelussa kartoitetaan ja huomioidaan tärkeimmät suojattavat kohteet ja varmistetaan teknisten järjestelmien toiminta.

Fyysinen tietoturva sisältää mm. kulun- ja tilojen valvonnan, vartioinnin, palo-, vesi-, sähkö-, ilmastointi- ja murtovahinkojen torjunnan sekä kuriirikuljetusten ja tietoaineistoja sisältävien postilähetysten suojaamisen vahinkoja ja asiatonta toimintaa vastaan.

Kaupungin tekninen toimiala ja Suupohjan Seutupalvelukeskus Oy vastaavat osaltaan fyysisen tietoturvan ylläpidosta ja henkilöstöä ohjeistetaan henkilöstön tietosuoja- ja tietoturvaoppaassa fyysisen tietoturvan käytänteistä.

## 3.5. Tietoaineiston turvallisuus

Tietojen käsittely sekä luokittelu ja säilyttäminen perustuvat tiedonhallintaa ohjaavaan lainsäädäntöön ja ohjeisiin. Perusteena henkilötietojen käsittelylle on lakisääteisyys tai käyttäjän tehtävästä johtuva asiayhteys asiakkaaseen ja häntä koskeviin tietoihin.

Tietojen saatavuus, käytettävyys ja säilytys varmistetaan teknisin toimin ja estetään tietojen tahaton tai tahallinen tuhoutuminen tai vääristyminen. Teknisillä toimilla pyritään varmistamaan toiminnan jatkuvuus häiriöttä ja varaudutaan mahdollisista häiriöistä toipumiseen. Samalla varmistetaan mahdollisen sähköisen asioinnin saatavuus, luotettavuus ja kiistämättömyys, joka perustuu sähköisen asioinnin toimintaprosessin huolelliseen suunnitteluun. Tietoturvatoimia sovelletaan tietoaineiston koko elinkaaren ajan, tiedon syntymisestä sen hävittämiseen.

## 3.6. Laitteistoturvallisuus

Laitteistoturvallisuudella turvataan 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.

Teknisin toimin pyritään varmistamaan tietojen keskeytyksetön käyttö ja toiminnan jatkuvuus sekä varaudutaan mahdollisista häiriöistä toipumiseen. Kriittisille laitteistoille toteutetaan katkoton sähkönsyöttö ja ylläpidon korkea palvelutaso.

ICT-laitteiden hankinnasta, ohjelmistoasennuksista, suojauksesta ja ylläpidosta vastaa keskitetysti Suupohjan Seutupalvelukeskus Oy palvelusopimuksen mukaisesti.

## 3.7. Ohjelmistoturvallisuus

Pääsynhallinnalla ja sen suunnittelulla estetään tietoaineiston, ohjelmien ja järjestelmien luvaton käyttö. Ohjelmistojen tietoturva huomioidaan jo niiden hankintavaiheessa, jolloin varmistutaan ohjelmistojen tietoturvasta ja vaatimustenmukaisuudesta.

Ohjelman hankinnan lähtökohta on sen tekninen ja toiminnallinen yhteensopivuus käytössä olevien ohjelmistojen ja arkkitehtuurin kanssa. Lisäksi huomioidaan EU:n yleisen tietosuoja-asetuksen asettamat vaatimukset. Ohjelmiston valmistajan ja myyjän vastuu ohjelmistotuotteista määräytyy hankinta- ja käyttöoikeussopimuksissa.

Esimies vastaa siitä, että hänen alaisuudessaan olevat käyttäjät perehdytetään ohjelmistojen tietoturvalliseen käyttöön.

Ohjelmien hankinta, asentaminen, suojaus, päivitykset ja varmuuskopiointi on suurelta osin keskitetty Suupohjan Seutupalvelukeskus Oy:lle palvelusopimuksen mukaisesti.

## 3.8. Tietoliikenneturvallisuus

Tietoliikenneturvallisuus pyrkii turvaamaan 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 Suupohjan Seutupalvelukeskus Oy:lle palvelusopimuksen mukaisesti.

## 3.9. Käyttöturvallisuus

Käyttöturvallisuus tarkoittaa turvallisen käytön toimintaolosuhteita, tekniikan toimivuuden valvontaa, käytön ja lokien valvontaa, ohjelmistotukea, ylläpitoa ja huollon turvallisuustoimenpiteitä, varmuuskopiointia sekä häiriöraportointia.

Käyttöturvallisuuden perustana on osaava ja sitoutunut henkilöstö sekä ajantasaiset ohjeistukset, joita toiminnassa noudatetaan. Tietojen käyttöoikeuksia rajataan tietojen käsittelyn suunnittelulla ja käyttöoikeuksien hallinnalla.

Esimiehet ja ohjelmien pääkäyttäjät opastavat ja kouluttavat henkilöstöä ohjelmistojen käyttöön ja tietoturvallisuuteen liittyvissä asioissa. Laitteiden ja ohjelmien käyttäjien tulee perehtyä annettuihin ohjeisiin ja noudattaa niitä.

Käyttöturvallisuuden tekninen ylläpito on keskitetty Suupohjan Seutupalvelukeskus Oy:lle palvelusopimuksen mukaisesti.

## 3.10. Etätyö ja matkatyö

Etätyöllä, samoin kuin matkatyöllä, tarkoitetaan muualla kuin organisaation vakituisessa toimipisteessä tehtävää työtä. Etätyöksi luetaan myös työnantajan järjestämä vakituinen etätyöpiste ja matkoilla esim. hotelli tai toisen organisaation tilat sekä matkalla käytetyt kulkuvälineet. Tyypillinen esimerkki etätyöstä tai matkatyöstä on sähköpostin tarkistaminen kännykällä oman työpaikan ulkopuolella.

Etä- ja matkatyön käyttöympäristöt vaihtelevat, eikä ympäristön turvallisuuteen voida aina vaikuttaa. Etätyöntekijän toimenpiteillä ja menettelytavoilla on tällöin erityisen suuri merkitys ja etätyöntekijän on kyettävä tekemään itsenäinen arvio etätyöympäristön turvallisuudesta sekä toimittava sen mukaisesti.

Puhelinten ja muiden mobiililaitteiden käytön turvallisuudesta sekä tietojen salassapidon toteutumisesta tulee huolehtia, kunkin käyttöpaikan erityisolosuhteet huomioiden. Kaikessa organisaation toimitilojen ulkopuolella tehtävässä työssä on noudatettava annettuja ohjeita.

### 3.11. Seuranta, valvonta ja raportointi

Tietoturvan kehittäminen ja ylläpito vaativat jatkuvaa seurantaa. Tähän kuuluvat tietoturvan valvonta sekä poikkeamien raportointi ja tilastointi. Seurannan toteuttaminen kuuluu pääosin ICT-palveluille, tietosuojavastaavalle ja tietoturvatyöryhmälle, mutta jokaisella on velvollisuus raportoida havaitsemistaan poikkeamista. Esimiesten velvollisuus on dokumentoida havaitut tietoturvaan ja tietosuojaan liittyvät poikkeamat ja ilmoittaa näistä eteenpäin tietoturvan tai tietosuojan vastuuhenkilöille.

Sisäisen valvonnan ja riskienhallinnan ohjeen mukainen jatkuva seuranta ja valvonta kuuluu nimettyjen henkilöiden lisäksi kaikille esimiehille. Lisäksi valvontaa tehdään rekisteröidyn pyynnöstä tai työntekijän ilmoituksen perusteella.

## 4. TIETOSUOJA

Tietosuoja koskee henkilötietojen käsittelyä, se määrittää henkilöiden yksityisyyden suojaamista ja sillä turvataan luonnollisten henkilöiden oikeuksia, tietoja ja luottamusta. Tietosuojan vaatimukset tulevat EU:n yleisestä tietosuoja-asetuksesta, jonka tarkoitus on turvata rekisteröityjen oikeudet sekä henkilötietojen käsittelyn läpinäkyvyys ja oikeasuhtaisuus sekä varmistaa tietosuojan toteutuminen.

Tietosuojaa ja sen vaatimuksia määrittelee EU:n yleinen tietosuoja-asetus sekä kansallinen lainsäädäntö, joka velvoittaa rekisterinpitäjän suunnittelemaan henkilötietojen käsittelyn ja osoittamaan käsittelyn lainmukaisuuden sekä suojaamaan tiedot asiattomalta käsittelyltä. Suojaamistoimet kattavat kaiken tiedon käsittelyn, siirron ja säilytyksen, riippumatta niiden tallennusmuodosta. Henkilötietojen turvallinen käsittely korostuu alueellisten ja kansallisten yhteisjärjestelmien käytössä.

Tietosuojan toteutumista seurataan ja havaittuun asiattomaan käyttöön puututaan. Työntekijällä on velvollisuus ilmoittaa havaitsemistaan tietosuojan ongelmista. Tietojen luvattomasta käytöstä saattaa seurauksena olla oikeudellisia seurauksia tai erilaisia työnantajan menettelyjä, riippuen tilanteen vakavuudesta. Näitä toimenpiteitä kuvataan liitteissä kaksi ja kolme.

### 4.1. Henkilötietojen kerääminen ja käsittely

Henkilötietoja käsitellään siinä laajuudessa kuin se on tarpeen palvelun tai työtehtävän kannalta. Käsittelytoimet suunnitellaan ja määritellään tiedon elinkaari huomioiden. Henkilötietojen käyttö on sallittua vain lainsäädännön nojalla tai henkilön suostumuksen perusteella. Tietojen säilytys ja käyttö tapahtuu tietoturvaperiaatteita noudattaen.

Henkilötietojen tulee säilyä virheettöminä ja niiden tulee olla saatavilla tarpeen mukaisesti. Henkilötietoihin pääsy on rajattu työtehtävän mukaiseksi. Mikäli henkilötietoja luovutetaan, tulee siirron olla tietoturvallinen ja perustua lakiin tai suostumukseen. Tietoja voidaan luovuttaa lakien ja asetusten nojalla tai rekisteröidyn suostumuksella. Rekisteröidyllä on EU:n yleisen tietosuoja-asetuksen mukaiset oikeudet itseään koskeviin tietoihin.

## 5. TIETOTURVARISKEIHIN VARAUTUMINEN

Valtaosa palveluista perustuu tietoaineiston käsittelyyn ja sähköisten tietovarantojen käyttöön, joiden toimivuutta voivat uhata luonnonilmiöiden, inhimillisen toiminnan tai tekniikan pettämisen aiheuttamat tilanteet sekä järjestelmiin kohdistuvat tahalliset sähköiset tai fyysiset hyökkäykset.

Näiden seurauksena voivat olla mm. tiedon saatavuuden heikentyminen, tiedon muuttuminen tai tiedon päätyminen ulkopuolisen tietoon.

Sähköiset tietojärjestelmät ja näitä yhdistävät tietoverkot muodostavat järjestelmäkokonaisuuksia, joiden häiriöt ja niiden vaikutukset, voivat laajentua yksittäistä työasemaa koskevista koko järjestelmän laajuisiksi. Tietojärjestelmäkokonaisuuteen kuuluvat mm. työasemat, puhelimet, palvelimet ja muu verkon infrastruktuuri.

Tietoturvariskejä arvioidaan ja niihin varaudutaan 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.

Henkilöstön osaaminen ja tietoisuus ovat merkittäviä tekijöitä tietoturvan toteutumisessa. Kouluttaminen sekä tietoisuuden lisääminen tietoturvasta ovat keskeisiä toimenpiteitä uhkien pienentämisessä.

ICT-palvelut ja verkon ylläpito ostetaan laajalti Suupohjan seutupalvelukeskukselta, jonka valmiussuunnittelua ja varautumista ohjataan perustamissopimuksen mukaisesti. Lisäksi käytössä on sisäisesti hankittuja ohjelmistokokonaisuuksia, joiden ylläpidosta vastataan sisäisesti tai yhteistyössä ohjelmatoimittajan kanssa. Useat näistä ohjelmistoista toimivat saas-palveluina, jolloin ylläpito tapahtuu järjestelmän toimittajan toimesta ja käyttö soveltuvan käyttöliittymän kautta etäyhteydellä.

## 5.1. Riskien arviointi

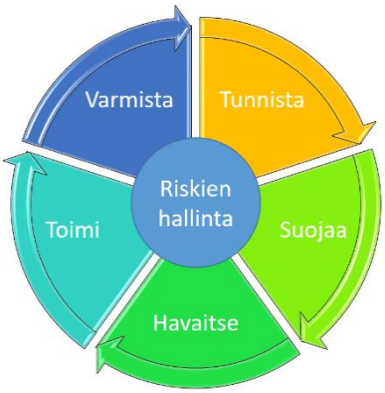
Tietoturvariskejä arvioitaessa on huomio kiinnitettävä erityisesti tietojen käsittelyn sisältämiin riskeihin. Riskejä syntyy aina kun tietoja käsitellään, erityisesti silloin, jos tietoja on tarpeen siirtää. Riskejä ovat myös tietojen vahingossa tapahtuva tai tarkoituksellinen tuhoaminen, muuttaminen, luvaton luovuttaminen tai tietojen oikeudeton käyttö.

Järjestelmien luokittelu tapahtuu niiden kriittisyyden mukaan. Järjestelmien turvajärjestelyt tarkastetaan säännöllisesti ja tarvittaessa niiden toimivuus testataan.

## 5.2. Riskienhallintasuunnitelma

Tietoturvariskejä arvioidaan ja hallitaan riskienhallinnan ohjeistuksen mukaisesti ja tietoturvan suurimmat riskit sisällytetään organisaation riskienhallintasuunnitelmaan.

Tiivistetysti riskienhallinta toteutetaan oheisen kuvion mukaisesti. Riskienhallinnassa tunnistetaan riskit, suojataan tiedot, havaitaan rikkomukset, toimitaan tilanteen vaatimalla tavalla ja varmistetaan toiminnan vaikutukset.




*Kuva 3: Riskienhallintaprosessi*

## 5.3. Häiriön tai uhkatilanteen tunnistaminen ja reagointi

Puutteiden ja haavoittuvuuksien seurauksena voi olla tietojärjestelmiin tai tietoaineistoon kohdistuva uhka tai poikkeama. Jokaisella työntekijällä ja luottamushenkilöllä on velvollisuus ilmoittaa havaitsemistaan tai tietoonsa tulleista tietosuojan tai tietoturvan puutteista, haavoittuvuuksista ja häiriötilanteista esimiehelle, ICT-tuelle tai tietosuojavastaavalle.

Häiriötilanteen tai uhkan toteutuessa alkuvaiheessa ei välttämättä ole tietoa siitä, onko häiriö tahallinen vai tahaton. Näiden käsittelyssä on merkittäviä eroja, joten tilannetta arvioidaan jatkuvasti tilannekuvan täydentyessä. Mikäli kyseessä on tahallinen häiriö, toimintatavat sovitetaan sellaisiksi, että mahdolliselle hyökkääjälle ei anneta harkitsemattomilla toimenpiteillä etua. Keskeistä on arvioida häiriön tyyppi ja sen aiheuttama uhka toiminnalle tai tietoturvallisuudelle.

Mikäli kyse on henkilötietoihin kohdistuneesta tapahtumasta, arvioidaan tapahtuneen vakavuus ja se, tuleeko tapahtuneesta tehdä ilmoitus tietosuojavaltuutetun toimistolle ja rekisteröidyille. Tilanteen arvioinnin ja päätöksen ilmoituksesta tekevät tietoturvatyöryhmä ja tietosuojavastaava.

Tiedonkulku ICT-palveluntuottajan ja rekisterinpitäjän välillä on oleellista. Tiedottaminen havaituista häiriöistä ja niiden selvittämisen etenemisestä sekä muista toimenpiteistä pidetään molempien osapuolten saatavilla.

### 5.4. Viestintä häiriötilanteessa

Häiriötilanne, jonka vaikutukset ovat laajat, vaatii usein viestintää organisaatiosta asiakkaille ja muille sidosryhmille. Viestinnässä noudatetaan pääsääntöisesti kriisiviestinnän ohjeistuksia ja vastuita. Viestintä toteutetaan siten, että tapahtuneen selvitys ei häiriinny, eikä viestinnällä anneta tietoa, josta voi olla hyötyä mahdolliselle ulkopuoliselle hyökkääjälle. Alkuvaiheen viestintä on näin ollen niukkaa ja rajoittuu tilanteen kannalta tarpeelliseen tietoon, yksityiskohtia tarkennetaan tilanteen ja selvitystyön edetessä.

### 5.5. Tietoturvarikkomusten seuraamukset

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

Tietoturvalainsäädäntöä ja organisaation tietoturva- ja tietosuojapolitiikkaa sekä näiden perusteella annettuja ohjeita vastaan rikkominen tulee aina ilmoittaa tietosuojavastaavalle tai esimiehelle. Valvontaprosessi etenee tietosuojavastaavan ja vastaavan viranhaltijan johdolla (liite 2). Seuraamuksista päättävät tietosuojavastaava ja rekisterinpidosta vastaava viranhaltija, seuraamustaulukon (liite 3) mukaisesti.

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.

## 6. VASTUUT JA ORGANISOINTI

Tietoturva on yhteinen asia ja se koskettaa koko henkilöstöä.

**Ylintä vastuuta** tietoturvasta ja tietosuojasta kantaa kunnanhallitus näitä johtaa kunnanjohtaja. Ylimmän johdon tehtävänä on valvoa kokonaisuutta sekä riskienhallinnan ja sisäisen valvonnan toteutusta, lisäksi tehtävä on myös vastata ja antaa tarkemmat ohjeet sopimusten hallinnasta sekä määrätä sopimusten vastuuhenkilöt. Tietoturva- ja tietosuojatyöhön huolehditaan riittävä resursointi ja tietosuojavastaavan työ mahdollistetaan organisaation toimenpitein. Kunnansihteeri vastaa teknisen ja hallinnollisen tietoturvan yleisestä järjestämisestä, kehittämisestä ja seurannasta.

**Tietosuojavastaava** auttaa johtoa velvoitteidensa toteuttamisessa rekisterinpitäjänä. Tietosuojavastaava osallistuu tietosuojaan liittyvään suunnittelutoimintaan, valmistelee ohjeita ja ylläpitää niitä sekä kouluttaa henkilöstöä tietosuojan toimintatavoista. Tietosuojavastaava tukee henkilökuntaa ja rekisteröityjä tietosuoja-asioissa ja seuraa sekä valvoo henkilötietojen käsittelyä ja suojausmenettelyä. Tietosuojavastaavalla on oikeus suorittaa tehtävänsä ja niihin liittyvä suunnittelu, seuranta ja raportointi itsenäisesti. Lisäksi tietosuojavastaavalla on oikeus organisoida henkilötietojen käsittelyn valvonta, ylläpitää käyttöloki- ja luovutuslokirekistereitä sekä ryhtyä jatkotoimenpiteisiin tietosuojan ongelmatilanteissa kaupunginhallituksen hyväksymän toimintatavan mukaisesti. Lainmukainen velvollisuus on ottaa tietosuojavastaava riittävän aikaisessa vaiheessa mukaan henkilötietojen käsittelyä koskevaan suunnittelutoimintaan sekä henkilötietoja sisältävien tietojärjestelmien hankintojen suunnitteluun.

**Tietoturvatyöryhmä** toimii yhteistyössä tietosuojavastaavan kanssa tietoturvan toteuttamisessa ja suunnittelussa. Työryhmään kuuluvat tietosuojavastaava, kunnanjohtaja ja toimialajohtajat. Tietoturvatyöryhmä käsittelee tietoturvan linjaukset ja ohjeet sekä huolehtii tietoturvan toteuttamisen vastuuttamisesta. Ryhmä seuraa ja toteuttaa tietoturvan eri vastuualueiden suunnitelmien, ohjeiden, selosteiden ja lomakkeiden laadintaa sekä ottaa tarvittaessa kantaa käytäntöihin ja kehittämishankkeisiin ja seuraa yleisesti tietoturvatilannetta.

Toimialajohtajat vastaavat palvelualueensa käytännön tietoturvasta, sen organisoinnista ja kehittämistoimista sekä tietoturvaa koskevasta sisäisestä ja ulkoisesta tiedottamisesta. Heidän tehtävänään on vastata palvelualueensa henkilötietojärjestelmien rekistereistä, rekisteröityjen ajantasaisesta informoinnista ja rekistereiden vastuuhenkilöiden nimeämisestä sekä vaikutustenarvioinnin tekemisestä omalla palvelualueellaan ja käsittelytoimista tehtävän selosteen ajantasaisuudesta sekä sopimusten ajantasaisuudesta. Toimialajohtajat antavat henkilötietojen ja tietoaineiston käsittelystä ja menettelytavoista ohjeita, jotka esimerkiksi tarkentavat kansallisia määräyksiä ja alueellisesti sovittuja toimintamalleja. Ohjeiden luontiin osallistuvat rekisterinpitäjä ja tietosuojavastaava sekä tarpeen mukaisesti määritellyt rekisterin yhteyshenkilöt.

**Asiakirjahallinnon johtava viranhaltija** laatii tiedonhallinnan ohjeet ja valvoo, että tehtävät hoidetaan annettujen ohjeiden mukaisesti sekä huolehtii asiakirjahallintoon liittyvästä koulutuksesta ja neuvonnasta. Asiakirjahallinnon johtavan viranhaltijan ja toimialojen arkistovastaavien vastuulla on asiakirjojen käytettävyyden, säilyttämisen ja lainmukaisen luovuttamisen sekä säilyttämisen toteuttaminen tiedonhallintaohjeistuksen mukaisesti.

**Esimiesten** vastuulla on tietoturvan ja tietosuojan toteutuminen vastuualueellaan. Keskeisimmät tehtävät tietoturvan ja tietosuojan kannalta ovat:

- Oman vastuualueensa henkilöstön perehdyttäminen työtehtäviin liittyviin tietoturva- ja tietosuojavastuisiin
- Henkilöstön tietoturva- ja tietosuojaoppaan sekä muiden tietoturva- ja tietosuojaohjeiden antaminen tiedoksi henkilöstölleen
- Oikeus velvoittaa henkilöstönsä lisäkoulutukseen tai -perehdytykseen
- Tietoturvan ja tietosuojan toteutumisen seuranta
- Palvelusuhteen päättyessä tai työtehtävän vaihtuessa ilmoitus ICT-palveluille käyttöoikeuksien päättämisestä tai muuttamisesta

**Pääkäyttäjät** vastaavat käyttöoikeuksiensa mukaisesti järjestelmän tai sovelluksen tietoturvan ja tietosuojan toteutumisesta sekä ohjeistavat ja kouluttavat muita käyttäjiä järjestelmän tai sovelluksen käytössä.

**Jokainen työntekijä ja luottamushenkilö** on velvollinen ilmoittamaan havaitsemistaan tietoturvapuutteista, uhista tai menettelyvirheistä esimiehelle, ICT-tuelle tai tietosuojavastaavalle. Lisäksi havaituista haavoittuvuuksista yms. puutteista laitteiden suojauksessa tulee ilmoittaa ICT-palveluille. Jokainen

työntekijä ja luottamushenkilö on omalta osaltaan vastuussa tietoturvan ja tietosuojan ohjeiden noudattamisesta sekä niiden toteuttamisesta toiminta-alueellaan.

**Suupohjan seutupalvelukeskus** ylläpitää alueella verkkopalveluita sekä leasing yms. laitteita. ICT-palvelujen tehtävä on osaltaan edistää tietoturvan ja tietosuojan toteutumista sekä toimia käyttäjien tukena erilaisissa tilanteissa.

## 7. KOLMANNET OSAPUOLET

Palveluja tuottavat kolmannet osapuolet ovat velvollisia noudattamaan ostajan antamia ohjeita sekä laissa määriteltyjä tietoturva- ja tietosuojavaatimuksia. Kolmannet osapuolet ovat velvollisia ilmoittamaan tietoturvapoikkeamista, joilla voi olla vaikutusta tietoturvan toteutumiselle. Ilmoitusvelvollisuus ja muut vastuut määritellään sopimuksin.

Kolmannet osapuolet velvoitetaan tarpeen mukaisesti nimeämään tietoturva- ja tietosuoja-asioihin yhteyshenkilö, joka vastaa ohjeiden sekä tietoturva- ja tietosuojatason noudattamisesta.

## 8. LISÄTIETOA

Tämä tietoturva- ja tietosuojapolitiikka pohjautuu kansalliseen lainsäädäntöön ja EU:n yleiseen tietosuoja-asetukseen. Lisätietoa löydät mm. seuraavista:

- Lainsäädäntö
  - www.finlex.fi
  - https://eur-lex.europa.eu/homepage.html?locale=fi
- Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän VAHTI-ohjeet
  - www.vahtiohje.fi
- Viestintäviraston kyberturvallisuuskeskuksen sivut
  - https://www.viestintävirasto.fi/kyberturvallisuus.html
- Tietosuojavaltuutetun toimisto
  - www.tietosuoja.fi

LIITE 1

**KÄYTTÖOIKEUSHAKEMUS JA SITOUMUS SALASSAPIDOSTA JA VAITIOLOVELVOLLISUUDESTA**

Me allekirjoittaneet osapuolet olemme sopineet salassapito- ja vaitiolovelvollisuudesta seuraavaa:
Asiakirjojen, tietojen ja tietojärjestelmien käsittely- ja käyttöoikeudet annetaan vain tämän sitoumuksen allekirjoittaneelle. Sitoumus tehdään työsuhteen alkaessa, sijaisten, opiskelijoiden ja harjoittelijoiden kanssa ensimmäisen palvelusuhteen alkaessa tai palvelusuhteen luonteen muuttuessa.

Jokainen työntekijä vastaa oman toimintansa tietoturvallisuudesta ja lainsäädännön, annettujen ohjeiden ja määräysten noudattamisesta tehtäviensä hoidossa.

Työnantajan tietoturva- ja tietosuojaohjeet sekä sitä täydentävä henkilöstön tietoturvaohjeet annetaan tiedoksi jokaiselle työntekijälle ja tietojärjestelmän käyttäjälle. Esimiehen velvollisuus on uuden työntekijän perehdytyksen yhteydessä läpikäydä henkilöstön tietoturva- ja tietosuojaohjeet.

**Vaitiolo- ja salassapitositoumus:**
Työntekijänä sitoudun olemaan käyttämättä, ilmaisematta tai luovuttamatta palvelusuhteen aikana asiakkaisiin, potilaisiin, henkilötietoihin sekä liike- ja ammattisalaisuuksiin liittyviä salassa pidettäviä tietoja, riippumatta siitä, miten tai mihin tieto on tallennettu tai millä tavalla tieto on saatu (kirjallisesti, suullisesti tai havainnoimalla) muutoin kuin työtehtävien vaatimassa laajuudessa ja yhteydessä. Tietojen luovutuksen tulee perustua aina asiakkaan tai potilaan kirjalliseen suostumukseen, asiayhteydestä ilmenevään suostumukseen tai lainsäädäntöön.

**Sitoudun noudattamaan seuraavia tietosuojaperiaatteita:**

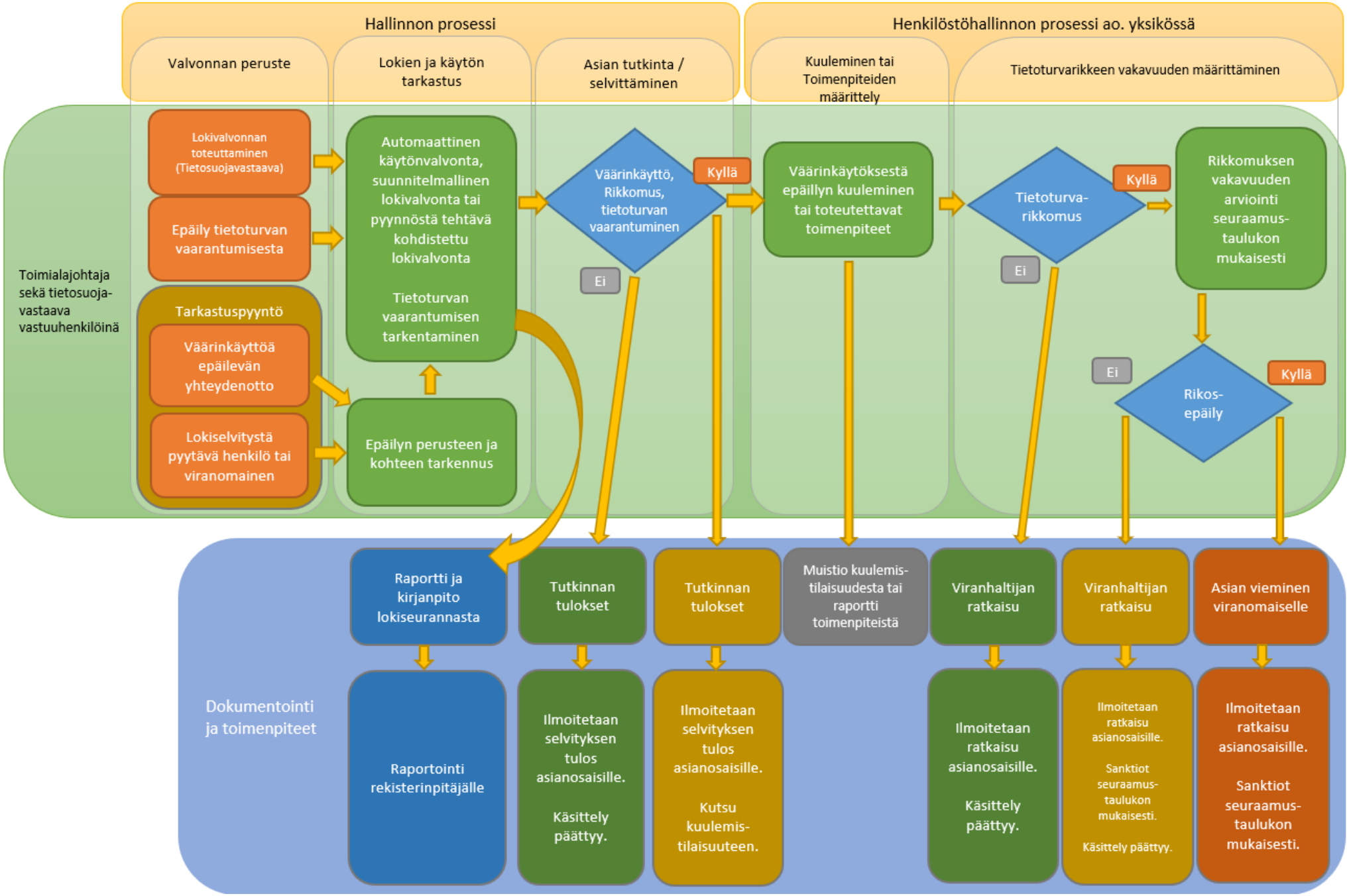
- Salassapito- ja vaitiolovelvollisuus koskee minua palvelusuhteeni aikana ja myös sen jälkeen
- Noudatan erityistä huolellisuutta käsitellessäni salassa pidettäviä tietoja
- Pidän salassa kaikki tietooni saamani arkaluonteiset tiedot esim. henkilön sairautta, tutkimusta, hoitoa, taloudellista asemaa tai sosiaalisia etuuksia koskevat tiedot sekä myös asiakkaaksi hakeutumisen ja asiakkuuden olemassaolon sekä turvallisuuteen, tietojärjestelmiin ja kiinteistön liittyvät tiedot.
- Käsittelen vain työtehtävieni edellyttämiä tietoja. En käsittele esim. työkavereiden, lähiomaisten, naapureiden tai julkisuuden henkilöiden tietoja, mikäli työtehtäväni eivät sitä sillä hetkellä edellytä.
- Vastaan käyttäjätunnuksillani ja/tai varmennekortin tunnuksillani tapahtuvasta tietojen käytöstä. Tunnuksia ei saa luovuttaa toisen henkilön käyttöön.
- Vastaan käytössäni olevasta kannettavasta tietokoneesta tai muusta laitteesta niin, ettei laite ja siinä olevat tiedot joudu vääriin käsiin.
- Olen tietoinen, että tietojärjestelmissä käyntini ja siellä tehdyt tapahtumat kirjautuvat lokitiedostoihin ja epäillystä väärinkäytöstä raportoidaan esimiehelleni ja tarvittaessa myös viranomaisille sekä henkilölle, jonka tiedoista on kyse.
- Olen tietoinen, että tietojen väärinkäyttö tai tahallinen ohjeiden vastainen toiminta on lainsäädännössä rangaistava teko. Rangaistavaa menettelyä henkilörekisteritoiminnassa koskevat säännökset sisältyvät EU:n yleiseen tietosuoja-asetukseen, tietosuojalakiin ja rikoslakiin. Tietojen oikeudettomasta käytöstä voi seurata rikos-, työ- ja vahingonkorvausoikeudellisia seuraamuksia.

Olen lukenut tämän sitoumuksen ja ymmärrän sen sisällön ja merkityksen.

Paikka ja aika:_____ _____ / _____ 20_____

| | |
|---|---|
| _____ | _____ |
| Työntekijän nimi | Työyksikkö |
| _____ | _____ |
| Työntekijän allekirjoitus | Esimiehen allekirjoitus |

LIITE 2. Tietoturvan tai tietosuojan vaarantumisepäilyn selvitysprosessi.



LIITE 3. Tietosuojarikkomusten seuraamustaulukko