

Luottamushenkilöiden tietosuoja- ja tietoturvaohje



Sisällys

1.	Johdanto	3
2.	Tietosuoja- ja tietoturvaohjeistus	3
2.1	Tietosuoja ja tietoturva koskevat kaikkia	3
2.2	Perehtyminen	4
3.	Salassapito- ja vaitiolovelvollisuus.....	4
3.1	Luottamushenkilöiden tiedonsaantioikeus	4
3.2	Luottamushenkilön virkavastuu	5
4.	Politiikat ja hallintomalli	5
5.	Riskienhallinta	6
6.	Salaisen ja luottamuksellisen tiedon käsittely	7
7.	Internet ja sähköposti	7
7.1	Sähköposti	7
7.1.1	Sähköpostiviestin lähettäminen	8
7.1.2	Sähköpostin liitetiedostot.....	8
7.2	Internetin käyttö.....	9
8.	Tietokoneet ja mobiililaitteet	9
8.1	Tietojen tallentaminen	9
8.2	Mobiililaitteet	9
8.3	Tietokoneen käyttö.....	9
8.4	Salasanat	10
8.5	Virustorjunta	10
9.	Poikkeamat ja niihin reagoiminen	11
9.1	Tietoturvapoikkeamat	11
9.2	Henkilötietojen tietoturvaloukkauksesta ilmoittaminen	11

1. Johdanto

Pirkanmaan hyvinvointialueen (jatkossa myös hyvinvointialue) luottamushenkilönä olet tekemisissä monenlaisen tiedon kanssa, joten on tärkeää varmistua, että tietoja käsitellään oikein ja turvallisesti. Siksi on tunnistettava, mitä tarkoitetaan esimerkiksi tietosuojalla, henkilötiedolla tai julkisella tiedolla. Tarkoituksena on taata tiedon luottamuksellisuus ja henkilöiden oikeuksien toteutuminen.

Luottamustoimen vastuullinen hoitaminen tarkoittaa, että kaikessa toiminnassa noudatetaan lakeja, määräyksiä, hyvinvointialueen hallintosääntöä ja muita organisaation ohjeita. Hyvinvointialueen tiedonhallintaa ohjaavat useat eri lait, uusimpana Laki julkisen hallinnon tiedonhallinnasta (906/2019). Henkilötiedon käsittelyä sääntelee ensisijaisesti EU:n yleinen tietosuoja-asetus (679/2016) ja kansallinen Tietosuoja laki (1050/2018) sekä useat toimialakohtaiset erityislait. Asiakirjajulkisuutta sääntelee puolestaan Julkisuuslaki (621/1999) ja luottamushenkilöiden tiedonsaantioikeutta Laki hyvinvointialueesta (611/2021).

Tämä yleinen ohjeistus on tarkoitettu luottamushenkilöille, ja sen tarkoituksena on ohjeistaa luottamushenkilöitä huomioimaan salassapidon ja henkilötiedon käsittelyn vaatimukset sekä tietoturvasuus luottamustehtävissään. Yleistä tietosuoja- ja tietoturvaohjeistusta täydentävät yksityiskohtaiset määräykset ja ohjeet.

2. Tietosuoja- ja tietoturvaohjeistus

2.1 Tietosuoja ja tietoturva koskevat kaikkia

Tietojen tehokas ja turvallinen tiedonhallinta tukee Pirkanmaan hyvinvointialueen palvelujen tuottamista. Tietosuoja ja tietoturva ovat lainsäädännön mukaisesti osa hyvinvointialueen päivittäistä toimintaa. Tietosuoja ja tietoturva koskevat sinua ja kaikkea toimintaasi.

Tavoitteena on tehokas ja tietoturallinen toiminta

Hyvinvointialueen toiminta hoidetaan tietoturallisesti. Tietoturvan tavoitteena on mm. tiedon suojaaminen erilaisilta uhkilta, toiminnan jatkuvuuden varmistaminen, toiminnallisten riskien minimointi sekä tehokkaan toiminnan mahdollistaminen kaikissa tilanteissa.

Tietoturvasta tulee huolehtia kaikissa tilanteissa ja kaikilla välineillä

Tietoturva- ja tietosuoja-asiat on otettava huomioon riippumatta siitä, millä välineillä toimitaan tai miten viestitään. Paperiset asiakirjat, sähköiset tietovarannot, tietoverkot, tietotekniset laitteet, tietojärjestelmät ja niihin liittyvät palvelut on suojattava sekä normaali- että poikkeusoloissa.

Toimimalla ohjeiden mukaan varmistat oman oikeusturvasi luottamustehtävissä ja tiedät, mitä sinulta odotetaan.

Tietoturvahäiriöt ovat salassa pidettävää tietoa, jota ei tule jakaa julkisesti. Kaikilla hyvinvointialueen tietojen ja tietojärjestelmien käyttäjillä on velvollisuus ilmoittaa tietoturvahäiriöistä.

2.2 Perehtyminen

Perehdy yleisiin tietosuoja- ja tietoturvaohjeisiin ja huolehdi osaamisesi ajantasaisuudesta. Tietosuoja- ja tietoturvaohjeita päivitetään säännöllisesti ja uusista ohjeista ilmoitetaan luottamushenkilöiden tiedotuskanavalta. Koska tietosuojaan ja tietoturvallisuuteen liittyvät uhat muuttuvat jatkuvasti, on tärkeää, että työskentelyssä noudatetaan ajantasaisia ohjeita.

Tietoturvaosaamisesi

Voit tutustua mm. seuraaviin kursseihin:

- [Digiturvallisuus hyvinvointialueiden luottamushenkilöille - eOppiva](#)
- [Riskienhallinta digimaailmassa - eOppiva](#)
- [Tietosuoja luottamushenkilöille - Eduhouse](#)
- [Julkisuus ja salassapito luottamustehtävissä - Eduhouse](#)

Kysy neuvoa, mikäli et ymmärrä jotain ohjetta

Kysy neuvoa, jos et ymmärrä ohjetta tai et tiedä, miten sinun tulisi toimia jossain tilanteessa.

Tietosuoja ja tietoturvallisuus ovat hyvin laajoja kokonaisuuksia, minkä vuoksi kaikkien tietosuojaan ja tietoturvallisuuteen liittyvien asioiden ohjeistaminen kattavasti ja yksiselitteisesti ei aina ole yksinkertaista. Tämän vuoksi on tärkeää, että kysyt neuvoa aina, jos et tiedä, miten tulisi toimia.

Anna tarvittaessa palautetta puuttuvista tai epäselvistä tietosuoja- ja tietoturvaohjeista tietoturvavastaavalle (tietoturvavastaava@pirha.fi) ja/tai tietosuojavastaavalle (tietosuojavastaava@pirha.fi).

Kysymykset ja palaute auttavat parantamaan toiminnan tietosuoja- ja tietoturvallisuutta sekä tietosuojaan ja tietoturvallisuuteen liittyviä ohjeita.

3. Salassapito- ja vaitiolovelvollisuus

Voit luottamustehtävää hoitaessasi saada pääsyn erilaisiin henkilötietoihin ja salassa pidettäviin tietoihin. Käsittele niiden osalta **ainoastaan luottamustehtävissäsi tarvitsemiasi tietoja**.

3.1 Luottamushenkilöiden tiedonsaantioikeus

Laissa hyvinvointialueesta (611/2021 § 88) säädetään, että sinulla on luottamushenkilönä oikeus saada hyvinvointialueen viranomaisilta tietoja ja nähtäväksesi asiakirjoja, joita toimestasi pidät tarpeellisina. Oikeus koskee myös asiakirjoja, jotka eivät vielä ole julkisia, elleivät salassapitosäännökset estä tietojensaantia.

Valtuutetun ja hallituksen jäsenen toimet koskevat hyvinvointialueen kaikkea toimintaa, ja heidän tietojensaantioikeutensa on laajempi kuin muiden luottamushenkilöiden. Muiden rajatusta tehtäväalueesta vastaavien toimielinten jäsenten tietojensaantioikeus rajoittuu toimielimen käsiteltävänä oleviin asioihin.

Toimielimen jäsenenä sinulla on oikeus niihin salassa pidettäviin tietoihin, joita tarvitaan päätöksenteon perusteena toimielimen käsiteltävänä olevassa asiassa. Ole erityisen huolellinen salassa pidettävien aineistojen ja tietojen käsittelyssä. Niitä ei saa kertoa tai luovuttaa muille.

3.2 Luottamushenkilön virkavastuu

Luottamushenkilönä sinulla on poliittinen ja eettinen vastuu toiminnastasi. Toimit myös virkavastuun alla. Virkavastuuseen kuuluu rikosoikeudellinen vastuu ja vahingonkorvausvastuu. Vahingonkorvausvastuu tarkoittaa, että julkista valtaa käytettäessä virheen tai laiminlyönnin seurauksena syntynyt vahinko on korvattava. Hoidat luottamustoimeasi vastuullisesti, kun noudatat kaikessa toiminnassa lakeja, määräyksiä, hallintosääntöä ja muita hyvinvointialueen ohjeita.

4. Poliitiikat ja hallintomalli

Tietosuojaan ja tietoturvallisuuteen liittyvä toiminta on organisoitua, systemaattista ja jatkuvasti kehittyvää. Ennalta sovitut toimintaperiaatteet, prosessit ja organisaatorakenteet luovat pohjaa tietosuojan ja tietoturvan huomioivalle toiminnalle.

Pirkanmaan hyvinvointialueen hallitus vastaa, että hyvinvointialue täyttää tietosuojalainsäädännön mukaiset velvoitteet, ja valvoo velvoitteiden toteutumista. Hallitus määrittelee henkilötietojen käsittelyn periaatteet ja vastuuhenkilöt. Hallitus vastaa hyvinvointialueen konsernin kokonaisturvallisuuden hallinnasta, johon kuuluvat uhkiin varautuminen, normaaliolojen häiriötilanteiden ja poikkeusolojen hallinta sekä niistä toipuminen.

Tietosuoja- ja tietoturvapoliittikka on aluehallituksen hyväksymä asiakirja, jossa otetaan kantaa tietosuojan ja tietoturvan ylläpitämiseen ja kehittämiseen. Poliittikka määrittelee ne periaatteet, tavoitteet, vastuut ja seurannan sekä valvonnan, joita noudatamme hyvinvointialueella potilaidemme, asiakkaidemme, työntekijöidemme ja yhteistyökumppaneidemme yksityisyyden suojan, luottamuksellisuuden, oikeusturvan ja tiedonhallinnan tehokkuuden sekä tietoturvallisuuden varmistamiseksi. Tietosuoja- ja tietoturvapoliittikkaa täydentävät hyvinvointialueen tietoturvasuunnitelma sekä yksityiskohtaiset periaatteet, päätökset ja ohjeet.

Tekoälypolitiikalla tuetaan hyvinvointialueen strategian toimeenpanoa, eikä se saa olla ristiriidassa hyvinvointialueen tietosuoja- ja tietoturvapoliitiikan kanssa. Hyvinvointialueen ydintehtävät sekä asiakas- ja potilasturvallisuus edellyttävät tietosuojan ja tietoturvan toteutumista kaikissa olosuhteissa, myös tekoälyn kaltaista uutta teknologiaa käyttöön otettaessa.

Tekoälypolitiikassa otetaan kantaa tekoälyn hyödyntämiseen hyvinvointialueen palvelujen tuottamisessa. Tekoälypolitiikka määrittelee ne periaatteet, tavoitteet, vastuut sekä seurannan ja valvonnan, joita noudatamme hyvinvointialueella asiakkaidemme, henkilöstömme ja yhteistyökumppaneidemme oikeuksien ja luottamuksen varmistamiseksi. Tekoälypolitiikkaa täydentävät yksityiskohtaisemmat tekoälyn hyödyntämistä koskevat periaatteet, ohjeet ja päätökset.

Kulloinkin voimassa olevat politiikat ja periaatteet löydät luottamushenkilöiden tiedotuskanavalta.

5. Riskienhallinta

Riskienhallinta on lakisääteinen osa julkisen organisaation johtamista ja toimintaa: Pirkanmaan hyvinvointialueen kaltaisella julkisella organisaatiolla riskienhallinnan perusteet lähtevät jo hyvän hallinnon periaatteista sekä muista lainsäädännön asettamista yksityiskohtaisemmista velvoitteista.

Yksittäisten riskienhallinnan osa-alueiden osalta asetetaan useita tarkentavia velvoitteita myös muussa lainsäädännössä. Tietosuojaan ja tietoturvallisuuteen liittyen keksiset lait ovat Laki julkisen hallinnon tiedonhallinnasta (906/2019) sekä EU:n yleinen tietosuoja-asetus (679/2016).

Sisäiset ohjaavat asiakirjat

Lainsäädännön asettamaa perustasoa tarkennetaan hyvinvointialueen sisäisissä toimintaa ohjaavissa suunnitelmissa ja asiakirjoissa. Näitä tarkentavia dokumentteja ovat muun muassa hyvinvointialueen hallintosääntö ja sisäisen valvonnan ja riskienhallinnan perusteet -asiakirja. Näissä asiakirjoissa määritellään tarkemmin esimerkiksi riskienhallinnan vastuut ja velvollisuudet sekä yleiset riskienhallinnan toteuttamisen periaatteet koko hyvinvointialueen toiminnalle.

Hyvinvointialueella laaditaan säännöllisesti riskienhallintasuunnitelma, jossa kuvataan lyhyemmän tähtäimen tavoitteet sekä yleiset menettelyt riskienhallinnan toteuttamiselle ja kehittämiselle.

Riskienhallinnan vastuut

Riskienhallinnan vastuut alkavat aina aluevaltuustosta ja koskettavat jollain tapaa kaikkia organisaatiomme tasoja ja jäseniä. Riskienhallinnan järjestämisen, ohjeistamisen ja käytännön toteuttamisen sekä seurannan vastuut on määritetty yleisesti johdon, johtavien viranhaltijoiden ja esihenkilöiden tehtäväksi.

On kuitenkin keskeistä, että jokainen henkilöstön jäsen muistaa omat vaikutusmahdollisuutensa riskienhallinnassa. Henkilöstön aktiivisuus, osallistuminen, havainnointi ja erilaisista havainnoista ilmoittaminen tukevat koko organisaation riskienhallintaprosessia.

Riskienhallinnan kokonaisuus hyvinvointialueella

Tietoturva-arviointi on osa hyvinvointialueen käytössä olevien ja käyttöön hankittavien järjestelmien sekä sovellusten tietoturvan varmistamista. Tietoturva-arviointi sisältää myös tietojärjestelmän käyttöön liittyvän riskiarvion.

Tietosuoja koskeva vaikutustenarviointi (DPIA) kohdistuu henkilötietojen käsittelyyn liittyviin riskeihin. Vaikutustenarviointi tehdään muun muassa silloin, kun uutta teknologiaa otetaan käyttöön, käsitellään arkaluonteisia tai muutoin hyvin henkilökohtaisia tietoja tai henkilötietoja käsitellään laajamittaisesti.

6. Salaisen ja luottamuksellisen tiedon käsittely

Luottamushenkilönä voit saada salaista tai luottamuksellista tietoa ja asiakirjoja, jota ei saa jakaa eteenpäin.

Käsitellessäsi tietoja esimerkiksi julkisessa tai jaetussa työtilassa varmista, etteivät muut näe luottamuksellisia tai salassa pidettäviä tietoja tai asiakirjoja. Tietokoneen näytön voit suojata erillisellä tummentavalla suojakalvolla. Varmista, että kaikki laitteet ovat valvonnassasi koko ajan.

Vältä avoimia julkisia yhteyksiä. Kun työskentelet julkisessa tilassa, käytä esimerkiksi matkapuhelimesi jaettua datayhteyttä.

Huolehdi paperilla olevien asiakirjojen salassapidosta. Varmista tietoja tulostaessasi, että tulostettavat tiedot menevät oikealle tulostimelle ja noudat tulosteet tulostimelta välittömästi tulostamisen jälkeen. Käsittele kaikkia paperilla olevia luottamuksellisia tietoja siten, etteivät sivulliset näe niiden sisältöä. Säilytä paperilla olevia tietoja turvallisessa ja lukituspaikassa, johon sivulliset eivät pääse. Huolehdi, etteivät tiedot ole sivullisten saatavilla myöskään silloin, jos hetkellisesti poistut niiden äärestä. Hävitä paperit turvallisella tavalla, esimerkiksi toimittamalla ne tietosuojajäteastiaan.

Tunnista vastapuoli ennen kuin alat keskustella luottamuksellisista tai salassa pidettävistä tiedoista. Varmista salassa pidettävistä tiedoista keskusteltaessa toisen osapuolen henkilöllisyys ja oikeus keskustella tiedoista. Vältä salassa pidettävistä tiedoista keskustelua julkisella paikalla. Jos keskustelu julkisella paikalla on kuitenkin jossain tilanteessa välttämätöntä, huolehdi, etteivät sivulliset kuule keskustelua eivätkä pysty yhdistämään keskustelussa käsiteltyjä tietoja.

Hyvinvointialueen valtuuston kokoukset ovat julkisia, joten niistä voit keskustella ja jakaa tietoa sosiaalisessa mediassa. Muiden toimielinten kokoukset eivät ole julkisia eikä niissä käytyjä keskusteluja saa kertoa ulkopuolisille – voit kertoa omista mielipiteistäsi ja puheenvuoroistasi niin, ettet paljasta muiden mielipiteitä.

Jos keskustelet vielä valmistelussa olevasta asiasta, kannattaa varmistaa, mitkä asiaan liittyvät tiedot ovat julkisia ja mitkä vielä salassa pidettäviä.

Huomioi sosiaaliseen mediaan julkaistessasi, että luottamushenkilönä edustat myös Pirkanmaan hyvinvointialuetta.

7. Internet ja sähköposti

7.1 Sähköposti

Käytä hyvinvointialueen pirha.fi-sähköpostia työtehtävien ja luottamustoimen hoitoon. Henkilökohtaisten asioiden ja vapaa-ajan harrastusten hoitamista varten tulee hankkia jokin toinen sähköpostiosoite. Älä käytä pirha.fi-sähköpostiosoitetta sosiaalisen median rekisteröinnin tai käytön yhteydessä.

Hyvinvointialueen sähköpostiosoitteen käyttäminen internetissä olevien palveluiden yhteydessä voi johtaa ei-toivottuun sähköpostiliikenteeseen. Älä vastaa roskaposteihin tai tietojenkalasteluyrityksiin, sillä niihin vastaaminen voi lisätä haitallista sähköpostiliikennettä entisestään.

7.1.1 Sähköpostiviestin lähettäminen

Sinun on aina varmistettava vastaanottajan sähköpostiosoitteen oikeellisuus erittäin huolellisesti. Sähköpostin otsikkokenttään ei saa koskaan laittaa henkilötunnusta eikä mitään salassa pidettävää tietoa. Huolehdi myös, ettei aiemman viestinvaihdon luottamuksellinen sisältö päädy sivullisille.

Salassa pidettäviä tietoja ei tule lähettää salaamattomalla sähköpostilla. Poikkeuksena on sisäinen sähköposti (osoitteisiin, jotka päättyvät @pirha.fi), jolla saa lähettää tietoja seuraavia lisäohjeita noudattaen:

- Lähettäjän on poistettava lähetetyt tiedot sähköpostiohjelmasta välittömästi lähettämisen jälkeen.
- Vastaanottajan on poistettava vastaanotetut tiedot niin nopeasti kuin mahdollista ja tarvittaessa siirrettävä tiedot luvalliseen säilytyspaikkaan.

Välttämättömiä salassa pidettäviä tietoja voi lähettää hyvinvointialueen ulkopuolelle vain salatussa sähköpostissa. Ensimmäinen viesti uudelle vastaanottajalle kannattaa lähettää salaamattomana salatun sähköpostin käyttöohjeiden kera ja pyytää varmistus, että vastaanottaja on oikea henkilö.

Salattu viesti luodaan samalla tavalla kuin normaali sähköpostiviesti, mutta vastaanottajan osoitteen perään lisätään **.sec** (esimerkiksi etunimi.sukunimi@sähköposti.fi.sec). Vastaanottaja saa sähköpostiinsa ilmoituksen "Olet saanut luottamuksellisen viestin", ja voi lukea ja vastata viestiin selaimeen avautuvasta linkistä.

Viestien jatkolähettäminen ulkoisiin sähköpostiosoitteisiin ei lähtökohtaisesti ole sallittua.

7.1.2 Sähköpostin liitetiedostot

Älä avaa epäilyttävää sähköpostin liitetiedostoa. Suhtaudu varauksella viesteihin, jotka tulevat sinulle yllättäen tuntemattomalta taholta tai joiden aihe on epäilyttävä.

Sähköpostin välityksellä leviää suuri osa erilaisista tietokoneviruksista, haittaohjelmista sekä erilaisista kiristysohjelmista. Huomaa myös, että tietokonevirus voi lähettää sinulle sähköpostia myös sinulle tutun henkilön nimissä. Ota epäselvissä tapauksissa ennen viestin avaamista yhteys lähettäjään ja varmista, että sähköposti liitetiedostoineen on juuri hänen lähettämänsä. Hyvinvointialueen käyttötuki ohjeistaa ja auttaa epäselvien tilanteiden tulkitsemisessa (puhelin 03 3117 4122).

7.2 Internetin käyttö

Internetin käytössä tulee olla huolellinen siihen liittyvien tietoturvariskien vuoksi. Useimmat käyttäjään kohdistuvat hyökkäykset, kuten haittaohjelmien levitys ja tietojenkalastelut, tehdään juuri internetin kautta.

Huomioi internetin käytössä mm. seuraavat asiat:

- Suhtaudu kriittisesti internetissä olevan tiedon luotettavuuteen ja oikeellisuuteen.
- Huomioi tekijänoikeudet ja asianmukaiset lähdeviittaukset, jos kopioit tietoa internetistä.
- Jos kirjaudut palveluun, jossa kysytään salasanaa, selain ehdottaa usein salasanan tallentamista. Tätä ei pidä tehdä varsinkaan yhteiskäyttöisellä laitteella, sillä se mahdollistaa tunnuksesi luvattoman käytön.

Poistu aina palvelusta sen omalla uloskirjautumistoiminnolla.

8. Tietokoneet ja mobiililaitteet

8.1 Tietojen tallentaminen

Salassa pidettävä tieto on tallennettava sähköisesti siten, että vain sen käyttöön oikeutetuilla henkilöillä on siihen pääsy. Älä lataa hyvinvointialueen salassa pidettäviä tietoja esimerkiksi toimielimen kokoustyötilasta omille laitteillesi, ellei se ole välttämätöntä tehtäväsi hoitamisessa.

Vältä myös luottamuksellisten tietojen säilyttämistä sähköpostissa. Jos virus tai haittaohjelma pääsee palvelimelle, saattaa se lähettää tietoja sähköposteistasi eteenpäin.

8.2 Mobiililaitteet

Mobiililaitteisiin (älypuhelimet ja tabletit) voidaan tallentaa merkittävät määrät tietoa. Mobiililaitteita käytettäessä on suurempi riski, että laite katoaa tai varastetaan. Noudata huolellisuutta ja huomioi, että suojaat mobiililaitteen suojakoodilla ja käytät automaattista lukitusta. Salaa mobiililaitte, kun se on mahdollista. Älä tallenna laitteeseen luottamuksellista tai salassa pidettävää tietoa.

Asenna mobiililaitteeseen uusimmat käyttöjärjestelmä- ja ohjelmistopäivitykset. Asenna sovelluksia vain luotetuista sovelluskaupoista, kuten Google Play Kauppa ja App Store.

8.3 Tietokoneen käyttö

Käytä tietokonetta verkossa säännöllisesti ja lataa ehdotetut käyttöjärjestelmän, internetselaimen ja muiden ohjelmistojen päivitykset.

Asenna ohjelmat ja sovellukset vain luotetuista sovelluskaupoista, kuten Google Play Kauppa, App Store tai Microsoft Store.

Kirjaudu ulos hyvinvointialueen tietojärjestelmistä ja sovelluksista, jos luovutat tietokoneen muiden käyttöön. Varmista, että muilla ei ole pääsyä luottamustehtävässä laitteella käsiteltäviin materiaaleihin, muista esimerkiksi tyhjentää ladatut tiedostot -kansio.

Lukitse tietokone, vaikka poistuisit vain tilapäisesti ja lyhyeksi aikaa sen äärestä. Laitetta ei saa koskaan jättää valvomattomana auki.

8.4 Salasanat

Salasana on aina henkilökohtainen salassa pidettävä tieto, jonka tarkoitus on varmistaa, että laitetta tai tietojärjestelmää ei käytetä luvatta.

Käytä salasanoja, joita muut eivät voi arvata missään tilanteissa. Voit käyttää apuna salasanan muodostamisessa muistisääntöjä, salasanalauseita tai muita apuvälineitä, joiden avulla sinun on itse helppo muistaa salasana, mutta muut eivät pysty sitä keksimään. Salasanalause voi muodostua esimerkiksi suosikkilaulun alusta tai kertosäkeestä, jolloin sanojen alkukirjaimet muodostavat salasanan.

Käytä eri salasanoja luottamustehtävissä, työelämässä ja yksityiselämässä. Saman salasanan tai tunnusluvun käyttäminen eri järjestelmissä ja yhteyksissä kasvattaa tietomurron riskiä myös hyvinvointialueella. Esimerkiksi monien yksityiselämässä käytettävien palveluiden salasanoja on paljastunut erilaisissa tietomurroissa ulkopuolisille tahoille.

Käsittele salasanoja ja tunnuslukuja huolellisesti. Älä kerro salasanoja tai tunnuslukuja kenellekään. Omia käyttäjätunnuksia ei saa luovuttaa toisen käyttöön, vaikka tällä olisikin oikeus katsoa tietoja. Älä pyydä käyttöä tai käytä kenenkään toisen tunnuksia. Tunnukset ovat henkilökohtaisia, ja tietojen katsomisesta ja muutoksista jää aina merkintä järjestelmän lokitietoihin. Tietojen käytön jäljitettävyyden vuoksi omien tunnusten käytöllä on perustavaa laatua oleva merkitys. Toisen henkilön käyttäjätunnuksen avulla tunkeutuminen tietojärjestelmään on tietomurto, joka on määritelty rikoslaissa rangaistavaksi teoksi. (Rikoslaki, 38 luku, 8 §)

Huomaa myös, että käyttö- tai lähituki ei koskaan kysy salasanaasi. Jos saat tällaisen tietojen kalasteluyrityksen tai arvelet salasanasasi paljastuneen, soita välittömästi käyttötukeen (puhelin 03 3117 4122).

8.5 Virustorjunta

Varmista, että laitteillasi on ajantasainen virustorjuntaohjelmisto. Älä koskaan sulje virustorjuntaohjelmistoa.

Tietokonevirus saattaa aiheuttaa huomattavaa vahinkoa, jos se pääsee leviämään hyvinvointialueen verkossa. Suuri osa viruksista ja haittaohjelmista leviää sähköpostin liitetiedostona, varomattoman internetselailun ja klikkausten välityksellä tai erilaisten tallennusvälineiden (kuten muistitikut, CD/DVD-levyt) välityksellä.

9. Poikkeamat ja niihin reagoiminen

9.1 Tietoturvapoikkeamat

Tietoturvahäiriöitä ovat kaikki tapahtumat, jotka saattavat vaarantaa tietoturvallisuuden. Tietoturvaheikkouksia ovat kaikki tietojärjestelmiin, toimintaprosesseihin tai toimintaan liittyvät puutteet, jotka saattavat heikentää tietoturvallisuutta.

Nopea reagointi tietoturvahäiriöihin ja -heikkouksiin on avainasemassa vahinkojen minimoinnissa ja tietoturvallisuuden parantamisessa. Nopeilla vastatoimilla voidaan rajata ja pienentää vahinkoja merkittävästi. Tämän vuoksi nopea ilmoittaminen on ensiarvoisen tärkeää.

Ilmoita havaitsemastasi tietoturvapoikkeamasta hyvinvointialueen käyttötukeen (puhelin 03 3117 4122). Ilmoittaessasi kerro, mitä tapahtui, missä tapahtui, milloin tapahtui ja omat yhteystietosi, jotta lisätietoja voidaan tarvittaessa kysyä. Häiriön selvittämisen kannalta on hyvä tietää mahdollisimman täsmällisesti, missä ohjelmassa tai tilanteessa häiriö ilmeni ja mitä tehtiin ennen häiriötä ja sen havaitsemista. Täsmällisten taustatietojen avulla hyvinvointialue pystyy parantamaan omaa toimintaansa jatkossa.

9.2 Henkilötietojen tietoturvaloukkauksesta ilmoittaminen

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

Tietoturvaloukkaus voi tapahtua vahingossa tai tahallisesti. Tietoturvaloukkauksia ovat esimerkiksi asiakas- tai potilastietojen postittaminen väärälle henkilölle, asiakas- tai potilastietojen katselu ilman asiallista syytä, tietojen kirjaaminen väärälle henkilölle, toisen henkilön käyttäjätunnuksen käyttäminen, kadonnut muistitikku, varastettu tietokone tai murtautuminen henkilötietoja sisältävään järjestelmään.

EU:n yleisen tietosuoja-asetuksen (679/2016) mukaan rekisterinpitäjän on dokumentoitava kaikki tietoturvaloukkaukset ja tehtävä niistä ilmoitus viranomaiselle sekä henkilölle, jonka tietoja on loukattu. Ilmoitus on tehtävä 72 tunnin kuluessa loukkauksen ilmitulosta, joten tietoturvaloukkauksiin on reagoitava nopeasti. **Ilmoita havaitsemastasi tai epäilemästäsi henkilötietojen tietoturvaloukkauksesta välittömästi hyvinvointialueen tietosuojavastaavalle (tietosuojavastaava@pirha.fi).**