Yhteistyötoimikunta 23.5.2019 § 6
Henkilöstöjaosto 24.5.2019 § 16
Hyväksytty Johtokunta 19.8.2019 § 86

Henkilöstön tietoturva- ja tietosuojaopas

Suupohjan peruspalvelu-liikelaitoskuntayhtymä

Hallintoaukio • PL 100, 61801 KAUHAJOKI • (06) 2413 2000 • www.llky.fi

Sisällys

1. JOHDANTO

Tietoturva ja tietosuoja ovat jatkuvasti muutoksessa, palveluja digitalisoidaan ja henkilörekisterien koot kasvavat. Tietoturva, jonka tärkeä osa tietosuoja on, perustuu lainsäädäntöön ja normiohjaukseen. Nykyisessä digitaalisessa maailmassa tietoturvaosaaminen kuuluu jokaiselle ja sitä voidaan pitää kaikille kuuluvana kansalaistaitona, jolla on merkitystä erityisesti työelämässä, mutta myös yksityiselämässä.

Palvelujen tuottaminen perustuu tietoon ja sen käsittelyyn, jolloin henkilöstön osaaminen on erityisen tärkeää korkean tietoturvan saavuttamisessa. Puutteellinen tietoturva vaarantaa asiakkaiden ja suupohjan peruspalveluliikelaitoskuntayhtymän (myöhemmin LLKY) etuja sekä aiheuttaa lisätyötä- ja kustannuksia, lisäksi mahdollisesti menetetty luottamus ja maine on vaikea palauttaa.

Tämä tietoturva- ja tietosuojaopas antaa käytännön neuvoja ja ohjeita tietoturvan toteuttamiseen henkilöstölle ja LLKY:n toimeksiannosta työskenteleville sekä tietoja ja tietojärjestelmiä tai toimitiloja käyttäville henkilöille, kuten ulkopuolisille palveluntuottajille, opiskelijoille ja työharjoittelijoille. Opas on johtokunnan hyväksymä ja se koskee koko henkilöstöä ja sidosryhmiä.

Oppaan tarkoitus on nostaa henkilöstön tietoisuutta tietoturvasta ja näin auttaa huolehtimaan sen toteutumisesta. Oppaaseen on koottu keskeisiä perusasioita ja se antaa neuvoja tietoturvan toteuttamiseen. Oppaan lisäksi palvelualueittain voi olla hyväksyttyjä poikkeuksia, lisäyksiä tai täsmennyksiä, joita toiminnassa tulee noudattaa.

Oppaan lopussa on koottuna liitteitä, jotka kannattaa myös lukea. Liite 1 sisältää salassapitositoumuksen, joka on allekirjoitettava ennen tunnusten avaamista tietojärjestelmiin. Viimeisessä liitteessä on koottuna tietoturvan keskeiset tekijät huoneentaulun muotoon.

Tietoturva- ja tietosuojapolitiikka sekä käyttölokien seuranta- ja valvontasuunnitelma ja tämä ohje ovat saatavilla organisaation verkkosivuilta www.llky.fi -kohdasta *asiakkaan oikeudet*.

2. YLEISTÄ TIETOTURVASTA

Lainsäädännössä lähtökohtana on tietoturvan ja tietosuojan asianmukainen hoitaminen viranomaistoiminnassa, jolloin sen on oltava osa päivittäistä toimintaa. Tietoturvasta huolehtiminen on myös osa LLKY:n toiminnan laatua.

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

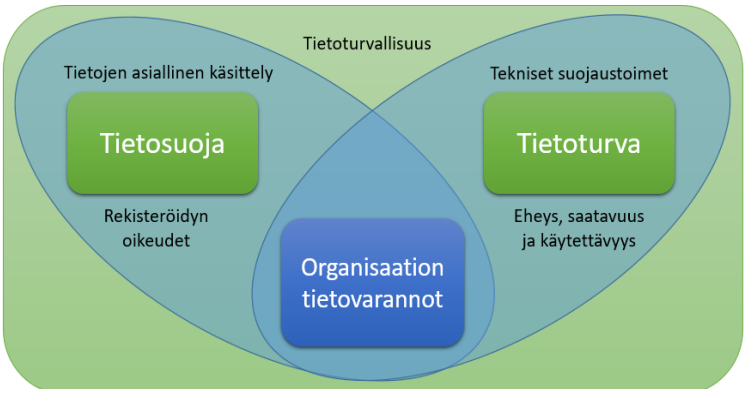
Tietoturvatyön päämääränä on:

- Organisaation toiminnalle tärkeiden tietojärjestelmien ja tietoverkkojen keskeytymätön toiminta
- tietojen ja tietojärjestelmien asiattoman käytön estäminen
- tiedon tahattoman tai tahallisen tuhoutumisten tai vääristymisen estäminen
- mahdollisten aiheutuvien vahinkojen minimointi

Sähköisen asioinnin yleistyessä on entisestään korostunut vaatimus osapuolten luotettavaan tunnistamiseen sekä asiointitapahtumien olemassaolon ja sisällön todistettavuudelle myös jälkeenpäin.

Tietoturva koostuu:

- **Tiedon luottamuksellisuudesta**, eli siitä, että tiedot ovat vain niihin oikeutettujen henkilöiden ja organisaatioiden saatavilla eivätkä ne päädy ulkopuolisten tietoon
- **tiedon eheydestä,** joka tarkoittaa tietojen muuttumattomuutta tai säilyvyyttä laitteisto- tai järjestelmävian tai inhimillisen toiminnan vuoksi
- **tiedon saatavuudesta,** jolloin tieto on oikeutettujen henkilöiden saatavilla tai käytettävissä silloin kun sitä tarvitaan.



Kuva 1: Tietoturvallisuus kokonaisuutena

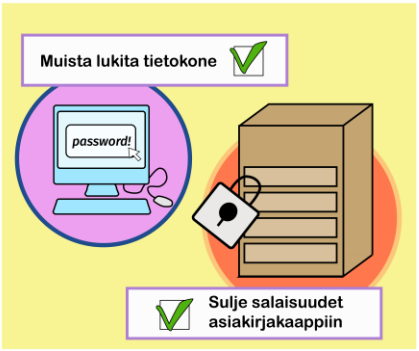
Tietojen käsittelyyn oikeutetut saavat käyttää tehtävänsä mukaisesti tietoja siinä määrin kuin se on tehtävän hoitamisen kannalta tarpeen.

LLKY:llä on lainmukainen velvollisuus seurata henkilötietojen käyttöä ja puuttua havaittuihin väärinkäytöksiin.

3. TIETOTURVAN TOTEUTTAMINEN

Tietoturvan toteutumiseksi tulee tietoturvaperiaatteiden noudattamisen olla jokapäiväistä niin työpaikalla kuin sen ulkopuolella. Tämän tavoitteen saavuttaminen edellyttää jokaiselta työntekijältä ja luottamushenkilöltä vastuullista toimintaa.

Suurimmat tietoturvan ongelmat liittyvät yleisesti kiireeseen, huolimattomuuteen, osaamattomuuteen ja tietojärjestelmien toteutuksen ja käytön tekijöihin. Tietoturva on niin hyvä kuin sen heikoin lenkki, pelkkä tekniikka ei riitä, vaan tietoturvan toteutuminen edellyttää oikeanlaisia toimintatapoja ja asennetta.



3.1. Miksi tietoturva on tärkeää

Tietoturvatoimien päämääränä on turvata yksilön, yhteisön ja yhteiskunnan etuja sekä varmistaa toiminnalle tärkeiden järjestelmien, tietoverkkojen sekä palveluiden keskeytymätön toiminta sekä varmistaa tiedon olevan saatavilla ja hyödynnettävissä siihen oikeutetuille riittävän esteettömästi, vaivattomasti ja nopeasti. Luottamuksellisiin tietoihin pääsy ja tietojen tahaton tai tahallinen tuhoaminen tai vääristyminen pyritään tietoturvatoimenpitein estämään.

Puutteet tietoturvassa voivat johtaa tietoturvaongelmiin sekä salassa pidettävän tiedon leviämiseen ulkopuolisten käyttöön ja näin aiheuttaa luottamuksen menetyksen sekä aiheuttaa merkittävää lisätyötä ja kustannuksia. Tietoturvaa kehittämällä parannetaan toiminnan luotettavuutta ja jatkuvuutta.

3.2. Tietojen käsittely

Tiedolla tarkoitetaan eri muodoissa tallennettavaa, käsiteltävää tai siirrettävää tietoa. Tieto voi olla esim. tietojärjestelmässä, yksittäisessä asiakirjassa, sähköposti- tai tekstiviestissä, tietokannassa, tietokoneen tai puhelimen muistissa, puheena tai yksittäisen ihmisen muistissa. Tietoturvanäkökulmasta merkittäviä käsittelyvaiheita ovat tiedon luominen, käyttäminen, muuttaminen, tallettaminen, siirtäminen, jakelu, kopiointi, arkistointi ja hävittäminen.

3.3. Työhön liittyvät tiedot

- Muista vaitiolovelvollisuus, joka koskee myös tietoja, jotka työtehtävissäsi olet saanut tietoosi esim. keskusteluista tai toisten viesteistä.
- Voit käyttää käyttöösi saamiasi salassa pidettäviä ja erityisluonteisia tietoja työtehtäviesi hoitamisessa asiakassuhteeseen perustuen ja siinä määrin kuin se tehtävän hoidossa on tarpeen.
- Käsittele tietoja huolellisesti riippumatta tiedon tallennusvälineestä.
- Pidä käsittelemäsi tiedot poissa sivullisten näkyviltä.
- Vältä tilannetta, jossa käsittelemäsi asiakirja tai muu aineisto on tallennettuna ainoastaan sellaisella laitteella, jonka varmuuskopiointi ei ole säännöllistä.
- Vältä turhaa tulostamista ja kopiointia, väliversiot ja epäkelvot kappaleet lisäävät tiedon vääriin käsiin joutumisen vaaraa.

- Varmista mihin tulostimeen tulostat ja hae tulosteet välittömästi. Käytä turvatulostusta jos se on mahdollista.
- Skannatessasi asiakirjoja varmista tiedoston vastaanottaja.
- Huolehdi salassa pidettävää tietoa siirtäessäsi tietojen salaamisesta. Varmistu, että vastaanottaja on oikeutettu saamaan aineiston.
- Käytä salassa pidettäviä tietoja hävittäessäsi oikean suojausluokituksen mukaisia silppureita tai hävittämispalvelun keräyssäiliöitä.
- Omien tietojen katselu ja käyttö järjestelmistä on pääsääntöisesti kiellettyä. Tutustu toimialakohtaisiin ohjeisiin, mikäli niitä on annettu.

3.4. Haastattelut, kyselyt, tutkimukset ja tietojen luovutus

- Ohjaa haastattelu- ja kyselypyynnöt tarvittaessa asian vastuuhenkilölle tai esimiehellesi. Toimi tiedotuspolitiikan mukaisesti.
- Varo antamasta viattomankin oloisten keskustelujen ja lomakkeiden yhteydessä tietoa salassa pidettävistä tai yksityisyyden suojan piiriin kuuluvista tiedoista.
- Ohjaa tietojen luovutus- ja tutkimuspyynnöt rekisterin vastuuhenkilölle, jonka tehtävä on varmistua tietojen luovutuksen perusteista ja mahdollisesta korvattavuudesta sekä päättää luovutuksesta.

3.5. Omat tiedostot ja yksityisyys

- Henkilökohtaisia tiedostoja ei tule tarpeettomasti tallentaa työpaikan puhelimeen, tietokoneelle tai verkkoasemalle.
- Kunnioita asiakkaiden ja työntekijöiden yksityisyyttä, älä paljasta salassa pidettävää tietoa muille.

- Terveydentila tai sairauslomatodistuksia saavat käsitellä vain ne, joiden tehtäviin se kuuluu.
- Tietojärjestelmien käytöstä kerätään yksityiskohtaista lokitietoa, jota voidaan käyttää ylläpidossa, vianmäärityksessä ja tietoturvan valvonnassa.
- Tukahduta juorut.

3.6. Tietoturvan toteuttaminen työpisteessäsi

Tietoturvan toteuttaminen työpisteessä on tärkeää, koska se luo perustan tietoturvan toteutumiselle. Noudata annettuja ohjeita ja käytäntöjä. Vie havaitsemasi puutteet tietoturvassa tai tietosuojassa tiettäväksi eteenpäin joko esimiehelle tai suoraan tietohallinnolle.

- Seuraa tietoturvaan liittyviä tiedotteita, tutustu ohjeisiin ja osallistu mahdollisuuksien mukaan koulutuksiin sekä toimi saamiesi ohjeiden mukaan.

3.6.1. Tietokoneen ja tietoverkon käyttö

- Tietokoneen käyttö sisältää sekä käytössä olevan tietokoneen käytön että verkon kautta käytettävien palveluiden käytön.
- Käyttäjänä vastaat käyttämästäsi laitteesta, ole siis huolellinen.
- Käyttäjätunnukset ja salasanat ovat henkilökohtaisia, älä luovuta niitä toisen henkilön käyttöön, ei edes perheenjäsenen tai työkaverin käyttöön.
    - Vastaat käyttäjätunnuksellasi tehdyistä toiminnoista.
- Toimikorttia ei tule jättää kortinlukijaan poistuessasi tietokoneeltasi.
- Mikäli epäilet salasanasi tai PIN-koodin paljastuneen, vaihda se.
- Mikäli käytössä on erikseen sovitusti käytettävä yhteistunnus järjestelmään, tulee salasana vaihtaa esim. käyttäjän käyttöoikeuden päättyessä tai jos epäillään sen päätyneen ryhmään kuulumattoman tietoon.
- Lukitse tietokoneesi siltä poistuessasi. Lukitseminen on nopeinta painamalla Windows-lippupainiketta ja L-kirjainta.
- Tallenna työsi käyttäen välitallennuksia ja muista tallentaa se poistuessasi tietokoneelta.
- Huomioi, että tietokoneen paikallinen levy (c:) ei ole varmistettu. Verkkolevyt (H: ja L) varmistetaan säännöllisesti.
- Mikäli käyttämäsi muistitikku, ulkoinen kiintolevy tai muu tallennusväline rikkoutuu, se tulee hävittää tietoturvallisesti. Kysy neuvoa seutupalvelukeskukselta.
    - Nämä eivät ole tietoturvallisia tapoja tallentaa tiedostoja ja salassa pidettävän tiedon tallennusta näille laitteille ei tule tehdä ilman asianmukaista suojausta.
    - Yleistä verkkolevyä (L:) ei tule käyttää erityisluonteisen henkilötiedon tallennukseen.
    - Henkilökohtainen verkkoasema (H:) on turvallinen ja varmistettu tallennuspaikka.
- Tarvittavat ohjelmat asentaa pääosin ICT-tuki, joka myös hallinnoi niitä.
    - Ohjelmistoja ei tule asentaa tai poistaa harkitsematta, vaikka siihen olisi riittävät käyttöoikeudet.
- Kirjaudu ulos ohjelmistoista ja tietokoneeltasi työpäivän päättyessä. Noudata saamiasi ohjeita.
- Älä kirjoita salasanoja muistiin siten, että ne ovat muiden löydettävissä.
- Työsuhteen päättyessä käyttäjätunnus passivoidaan tai poistetaan, jolloin viestit ja mahdolliset asiakirjat häviävät. Siirrä nämä tarpeen mukaan työnantajan käyttöön sekä tallenna viestit ja asiakirjat saamiesi ohjeiden mukaan.

3.6.2. Internet ja sähköposti

Internet ja sähköposti ovat hyviä työvälineitä tiedonhakuun ja yhteydenpitoon. Niitä käytettäessä on kuitenkin muistettava, että sähköposti tai internet-palvelut eivät oletuksena sisällä mitään suojausta, vaan tiedot liikkuvat salaamattomina julkisessa verkossa.

Asiakkaita koskeva tieto on luottamuksellista. Verkossa viesti saattaa päätyä julkiseksi, eikä sanojaan saa takaisin. Myös yksityishenkilönä sinut voidaan yhdistää työnantajaasi, vaikka et sitä haluaisikaan, älä siis luota ja vastaa kaikkeen mitä Sinulta mahdollisesti kysytään. Neuvoa kannattaa aina kysyä, jos asia epäilyttää.

Skype for business on riittävän luotettava, jotta sen kautta voidaan järjestää neuvotteluja sekä mahdollisesti, harkinnan mukaan, välittää myös liitteitä.

Noudata ohjeita, joita ohjelmistojen käytöstä on annettu.

- Käytä vain asiallisiksi tietämiäsi ja LLKY:n hyväksymiä palveluita.
- Internetin tai avoimen sähköpostin kautta ei ole luvallista välittää salassa pidettävää tietoa ilman asianmukaista salausta.
    - Verkkosivuilla salauksen käytöstä kertoo osoitteen alussa oleva https:// -teksti tai selaimen osoiterivin vieressä oleva esim. lukon kuva.
- Sisäinen sähköpostiliikenne on vahvasti salattu ja sen kautta on turvallista välittää myös salassa pidettävää tietoa erityisen harkinnan mukaisesti.
- Tarkista etenkin salassa pidettävää tietoa lähettäessäsi sähköpostin vastaanottaja ennen lähetystä.
- Työhön liittyvä sähköposti ohjataan työsähköpostiin, sitä ei saa automaattisesti ohjata ulkopuoliseen sähköpostiin.
- Työsähköposti on tarkoitettu työasioiden hoitoon.
- Mikäli henkilökohtaiseen sähköpostiisi saapuu työhön liittyvää postia, vastaat niistä työvelvollisuuksiesi mukaisesti.
- Varmista sähköpostin käsittelyyn liittyvien velvollisuuksien tulevan hoidetuksi myös poissaolosi aikana.
- Mikäli saat toiselle henkilölle tarkoitetun sähköpostin, ohjaa viesti oikealle vastaanottajalle ja ilmoita lähettäjälle oikea osoite. Muista vaitiolovelvollisuus saamastasi viestistä.
- Sähköpostin liitetiedostot voivat sisältää haittaohjelmia. Varo epätavallisia sähköposteja sekä posteissa olevia suoria www-linkkejä. Älä avaa epäilyttäviä viestejä tai liitteitä, vaan ilmoita asiasta tarvittaessa tietohallintoon.
- Sähköpostin lähettäjä on helppo väärentää. Voit tarkistaa lähettäjän tiedot viemällä hiiren osoittimen lähettäjän nimen päälle sähköpostiohjelmassa (Outlook).
- Varo tietojenkalasteluviestejä, joissa pyydetään lähettämään tai syöttämään tunnuksia palveluihin.
- Roskapostia ovat esim. tilaamatta tulleet mainokset. Roskapostiin ei kannata vastata, vaan poistaa se tai lisätä se roskaposti-listalle, vastaaminen yleensä lisää saapuvan roskapostin määrää.
- Jakelulista luetaan henkilöluetteloksi, joka näkyy kaikille vastaanottajille. Voit tarpeen vaatiessa käyttää sähköpostin piilokopio-toimintoa, jolloin vastaanottajat eivät näe toistensa nimiä.
- Pysäytä ketjukirjeet ja vältä turhien sähköpostien lähettämistä. Esimerkiksi laaja joulutervehdysten lähettäminen kuormittaa sähköpostijärjestelmää.
- Sähköposti ei sovellu tärkeiden liitetiedostojen pitkäaikaiseen tallennukseen. Tallenna nämä tiedostot verkkoasemalle tai muuhun soveltuvaan järjestelmään.

3.7. Huijaukset ja tietojen kalastelut

Erilaiset netti-/sähköpostihuijaukset ovat muuttuneet jatkuvasti ammattimaisemmiksi, huijausta ei enää välttämättä tunnista siitä, että se on kirjoitettu huonosti. Viesti voi olla kirjoitettu hyvällä kielellä ja tulla tutusta osoitteesta.

Huijausviestit ovat yleensä sähköpostin, viestisovellusten tai sosiaalisen median kautta lähetettäviä viestejä, joiden tarkoituksena on saada tietoon käyttäjien käyttäjätunnuksia, salasanoja, verkkopalvelutunnuksia tai muita henkilökohtaisia tietoja. Yleensä nämä viestit naamioidaan näyttämään viralliselta ja usein lähettäjä näyttää olevan pankki, verottaja tai muu vastaava. Yleensä huijausviestissä pyydetään siirtymään verkkosivulle viestin mukana olevan linkin kautta, jonka kohdesivusto on naamioitu näyttämään aidolta verkkosivulta.

Esimerkkejä mahdollisista huijauksista

- Sähköpostit, joissa kerrotaan tunnuksen tai palvelun voimassaolon päättyvän pian ja voit jatkaa sitä alla olevan linkin kautta.
- Ilmoitukset, joissa luvataan palkinto ja sen voi lunastaa käyttäen viestiin liitettyä linkkiä.
- Asiakirja tai tiedosto, joka näyttää tulevan luotettavalta lähettäjältä ja jonka voi avata verkkopalvelusta antamalla käyttäjätunnuksesi ja salasanasi.
- Lasku, joka näyttää tulevan luotettavalta lähettäjältä.
- Ilmoitus erittäin edullisesta tuotteesta, jonka lunastamiseksi täytyy vain syöttää yhteystiedot ja luottokortin tiedot.
- Ilmoitus, jossa varoitetaan esim. verkkosivulla vieraillessa, tietokoneella tai mobiililaitteella olevan ongelmia ja/tai viruksia ja tarjotaan näiden poistoa. Lähes poikkeuksetta nämä eivät ole todellisia ongelmia, vaan tällä yritetään saada käyttäjä asentamaan tai ostamaan ohjelma, joka itsessään on haitallinen tai ei tee mitä lupaa.
- Kiristysviestit, joissa lähettäjä kertoo saaneensa haltuunsa yksityistä tietoa, joka uhataan julkaista, ellei lähettäjälle makseta ns. lunnaita.

Yhteistä näille kaikille on usein kiireellisyys. Suhtaudu terveen epäilevästi viesteihin, joissa vaikuttaa olevan jotain outoa. Tarkista sähköpostin lähettäjä ja kysy tarvittaessa neuvoja esimieheltä tai ICT-tuelta.

3.8. Toimitilaturvallisuus

Toimitilojen turvallisuudella varmistetaan tietojen, asiakirjojen ja laitteiden asianmukainen säilytys ja käsittely turvallisissa tiloissa. Toimitilojen turvallisuus sisältää mm. kulunvalvonnan, teknisen valvonnan ja vartioinnin sekä palo-, vesi-, sähkö-, ilmastointi ja murtovahinkojen torjunnan.

- Pyri noudattamaan ns. puhtaan pöydän periaatetta. Työpöydällä ei tule säilyttää salassa pidettävää aineistoa.
- Käytä mahdollisuuksien mukaan vierailuihin ns. julkisen alueen neuvottelutiloja.
- Neuvottelutiloissa tulee huolehtia siitä, että asiaankuulumatonta materiaalia ei ole esillä. Huolehdi myös esityksen päätyttyä siitä, että tiloihin ei jää sinne kuulumatonta materiaalia tai luottamuksellisia tietoja.
- Suuntaa tietokoneesi näyttö harkitusti. Onko tietojen tarkoitus näkyä asioijalle vai ei?
- Älä jätä kannettavia laitteitasi ilman valvontaa yleisissä tiloissa ja säilytä niitä lukitussa tilassa. Huolehdi myös USB-tikkujen ja muiden tallennusvälineiden, paperitulosteiden ym. asianmukaisesta säilyttämisestä.
- Vieraita ei tule päästää valvomatta työhuoneeseen tai muihin ulkopuolisilta suljettuihin tiloihin. Älä päästä ulkopuolisia henkilöitä toimitiloihin lukittujen ovien ohi esim. töistä lähtiessäsi. Ulkopuolisia ovat myös perheenjäsenet.
- Ohjaa vieraat tai eksyneet henkilöt oikeisiin paikkoihin.
- Kulunvalvonnassa olevia tai muuten lukittavaksi tarkoitettuja ovia ei tule jättää auki, varmista ovien lukittuminen. Noudata kulunvalvonnasta annettuja ohjeita.
- Käytä henkilökorttia, jos siihen on ohjeistettu.

3.9. Liikkuva työ, etätyö, matkatyö

3.9.1. Liikkuva työ ja matkatyö

Liikkuvan työn välineisiin ja niiden käyttöön liittyy vastaavia uhkia kuin kiinteämmin asennettuihin laitteisiin, joten samat turvallisuusohjeet koskevat myös niitä, mutta laitteiden kuljettaminen työpaikan ulkopuolella vaatii erityistä huolellisuutta.

- Älä säilytä laitteilla ylimääräistä tietoa ja huolehdi laitteiden suojauksesta.
- Tutustu laitteen ja ohjelmien turvallisuusominaisuuksiin, kuten lukitseminen, suojakoodit, Bluetooth-asetukset, sovellusten asennus ja päivittäminen.
- Huolehdi matkapuhelimesi suojauksesta, vaihda laitevalmistajan oletusarvoiset PIN-koodit.
    - Suojaukseksi ei riitä kuvion piirtäminen.
- Älä asenna tarpeettomasti ohjelmia laitteille ja tarkista ohjelmien vaatimat oikeudet.
- Huolehdi tietojen varmuuskopioinnista ohjeiden mukaisesti.

Matkatyössä tulee erityisen huolellisesti huomioida salassapito ja laitteiden turvallisuus.

- Vältä puhumista luottamuksellisista työasioista julkisilla paikoilla ja kulkuvälineissä.
- Mikäli työskentelet esim. julkisessa kulkuvälineessä tai kahvilassa tms., varmistu, että ulkopuoliset eivät pääse näkemään salassa pidettävää tietoaineistoa.
- Varo aiheettomien langattomien yhteyksien aktivoitumista laitteisiisi.
- Kuljeta mukana vain tarpeelliset laitteet ja asiakirjat. Lähtökohtaisesti mukaan ei tule ottaa aineistoa, joka voi vääriin käsiin joutuessaan aiheuttaa vahinkoa LLKY:lle.
- Säilytä tieto ja laitteet turvassa. Älä jätä laitteita valvomatta esim. auton penkille.
- Harkitse, onko tarpeen jakaa tietoja tai kuvia työmatkasta sosiaaliseen mediaan. Kerro mieluummin mitä olet tehnyt kuin se, mitä tulet tekemään.
- Erilaisten messulahjojen tms. käyttöä tulee varoa, eikä ottaa niitä käyttöön ilman harkintaa. Esim. muistitikut, laturit tai muut USB-väylään liitettävät laitteet voivat sisältää haitallisen ohjelman. Kysy neuvoa tietohallinnolta.

3.9.2. Etätyö ja etäkäyttö

Etätyö on muualla kuin organisaation vakituisessa toimipisteessä tehtävää työtä. Tyypillinen etätyö on kotoa tehtävää toimistotyötä. Etätyötä on myös esim. kotimatkan, koulutusmatkan tai loman aikana sähköpostin tarkistaminen puhelimella tai muulla päätelaitteella.

- Etätyö on sallittua silloin kun esimies on sen hyväksynyt.
- Kiinnitä huomio tietoturvaan. Etätyössä tulee noudattaa samoja turvallisuusperiaatteita, kuin toimiessasi vakituisissa toimitiloissa.
- Kaikkea työtä ei voi tehdä turvallisesti etätyönä, tunnista nämä työt.
- Huolehdi laitteiston, ohjelmistojen ja tietoaineiston pysymisestä vain sinun käytössäsi.
- Käytä sovittuja suojausohjelmia.
- Kuljeta mukanasi vain välttämätön määrä tietoaineistoa ja varmistu sen suojaamisesta.
- Aineiston luokittelu on otettava huomioon myös etätyössä.
- Huolehdi laitteiden turvallisesta säilytyksestä ja tietojen varmuuskopioinnista.

3.10. Sosiaalinen media

- Erottele sosiaalisen median käytössä työnantajan käyttämät sivut ja ryhmät sekä henkilökohtainen käyttäjätili. Työnantajan hallinnoiman sosiaalisen median palveluiden käyttöön työnantaja antaa erilliset ohjeet, mikäli sosiaalisen median päivittäminen kuuluu työtehtäviisi.
- Mikäli mainitset sosiaalisen median henkilökohtaisessa profiilissa työantajasi, esiinnyt tällöin myös organisaation epävirallisena edustajana.
- Liian henkilökohtaista tai yksityiskohtaista tietoa, valokuvia tai muuta materiaalia ei kannata julkaista. Huomaa, että palveluntarjoaja voi hyödyntää profiiliisi syöttämiäsi tietoja laajasti.
- Tutustu palveluiden sopimusehtoihin.
- Tarkista käyttäjäprofiilin yksityisyysasetukset ja muuta niitä tarvittaessa niin, että tiedot eivät leviä kuin haluamallesi käyttäjäjoukolle.
- Kunnioita perheesi ja ystäviesi sekä työkavereiden ja muiden henkilöiden suhtautumista sosiaalisiin medioihin. Vaikka itse olisit niistä innostunut, kaikki eivät sitä ole. Älä esim. laita kuvia heistä sosiaaliseen mediaan, jos he eivät sitä halua.
- Tuntemattomien kaveripyyntöjä tai yhteydenottoyrityksiä ei kannata hyväksyä, eikä avata vieraita, hämäräperäisiä linkkejä, videoita tai kuvia.
- Jos epäilet joutuneesi huijatuksi tai huijaus- tai muun hyökkäyksen kohteeksi, älä epäröi pyytää apua. Tee asiasta tarvittaessa rikosilmoitus, vaikka taloudellinen menetys tai muu seuraus olisi vähäinenkin.
- Työasioista ei tule keskustella muissa kuin työtehtäviin hyväksytyissä sosiaalisen median palveluissa tai hyväksyttyjen viestintäsovellusten kautta. Ole erityisen huolellinen salassa pidettävän tiedon suhteen.
    - Palvelun ylläpitäjät pääsevät yleensä teknisesti käsiksi palvelun kautta välitettävään tietoon ja myös yksityisviestien sisältöön.

4. ONGELMATILANTEET

Mikäli kaikesta huolimatta kohtaat ongelmia tietoturvaan tai tietosuojaan liittyen, kannattaa pysyä rauhallisena ja noudattaa annettuja ohjeita. Ongelmia kohdatessasi ota tarpeen mukaan yhteys ICT-tukeen, esimieheesi tai tietosuojavastaavaan.

Jos epäilet tietoturvaloukkausta tai haittaohjelmaa

- Älä hätiköi.
- Tietokonetta ei tule sammuttaa, mutta irrota lähiverkkokaapeli ja/tai katkaise langaton verkkoyhteys.
- Ota mahdollisesta varoituksesta tai ilmoituksesta kuvakaappaus tai kirjoita muistiin, mitä ilmoituksessa tai varoituksessa luki.
- Kirjaa tekemäsi toimenpiteet ja menetetty työaika.
- Kerro ICT-tuelle mitä olit tekemässä kun laite alkoi toimia odottamattomasti.
- Toimi saamiesi ohjeiden mukaisesti.

4.1. Ilmoitusvelvollisuus

- Mikäli laite, kulkukortti tai muu tunniste katoaa tai varastetaan, ilmoita siitä välittömästi esimiehelle ja ICT-tuelle riskien pienentämiseksi ja oman vastuusi rajaamiseksi.
- Ilmoita aina tietoturvaan tai tietosuojaan liittyvistä epäilyistä, suojauspuutteista tai muista ongelmista ICT-tuelle ja esimiehellesi.
- Ilmoita haittaohjelmista välittömästi ICT-tuelle.
- Muista myös tietoturvan ja tietosuojan HaiPro-ilmoitus.
- Mikäli sinulla on tietoturvaan tai tietosuojaan liittyen kehittämisidea, tee siitä aloite.

5. SEURAAMUKSET

Lakien, määräysten ja ohjeiden rikkomisesta käyttöoikeudet järjestelmiin voidaan peruuttaa. Rikkomuksista tiedotetaan aina esimiehelle ja vakavissa tapauksissa väärinkäyttö voi johtaa vahingonkorvausvaatimuksiin, työ- tai rikosoikeudellisiin seuraamuksiin.

Seuraamuksissa punnitaan aina teon tahallisuutta sekä sen vakavuuden ja vaikutuksen astetta. Seuraamusten arvioinnissa käytetään hyväksi tietosuojapolitiikan käyttölokien seuranta- ja valvontasuunnitelman mukaista seuraamustaulukkoa.

6. TIETOTURVAN TOTEUTTAMINEN KOTONA

Useimmilla on oma tietokone tai muu laite internet-liittymällä ja myös niiden tietoturvasta on tärkeää huolehtia. Tässä ohjeessa kuvatut periaatteet pätevät myös kotona soveltuvin osin.

- Tarkista, että laite- ja ohjelmistoympäristösi on tietoturvallinen. Mikäli on tarpeen ja mahdollista, pyydä luotettavaa asiantuntijaa tarkistamaan nämä.
- Jokaisella käyttäjällä on hyvä olla oma käyttäjätunnus, joilla on normaalikäyttäjän oikeudet.
- Käytä ylläpitäjän tunnusta (järjestelmänvalvoja, administrator) vain ylläpitotehtäviin.
- Asenna virallisia ja ajan tasalla olevia ohjelmistoja.
- Huolehdi käyttöjärjestelmän ja muiden ohjelmistojen jatkuvasta päivittymisestä. Ota käyttöön automaattiset päivitykset.
- Käytä tunnettua ja hyvämaineista tietoturvaohjelmistoa.
- Älä avaa epäilyttäviä sähköpostiviestejä, etenkään niiden sisältämiä linkkejä tai tiedostoja.
- Tee säännöllisesti varmuuskopiot tärkeistä tiedostoista.
- Kirjautuessasi internetin palveluihin tai tehdessäsi ostoksia netissä, käytä vain luotettavia palveluita ja toimittajia.

- Älä anna henkilökohtaisia tietoja enemmän kuin on tarpeen.
- Älä käytä samoja salasanoja kuin työpaikan järjestelmissä.

7. TIETOTURVAN OHJAUS JA SEURANTA

Tietoturvaa johtaa ja siitä vastaa ensisijaisesti ylin johto. Vastuu on riippumatonta siitä, onko toimintoja ulkoistettu vai ei. Rekisterinpitäjä on aina vastuussa henkilötietojen asianmukaisesta käsittelystä ja tietoturvan toteutumisesta.

Tietoturvan ohjausryhmänä toimii tietoturvatyöryhmä, johon kuuluvat liikelaitoskuntayhtymän johtaja, tietosuojavastaava, tietoturvavastaava, palvelualuejohtajat, henkilöstöpäällikkö ja hallintopäällikkö.

Tietoturvaohjeiden noudattamisesta yksiköissä vastaa ko. yksikön esimies, jonka vastuulla on myös henkilökunnan perehdytys ja ohjeiden tuominen tiettäväksi henkilöstölle. Esimies opastaa henkilökuntaa ja vie tarvittaessa tietoa eteenpäin.

Jokaisella työntekijällä on henkilökohtainen vastuu huolehtia oman toimintansa tietoturvallisuudesta ja noudattaa saamiaan ohjeita ja määräyksiä sekä voimassa olevaa lainsäädäntöä.

8. MISTÄ LISÄTIETOA

Tämän oppaan lisäksi tietoa on saatavissa mm. seuraavista:

- Sisäinen intranet ja verkkosivut
- Tietoturva- ja tietosuojapolitiikka
- Käyttölokien seuranta- ja valvontasuunnitelma
- Palvelualuekohtaiset lisäohjeet
- Lainsäädäntö:
  - Valtion säädöstietopankki www.finlex.fi
  - EU:n säädöstietopankki www.eurlex.fi
- Kyberturvallisuuskeskus: www.kyberturvallisuuskeskus.fi
- Tietosuojavaltuutetun toimiston ohjeet: www.tietosuoja.fi
- Juhta/Vahti tietosuojan-yhteishankkeen materiaalit: www.wm.fi/tietosuojan-yhteishankkeet
- JUDO-hanke: www.vrk.fi/judo
- Traficom: www.traficom.fi

LIITE 1

SOPIMUS 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. Omien tietojen käsittely on kiellettyä.
- 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 henkilötietolakiin 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_____

Työyksikkö:_____

_____	_____
Työntekijän nimi	Esimiehen nimi
_____	_____
Työntekijän allekirjoitus	Esimiehen allekirjoitus

LIITE 2

Kuvaaminen ja tallentaminen SOTE-palveluissa

Kuvaaminen ja tallentaminen SOTE-palvelujen tiloissa voi olla luvanvaraista ja kuvan tai tallenteen julkaisemiseen tarvitaan erillinen lupa. Esim. vuodeosastoilla ja poliklinikoilla kuvaamista ja tallentamista rajoittavat yksityisyyden suoja ja potilasturvallisuus.

Omaa ja läheisen hoitoa voi kuvata

Rakennuksen pääaula ja kahvilat yms. ovat julkisia paikkoja, joissa kuvaaminen ei vaadi lupaa. Ilman lupaa jokainen voi myös kuvata itseään ja läheisiään, mikäli läheinen tähän suostuu, osastoilla, poliklinikoilla tai toimenpidetiloissa. Potilas/asiakas voi lähtökohtaisesti kuvata ja tallentaa oman tai läheisensä hoitotilanteen ja tallentaa oman puhelunsa.

Henkilökunnan, toisen potilaan/asiakkaan tai vierailijoiden kuvaamiseen tai tallentamiseen muualla kuin julkisissa tiloissa tulee aina kysyä lupa. Kuvausluvan voi antaa omasta puolestaan kuvattava henkilökunta. Toisten potilaiden, asiakkaiden ja vierailijoiden osalta vastaavat yksikön esimies, sairaalan johto tai viestinnästä vastaavat sillä edellytyksellä, potilas, asiakas tai vierailija suostuu kuvaamiseen. Median kysyessä kuvauslupaa, henkilökunta kysyy luvan potilaalta/asiakkaalta toimittajan puolesta.

Potilaan, asiakkaan tai hänen läheisensä kuvaamista tai muuta tallentamista hoitotilanteessa voidaan rajoittaa yksityisyyteen tai potilasturvallisuuteen liittyvistä syistä. Kuvaaminen tai tallentaminen voi häiritä hoitotapahtumaa, haitata teknisten hoitolaitteiden käyttöä sekä häiritä näiden toimintaa tai muuten vaikutta hoitotilanteeseen. Potilasta/asiakasta voidaan pyytää lopettamaan kuvaaminen tai tallentaminen hoitotoimenpiteen ajaksi. Potilaan hoitoa voidaan myös siirtää, mikäli asiasta ei päästä yhteisymmärrykseen.

Kuvan ja tallenteen julkaiseminen

Vaikka kuvaamiseen tai muuhun tallentamiseen olisi lupa, julkaisemiseen tarvitaan yleensä erillinen lupa. Mitään kuvia tai tallenteita ei voi julkaista ilman ao. henkilöiden suostumusta. Mikäli henkilökunnalla on epäily, että näitä julkaistaan esim. sosiaalisessa mediassa ilman lupaa, tulee tallentaminen pyytää lopettamaan. Työyhteisöstä otettujen kuvien yms. julkaisuun tulee pyytää lupa kaikilta kuvassa olevilta.

Pyrkimys yhteistyöhön

Kuvaamisessa ja tallentamisessa tulee pyrkiä yhteisymmärrykseen. Kuvaamisesta voi olla myös hyötyä sosiaali- ja terveydenhuollon toiminnalle. Henkilökunnan osallistuminen potilaiden ja asiakkaiden kuviin tai videoihin voi edistää yksikön hyvää mainetta. Lähtökohtaisesti potilas- ja asiakastyö tehdään aina niin hyvin, että se kestää julkisen tarkastelun.

LIITE 3

Turvakielto

Turvakielto on arkikielessä käytettävä ilmaus. Asiassa on kyse väestötietolain mukaisesti henkilön kotikunnan, asuinpaikan, osoitteen tai muun yhteystiedon luovutusrajoituksesta. Perustellusta pyynnöstä maistraatti voi määrätä, että henkilön tietoja ei luovuteta kuin viranomaisille. Määräyksen perusteena ovat henkilön tai hänen perheensä terveyden tai turvallisuuden uhka.

Mikäli henkilöllä on turvakielto, hänen yhteystietojaan ei luovuteta useissa tapauksissa viranomaisillekaan. Turvakielto ei estä viranomaista saamasta henkilön kyseisiä tietoja lakisääteisten tehtävien hoitamista varten.

Saatuja tietoja ei saa luovuttaa millekään sivulliselle taholle. Turvakiellon alaiset tiedot pitää pystyä rajaamaan vain niille henkilöille, joiden työtehtävään ko. tietojen käsittely välttämättömästi kuuluu. Tietojärjestelmissä käyttöä valvotaan käyttölokien avulla.

Muistilista

Tietojärjestelmiin tulee merkitä selkeästi, mikäli henkilöllä on voimassa oleva turvakielto. Tieto päivittyy väestörekisterikeskukselta.

Huomioi, että turvakiellon alaiset tiedot eivät vahingossa paljastu sivullisille esim. johonkin kysymykseen tapahtuvan vastauksen tai jostain asiasta tiedottamisen yhteydessä jollekin kohderyhmälle.

Varmista, että kysyjällä on oikeus saada tietoja, mikäli ne koskevat toista henkilöä. Varmista kysyjän henkilöllisyys.

LIITE 4

Tietoturvaan ja tietosuojaan keskeisesti liittyvät säädökset

Tärkeimpiä tietoturvaa ja tietosuojaa säänteleviä lakeja ovat:

- Euroopan unionin yleinen tietosuoja-asetus (2016/679)
- Tietosuojalaki (1050/2018)
- Arkistolaki (831/1994): Asiakirjojen laatiminen, säilyttäminen ja käyttö – 1.1.2020 lähtien Tiedonhallintalaki
- Laki viranomaisten toiminnan julkisuudesta (621/1999)
- Asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999)
- Laki kunnallisesta viranhaltijasta (304/2003)
- Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007)
- Laki sähköisen viestinnän palveluista (917/2014)
- Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003): Tietoturvallisuus asioinnissa ja viran-omaisten keskinäisessä tietojenvaihdossa
- Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (617/2009)
- Laki yksityisyyden suojasta työelämässä (759/2004): Työntekijää koskevien henkilötietojen käsittely
- Rikoslaki (39/1889): Tieto- ja viestintärikokset
- Suomen perustuslaki (731/1999) 2. luku 10 §: Yksityiselämän suoja ja luottamuksellisen viestin sa-laisuus
- Suomen perustuslaki (731/1999) 2. luku 12 §: Viranomaisten hallussa olevien asiakirjojen ja tallen-teiden julkisuus
- Turvallisuusselvityslaki (726/2014)
- Työsopimuslaki (55/2001)
- Vahingonkorvauslaki (41/1974)

Lisäksi on olemassa toimialakohtaista erityislainsäädäntöä, jossa käsitellään tietosuojaan (henkilö-tietojen käsittelyyn) ja tietoturvaan liittyviä asioita.

Ajantasainen lainsäädäntö löytyy Finlex-palvelusta osoitteesta www.finlex.fi

Tietoturva kuuluu jokaiselle

Käyttäjätunnukset

- Tunnukset ja salasanat ovat henkilökohtaisia, niitä ei saa luovuttaa muiden käyttöön ja säilytä salasanat, PIN-koodit, toimikortit ja muut kirjautumistunnisteet huolellisesti.
    - Käsittele näitä samoin kuin pankkikorttiasi ja tunnuslukuasi.
- Lukitse tietokoneesi kun poistut sen läheisyydestä, nopeinta on käyttää näppäinyhdistelmää Win + L 

Luottamukselliset tiedot

- Muista keskustellessasi työkaverin tai asianosaisen kanssa, ettet paljasta luottamuksellisia tietoja sivullisille. Huomioi tämä myös puhelinkeskusteluissa.
- Mikäli käsittelet työsi vuoksi luottamuksellisia tietoja kotonasi tai matkoilla, muista huolehtia niiden salassapidosta.
- Kunnioita asiakkaiden ja työkaverien yksityisyyttä.

Tietosuoja-aineisto

- Huolehdi paperien, muistitikkujen ja muiden tallennusvälineiden, puhelinten, avainten, kulkunappien, toimikorttien yms. asianmukaisesta käsittelystä ja säilytyksestä. Älä luovuta niitä sivullisten käyttöön.
- Säilytä salassa pidettävät tiedot asianmukaisesti, noudata ns. puhtaan pöydän periaatetta.
- Hävitä salassa pidettävät tiedot asianmukaisesti siten, etteivät sivulliset pääse näkemään niitä.
- Tieto tulee suojata sen kaikissa käsittelyvaiheissa.
    - Luominen, käyttäminen, muuttaminen, tallentaminen, siirtäminen kerääminen, käsittely, tuhoaminen

Mobiililaitteet ja kannettavat tietokoneet

- Huolehdi etätyössä ja matkoilla mobiililaitteiden ja niiden kautta käytettävien salassa pidettävien tietojen suojaamisesta ulkopuolisten katseilta.
- Puhelin ja muut mobiililaitteet, joista on pääsy tietosuojan alaisiin tietoihin tai esim. sähköpostiin, tulee suojata PIN-koodilla tai salasanalla, kuvion piirtäminen ei ole riittävä suojaus.
- Huolehdi laitteiden valvonnasta, älä jätä niitä näkyville esim. autoon tai hotelliin.
- Julkiset päätelaitteet ja avoimet verkot ovat riski, eikä niiden kautta ei tule käsitellä salassa pidettävää tietoa tai kirjautua palveluihin.

Muuta huomioitavaa

- Anna ICT-tuen asentaa ohjelmistot ja tehdä niihin tarvittavat muutokset.
- Kerro tietosuojavastaavalle tai esimiehellesi, mikäli havaitset ongelmia tai rikkomuksia tietosuojan tai tietoturvan toteutumisessa tai tapahtuu jotain normaalista poikkeavaa.
- Työtiloihin ei tule tarpeettomasti päästää ulkopuolisia eikä jättää näihin ulkopuolisia yksinään.
    - Ovia ei saa kiilata auki esim. harjanvarrella tms.
    - Ulkopuolisia ei saa päästää lukittuihin tiloihin. Tapaamisen järjestänyt työntekijä huolehtii ovien avaamisen.
    - Kysy kuka ja millä asialla henkilö on, mikäli näet lukituissa tiloissa ulkopuolisia yksinään.
    - Lukitse toimiston ovi lähtiessäsi, ellei tiloihin jää toista työntekijää.
- Mikäli olet epävarma jostain, kysy.