TIETOTURVAOPAS

HENKILÖSTÖLLE

SISÄLTÖ

1 Johdanto

Tietoturvallisuus perustuu lainsäädäntöön, normiohjaukseen sekä sopimuksiin. Vastuu tietoturvallisuudesta ja siihen liittyvästä osaamisesta kuuluu omalta osaltaan jokaiselle, myös sinulle. Turvallisuus ja tietoturvallisuus kokonaisturvallisuuden osana muodostuvat suurelta osin yksilöiden tekemistä
valinnoista erilaisissa arkipäivän tilanteissa.

Tämä tietoturvaohje on tarkoitettu:

- Raision kaupungin henkilöstölle noudatettavaksi niin työvälineiden kuin palveluiden käytössä,
- Raision kaupungin tietojärjestelmiä tai toimitiloja säännönmukaisesti käyttäville henkilöille (esim. harjoittelijat, opiskelijat).

Ohjeeseen on koottu keskeisimmät tietoturvallisuuden perusasiat. Se antaa neuvoja tietoturvallisuuden toteuttamiseen omassa työssä ja muissa käytännön tilanteissa.

Kun saat hyvän idean tietoturvallisuuden parantamisesta, tee siitä aloite Raision kaupungin tietosuojavastaavalle tai omalle esimiehellesi!

Tämä opas perustuu Valtiovarainministeriön antamaan henkilöstön tietoturvaohjeeseen, VAHTI 4/2013 (ISBN 978-952-251-514-8 (PDF).

Kiitos VSSHP:lle että saimme käyttää tietoturvaopastanne tämän työn pohjana.

Tietoturvaopas on laadittu 05/2017. Päivitetään vuosittain toukokuussa tai tarvittaessa.

2 Toimitilaturvallisuus

Toimitilojen turvallisuudella varmistetaan, että tietoja, asiakirjoja ja ICT-laitteita säilytetään turvallisissa tiloissa. Toimitilojen turvallisuus sisältää mm. kulunvalvonnan, teknisen valvonnan, vartioinnin, palo-, vesi-, sähkö-, ilmastointi- ja murtovahinkojen torjunnan sekä lähettipalvelujen ja tietoaineistoja sisältävien lähetysten turvallisuuden.

- Asiakaspalvelupisteessä tai -tilanteessa päätelaitteen näyttö ei saa näkyä asioijalle.
- Huolehdi, ettei neuvottelutiloissa ole esillä asiaan liittymätöntä materiaalia. Huolehdi neuvottelun päättyessä, ettei pöydille, tauluihin, roskakoreihin tai muualle jää käsiteltyjä salassa pidettäviä aineistoja tai muistiinpanoja.
- Säilytä tieto ja laitteet turvallisessa paikassa, tarpeen mukaan lukitussa kaapissa ja huoneessa.
- Älä jätä kannettavaa päätelaitetta ilman valvontaa. Huolehdi myös muistitikkujen, CD-/ DVD-levyjen, paperitulosteiden ym. asianmukaisesta säilyttämisestä.
- Noudata “puhtaan pöydän” periaatetta. Työpöydällä ei saa säilyttää salassa pidettävää tietoa, kun tietoa ei tarvita työtehtävien suorittamisessa.
- Kuvaaminen organisaation tiloissa voi olla kiellettyä. Kuvaukseen pitää saada yksikön esimiehen lupa. Valvo myös vieraidesi toimintaa ja esimerkiksi kameroiden käyttöä.
- Lukitse työhuoneesi ovi työpäivän päättyessä tai poistuessasi pidemmäksi aikaa työpisteestäsi. Huolehdi tarvittaessa myös siitä, että toimitilan ulko-ovi lukittuu poistuessasi.
- Ohjaa vieraat tai “eksyneet” henkilöt oikeisiin paikkoihin, tarvittaessa saata henkilö aulaan tai ulos. Älä päästä asiattomia henkilöitä lukittuihin toimitiloihin esim. töistä lähtiessäsi.
- Älä jätä auki kulunvalvonnassa olevia ovia tai ovia, jotka on muuten tarkoitettu pidettäväksi suljettuina

3 Päätelaitteet ja käyttöoikeudet

Päätelaitteella tarkoitetaan tässä ohjeessa työtehtävien hoitoon tarkoitettua elektronista laitetta, joka voi olla esimerkiksi puhelin, älypuhelin, kannettava-, tabletti-, pöytätietokone tai jokin vastaava laite. Käyttö sisältää sekä päätelaitteen että verkon kautta käytettävät palvelut.

3.1. Päätelaitteet

- Vastaat käyttäjänä omasta päätelaitteestasi. Ole siis huolellinen.
- Vain asennusoikeudet saanut henkilö (ATK-help) saa asentaa tietokonelaitteita verkkoon ja asentaa tai päivittää ohjelmia laitteisiin.
- Kirjaudu laitteelle aina omilla käyttöoikeuksillasi.
- **Estä asiaton pääsy tietojärjestelmiin lukitsemalla työasemasi aina kun poistut työpisteestäsi.**
- Jos työaseman kiintolevy tai muu tallennusväline, kuten esimerkiksi muistitikku tai CD-/DVD-levy rikkoutuu tai poistetaan muuten käytöstä, ei sitä saa laittaa roskakoriin. Toimi Raision kaupungin **ohjeen** mukaisesti.
- Siirrä tietokone virranhallintatilaan tai sammuta se työpäivän päättyessä, ellei muuta ole ohjeistettu työyksikössä tai esimerkiksi tietoturvapäivitysten johdosta.
- Tutustu laitteen ja siinä olevien ohjelmien käyttöohjeisiin ja turvallisuusominaisuuksiin, joita ovat mm. PIN- tai salasanakyselyt, laitteen automaattinen lukitus ja suojakoodikyselyt, tietoliikenneyhteyksien käyttäminen ja salaaminen.
- Huolehdi, että matkapuhelimessasi on päällä PIN- ja suojakoodikysely. Vaihda laitevalmistajan tai palveluntarjoajan antamat oletuskoodit.

Jos kadotat kannettavan päätelaitteen, toimi kaupungin ohjeistuksen mukaisesti; tee välittömästi ilmoitus kadonneesta laitteesta ohjeiden mukaisesti (ks. luku 8), jotta sen väärinkäyttö voidaan estää. Kannettavat päätelaitteet muodostavat suuremman riskin kuin perinteiset pöytäkoneet niin vahingossa tapahtuvan kadottamisen kuin varastamisen näkökulmasta. Huolehdi tämän takia laitteiden automaattisesta lukittumisesta.

3.2. Salasanat ja käyttäjätunnukset

Tietojärjestelmien käyttöön tarvitaan käyttöoikeus. Käyttöoikeus on henkilökohtainen ja se on yhdistetty sinun henkilöllisyyteesi ja työtehtävääsi. Käsittele käyttäjätunnusta ja salasanaa samalla tavalla kuin pankkikorttiasi ja tunnuslukuasi.

- Älä luovuta henkilökohtaisia käyttäjätunnuksiasi, salasanojasi, toimikorttiasi tai PIN-koodejasi toisen henkilön käyttöön – älä edes lomien aikana. Suhtaudu epäilevästi kaikkiin tiedusteluihin, jotka liittyvät salasanoihisi tai järjestelmien käyttöoikeuksiin. Myöskään tietohallintohenkilöstö ei tarvitse tehtäviensä hoitamiseksi salasanaasi.
- Vaihda salasanasi riittävän usein ja heti, jos epäilet niiden paljastuneen.
- Huolehdi, että salasanat ovat riittävän monimutkaisia ja vältä tuttujen jokapäiväisten sanojen käyttöä. Hyvässä salasanassa on pieniä ja isoja kirjaimia, numeroita ja erikoismerkkejä. Hyvä salasana on helppo muistaa, mutta vaikea arvata.
- Älä kirjoita salasanoja muistiin tai säilytä sellaisessa paikassa, mistä ne ovat helposti löydettävissä.
- Älä käytä työnantajan antamaa käyttäjätunnusta ja salasanaa internet-palveluihin rekisteröityessäsi tai niitä käyttäessäsi.

4 Tietojen ja asiakirjojen käsittely

- Ole erityisen huolellinen salassa pidettävän tiedon, kuten potilastiedon käsittelyssä.
- Muista, että voit käyttää ja käsitellä potilastietoja tai muita salassa pidettäviä tietoja vain työtehtäviesi hoitamisessa. Esimerkiksi potilasrekisterin tietojen käyttötarkoituksen vastainen käyttö on lainvastaista. Käyttötarkoitus on kuvattu potilasrekisteriselosteessa. Huomioi myös, että tietojärjestelmien käyttöä valvotaan.
- Kun käsittelet salassa pidettävää tietoa, huolehdi, etteivät sivulliset näe tietoja asiakirjoistasi tai tietokoneesi näytöltä. Varo syöttämästä salasanojasi siten, että joku ”näkee” salasanan sormiesi liikkeistä.
- Varo antamasta viattomankin oloisten keskustelujen yhteydessä sivulliselle potilastietoja tai muuta salassa pidettävää tietoa. Ole tarkka etenkin erilaisissa internetissä toimivissa sosiaalisen median palveluissa. Muista, että myös tieto sairaanhoitopalveluiden käytöstä on salassa pidettävä tieto.
- Ohjaa tietojen luovutus- ja tutkimuspyynnöt vastuuhenkilölle, jonka tehtävänä on varmistua tietojen luovutuksen perusteista sekä päättää luovutuksesta. Ellet tiedä oikeaa tahoa, ota yhteys esimieheesi.
- Varo toimisto-ohjelmilla (esim. tekstinkäsittely, esitysgrafiikka, taulukkolaskenta, PDF) tehtyjen tiedostojen piiloon jääviä tietoja (ns. meta-, jäännös- ja piilotiedot) erityisesti lähettäessäsi tiedostoja Raision kaupungin ulkopuolelle tai siirtäessäsi niitä tietovälineellä. Tiedosto voi sisältää siinä aiemmin ollutta tietoa tai muuta järjestelmässä olevaa tietoa, vaikka se ei näytöllä näkyisikään.
- Tarkista Raision kaupungin ulkopuolelta tuotu muistitikku, CD-/DVD-levy tai muu tietoväline haittaohjelmien torjuntaohjelmalla ennen käyttöä, ellei torjuntaohjelma suorita sitä automaattisesti.
- Jos joudut lähettämään salassa pidettävää aineistoa sähköpostilla, salaa se sähköpostin salaamisesta annetun ohjeen mukaisesti. Varmistu vastaanottajan oikeudesta lukea aineistoa sekä sen perille menosta.
- Telekopiota (faxia) voi poikkeustapauksissa käyttää salassa pidettävän aineiston lähettämiseen. Varmistu tällöin, että vastaanottaja on paikalla.
- Vältä tulostamista ja kopiointia. Ylimääräiset kopiot, väliversiot ja epäkelvot kappaleet (kustannus- ja ympäristövaikutusten ohella) lisäävät tiedon vääriin käsiin joutumisen vaaraa. Varmista, mihin tulostimeen tulostat ja missä tulostin sijaitsee. Hae tulosteesi verkkotulostimesta heti tulostuksen jälkeen.
- Kun hävität salassa pidettäviä tietoja, käytä aina Raision kaupungin omia silppureita tai lukollisia tietosuojajätesäiliöitä.
- Selvitä itsellesi tietojen ja asiakirjojen käyttöä, luovutusta, käsittelyä ja arkistointia koskevat säännöt ja rajoitukset.

© Grafiant / Antti Laitinen 2010

5 Internetin ja sähköpostin käyttö

Internet ja viestintäratkaisut (sähköposti, kalenteri, pikaviestintä, sähköiset kokouspalvelut) ovat hyviä työvälineitä tiedon hakuun ja työskentelyyn ajasta ja paikasta riippumatta. On kuitenkin muistettava, että sähköpostissa tai internetissä ei itsessään ole mitään suojausta, vaan tiedot liikkuvat salaamattomana julkisessa verkossa. Internetin ja viestintäratkaisuiden käyttö vaativatkin käyttäjältä huolellisuutta.

- Internet ja viestintäratkaisut ovat työpaikalla tarkoitettu työkäyttöön. Käytä henkilökohtaiseen viestintään yksityistä vapaa-ajan sähköpostia.
- Omia henkilökohtaisia tiedostoja ei saa tarpeettomasti tallentaa työnantajan päätelaitteisiin tai palvelimille.
- Käytä vain sellaisia palveluita, jotka tiedät turvallisiksi ja joiden käytön Raision kaupunki on sallinut.
- Pääsääntöisesti ohjelmien lataaminen internetin kautta ja asentaminen on kiellettyä. Jos tarvitset tiettyä ohjelmaa työtehtäviesi hoitamiseen, pyydä ATK-helpiä asentamaan se.
- Työsähköpostia saa käsitellä vain Raision kaupungin omistamilla laitteilla tai kaupungin etäkäyttöyhteyden kautta.
- Työhön liittyvä sähköposti vastaanotetaan ja ohjataan Raision kaupungin sähköpostijärjestelmään. Sitä ei saa ohjata tai jatko lähettää automaattisesti Raision kaupungin sähköpostijärjestelmän ulkopuolelle.
- Sähköinen kirjeenvaihto potilaan kanssa ei ole sallittua muuta kuin salatun sähköpostin kautta. Potilastietoja ei tule lähettää sähköpostin kautta.
- Sähköpostin liitetiedostot voivat sisältää haittaohjelmia. Varo kaikkia epätavallisia sähköposteja ja erityisesti liitetiedostoja. Älä avaa epäilyttäviä viestejä. Tarvittaessa voit ilmoittaa asiasta atk-tukeen.
- Roskapostia voivat olla esim. sähköpostiin tilaamatta tulleet mainokset. Roskapostiin ei vastata, vaan se pitää poistaa.
- Suhtaudu terveen epäluuloisesti sähköpostiviestin luotettavuuteen. Sähköpostiviesti voi tulla myös muualta kuin viestin lähettäjäkentässä näkyvältä taholta. Varo ns. ”kalasteluviestejä”, joissa sinua pyydetään syöttämään tunnuksia ja salasanoja aidontuntuisiin palveluihin. Vältä myös napauttamasta sähköpostiviesteissä olevia linkkejä, jos et tiedä minne kyseinen linkki johtaa tai jos viesti ei liity työtehtäviisi.
- Älä välitä ketjukirjeitä eteenpäin.

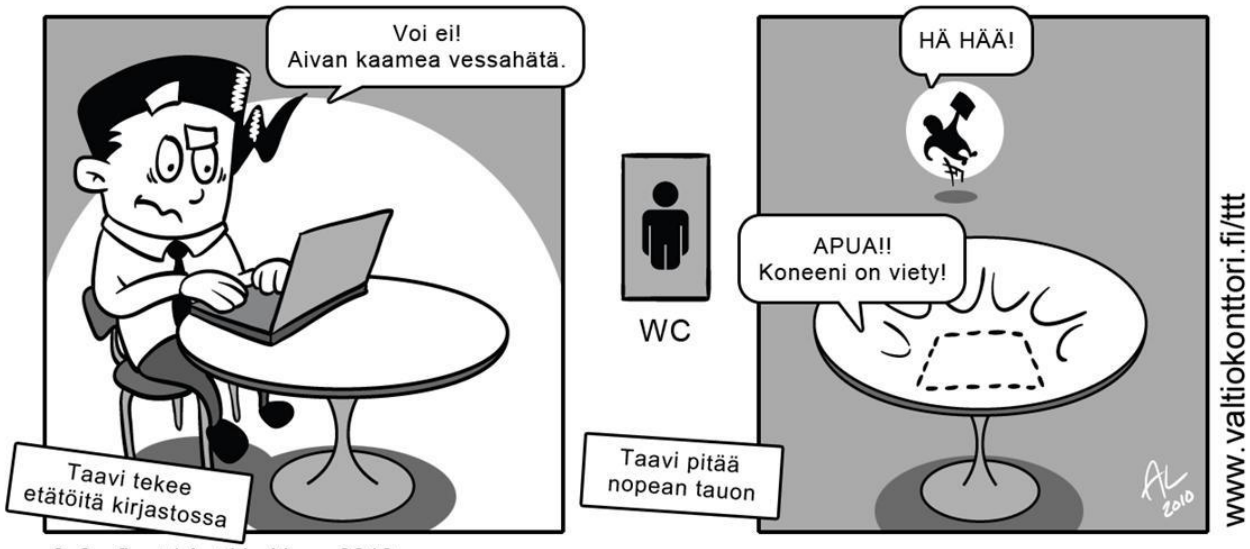
- Jos saat toiselle henkilölle kuuluvan sähköpostin, ohjaa viesti oikealle vastaanottajalle ja ilmoita lähettäjälle vastaanottajan oikea sähköpostiosoite. Jos oikea osoite ei ole tiedossa, ilmoita virheellisestä lähetyksestä lähettäjälle. Muista, että sinulla on vaitiolovelvollisuus saamastasi viestistä.
- Jakelulista on henkilöluettelo (sähköpostiosoitteita), jonka jokainen vastaanottaja saa tietoonsa. Se voi olla henkilörekisteritieto tai salassa pidettävä tieto, jonka luovuttamisesta on erikseen säädetty. Voit käyttää sähköpostin piilokopiotoimintoa, jos haluat estää sähköpostin jakelussa olevien osoitteiden näkymisen vastaanottajille.
- Huolehdi, että lähettämäsi sähköpostiviesti on kohdistettu oikeille henkilöille ja oikeisiin osoitteisiin, myös valmiita jakelulistoja käyttäessäsi. Vältä turhien sähköpostien lähettämistä. Ennen kuin napautat Lähetä–painiketta, varmista että Vastaanottaja ja mahdollisissa Kopio sekä Piilokopio–kentissä olevat vastaanottajat ovat juuri ne henkilöt, joille tarkoituksesi on viesti lähettää.
- Työsuhteen päättyessä sähköpostiosoite ja -laatikko poistetaan. Siirrä käsittelyä edellyttävä työpostisi työnantajan käyttöön ja poista mahdolliset henkilökohtaiset viestit.
- Virkavapaan tai työloman ajaksi käytäntönä on että tunnukset suljetaan poissaolon ajaksi.
- Huomioi, että tietojärjestelmiin ja tietoverkon laitteisiin tallentuu yksityiskohtaista lokitietoa järjestelmien käytöstä, sähköpostiliikenteestä ja internet-selauksesta. Tietoja käytetään ylläpidossa, vianmäärityksessä ja tietoturvallisuuden valvonnassa. Väärinkäytöksiin voidaan puuttua.
- Olet vaitiolovelvollinen myös vahingossa saamistasi viesteistä tai kuulemistasi asioista.
- Ohjaa sähköisesti asioivat asiakkaat lähettämään käsittelyyn tulevat ja vireille saatetut asiat organisaation määrittelemään sähköpostiin, asiointipalveluun tai muuhun vastaavaan sähköiseen palveluun. Raision kaupungin virallinen sähköpostiosoite on raision.kaupunki(at)raisio.fi

Muista, että aina kun käytät Raision kaupungin laitteita, verkkoa tai sähköpostia, esiinnyt tietoverkossa kaupungin edustajana.

6 Etätyöskentely, liikkuva työ ja matkatyö

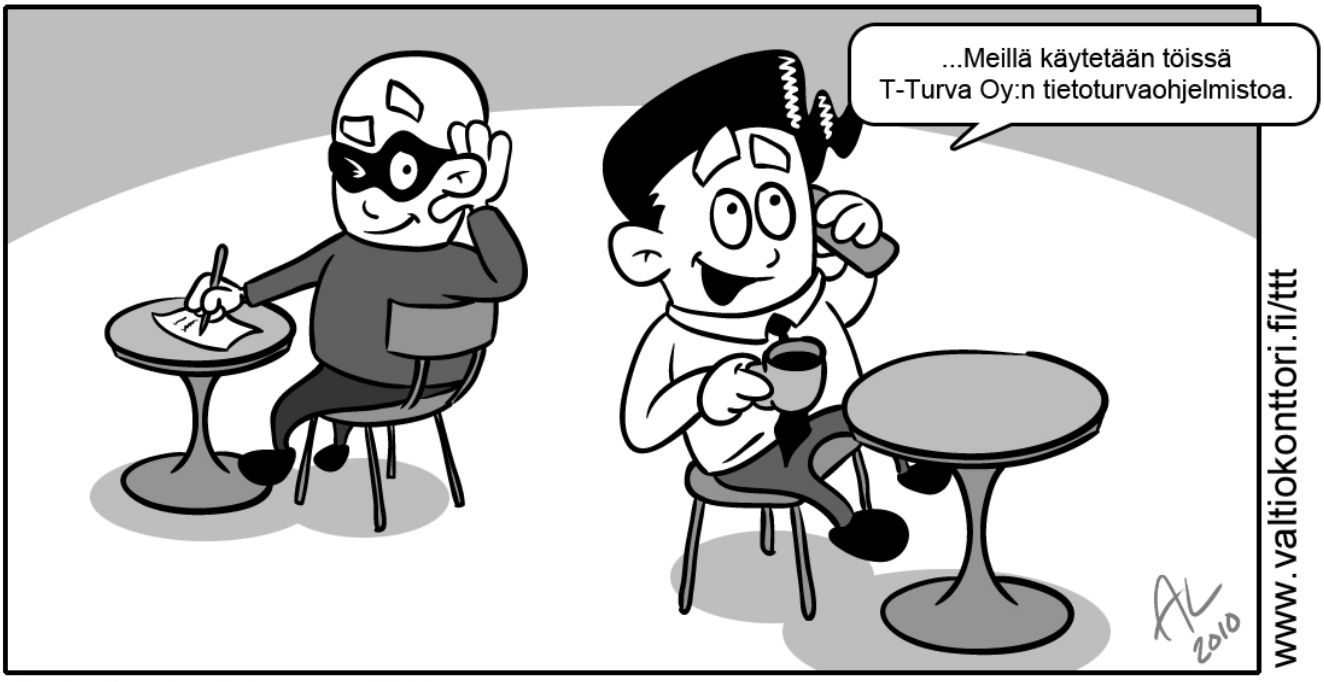
Etätyöllä tarkoitetaan muualla kuin organisaation vakituisessa toimipisteessä tehtävää työtä, jolloin käyttöympäristöt vaihtelevat eikä ympäristön turvallisuuteen voida juurikaan vaikuttaa. Etätyöntekijän omilla toimenpiteillä ja menettelytavoilla on tällöin suuri merkitys. Etäyhteys on tietoliikenneyhteys organisaation sisäverkon ulkopuolelta ja etäkäyttö tietoteknisten palvelujen käyttöä etäyhteyden avulla. Etätyöntekijän on kyettävä tekemään itsenäiset arviot etätyöympäristön turvallisuudesta.

- Kiinnitä kaikessa toiminnassasi huomiota tietoturvallisiin menettelytapoihin. Erityisen tärkeää tämä on silloin, kun toimit vakituisen työpisteen ulkopuolella. Etätyössä sinun tulee noudattaa soveltuvin osin kaikkia samoja turvallisuusperiaatteita kuin ollessasi kaupungin varsinaisissa toimitiloissa.
- Huolehdi, että etätyössä käyttämäsi laitteistot, ohjelmistot, tietoliikenneyhteydet ja paperiaineistot ovat ja pysyvät vain sinun käytössäsi.
- Huolehdi, että käyttämäsi käyttäjätunnukset, salasanat, toimikortit, PIN-koodit ja muut tunnistusvälineet ovat vain sinun hallussasi ja tiedossasi.
- Kuljeta mukanasi vain välttämätön määrä tietoaineistoa ja varmistu aina aineiston asianmukaisesta suojauksesta.
- Älä lataa tai asenna laitteisiin mitään työhön kuulumatonta.
- Käytä tietojen salausta silloin kun sitä edellytetään.



Matkoilla, julkisissa kulkuneuvoissa, nettikahviloissa…

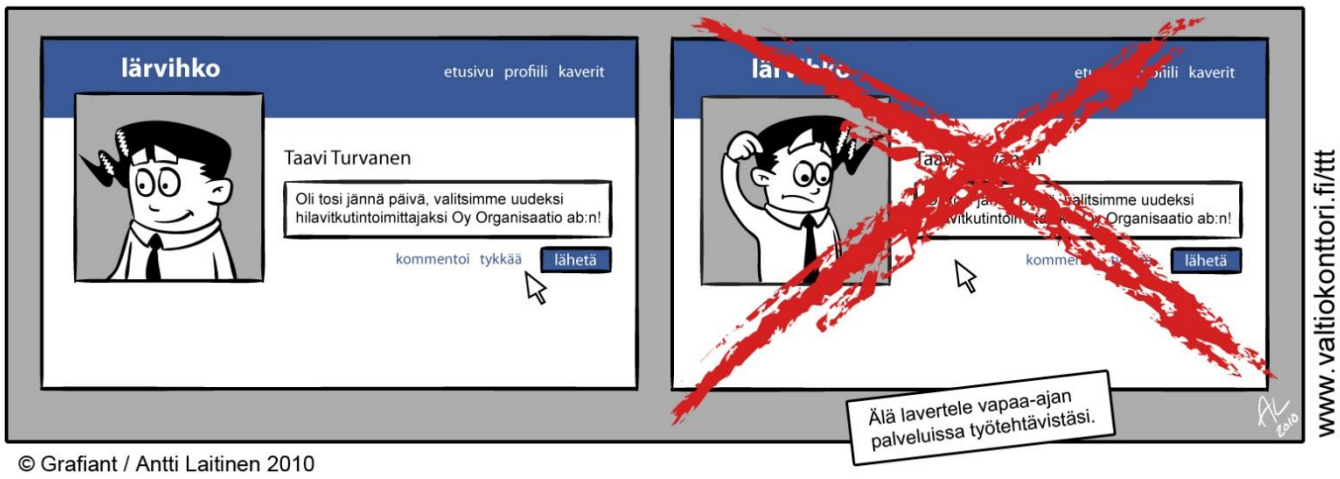
- Vältä puhumasta luottamuksellisista työasioista julkisilla paikoilla ja kulkuvälineissä ml. henkilötiedot.
- Jos työskentelet julkisissa tiloissa, varmistu, etteivät muut henkilöt pysty kurkistamaan ja näkemään käsittelemiäsi tietoja ja asiakirjoja. Voit käyttää tarvittaessa näyttösuojaa.
- Säilytä tieto ja laitteet turvallisessa paikassa. Älä jätä kannettavaa tietokonetta tai puhelinta ilman valvontaa. Muista myös tietovälineiden, paperitulosteiden ym. asianmukainen säilyttäminen.
- Älä käytä julkisia päätteitä (esim. nettikahvilat, kirjastot) työasioihin. Et voi vaikuttaa siihen, mitä tietoja käytöstäsi kerätään ja mitä tiedoilla tehdään. Yleensä sinulla ei myöskään ole mahdollisuutta poistaa näitä tietoja laitteelta.



7 Sosiaalinen media

Sosiaalisen median palvelut sisältävät samanlaisia uhkia ja riskejä kuin muutkin perinteiset internetin kautta käytettävät palvelut, mutta erityisesti tietosuojaan, henkilön yksilöivään tietoon liittyvät asiat nousevat näissä palveluissa esille.

1. Noudata Raision kaupungin **ohjetta sosiaalisen median käyttämisestä**.
2. Jos mainitset sosiaalisen median palvelun henkilöprofiilissasi työnantajasi, esiinnyt tällöin Raision kaupungin epävirallisena edustajana. Muista käyttäytyä sen mukaisesti!
3. Varo syöttämästä liian henkilökohtaista tai yksityiskohtaista tietoa, valokuvia tai muuta materiaalia itsestäsi. Huomaa, että palvelun tarjoaja voi hyödyntää profiiliisi syöttämiäsi tietoja laajasti.
4. Huomioi, että palvelun ylläpitäjät pääsevät käsiksi kaikkeen palvelussa käsiteltävään tietoon, myös kahdenvälisiin keskusteluihin. Internetverkkoon päätynyttä tietoa voi olla mahdotonta poistaa jälkikäteen.
5. Tutustu huolellisesti käyttämiesi palveluiden sopimusehtoihin.
6. Tarkista käyttäjäprofiilin yksityisyyden suojaa koskevat asetukset ja muuta niitä tarvittaessa siten, että tietosi eivät leviä laajemmalle kuin haluamallesi käyttäjäjoukolle. Esim. hae tietoja nimelläsi ja säädä palveluiden yksityisyydensuoja-asetuksia tarvittaessa tiukemmiksi. Voit pyytää samaa palvelua käyttävää kaveria tarkistamaan miltä tietosi ja profiilisi näyttävät.
7. Kunnioita perheesi ja ystäviesi suhtautumista sosiaalisiin medioihin. Vaikka olisit itse niistä innostunut, eivät kaikki sitä kuitenkaan ole. Jos kanssaihmisesi eivät halua sinun laittavan kuvia tai tietoa heistä sosiaaliseen mediaan, noudata heidän toiveitaan.
8. Älä hyväksy tuntemattomia yhteydenottoyrityksiä verkostoosi äläkä napsauta vieraita, hämäräperäisiä linkkejä.
9. Älä keskustele työasioista muissa kuin työtehtäviin hyväksytyissä sosiaalisissa medioissa. Ole erityisen huolellinen salassa pidettävän tiedon suhteen.
10. Jos epäilet, että olet joutunut huijatuksi tai muun hyökkäyksen kohteeksi, älä epäröi pyytää apua. Älä jätä tekemättä asiasta rikosilmoitusta, vaikka taloudellinen menetys saattaa osaltasi jäädä vaatimattomaksi.



© Grafiant / Antti Laitinen 2010

Sosiaalinen media on ensisijaisesti tarkoitettu julkisten asioiden käsittelyyn ja keskusteluun.

8 Havaitsitko ongelman?

Sinulla on aina velvollisuus kertoa, jos sinulla on ongelmia tietoturvallisuusasioissa.
Ajantasaiset ohjeet ja yhteystiedot löydät Raitilta

- Jos hallussasi oleva kulkuavain, muut avaimet tai henkilökortti katoaa tai varastetaan, ilmoita siitä välittömästi esimiehelle.
- Jos päätelaitteesi katoaa tai varastetaan, ilmoita siitä välittömästi atk-tukeen.
- Jos VRK-korttisi katoaa, tee välittömästi katoamisilmoitus VRK-korttien sulkupalveluun soittamalla numeroon: 0800 162 622.
- Ilmoita aina haittaohjelmista (esim. virushälytys päätelaitteella) ja muista tietoturvallisuuteen liittyvistä ongelmista **välittömästi** atk-tukeen ja omalle esimiehellesi.

Jos epäilet tietoturvaloukkausta tai haittaohjelmatartuntaa:
- Älä hätiköi.
- Älä sulje päätelaitetta, mutta irrota lähiverkkokaapeli tai katkaise langaton (wlan/3/4G) yhteys työasemastasi.
- Kirjoita ylös, mitä mahdollisessa ilmoituksessa tai varoituksessa luki tai ota siitä kuva kännykälläsi.
- Ota yhteyttä atk-tukeen ja/tai tietoturvavastaavaan. Auta tutkinnassa. Kerro mitä olit tekemässä, kun kone alkoi toimia odottamattomasti. Toimi saamiesi ohjeiden mukaisesti.

Lakien, määräysten ja ohjeiden rikkomisen seurauksena käyttöoikeudet tietojärjestelmiin voidaan peruuttaa. Rikkomuksista tiedotetaan aina esimiehellesi. Vakavissa tapauksissa väärinkäyttö voi johtaa myös vahingonkorvausvaatimuksiin tai rikosoikeudellisiin seuraamuksiin. Seurauksena voi olla myös työsuhteen päättäminen.

9 Tietoturvaohjeistus ja koulutus

Raision kaupungin henkilöstö on velvoitettu suorittamaan tietoturvan ja – suojan koulutuksia:

THL: Tietoturva ja tietosuoja terveydenhuollossa – opiskelukokonaisuus
- Jokainen työntekijä käy läpi THL:n verkkokoulutuksen.
- https://verkkokoulut.thl.fi/web/kanta/tietoturva/sisallot

10 Tietoturvallisuus osana toiminnan laatua

10.1 Mitä tietoturvallisuudella tarkoitetaan?

Tietoturvallisuus on osa organisaation toiminnan laatua. Tietoturvajärjestelyjen tarkoituksena on varmistaa tietoaineistojen, tietojärjestelmien ja palveluiden asianmukainen suojaus siten, että niiden luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvät riskit otetaan huomioon. Käytännössä tämä merkitsee mm. sitä, että tiedot ja tietojärjestelmät pidetään vain niiden käyttöön oikeutettujen saatavilla. Sivullisille ei anneta mahdollisuutta käsitellä, muuttaa tai poistaa tietoja. Tietojen käsittelyyn oikeutetutkin saavat käyttää tietoja ja järjestelmiä vain asianmukaisesti työtehtävissään. Tietojen, järjestelmien ja palveluiden on oltava luotettavia, oikeita ja ajantasaisia. Ne eivät saa paljastua, muuttua tai tuhoutua hallitsemattomasti asiattoman toiminnan, haittaohjelmien, laitteisto- tai ohjelmistovikojen tai muiden vahinkojen, tapahtumien tai häiriötilanteiden vuoksi. Tietojen, järjestelmien ja palveluiden on myös pysyttävä toiminnassa ja oltava saatavilla silloin kun niitä tarvitaan. Etenkin sähköisissä asiointipalveluissa tarve käyttää palveluita ympärivuorokautisesti ja paikasta riippumatta on lisääntynyt, kun virkamiesten ja kansalaisten käyttötavat ovat muuttuneet. Palveluiden täytyy kyetä tunnistamaan käyttäjät luotettavasti sekä tuottamaan tarvittavaa lokia, josta tapahtumat voidaan tarvittaessa jälkikäteen selvittää.

10.2 Miksi tietoturvallisuus on tärkeää?

Tietoturvatoimenpiteillä turvataan yksilön, yhteisön ja yhteiskunnan etuja. Siksi tietoturvallisuus on yhteiskunnan toimintojen, palvelujen, sovellusten ja tietoteknisen infrastruktuurin perusedellytys. Yhteiskunnan toiminnot ovat suurelta osin riippuvaisia tietojen käsittelystä ja siirrosta. Verkottuneessa toimintaympäristössä harva organisaatio on enää vastuussa yksinomaan omasta tietoturvallisuudestaan. Tietoturvallisuudesta huolehtiminen on jokaisen organisaatiossa työskentelevän velvollisuus. Suurimmat tietoturvallisuuden ongelmat liittyvät yleisesti kiireeseen, huolimattomuuteen, osaamattomuuteen sekä muihin tietojärjestelmien toteutuksen ja käytön laadullisiin tekijöihin. Tietoturvallisuus on juuri niin hyvä kuin sen heikoin lenkki. Tämä ei koske vain tekniikkaa, vaan myös jokapäiväiset toimintatapamme ja asenteemme vaikuttavat – vahvin lenkki on oikealla tavalla toimiva yksilö! Puutteellinen tietoturvallisuus vaarantaa valtion, kansalaisten, yhteisöjen ja asiakkaiden etuja sekä aiheuttaa lisätyötä ja -kustannuksia. Tietoturvallisuutta kehittämällä parannetaan toimintojen luotettavuutta ja jatkuvuutta. Mitä paremmin häiriötilanteiden hallinta on otettu huomioon organisaation toiminnassa, sitä nopeammin toiminta saadaan palautettua vakiotasolle ja tiedotettua häiriöstä asiakkaille.

10.3 Lainsäädäntö tietoturvallisuuden perustana

Sairaanhoitopiirissä käsitellään runsaasti sekä julkista että salassa pidettävää tietoa. Julkisuuslainsäädännön mukaan tieto on julkista, ellei se julkisuuslain tai muiden säädösten perusteella ole erikseen määrätty salassa pidettäväksi. Suomen lainsäädännössä on paljon tietoturvavelvoitteita – toisin sanoen myös lainsäädäntö lähtee siitä, että tietoturvallisuus on hoidettava asianmukaisesti. Tietoturvallisuus perustuu viranomaisten toiminnan julkisuudesta annetun lain (621/1999) ja asetuksen (1030/1999) lisäksi useisiin muihin lakeihin. Yksityiselämän suoja ja julkisuusperiaate ovat jo perustuslaissa säädeltyjä perusoikeuksia. Tietojen lainmukaisesta käsittelystä on aina huolehdittava.

Joitakin keskeisiä laeissa asetettuja tietoturvavelvoitteita ovat:

- “Viranomaisen tulee hyvän tiedonhallintatavan luomiseksi ja toteuttamiseksi huolehtia asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen asianmukaisesta saatavuudesta, käytettävyydestä ja suojaamisesta sekä eheydestä ja muista tietojen laatuun vaikuttavista tekijöistä.” (Laki viranomaisten toiminnan julkisuudesta 18 §, Hyvä tiedonhallintatapa)
- “Rekisterinpitäjän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä.” (Henkilötietolaki 32 §, Tietojen suojaaminen)

Tietoturvallisuuteen keskeisesti liittyvien säädösten luettelo on listattu luvussa 10.6.

10.4 Kyberturvallisuus keskittyy yhteiskunnan toimivuuden takaamiseen

Suomen kyberturvallisuusstrategia julkaistiin tammikuussa 2013. Kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa sähköisessä muodossa olevaan tiedonkäsittelyyn tarkoitettuun, yhdestä tai useammasta tietojärjestelmästä koostuvaan, palveluun tai ICT-järjestelmään voidaan luottaa ja jossa sen toiminta turvataan (= kybertoimintaympäristö). Tämä edellyttää myös sitä, että tiedonkäsittelyyn liittyvät fyysiset rakenteet suojataan tarkoituksenmukaisesti. Kyberturvallisuus keskittyy ensisijaisesti yhteiskunnan toimivuuden kannalta elintärkeiden toimintojen kokonaisvaltaiseen suojaamiseen (esimerkiksi sähkönjakelu, kriittisten tietoliikenneyhteyksien ylläpito), kun tietoturvallisuus keskittyy tietojen luottamuksellisuuden, eheyden ja saatavuuden varmistamiseen. Kyberturvallisuus käsittää yhteiskunnan elintärkeisiin toimintoihin ja kriittiseen infrastruktuuriin kohdistuvat toimenpiteet, joiden tavoitteena on hallita
ennakoivasti ja tarvittaessa sietää kyberuhkia ja niiden vaikutuksia. Kyberuhkien toteutuminen voi aiheuttaa merkittävää haittaa tai vaaraa Suomelle tai sen väestölle. Kyberturvallisuuteen liittyy myös sotilaallista tiedustelu- ja vaikuttamiskykyä, joka tarkoittaa kyberpuolustuksen kehittämistä osana muun sotilaallisen voimankäytön kehittämistä. Tästä päävastuu on puolustusvoimilla.

Siinä missä tietoturvallisuus keskittyy tietoaineistojen suojaamiseen, kyberturvallisuus kattaa kaiken infrastruktuurin tuottamisessa tarvittavat osa-alueet. Pääpaino kyberturvallisuuden puolella on tietoverkkojen kautta tulevien uhkakuvien pienentämisessä ja torjumisessa. Lisätietoa löydät esimerkiksi yhteiskunnan turvallisuusstrategiasta ja Suomen kyberturvallisuusstrategiasta.

10.5 Kohdistetut hyökkäykset

Viestintävirasto on tiedottanut kohdistetuista hyökkäyksistä 5.8.2011 Tietoturva nyt -artikkelissa seuraavaa:
”Kohdistettu hyökkäys on tiettyyn toimijaan tai toimijajoukkoon suunnattu kohteen erityispiirteet huomioiva tietoturvaloukkaus. Hyökkääjä valikoi kohteensa tarkasti tämän hallussa olevien tietoaineistojen tai muiden vastaavien seikkojen perusteella. Hyökkääjän motiivina voi olla esimerkiksi yritysten tai valtioiden arkaluontoisten tietojen varastaminen. Kohteiden valikoimisesta johtuen hyökkäyksestä voi aiheutua merkittäviä vahinkoja. Kohdistettu hyökkäys käynnistyy usein lähettämällä kohteelle räätälöity sähköpostiviesti. Sähköpostissa on haitallista koodia sisältävä liitetiedosto tai linkki haittaohjelmaa levittävälle web-sivustolle. Jos käyttäjä avaa liitetiedoton tai seuraa linkkiä, voi haittaohjelma saastuttaa hänen koneensa. Asennuttuaan haittaohjelma ottaa yhteyden hyökkääjän ylläpitämään haittaohjelman ohjaamiseen käytettävään komentopalvelimeen. Tämän jälkeen hyökkääjällä on käytännössä suora tietoliikenneyhteys hyökkäyksen kohteena olevaan tietokoneeseen. Hyökkääjä voi kerätä tietoja kohteen tietokoneelta ja mahdollisesti laajentaa hyökkäystä kohteen sisäverkon muihin osiin. Joissain tapauksissa hyökkäyksiä on yritetty ulottaa julkisesta verkosta irrallisiin tietokoneisiin saastuttamalla tiedonsiirtoon käytettyjä USB-tikkuja. Hyökkääjä pyrkii räätälöimään sähköpostiviestin sellaiseksi, että vastaanottaja pitää viestiä mahdollisimman luotettavana ja päivittäiseen toimintaan liittyvänä. Usein sähköpostin lähettäjätiedot on väärennetty siten, että viesti näyttäisi tulevan kohteen kollegalta tai muulta luotetulta osapuolelta. Joissakin hyökkäyksissä on myös hyödynnetty luotetuilta tahoilta kaapattuja sähköpostitilejä. Hyökkääjä voi myös yrittää huijata vastaanottaja avaamaan liite lähettämällä ensin vaarattoman tiedoston liitteenä ja heti perään ”korjatun”, esim. haittaohjelmaa sisältävän PDF-tiedoston.”

Miten kohdistetun hyökkäyksen voi välttää?

- ole erityisen varovainen, jos saat vieraskielisen sähköpostiviestin, jonka mukana on liitetiedosto tai linkki ulkoiselle www-sivustolle, vaikka lähettäjä olisi hyvin tuntemasi henkilö, vaikka viestin asiasisältö vaikuttaa tai liitetiedoston nimi ja tyyppi vaikuttavat työtehtäviisi liittyviltä
- uusimmat kohdistetut hyökkäykset tapahtuvat suomenkielellä, joten ole huolellinen aina avatessasi organisaation ulkopuolelta saapuvia myös suomenkielisiä liitetiedostoja
- pyydä tarvittaessa organisaatiosi tietohallintoa tutkimaan saamasi epäilyttävä liitetiedosto ennen sen avaamista – noudata tässä organisaatiosi ohjeistusta.

10.6 Tietoturvallisuuteen keskeisesti liittyvät säädökset

Eri lakeihin sisältyvien salassapitosäännösten lisäksi laeista tärkeimpiä ovat:

- Suomen perustuslaki (731/1999) 2.luku 10 §: Yksityiselämän suoja ja luottamuksellisen viestin salaisuus
- Suomen perustuslaki (731/1999) 2.luku 12 §: Viranomaisten hallussa olevien asiakirjojen ja tallenteiden julkisuus
- Laki viranomaisten toiminnan julkisuudesta (621/1999)
- Asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintotavasta(1030/1999)
- Laki kunnallisesta viranhaltijasta (304/2003)
- Työsopimuslaki (55/2001)
- Arkistolaki (831/1994): Asiakirjojen laatiminen, säilyttäminen ja käyttö
- Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004): Arkaluonteiset kansainväliset asiakirjat
- Henkilötietolaki (523/1999): Henkilötietojen käsittelyä koskevat yleiset periaatteet
- Laki turvallisuusselvityksistä (177/2002): Henkilöiden taustat
- Laki yksityisyyden suojasta työelämässä (759/2004): Työntekijää koskevien henkilötietojen käsittely
- Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003): Tietoturvallisuus asioinnissa ja viranomaisten keskinäisessä tietojenvaihdossa
- Laki sähköisistä allekirjoituksista (14/2003)
- Sähköisen viestinnän tietosuojalaki (516/2004): Sähköisen viestinnän luottamuksellisuus ja yksityisyyden suoja
- Rikoslaki (39/1889) 34.luku 9a §: Vaaran aiheuttaminen tietojenkäsittelylle
- Rikoslaki (39/1889) 38.luku 8 §: Tietomurto
- Rikoslaki (39/1889) 38.luku 9 § 1. kohta: Henkilötietorikos
- Henkilötietolaki (523/1999) 48 §: Henkilörekisteririkkomus
- Vahingonkorvauslaki (41/1974)
- Valtioneuvoston periaatepäätös Suomen kyberturvallisuusstrategiasta

Uudistuvat säädöstekstit löytyvät ajantasaisina mm. Valtion säädöstietopankki –sivustolta (www.finlex.fi).

Lisää tietoa tietoturvasta:
- Lainsäädäntö – Valtion säädöstietopankki (www.finlex.fi)
- Tietoturvallisuutta ohjeistavat ja säätelevät organisaatiot, esimerkiksi
- Valtiovarainministeriön VAHTI-ohjeet (www.vm.fi/vahti, www.vahtiohje.fi)
- Arkistolaitoksen ohjeet (www.narc.fi)
- Tietosuojavaltuutetun toimiston ohjeet (www.tietosuoja.fi)
- Tietoyhteiskunnan kehittämiskeskuksen ohjeet (www.tieke.fi)
- Viestintäviraston ohjeet (www.ficora.fi)
- Julkishallinnon ja elinkeinoelämän yhteiset ohjeet (www.tietoturvaopas.fi)
- Valtiokonttorissa toimivan Valtion IT-palvelukeskuksen tietoturvasarjakuvat (www.valtiokonttori.fi/ttt)

Tietoturvan ja tietosuojan huoneentaulu

1.
Noudata annettuja tietoturvaohjeita ja -käytäntöjä.

2.
Lukitse tietokoneesi/ohjelmistot tai kirjaudu niistä ulos aina kun poistut sen läheisyydestä. Pyri käyttämään eri salasanaa eri järjestelmissä. Säilytä salasanat ja muut kirjautumisessa käytettävät tunnisteet, kuten toimikorttisi ja PIN-koodi huolellisesti.

3.
Varo paljastamasta luottamuksellisia tietoja sivullisille työpaikalla tai sen ulkopuolella esim. sosiaalisessa mediassa.

4.
Älä surffaa arveluttavilla nettisivuilla. Älä avaa outoja sähköpostiviestejä tai niiden liitteitä.

5.
Huolehdi papereiden, muistitikkujen, CD-/DVD-levyjen, puhelinten, salasanojen, avainten, kulkunappien, toimikorttien ym. asianmukaisesta käsittelystä ja säilyttämisestä.

6.
Hävitä tietosuojattava jäte asianmukaisesti.

7.
Huolehdi erityisesti etätyössä kannettavan tietokoneen ja sen tietojen suojaamisesta. Hanki kannettavaan tietokoneeseen suojakalvo, joka estää sivulta tapahtuvan salakatselun.

8.
Muista kunnioittaa potilaiden, asiakkaiden ja työkavereiden yksityisyyttä.
Näin ylläpidät luottamusta.

9.
Kerro esimiehellesi, mikäli havaitset tietoturva- tai tietosuojarikkomuksia.

10.
Älä hätäänny, jos jotain poikkeavaa tapahtuu. Soita rohkeasti atk-tukeen.