Sisällys

Liite 1 Tietosuojan periaatteet tarkemmin avattuna
Liite 2 PTTK-ohje-Sähköpostin käyttöohjeistus
Liite 3 Keskeistä tietosuojaan ja tietoturvaan liittyvää sanastoa
Liite 4 Tietoturvan ja tietosuojan huoneentaulu
Liite 5 Esimiehen vastuut tietosuojasta

Johdanto

Tietoturvallisuus perustuu lainsäädäntöön ja normiohjaukseen. Vastuu tietoturvallisuudesta ja siihen liittyvä osaaminen, kuuluu omalta osaltaan jokaiselle, myös Sinulle. Tietoturva- ja tietosuoja-asioiden hallintaa voidaan pitää kaikille kuuluvana ”kansalaistaitona”, josta on hyötyä myös joka päiväisessä elämässä.

EU:n tietosuojauudistus on edellyttänyt 25.5.2018 alkaen, että organisaatiossa on nimetty tietosuojavastaava ja että henkilöstö osallistuu tarjottuun koulutukseen ja sisäistää tietosuoja- ja tietoturvaohjeet ja toimii niiden mukaisesti.

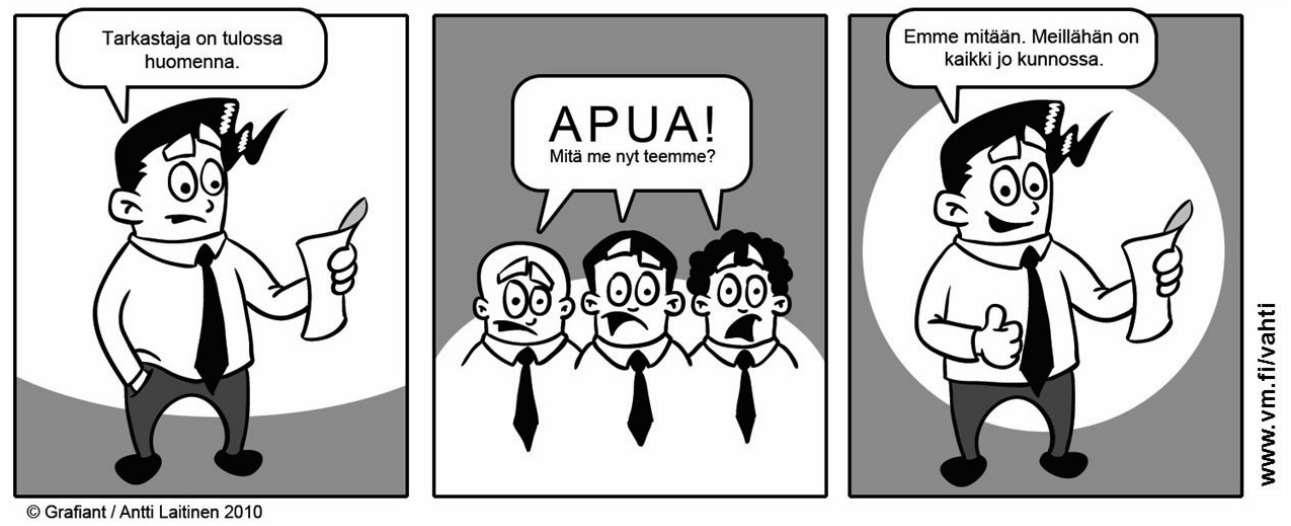
Tämä henkilöstön tietoturva- ja tietosuojaopas on tarkoitettu Lieksan kaupungin henkilöstölle sekä niiden tietoja ja tietojärjestelmiä tai toimitiloja käyttäville henkilöille kuten ulkopuoliset palveluntuottajat, opiskelijat, työharjoittelijat, siviilipalvelusmiehet ja tutkijat.

Oppaan tarkoitus on nostaa henkilöstön tietoturva- ja tietosuojatietoisuutta ja täten edesauttaa jokaista huolehtimaan omalta osaltaan sen toteuttamisesta.

Oppaaseen on koottu keskeisiä tietoturvaan ja tietosuojaan liittyviä perusasioita. Se antaa neuvoja tietosuojan ja -turvallisuuden toteuttamiseen omassa työssä ja muissa käytännön tilanteissa. Lieksan kaupungin tietosuoja- ja tietoturvaohjeet perustuvat Lieksan kaupungin tietosuoja- ja tietoturvapolitiikkaan. Huomioithan että olet tutustunut myös muuhun tietosuojaa ja tietoturvaa käsittelevään dokumentaatioon ja työalaasi koskevaan lainsäädäntöön. Oman organisaation dokumentaatio on kerrottu luvussa 10.1.

Oppaan tekstien joukkoon ja loppuun on lisätty hyödyllisiä linkkejä, joihin kannattaa perehtyä huolellisesti. Oppaan lopussa olevat tiedot ovat myös huomion arvoisia.

Antoisia lukuhetkiä!



Noudatettavat tietoturvan ja tietosuojan periaatteet

1. Mitoitettava ja järjestettävä käyttöympäristö ja resurssit siten, että toiminta on tehokasta ja se edistää tietoturvan ja tietosuojan toteutumista kunnan eri toiminnoissa.
2. On turvattava tärkeiden tietojärjestelmien ja tietoverkkojen häiriötön toiminta.
3. On varmistettava, että toiminnassa käytettävä tieto on oikeaa, ajantasaista, luotettavaa ja sitä käsitellään lainmukaisesti.
4. Julkinen tieto on helposti löydettävissä ja käytettävissä.
5. On turvattava rekisteröidyn laissa määritellyt oikeudet.
6. On varmistettava, että tiedot eivät joudu tahattomasti tai tahallisesti asiattomien haltuun tai tuhottavaksi.
7. Varmistettava, että tietoja ja tietojärjestelmiä käyttävät vain henkilöt, joilla on niihin oikeus työtehtäviensä hoitamiseksi.
8. Noudatettava henkilötietojen käsittelyssä periaatteita, joita ovat kohtuullisuus ja läpinäkyvyys, käyttötarkoitussidonnaisuus, tietojen minimointi, täsmällisyys, säilytyksen rajoittaminen, eheys ja luottamuksellisuus. Tarkemmin henkilötietojen tietosuojan periaatteet liite 1
9. Osoitettava dokumentoinnilla, että lainmukaisuusperiaatteita on noudatettu.

Tietoturvan ja tietosuojan tavoitteet ja periaatteet on määritelty Lieksan kaupungin tietosuoja- ja tietoturvapolitiikassa, joka lisäksi määrittelee myös muita tietosuojaan ja tietoturvallisuuteen liittyviä linjauksia, asioita ja vastuita.

Tietoturvallisuuden ohjeet pähkinänkuoressa

Tiedottaminen ja koulutus

- Seuraa tietoturvallisuuteen liittyviä organisaatiosi tiedotteita, tutustu ohjeisiin ja osallistu tietoturvakoulutukseen.
- Noudata organisaatiosi tietoturvaohjeita.

Toimitilaturvallisuus

- Noudata organisaatiosi kulunvalvontaohjetta. Pidä kuvallinen henkilökorttisi
- tai muu sinulle annettu tunniste tarvittaessa esillä, jos sinulla on sellainen.
- Tarkista vieraalta henkilöltä kulkuoikeus työpaikkasi tiloissa. Kysy vierailijalta millä asialla hän on tai ketä hän etsii? Auta oikean henkilön luokse. Se on myös kohteliasta. Ohjaa asiattomat henkilöt ulos.
- Älä jätä työvälineitä valvomatta neuvottelutiloihin.
- Älä jätä vieraita yksin neuvottelu- tai työtiloihin. Saata vieraat aulaan tai ulos kokouksen jälkeen.

Päätelaitteet

- Päätelaitetta (kannettava tietokone, pöytäkone, älypuhelin, tabletti jne.) käytetään yhä useammin maksu- ja tunnistautumisvälineenä. Suojele sitä kuten lompakkoasi.
- Älä anna henkilökuntaan kuulumattoman, edes tutun, käyttää päätelaitettasi.

- Estä päätelaitteesi, esimerkiksi puhelimen, luvaton käyttö asettamalla siihen laitteen käyttöohjeen mukaiset automaattiset lukitukset. Lukitse päätelaite aina, kun poistut sen ääreltä. Tietokone lukittuu näppärästi näppäinyhdistelmillä Ctrl+Alt+Del tai (Windows-ikkuna)+L.

Tietoaineistojen käsittely

- Merkitse asiakirjaan sen salassapidosta kertova tunniste. Niitä ovat mm. ”salassa pidettävä”, ”suojaustaso” ja ”turvaluokiteltu”. Salassapitotunniste on laitettava asiakirjan etusivulle ylätunnisteeseen tai riittävän ylös, jotta se on helppo huomata. Salassapidon voi joko kirjoittaa tai leimata asiakirjaan. Merkitseminen on laatijan vastuulla.

- Käsittele (mm. tallenna, siirrä, tulosta, lähetä, kopioi, kuljeta, säilytä, arkistoi, hävitä) salassa pidettäviä tietoja siten, ettei ne ole tietoihin oikeudettomien saatavilla.
- Huomioi, että salassa pidettävää tietoa voidaan tallentaa, siirtää ja arkistoida usealla eri tallennusvälineellä ja tavalla.
- Hävitä salassa pidettävät asiakirjat Encoren tietoturva-astioihin, joita voi tarvittaessa tilata työpisteeseen. Levykkeille, jotka sisältävät salaista tietoa, on erillinen hävitysastia Pielisentie 3:ssa. Lisäohjeita salassa pidettävän aineiston hävittämisestä antaa tietosuojavastaava.

- Noudata tulostamisessa ja tulosteiden noutamisessa organisaation antamia ohjeita. Selvitä mahdollisuus tietoturvalliseen tulostukseen PIN- koodilla, kun tulostat arkaluontoisia ja salassa pidettäviä asiakirjoja. Tulostaessa henkilötietoja tai muuta salattavaa tietoa huolehdi, että olet noutamassa tulosteet välittömästi tulostimesta. Käytä salattavan tiedon tulostamiseen PIN-koodia, jos se on mahdollista ja ainakin silloin, jos tulostin ei ole näköetäisyydellä työpisteestäsi. PIN-koodin asettamisesta saat apua Helpdeskistä.
- Ole erityisen varovainen työskennellessäsi julkisissa tiloissa ja huomioi, että joku voi nähdä syöttämiäsi tunnuksia tai muita tietoja huomaamattasi tai salakuunnella keskusteluitasi.
- Julkista tietoa voi välittää internetin kautta tavallisella salaamattomalla sähköpostilla. Salassa pidettävän tiedon välittämisessä internetin kautta on käytettävä suojattua sähköpostia.
  Suojattua sähköpostia on käytettävä, jos viestissä välitetään henkilötietoja (esim. henkilölistoja henkilötunnuksineen). Ohje tilaamiseen
- Älä anna ulkopuolisten nähdä tietokoneesi näyttöruutua, kun käsittelet salassa pidettävää tietoa tai näppäimistöä, kun syötät käyttäjätunnuksia ja salasanoja. Pyri käyttämään päätelaitteissasi näytönsuojakalvoa.

Tunnukset ja salasanat

- Pankkiautomaatillakin suojaat tunnuslukusi ja tarkkailet ympäristöäsi. Noudata vastaavaa varovaisuutta työpaikallasi ja erityistä varovaisuutta sen ulkopuolella.
- Älä anna henkilökohtaisia käyttäjätunnuksiasi tai salasanojasi toisen henkilön käyttöön. Älä edes tietohallintohenkilöstölle, koska he eivät tarvitse niitä työtehtäviensä hoitamiseen.
- Käytä eri salasanaa eri palveluissa – työkäyttöön liittyviä tunnuksia tai salasanoja ei saa koskaan käyttää vapaa-ajan palveluissa.
- Huolehdi salasanasi laadusta käyttämällä vain vahvoja salasanoja, jotka ovat mahdollisimman pitkiä. Vaihda salasanasi silloin kun sitä edellytetään tai kun epäilet sen paljastuneen.
- Vahvassa salasanassa on vähintään 10 merkkiä ja sisältää kolme neljästä luokasta:
    1. pieniä kirjaimia
    2. isoja kirjaimia
    3. numeroita
    4. erikoismerkkejä.

Työvälineiden ja internetin käyttö

- Käytä työhösi liittyviä tietoaineistoja ja organisaatiosi antamia työvälineitä vain työtehtäviesi hoitamiseen.
- Älä selaa sellaisia www-sivustoja, jotka eivät liity työtehtäviisi. Sivujen kautta saatetaan yrittää siirtää päätelaitteeseesi haitta- tai vakoiluohjelmia.
- Ole varovainen – valitse tarvittaessa ”Peruuta”, jos www-sivu ei vaikuta luotettavalta ja sivusto ehdottaa tai edellyttää tiedoston lataamista tietokoneellasi! Pyydä tarvittaessa apua.
- Lataa työkoneellesi vain Meidän IT ja talous Oy:n sallimia ohjelmia.
- Käytä vain organisaatiosi tietohallinnon hyväksymiä muistitikkuja tai muita lisälaitteita.
- Salaamaton muistitikku soveltuu vain julkisen tiedon siirtämiseen.
- Salatulla muistitikulla voit siirtää salassa pidettäviä tietoaineistoja vain organisaatiosi tietoaineistojen käsittelyohjeistuksen mukaisesti.
- Lahjaksi saatuja tai löydettyjä muistitikkuja ei saa liittää päätelaitteeseen.
- Tallenna laatimasi asiakirjat mieluummin verkkolevylle esim. X-asemalle, josta tiedot varmistetaan keskitetysti. Huom! työpöydällä olevat kuvakkeet, kansiot ja tiedostot eivät kuulu varmuuskopioinnin piiriin.

Tietoturva	
M	Mieti
M	Mitä
K	Klikkaat
T	Turvallisesti

Sosiaalinen media

- Muista, että aina kun käytät oman työorganisaatiosi laitteita, verkkoa tai sähköpostia, esiinnyt tietoverkossa organisaatiosi edustajana.
- Huomioi, että palvelun ylläpitäjät pääsevät käsiksi kaikkeen palvelussa käsiteltävään tietoon, myös kahdenvälisiin keskusteluihin. Internetverkkoon päätynyttä tietoa voi olla mahdotonta poistaa jälkikäteen.
- Käsittele palveluissa vain sellaista tietoa, jonka käyttöön palvelu on organisaatiossasi hyväksytty (huomioi mikä tieto on julkista ja mikä salassa pidettävää).

- Älä keskustele työasioista muissa kuin työtehtäviin hyväksytyissä palveluissa tai järjestelmissä. Tämä koskee myös sosiaalisen median käyttöä.
- Käytä työsähköpostia vain työtehtäviesi hoitamiseen. Käytä muuhun kuin työtehtävien hoitamiseen vapaa-ajan sähköpostiasi.
- Tiedätkö, mitä tietoa sinusta on kertynyt sosiaalisen median palveluihin?
- Hae tietoja nimelläsi ja säädä palveluiden yksityisyydensuoja-asetuksia tarvittaessa tiukemmiksi.
- Tarkista erityisesti sosiaalisen median verkkopalveluissa yksityisyyden suojaa koskevat asetukset. Muuta käyttäjäprofiilisi suojausasetuksia tarvittaessa siten, etteivät tietosi näy tai leviä laajemmalle kuin haluat. Testaa eri vaihtoehtoja yksityisyyden suojaa koskevissa asetuksissa. Voit pyytää samaa palvelua käyttävää ystävääsi tarkistamaan miltä tietosi ja profiilisi näyttävät.

Havaitsitko ongelman?

- Jos huomaat tietoturvaongelman, velvollisuutesi on tarttua asiaan. Älä luota siihen, että joku muu ilmoittaa tai korjaa ongelman.
- Ilmoita tietoturvallisuuteen liittyvistä ongelmista, uhkista tai suojauspuutteista organisaatiosi tietosuojavastaavalle tai esimiehellesi. Heidän velvollisuutenaan on ryhtyä toimenpiteisiin.

Mitä tietoturvallisuudella tarkoitetaan ja miksi se on niin tärkeää?

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 on huomioitu. 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 lokia, josta tapahtumat voidaan tarvittaessa jälkikäteen selvittää.

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.

Lainsäädäntö tietoturvallisuuden perustana

Julkishallinnossa 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. Yksityiselämän suoja ja julkisuusperiaate ovat jo perustuslaissa säädeltyjä perusoikeuksia. Tietojen lainmukaisesta käsittelystä on aina huolehdittava.

Keskeisiä 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
  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.
  Salassa pidettävät asiakirjat tai niihin sisältyvät tiedot voidaan luokitella sen mukaan, minkälaisia tietoturvallisuutta koskevia vaatimuksia niiden käsittelyssä on tarpeen noudattaa. Luokittelu voidaan suorittaa myös siten, että tietoturvallisuutta koskevat vaatimukset kohdistetaan vain sellaisiin asiakirjoihin tai sellaisiin asiakirjan käsittelyvaiheisiin, joissa erityistoimenpiteet ovat suojattavan edun vuoksi tarpeen.
  EU:n tietosuojauudistus

EU:n yleinen tietosuoja-asetus (GDPR) on tullut voimaan 25.5.2016, ja sen soveltaminen alkoi jäsenvaltioissa 25.5.2018. Tietosuoja-asetus tulee sovellettavaksi sekä julkisella että yksityisellä sektorilla. Vaikka EU:n yleinen tietosuoja-asetus on kansallisesti suoraan sovellettava säädös, se jättää jäsenvaltioille direktiivinomaista kansallista liikkumavaraa.

Suomessa EU:n yleisen tietosuoja-asetuksen mukaiset muutokset toteutettiin säätämällä uusi tietosuojalaki, joka toimii henkilötietojen käsittelyä koskevana yleislakina. Tietosuojalailla täydennetään ja täsmennetään EU:n yleistä tietosuoja-asetusta. Yleinen tietosuoja-asetus koskee lähtökohtaisesti kaikenlaista henkilötietojen käsittelyä. Se sisältää säännökset rekisteröidyn oikeuksista sekä rekisterinpitäjän ja henkilötietojen käsittelijän velvollisuuksista.

Tietosuojavastaavan tehtävät

Kuntatoimijoiden tietosuojavastaavan tehtävät

- Kartoittaa tietojen käsittelyn nykytilaa ja ottaa tietosuoja osaksi toimintojen suunnittelua
- Arvioida henkilötietojen käsittelyyn liittyvät riskit ja toimenpiteet riskien minimoimiseksi
- Seurata tietosuoja-asetuksen ja muun tietosuojalainsäädännön noudattamista sekä toimintamenettelyjä, jotka liittyvät henkilötietojen suojaan
- Ylläpitää ja kehittää käyttölokien seuranta- ja valvontasuunnitelmaa
- Seurata ja valvoa henkilötietojen käsittelyä sekä tietojen suojausmenetelmiä valvontasuunnitelman mukaisesti, sekä laatia käytönvalvonnan raportit ja dokumentit
- Raportoida organisaation johdolle tietosuojan tilasta ja kehittämistarpeista

- Kartoittaa henkilöstön tietosuojan koulutustarpeita ja organisoi tietosuojakoulutusta henkilöstölle
- Neuvoa ja ohjata henkilöstöä kaikissa tietosuojakysymyksissä
- Tukea rekisteröityjen oikeuksien toteutumista sekä ohjata heitä tietosuoja-asioissa
- Seurata ilmoitusvelvollisuuden toteutumista
- Toimia tietosuojan asiantuntijana tietojärjestelmien hankinnoissa ja käyttöönottoprojekteissa
- Antaa pyydettäessä neuvoja tietosuojaa koskevasta vaikutustenarvioinnista ja valvoo sen toteutusta
- Osallistua rekisterinpitäjän hyväksymien tietosuoja- ja tietoturvaohjeiden valmisteluun ja ylläpitoon
- Laatia ohjeita ja dokumentaatioita sekä valvoa näiden saatavuutta ja säilyttämistä
- Tehdä yhteistyötä valvontaviranomaisen kanssa
- Toimia valvontaviranomaisen yhteyspisteenä henkilötietojen käsittelyyn liittyvissä kysymyksissä
- Toimia tietosuojavastaavien maakunnallisessa yhteistyöverkostossa ja kehittää toimintaa

Asianhallinta ja tietojen käsittely

Asianhallinta tarkoittaa organisaation toimintaprosesseihin sisältyvien asioiden ja asiakirjojen käsittelyn ohjaamista niiden koko elinkaaren ajan. Asianhallinta pyrkii tehostamaan asioiden valmistelua, käsittelyä, päätöksentekoa, julkaisemista ja arkistointia sekä asiakirjamuodossa olevien tietojen (asiakirjalliset tiedot) hallintaa.

Asiakirjalliset tiedot ovat osa organisaation pääomaa, jolloin niiden laatuvaatimukset on turvattava, käsittelykäytännöt suunniteltava huolellisesti ja suojaaminen varmistettava. Asiakirjallisten tietojen laatuun liittyviä vaatimuksia ovat alkuperäisyyden, eheyden, luotettavuuden ja käytettävyyden takaaminen.

Tiedolla tarkoitetaan tässä yhteydessä eri muodoissa talletettavaa, käsiteltävää tai siirrettävää tietoa. Tieto voi olla esimerkiksi yksittäisessä asiakirjassa, puheessa, sähköposti- tai tekstiviestissä, tietokannassa, tietokoneen tai puhelimen muistissa, ääni- tai kuvanauhassa tai vaikkapa yksittäisen ihmisen muistissa. Tietoa on tarkasteltava sen koko elinkaaren ajalla, jolloin tietoturvanäkökulmasta merkittäviä käsittelyvaiheita ovat mm. tiedon luominen, käyttäminen, muuttaminen, tallettaminen, siirtäminen, jakelu, kopioiminen, arkistointi ja hävittäminen. Tietoja käsiteltäessä tulee huomioida, että käsiteltävät tiedot ovat usein merkittävästi arvokkaampia kuin tietojen käsittelyyn mahdollisesti liittyvä tekninen väline.

Työhön liittyvät tiedot

- Mikäli laadit salassa pidettävää asiakirjaa, vastaat tehtäviesi mukaisesti myös sen luokittelusta ja merkinnästä (esim. julkisuuslain pykälä, mihin salassapito perustuu).
- Käsittele tietoja huolellisesti käsittely- tai tallennusvälineestä riippumatta.
- Muista, että voit käyttää ja käsitellä käyttöösi saamiasi salassa pidettäviä ja arkaluonteisia tietoja vain työtehtäviesi hoitamisessa. Esimerkiksi henkilörekisterin tietojen käyttötarkoituksen vastainen käyttö on lainvastaista. Huomioi myös, että tietojärjestelmien käyttöä valvotaan ja luvattomaan käyttöön puututaan.
- Kun käsittelet salassa pidettävää tietoa, huolehdi, etteivät sivulliset näe tietoja asiakirjoistasi tai tietokoneesi näytöltä (käytä mahdollisuuksien mukaan näytönsuojakalvoa).

Varo myös syöttämästä salasanoja tai tunnuskoodeja siten, että joku näkee ne sormiesi liikkeistä.
Tallenna tekemäsi työ mahdollisuuksien mukaan palvelimelle, jonka varmuuskopioinnista tietohallinto huolehtii.
Vältä tilannetta, jossa asiakirja tai muu aineisto olisi ainoastaan sellaisella laitteella tai tietovälineellä, jonka varmuuskopiointi on epäsäännöllistä. Mikäli aineistoa siirretään muistitikun tai muun muistivälineen avulla, valvo siirtoa aina henkilökohtaisesti. Varo tilannetta, jossa omalla tietovälineelläsi olisi siirrettävän tiedoston lisäksi muuta aineistoa salaamattomana.

- Varo toimistosovelluksilla (esim. Word ja Excel) tehtyjen tiedostojen piiloon jääviä tietoja sekä esim. kännykällä otettuja kuvia (ns. meta-, muutos-, jäännös- ja piilotiedot) erityisesti organisaation ulkopuolelle tiedostoja lähettäessäsi tai tietovälineellä siirtäessäsi. Sovelluksissa on usein ”Tarkasta asiakirja” -toiminto, jolla voi etsiä mahdolliset piilotiedostot ja tarvittaessa poistaa ne.
  Mikäli joudut lähettämään salassa pidettävää aineistoa, lähetä se salattuna. Varmistu, että vastaanottaja on oikeutettu sen saamaan ja että lähetys on mennyt perille.
  Vältä turhaa tulostamista ja kopiointia. Ylimääräiset kopiot, väliversiot ja epäkelvot kappaleet (kustannus- ja ympäristövaikutusten ohella) lisäävät tiedon vääriin käsiin joutumisen vaaraa ja turvaamistehtäviä, erityisesti säilyttämisen tai hävittämisen osalta.
  Varmista, mihin tulostimeen tulostat ja missä tulostin sijaitsee. Hae tulosteesi verkkotulostimesta heti tulostuksen jälkeen. Mikäli käytettävissä on ns. turvatulostus (Secure), niin käytä sitä. Pyydä tarvittaessa apua käyttäjätuesta.
- Käytä salassa pidettäviä tietoja hävittäessäsi suojausluokituksen mukaisia silppureita tai tietoturva-astioita.

Haastattelut, kyselyt, tutkimukset ja tietojen luovutus

- Ohjaa haastattelu- ja kyselypyynnöt asian vastuuhenkilölle ja toimi organisaation tiedotuspolitiikan mukaisesti.
  Varo antamasta viattomankin oloisten keskustelujen ja lomakkeiden yhteydessä tietoa salassa pidettävistä ja yksityisyyden suojan piiriin kuuluvista tiedoista.
  Ohjaa tietojen luovutus- ja tutkimuspyynnöt aineiston vastuuhenkilölle, jonka tehtävänä on varmistua tietojen luovutuksen perusteista ja mahdollisesta korvattavuudesta sekä päättää luovutuksesta. Mikäli aineisto luovutetaan tietovälineellä sähköisessä muodossa, tulee käytettävän tietovälineen ehdottomasti olla uusi ja aiemmin käyttämätön tai tietoturvallisesti tyhjennetty ennen aineiston lisäämistä.
  Omat tiedot ja yksityisyys
- Käytä henkilökohtaiseen viestintääsi yksityistä sähköpostiosoitettasi. Hanki yksityiskäyttöön työnantajasta riippumaton vapaa-ajan sähköpostiosoite.
- Omia henkilökohtaisia tiedostoja ei saa tarpeettomasti tallentaa työnantajan puhelimeen, työasemaan tai palvelimelle.
- Olet vaitiolovelvollinen myös vahingossa saamistasi viesteistä tai kuulemistasi asioista.
- Huomioi, että tietojärjestelmiin ja tietoverkon laitteisiin tallentuu yksityiskohtaista lokitietoa järjestelmien käytöstä, sähköpostiliikenteestä ja internet-selauksesta. Tietoja voidaan käyttää ylläpidossa, vianmäärityksessä ja tietoturvallisuuden valvonnassa.
- Huomioi myös, että väärinkäytöksiin puututaan.

Työpaikalla tietoturvan toteuttaminen

Päätelaitteen käyttö

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.

- Puhelimien ja tablettien tietoturva
  - muista tehdä päivitykset, kun laite päivitystä tarjoaa
  - puhelimet ja tabletit MDM:n eli Mobiilietähallinnan piirissä
  - MDM ohjeet palvelupiste – sivustolla (puhelimen lukitus, tyhjennys ja paikannus etänä esim. viikonloppuna, jos puhelin kadonnut)
- Vastaat käyttäjänä omasta päätelaitteestasi, ole siis huolellinen.
- Vain tietohallinto-organisaatio saa asentaa tietokonelaitteita verkkoon ja asentaa tai päivittää niihin ohjelmia. Kirjaudu koneelle aina omilla käyttötunnuksillasi.
- Estä asiaton pääsy tietojärjestelmiin lukitsemalla työasemasi (Windows-lippupainike ja kirjain L) aina kun poistut sen luota.
- Tallenna työsi käyttäen välitallennuksia. Älä jätä työtä tallentamatta, kun poistut koneesi luota.
- Jos työaseman kiintolevy tai muu tallennusväline (esim. muistitikku tai CD-/DVD-levy) rikkoutuu tai poistetaan muuten käytöstä, ei sitä saa laittaa roskakoriin, vaan se pitää hävittää tietoturvallisesti.
- Kirjaudu ulos sekä ohjelmistoista että koneeltasi ja sammuta tietokoneesi työpäivän päättyessä.

Käyttöoikeudet ja salasanat

- Tietojärjestelmiin tarvitaan käyttöoikeus. Käyttöoikeus on henkilökohtainen ja se on yhdistetty juuri sinun henkilöllisyyteesi ja työtehtävääsi. Käyttöoikeudet pyydetään esimieheltä.
- Hyvä salasana on sinun helppo muistaa, mutta vaikea ulkopuolisen arvata.
- Älä lainaa tai luovuta henkilökohtaisia käyttäjätunnuksiasi, salasanojasi, toimikorttiasi tai PIN-koodejasi toisen henkilön käyttöön, älä edes IT-tukihenkilölle. Suhtaudu epäilevästi kaikkiin tiedusteluihin, jotka liittyvät salasanoihisi tai järjestelmien käyttöoikeuksiisi.
- Vaihda salasanat riittävän usein ja heti, jos epäilet niiden paljastuneen.
- Huolehdi, että salasanat ovat riittävän monimutkaisia ja vältä tuttujen jokapäiväisten sanojen käyttöä salasanana. Hyvässä salasanassa on pieniä ja isoja kirjaimia, numeroita ja jopa erikoismerkkejä.
- Älä kirjoita salasanoja muistiin ainakaan sellaiseen paikkaan, mistä ne ovat muiden löydettävissä.
- Matkapuhelimelle on tarjolla salasanojen tallennustyökaluja mm. FSecure Key.
- Älä käytä organisaation antamaa käyttäjätunnusta tai salasanaa Internetin palveluihin rekisteröityessäsi.
- Työsähköpostiosoitetta voi käyttää, jos palvelua käytetään työtehtävissä.
- Yhteiskäyttötunnuksiin liittyy useita riskejä ja ongelmia, jonka vuoksi niiden käyttöä pyritään välttämään. Jos erikseen on sallittu ja sovittu yhteiskäyttötunnuksen käytöstä, niin senkin salasana täytyy vaihtaa aina, kun jonkun käyttäjän käyttöoikeus siihen lakkaa tai epäillään jonkun ryhmään kuulumattoman saaneen sen tietoonsa. Salasana tulee muutoinkin vaihtaa riittävän usein.

Internet, some ja sähköposti

Internet ja sähköposti ovat hyviä työvälineitä sekä tiedon hakuun että yhteydenpitoon. On kuitenkin muistettava, että sähköpostissa tai Internetissä ei itsessään ole oletuksena mitään suojausta, vaan tiedot liikkuvat salaamattomana julkisessa verkossa. Sähköpostin ja Internetin käyttö vaativatkin käyttäjältä huolellisuutta. Internet ja sähköposti ovat työpaikoilla tarkoitettu pääasiallisesti vain työkäyttöön.

Muista, että kaikki asiakkaitamme koskeva tieto on aina luottamuksellista. Verkossa viestitty voi päätyä julkiseksi eikä sanojaan saa takaisin. Ota huomioon, että vaikka esiintyisit kotikoneeltasi käsin yksityishenkilönä, sinut voidaan nimesi perusteella yhdistää työnantajaasi – vaikka et sitä haluaisikaan. Verkossa on monia, jotka yrittävät kalastella eri organisaatioiden salaisuuksia. Voit aina kysyä esimieheltäsi neuvoa epäselvissä tapauksissa.

Internetin ja sähköpostin käytön muistilista:

- Käytä vain sellaisia palveluita, jotka tiedät asiallisiksi.
- Internetin kautta ei ole luvallista välittää salassa pidettävää tietoa ilman asianmukaista
- salausta/suojausta. Tällaiset viestit ja tiedostot on salattava tietohallinto-organisaation
- hyväksymillä tuotteilla.
- Opettele salaustuotteiden oikea käyttö, jotta tieto ei vahingossa lähde salaamattomana.
- Mikäli organisaatiokohtaisen ohjeistuksen ja työtehtäviesi perusteella lataat ohjelmia, pyri aina varmistumaan ohjelmiston ja lähteen luotettavuudesta sekä ohjelmiston soveltuvuudesta kaupungin tai kunnan tietoarkkitehtuuriin.
- Jos käytät julkisia päätteitä tai tilapäisesti toisen henkilön hallussa olevaa tietokonetta, muista tyhjentää Internet -selaimen välimuisti ja evästeet (cookies). Selaushistoria poistetaan selaimen internet-asetuksissa. Pyydä tarvittaessa apua käyttäjätuesta.
- Työhön liittyvä sähköposti vastaanotetaan ja ohjataan oman organisaation sähköpostijärjestelmään. Sitä ei saa ohjata tai jatko lähettää automaattisesti organisaation sähköpostijärjestelmän ulkopuolelle.
- Jos saat henkilökohtaiseen sähköpostiin työpostia, niin vastaat niistäkin työvelvollisuuksien mukaisesti.
- Varmista, että sähköpostisi käsittelyyn liittyvät velvollisuudet tulevat hoidettua myös poissaolosi aikana.
- Sähköpostin liitetiedostot voivat sisältää haittaohjelmia (viruksia, matoja tai troijalaisia).
- Varo kaikkia epätavallisia sähköposteja ja erityisesti liitetiedostoja sekä posteissa olevia suoria www-linkkejä. Älä avaa epäilyttäviä viestejä. Tarvittaessa voit ilmoittaa asiasta käyttäjätukeen.
- Roskapostia voivat olla esim. sähköpostiin tilaamatta tulleet mainokset. Roskapostiin ei kannata vastata, vaan se kannattaa tuhota heti. Jos viestiin vastaa, tietää roskapostittaja sähköpostiosoitteesi toimivaksi ja lisää roskapostien lähettämistä ja lisäksi välittää /myy osoitteesi myös muille roskapostittajille.
- Älä anna työsähköpostiosoitettasi ulkopuolisille muissa kuin työhön liittyvissä yhteyksissä.
- Ole terveen epäluuloinen sähköpostiviestin luotettavuuteen. Sähköpostiviesti voi tulla myös muualta kuin viestin lähettäjäkentässä näkyvältä taholta. Myös haittaohjelmat voivat lähettää sähköpostia ilman käyttäjän toimenpiteitä.
- Varo ns. kalasteluviestejä, joissa sinua pyydetään syöttämään tunnuksia ja salasanoja aidontuntuisiin palveluihin.
- Älä välitä ketjukirjeitä eteenpäin.

- Mikäli saat toiselle henkilölle kuuluvan sähköpostin, ohjaa viesti oikealle vastaanottajalle
- ja ilmoita lähettäjälle vastaanottajan oikea sähköpostiosoite. Mikäli oikea osoite ei ole tiedossa, ilmoita virheellisestä lähetyksestä lähettäjälle. Muista, että sinulla on vaitiolovelvollisuus saamastasi viestistä.
- Jakelulista on henkilöluettelo, jonka jokainen vastaanottaja saa tietoonsa ja se voi olla henkilörekisteritieto tai salassa pidettävä tieto, jonka luovuttamisesta on erikseen säädetty. Voit käyttää sähköpostin piilokopiotoimintoa, jos haluat estää jakelulistalla olevien osoitteiden näkymisen vastaanottajille.
- Huolehdi, että lähettämäsi sähköpostiviesti on kohdistettu oikeille henkilöille ja oikeisiin
- osoitteisiin, myös valmiita jakelulistoja käyttäessäsi. Vältä turhien sähköpostien lähettämistä.
- Työsuhteen päättyessä sähköpostiosoite ja -laatikko poistetaan. Siirrä työpostisi työnantajan käyttöön ja poista tai tallenna itsellesi mahdolliset yksityiset/henkilökohtaiset viestit.

Skannauksen riskit

- Skannauksen riskit, tällä hetkellä esim. osallistujalistat muutetaan pdf-muotoon monitoimilaitteella. Pdf liitetään laskuun tai hankkeiden maksatushakemukseen.
    - Monitoimilaitteeseen todennäköisesti jää pdf-tiedosto käytettäväksi, kunnes laite poistetaan. Laite lähettää pdf:n sähköpostilla, joka on turvaton viestinvälitystapa
    - Ainahan on riski, että esim. joku muokkaa pdf:ää ja riski määräytyy skannattavan aineiston mukaan. Jos pdf ei sisällä arkaluontoista tietoa, todennäköisesti korkean riskin määritelmät eivät täyty.
    - Skannaa henkilötietoja sisältävä aina turvalliseen tiedostoon, älä suoraan normaaliin sähköpostiin.

Toimitilojen turvallisuus

- Toimitilojen turvallisuudella varmistetaan, että tietoja, asiakirjoja ja tietokonelaitteita säilytetään ja käsitellään asianmukaisesti turvallisissa tiloissa. Toimitilojen turvallisuus sisältää mm. kulunvalvonnan, teknisen valvonnan ja vartioinnin, palo-, vesi-, sähkö-, ilmastointi- ja murtovahinkojen torjunnan sekä lähettipalvelujen ja tietoaineistoja sisältävien lähetysten turvallisuuden.
- Suuntaa asiakaspalvelupisteessä ja –tilanteessa tietokoneesi näyttö harkitusti. Onko tarkoitus, että tiedot näkyvät asioijalle vai ei? Hanki tarvittaessa näytönsuoja.
- Noudata kulunvalvonnasta annettuja ohjeita.
- Pyri käyttämään vierailuihin ns. julkisen alueen neuvottelutiloja.
- Huolehdi, ettei neuvottelutiloissa ole esillä asiaankuulumatonta materiaalia. Vastaavasti neuvottelun päättyessä huolehdi, ettei pöydille, tauluihin, roskakoreihin tai muualle jää käsiteltyjä luottamuksellisia aineistoja tai muistiinpanoja. Varmista myös, että USB-tikut on otettu esityslaitteistoista pois.
- Älä jätä kannettavaa tietokonetta tai puhelinta ilman valvontaa. Säilytä laitteita lukitussa tilassa.
- Huolehdi myös muistitikkujen, CD-/DVD-levyjen, paperitulosteiden ym. asianmukaisesta säilyttämisestä. Huomioi asiakirjojen erilaiset säilytysajat. Asiakirjojen säilytysaikaohjeet löytyvät Laatukäsikirjasta. Tarpeeton aineisto hävitetään. Salainen ja/tai henkilötietoja sisältävä aineisto hävitetään tietoturva-astioihin.
- Noudata puhtaan pöydän periaatetta. Työpöydällä ei saa säilyttää salassa pidettävää tietoa.

- Älä jätä vierasta ilman valvontaa työhuoneeseesi tai muihin toimitiloihin.
- Ohjaa vieraat tai ”eksyneet” henkilöt oikeisiin paikkoihin. Älä päästä asiattomia henkilöitä toimitiloihin samalla oven avauksella esim. töistä lähtiessäsi.
- Älä jätä kulunvalvonnassa olevia tai muuten lukittuna pidettäväksi tarkoitettuja ovia auki eli varmista, että tällaiset ovet lukkiutuvat takaisin kuljettuasi niistä. Sulje myös työhuoneesi ovi, kun poistut muualle.

Liikkuva työ ja mobiililaitteet

Liikkuvan työn välineisiin ja niiden käyttöön liittyy vastaavia uhkia kuin kiinteämmin asennettuihin, joten kyseeseen tulevat soveltuvin osin samat turvallisuusohjeet. Kun välineitä lisäksi kuljetetaan ja käytetään työpaikan toimitilojen tarjoamien turvatoimien ulkopuolella, tarvitaan erityistä huolellisuutta.

- Huolehdi työnteossa käyttämiesi tietokoneiden, älypuhelimien ja USB-tikkujen turvallisuudesta. Älä säilytä niissä ylimääräistä tietoa suojaamattomana. Meidän IT ja talous Oy:n palvelusivustolta voi pyytää salausta. Kaikki uudet koneet salataan automaattisesti,
- Tutustu laitteen ja siinä olevien ohjelmien käyttöohjeisiin ja turvallisuusominaisuuksiin (mm. lukitseminen, suojakoodikyselyt, Bluetooth-asetukset, sovellusten lataaminen, päivitykset).
- Huolehdi, että matkapuhelimessasi on päällä PIN-kysely. Vaihda laitevalmistajan tai palveluntarjoajan antamat oletusarvoiset PIN-koodit.
- Älä lataa ja asenna laitteisiin mitään työhön kuulumatonta.
- Huolehdi tietojen varmuuskopioinnista ja/tai tarvittaessa synkronoinnista muuhun tietojärjestelmään.

Etätyö ja etäkäyttö

Etätyöllä tarkoitetaan muualla kuin organisaation vakituisessa toimipisteessä suoritettavaa työtä. Tyypillinen etätyö on kotoa tehtävää toimistotyötä. Etätyötä voidaan tehdä tai tietojärjestelmiä käyttää myös muusta paikasta (esim. organisaation järjestämä etätyöpiste) tai matkoilla (esim. hotelli tai toisen organisaation tilat), jolloin käyttöympäristöt vaihtelevat eikä ympäristön turvallisuuteen voida juurikaan vaikuttaa. Työntekijän omilla toimenpiteillä ja menettelytavoilla on tällöin suuri merkitys. Etäyhteys on tietoliikenneyhteys organisaation sisäverkon ulkopuolelta ja etäkäyttö tietoteknisten palvelujen käyttöä etäyhteyden avulla. Langattomien verkkoyhteyksien yleistyessä etätyöntekijän on entistä useammin kyettävä tekemään itsenäiset arviot etätyöympäristön turvallisuudesta.

Kiinnitä kaikessa toiminnassasi huomiota tietoturvallisiin menettelytapoihin. Erityisen tärkeää tämä on toimittaessa vakituisten toimistotilojen ulkopuolella. Etätyössä sinun tulee noudattaa soveltuvin osin kaikkia samoja turvallisuusperiaatteita kuin ollessasi organisaation varsinaisissa toimitiloissa.

- Etäkäytön osalta tarkista asia organisaatiokohtaisesta ohjeistuksesta.
- Muista, että kaikkea organisaatiossa tehtävää työtä ei voida tehdä tietoturvallisesti etätyönä. Tunnista nämä työt. Joidenkin järjestelmien etäkäyttö voi olla kielletty tai estetty.

- Pääsääntöisesti työnantaja hoitaa etäkäytössä vaadittavien laitteiden, ohjelmistojen ja tietoliikenneyhteyksien hankinnan ja asentamisen.
  - Huolehdi, että etätyössä käyttämäsi laitteistot, ohjelmistot, tietoliikenneyhteydet ja paperiaineistot ovat ja pysyvät vain sinun käytössäsi.
  - Huolehdi, että käyttämäsi käyttäjätunnukset, salasanat, mahdolliset toimikortit ja muut todennus-välineet ovat vain sinun hallussasi ja tiedossasi.
  - Käytä sovittuja suojausohjelmia ja varmista, että ne ovat ajan tasalla.
  - Kuljeta mukanasi vain välttämätön määrä tietoaineistoa ja varmistu aina aineiston asianmukaisesta suojauksesta.
  - Asiakirjojen käsittelyssä on noudatettava samoja periaatteita kuin normaalisti, etätyön erityisriskit huomioon ottaen. Etätyö on rajattava aineistoon, jonka paljastuminen ei vaaranna tietoturvallisuutta tai tietosuojaa. Myös etätyössä on otettava huomioon aineiston luokittelu ja siihen liittyvät käyttösäännöt sekä luovutusta, käyttöä ja käsittelyä koskevat rajoitukset.
  - Huolehdi tietoaineistosi varmuuskopioinnista sekä turvallisesta säilytyksestä ja hävittämismenettelystä.
  - Riski, kotona olevan internet yhteyden käyttäminen työasioiden hoitamiseen työlaitteella (kannettava, puhelin, tabletti) tai työsähköpostien käsittely kotikoneella posti.pohjoiskarjala.net kautta.

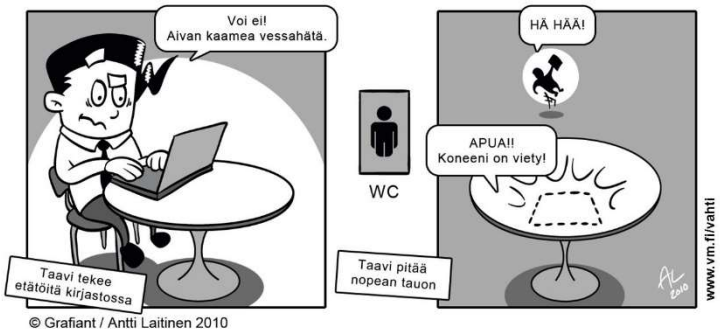
    - Posti.pohjoiskarjala.netin käyttö on salattua, mutta kotikoneen tietoturvaa emme voi taata. (Citrixin käyttöä suositellaan)
    - Päivitykset tulevat keskitetysti Meidän It ja talous Oy:n toimesta työasemiin, siihen ei tarvitse käyttäjän puuttua. Puhelimet pitää käyttäjän itse päivittää.
    - Etäyhteyden saaminen eli miten saa verkkokansiot käyttöön ns. tien päältä/yrityksissä.
    - Etäkäyttötunnuksen tilaaminen
    - Kun asiakaskäynneillä on tarve jakaa nettiyhteys kännykästä kannettavaan tietokoneeseen, on käytettävä citrixiä, niin tietoturvariski pienenee (muodostaa salatun yhteyden koneen ja Meidän It ja talous Oy:n välille).
    - Ehdottomasti on käytettävä vahvaa salasanaa. Yleensäkin wifi-yhteyden käyttö esim. hotelleissa yms. on tietoturvatonta. Suosittelemme Citrix-yhteyden käyttöä, koska se salaa yhteyden koko ketjuun.

Matkatyö

Vältä puhumasta luottamuksellisista työasioista julkisilla paikoilla ja kulkuvälineissä.

- Mikäli työskentelet julkisessa kulkuvälineessä, varmistu, etteivät kanssamatkustajat pysty kurkistamaan ja näkemään käsittelemiäsi tietoja ja asiakirjoja. Varo myös aiheettomien langattomien yhteyksien aktivoitumista koneeseesi.
- Säilytä tieto ja laitteet turvassa. Älä jätä kannettavaa tietokonetta tai puhelinta ilman valvontaa.
- Vältä julkisten päätteiden (esim. nettikahvilat, kirjastot) käyttöä työasioihin. Et voi vaikuttaa siihen, mitä tietoja käytöstäsi kerätään ja mitä tiedoilla tehdään. Yleensä sinulle ei myöskään tarjoudu mahdollisuutta poistaa näitä tietoja laitteelta.
- Säilytä laitetta lukitussa paikassa. Muista myös tietovälineiden, paperitulosteiden ym. asianmukainen säilyttäminen. Kannettavia tietokoneita ja matkapuhelimia ei saa jättää autoon näkyvälle paikalle, eikä niitä saa säilyttää autossa yön yli.

Muista huolehtia tietokoneesta ja matkapuhelimesta hyvin!



Ongelmatilanteet

Ilmoitusvelvollisuus ja toiminta ongelmatilanteissa

- Mikäli hallussasi oleva laite, kulkukortti, tunniste tms. katoaa tai varastetaan, ilmoita siitä välittömästi ao. vastuuhenkilölle riskien pienentämiseksi ja oman vastuusi rajaamiseksi.
- Ilmoita aina haittaohjelmista (esim. virukset tai kiristyshaittaohjelmat) ja muista tietoturvallisuuteen liittyvistä ongelmista välittömästi Servicedeskiin ja oman organisaatiosi tietoturvavastaavalle tai omalle esimiehellesi.
- Ilmoita aina myös muista turvallisuuteen liittyvistä epäilyistä, suojauspuutteista tai ongelmista turvallisuusvastaaville tai omalle esimiehellesi.
- Jos epäilet tietoturvaloukkausta tai haittaohjelmatartuntaa:
    - Älä hätiköi!
    - Tietokonetta ei tarvitse sulkea, mutta irrota lähiverkkokaapeli työasemastasi ja sulje langaton verkkoyhteys (WLAN/ WI-FI).
    - Kirjoita ylös tai nappaa puhelimella valokuva, mitä mahdollisessa ilmoituksessa tai varoituksessa luki.
    - Ota yhteyttä Tukikeskukseen ja/tai oman organisaatiosi tietoturvavastaavaan.
    - Kerro mitä olit tekemässä, kun kone alkoi toimia odottamattomasti. Toimi saamiesi ohjeiden mukaisesti. Auta tutkinnassa.

Seuraamukset ja sanktiot

Lakien, määräysten ja ohjeiden rikkomisesta käyttöoikeudet tietojärjestelmiin voidaan peruuttaa. Rikkomuksista tiedotetaan aina esimiehelle. Vakavissa tapauksissa väärinkäyttö voi johtaa myös vahingonkorvausvaatimuksiin, työoikeudellisiin seuraamuksiin ja rikosoikeudellisiin seuraamuksiin. Seurauksena voi olla irtisanominen tai palvelussuhteen purkaminen. Seuraamuksista ja sanktioista on tarkemmin tietosuojan valvontasuunnitelmassa.

Koulutukset ja testit

Organisaatio järjestää tietosuoja- ja tietoturvakoulutusta esim. uudet työntekijät suorittavat intrassa olevan Granite-tietosuoja- ja tietoturvakurssit ja suorittavat kurssin aikana testin, josta saadaan todistus. Se toimitetaan esimiehelle, jonka vastuulla on että oma henkilöstö on suorittanut nämä kurssit.

- Granite, audit.pohjoiskarjala.net
- Arjentietosuojasivusto, ellei sinulla ole mad-tunnuksia. https://arjentietosuoja.fi/

Kotikoneella tietoturvan toteutuminen

- Mikäli sinulla on kotona oma tietokone ja Internet-liittymä, on tärkeää huolehtia myös niiden tietoturvallisuudesta.
- Mikäli mahdollista, niin pyydä ajoittain luotettavaa tietotekniikka-asiantuntijaa tarkistamaan, että työasemaympäristösi on turvallinen.
- Tee jokaiselle käyttäjälle omat henkilökohtaiset tunnukset, joilla on vain ns. normaalikäyttäjän oikeudet
- Käytä ylläpitäjän tunnusta (esim. Järjestelmänvalvoja, Administrator) vain ylläpitotehtäviin
- Asenna vain virallisia, ajan tasalla olevia ohjelmistoja
- Huolehdi käyttöjärjestelmän ja muiden ohjelmien jatkuvasta (automaattisesta) päivittymisestä
- Käytä jotain tunnettua ja hyvämaineista tietoturvaohjelmistoa (joka sisältää mm. virus-, vakoilu- ja muiden haittaohjelmien torjunnan sekä palomuurin ellei käyttöjärjestelmän oma palomuuri ole käytössä) ja huolehdi sen jatkuvasta automaattisesta päivittymisestä
- Älä avaa epäilyttäviä sähköpostiviestejä ja – liitteitä
- Tee säännöllisesti varmuuskopiot ja harjoittele niiden käyttöönottoa
- Kun kirjaudut Internetin palveluihin ja teet esim. ostoksia, käytä vain luotettavia palveluita ja toimittajia. Älä anna enempää henkilökohtaista tietoa kuin on tarpeen. Älä käytä samoja salasanoja kuin työpaikan järjestelmissä.
- Sammuta tietokone ja katkaise Internet-yhteys, kun et käytä sitä.
- omat laitteet, tietoturva, käyttö (laitehallinta)
- suositellaan työasioihin käytettävän työlaitteita

Mistä löydän lisää tietoa

Kun tarvitset lisätietoa ja neuvoa, käänny oman organisaatiosi tietosuoja-, tietoturvavastaavan tai tietosuojaryhmän jäsenen puoleen. Tietoteknisiin kysymyksiin vastaa Meidän IT ja talous. Voit myös kysyä lähiesimieheltä ja tutkia intran ohjeet.

Oman organisaation dokumentit

- Tietoturva- ja tietosuojapolitiikka
- Tietoturva- ja tietosuojasuunnitelma
- Tietosuojan valvontasuunnitelma

Muita lähteitä

Lainsäädäntö: Valtion säädöstietopankki (www.finlex.fi)
Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän VAHTI-ohjeet (www.vahtiohje.fi)
Viestintäviraston kyberturvallisuuskeskuksen sivut
(https://www.viestintavirasto.fi/kyberturvallisuus.html)
Tietosuojavaltuutetun toimiston ohjeet (www.tietosuoja.fi)

LINKIT JA LIITTEET:

Liite 1 Tietosuojan periaatteet tarkemmin avattuna
Liite 2 PTTK-ohje-Sähköpostin käyttöohjeistus
Liite 3 Keskeistä tietosuojaan ja tietoturvaan liittyvää sanastoa
Liite 4 Tietoturvan ja tietosuojan huoneentaulu
Liite 5 Esimiehen vastuut tietosuojasta

Eri lakeihin sisältyvien salassapitosäännösten lisäksi laeista tärkeimpiä ovat:

- Suomen perustuslaki (731/1999) 2.luku 10 §: Yksityiselämän suoja
- Suomen perustuslaki (731/1999) 2.luku 12 §: Sananvapaus ja julkisuus
- Laki viranomaisten toiminnan julkisuudesta (621/1999)
- Asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintotavasta (1030/1999)
- Laki kunnallisesta viranhaltijasta (304/2003)
- Työsopimuslaki (55/2001)
- Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuudesta (VM0024:00/02/99/1998)
- Arkistolaki (831/1994): Asiakirjojen laatiminen, säilyttäminen ja käyttö
- Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004)
- Laki yksityisyyden suojasta työelämässä (759/2004): Työntekijää koskevien henkilötietojen käsittely
- Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)
- Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009)
- Sähköisen viestinnän tietosuojalaki (516/2004): Sähköisen viestinnän luottamuksellisuus ja yksityisyyden suoja
- Rikoslaki (578/1995) 38.luku: Tieto- ja viestintärikoksista
- Rikoslaki (578/1995) 47.luku: Työrikoksista
- Vahingonkorvauslaki (412/1974)
- Asetus tietoturvallisuudesta valtionhallinnossa (681/2010)

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