



L A P I N L A H T I

Henkilöstön tietoturvaohje

Sisällys

Johdanto	2
Tietoturvallisuus	3
Asianhallinta ja tietojen käsittely	3
Tietoaineistojen käsittely	4
Omat tiedot ja yksityisyys.....	4
Tietoturvallisuuden ohjeet.....	4
Tiedottaminen ja koulutus	4
Toimitilaturvallisuus	4
Noudata organisaatiosi kulunvalvontaohjetta.	5
Päätelaitteet	5
Tunnukset ja salasanat	5
Työvälineiden ja internetin käyttö	6
Sosiaalinen media ja sähköposti.....	6
Noudata Sosiaalisen median tietoturvaohjeita (VAHTI 4/2010):	7
Etätyö.....	8
Haastattelut, kyselyt, tutkimukset ja tietojen luovutus	8
Havaitsitko ongelman?	8

Johdanto

Vastuu tietoturvallisuudesta ja siihen liittyvästä osaamisesta kuuluu omalta osaltaan jokaiselle, myös Sinulle.

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!

Tätä tietoturvaohjetta tulee noudattaa koko kuntaorganisaatiossa. Osassa työyksiköitä on omia tarkempia ammattialakohtaisia ohjeita, joita noudatetaan rinnan tämän ohjeen kanssa. Osassa yksiköitä on toiminnan luonteen takia tarve noudattaa tiukempaa ohjeistusta. Tässä ohjeessa on asetettu kuntaorganisaation minimitaso tietoturvassa, jota voidaan yksiköiden omissa ohjeissa tiukentaa.

Tämä ohje koskee jokaista kunnan työntekijää, viranhaltijaa, luottamushenkilöä ja yhteistyökumppania, joka työnsä tai toimeksiantonsa perusteella käsittelee Lapinlahden kunnan omistamaa tai hallinnoimaa tietoa.

Ohjeeseen on koottu keskeisimmät työhösi liittyvät tietoturvallisuuden perusasiat. (Oman toiminnan ohella tätä ohjetta tulee noudattaa kunnan toimeksiannosta tehtävässä työssä (esim. palvelutoimittajat). Ohjetta tulee noudattaa myös mm. harjoittelijoiden osalta.

Kun saat idean tietoturvallisuuden parantamisesta, tee siitä aloite omalle esihenkilöllesi, ict-asiantuntijalle sekä johtoryhmälle.

Tietoturvallisuus

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.

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.

Tietoaineistojen käsittely

Merkitse salassa pidettäviin asiakirjoihin sen salassapidosta kertova tunniste. Laatiessasi salassa pidettävää asiakirjaa, vastaat sen luokittelusta ja luokittelun merkitsemisestä. Käsitle (tallenna, siirrä, tulosta, lähetä, kopioi, kuljeta, säilytä, arkistoi, hävitä) salassa pidettäviä tietoja annettujen ohjeiden mukaan.

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. Salassa pidettävää tietoa voidaan tallentaa, siirtää ja arkistoida usealla eri tallennusvälineellä ja tavalla. Noudata tietoaineistojen ja tallennusvälineiden hävittämisessä annettuja ohjeita. Selvitä, missä sijaitsevat lähimmät salassa pidettävän materiaalin hävittämiseen tarkoitetut tietoturvalliset säiliöt tai tuhoajat.

Käytä tulostamisessa turvatulostusta

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 turvasähköpostia.

Omat tiedot ja yksityisyys

Käytä pääsääntöisesti henkilökohtaiseen viestintääsi yksityistä sähköpostiosoitettasi.

Hanki yksityiskäyttöön työnantajasta riippumaton vapaa-ajan sähköpostiosoite.

Omia henkilökohtaisia tiedostoja ei saa tarpeettomasti tallentaa työnantajan päätelaitteisiin tai palvelimille.

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 käytetään ylläpidossa, vianmäärityksessä ja tietoturvallisuuden valvonnassa. Väärinkäyttöksiin voidaan puuttua.

Tietoturvallisuuden ohjeet

Tiedottaminen ja koulutus

Seuraa tietoturvallisuuteen liittyviä organisaatiosi tiedotteita Teams:stä, tutustu ohjeisiin ja osallistu tietoturvakoulutukseen.

Noudata organisaatiosi tietoturvaohjeita.

Toimitilaturvallisuus

Toimitilojen turvallisuudella varmistetaan, että tietoja, asiakirjoja ja ICT-laitteita säilytetään turvallisissa tiloissa.

Noudata organisaatiosi kulunvalvontaohjetta.

Mikäli epäilet, että ulkopuolinen henkilö oleskelee kunnan tiloissa ilman asiallista syytä, tarkista henkilön kulkuoikeus kyseiseen tilaan ja huolehdi, että henkilö poistuu tarvittaessa tilasta. Ohjaa vieraat tai "eksyneet" henkilöt oikeisiin paikkoihin, tarvittaessa saata henkilö aulaan tai ulos.

Älä päästä asiattomia henkilöitä toimitiloihin esim. töistä lähtiessäsi.

Älä jätä työvälineitä valvomatta neuvottelutiloihin.

Älä jätä vieraita yksin neuvottelu- tai työtiloihin. Saata vieraat aulaan tai ulos kokouksen jälkeen.

Asiakaspalvelupisteessä tai -tilanteessa päätelaitteen näyttö ei saa näkyä asioijalle.

Älä jätä vierasta yksin tai ilman valvontaa työhuoneeseesi tai henkilökunnan tiloihin.

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.

Noudata "puhtaan pöydän" periaatetta. Työpöydällä ei saa säilyttää salassa pidettävää tietoa.

Lukitse työhuoneesi ovi työpäivän päättyessä tai poistuessasi pidemmäksi aikaa työpisteestäsi.

Huolehdi myös siitä, että toimitilan ulko-ovi lukittuu poistuessasi.

Älä jätä auki kulunvalvonnassa olevia tai ovia, jotka on muuten tarkoitettu pidettäväksi suljettuina.

Päätelaitteet

Päätelaitteella tarkoitetaan tässä ohjeessa työtehtävien hoitoon tarkoitettua elektronista laitetta, joka voi olla esimerkiksi puhelin, kannettava-, tabletti-, pöytätietokone tai jokin muu vastaava laite.

Päätelaitetta (kannettava tietokone, pöytäkone, älypuhelin, tabletti jne.) käytetään yhä useammin maksu- ja tunnistautumisvälineenä. Suojele sitä kuten lompakkoasi.

Työnantajan älypuhelimessa ei saa käyttää henkilökohtaisen liittymän sim-korttia.

Työnantajan älypuhelin on vain työasioiden hoitoa varten.

Älä anna ulkopuolisen henkilön, edes tutun, käyttää päätelaitettasi.

Estä päätelaitteesi, esimerkiksi puhelimen, luvaton käyttö asettamalla siihen laitteen käyttöohjeen mukaiset automaattiset lukitukset.

Huolehdi, että matkapuhelimessasi on päällä SIM-kortin PIN- ja puhelimen suojakoodikysely.

Päätelaite on aina henkilökohtainen työväline, mikäli sitä ei ole erikseen asetettu yhteiskäyttöön. Kirjaudu laitteelle aina omilla käyttöoikeuksillasi. Lukitse käyttämäsi päätelaite aina kun se ei ole valvonnassasi.

Tunnukset ja salasanat

Älä luovuta 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 pieniä ja isoja kirjaimia, numeroita ja erikoismerkkejä. Se on helppo muistaa, mutta vaikea arvata.

Älä kirjoita salasanoja muistiin tai säilytä sellaisessa paikassa, mistä ne ovat helposti löydettävissä.

Työvälineiden ja internetin käyttö

Käytä työhösi liittyviä tietoaaineistoja ja organisaatiosi antamia työvälineitä vain työtehtäviesi hoitamiseen. Kunnan internet yhteys on tarkoitettu työasioiden hoitamiseen. Omia yksityisasiaita voi hoitaa vain vähäisessä määrin (esim. pankin sivujen kautta tapahtuva laskujen maksaminen). Älä selaa sellaisia epäilyttäviä 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. Älä asenna ohjelmistoja tai tee niiden asetusmuutoksia, ellei se kuulu työtehtäviisi. Peruskäyttäjänä sinulla näitä oikeuksia ei tulisi olla. Jos huomaat, että sinulla on johonkin palveluun tai toimintoon liikaa oikeuksia, velvollisuutesi on pyytää niiden korjaamista.

Tallenna laatimasi asiakirjat tietojärjestelmiin, team:siin tai OneDriveen. Tietokoneen paikallista (C asema) ei tule käyttää asiakirjojen tallennukseen. Omia henkilökohtaisia tiedostoja ei saa tarpeettomasti tallentaa työnantajan päätelaitteisiin tai palvelimille.

Jos käytät muistitikkoa, se soveltuu vain julkisen tiedon siirtämiseen. Lahjaksi saatuja tai löydettyjä muistitikkoja ei saa liittää päätelaitteeseen. Huolehdi käytöstä poistetun muistitikun asianmukaisesta hävittämisestä. Kunnantalon postihuoneessa on tietosuoja-säiliö, johon käytöstä poistetut muistitikut, cd/dvd, levykkeet toimitetaan hävitettäväksi tietoturvalisesti.

Jos käytät julkisia päätelaitteita tai tilapäisesti toisen henkilön hallussa olevaa tietokonetta, muista tyhjentää Internet-selaimen välimuisti ja evästeet (cookies). Säilytä tieto ja laitteet turvallisessa paikassa. Älä jätä kannettavaa tietokonetta tai puhelinta ilman valvontaa. Muista myös tietovälineiden, paperitulosteiden ym. asianmukainen säilyttäminen. Kannettavia tietokoneita tai puhelimia ei saa jättää autoon näkyvälle paikalle, eikä niitä saa säilyttää autossa yön yli. Vältä julkisten päätteiden (esim. nettikahvilat, kirjastot) käyttöä työasioihin. Et voi vaikuttaa siihen, mitä tietoja käytöstäsi kerätään ja mitä tiedoilla tehdään. Yleensä sinulla ei myöskään ole mahdollisuutta poistaa näitä tietoja laitteelta.

Sosiaalinen media ja sähköposti

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 hyväksytty (huomioi mikä tieto on julkista, mikä salassa pidettävää). Älä keskustele työasioista tai jaa työhön liittyviä kuvia muissa kuin työtehtäviin hyväksytyissä palveluissa tai järjestelmissä. Tämä koskee myös sosiaalisen median käyttöä.

Noudata Sosiaalisen median tietoturvaohjeita (VAHTI 4/2010):

1. Selvitä ja noudata organisaatiosi sosiaalisten medioiden käyttöpolitiikkaa.
2. 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.
3. Jos mainitset sosiaalisen median palvelun henkilöprofiilissasi työnantajasi, esiinnyt tällöin organisaatiosi (epävirallisena) edustajana. Muista käyttäytyä sen mukaisesti!
4. Varo syöttämästä liian henkilökohtaista tai yksityiskohtaista tietoa, valokuvia tai muuta materiaalia itsestäsi. Huomaa, että palvelun tarjoaja voi hyödyntää profiiliisi syöttämiäsi tietoja laajasti. Tutustu huolellisesti käyttämiesi palveluiden sopimusehtoihin.
5. Tarkista käyttäjäprofiilin yksityisyyden suojaa koskevat asetukset ja muuta niitä tarvittaessa siten, että tietosi eivät leviä laajemmalle kuin haluamallesi käyttäjajoukolle.
6. Kunnioita perheesi ja ystäväsi suhtautumista sosiaalisiin medioihin. Vaikka olisit itse niistä innostunut, eivät kaikki sitä kuitenkaan ole. Jos kanssaihmissesi eivät halua sinun laittavan kuvia tai tietoa heistä sosiaaliseen mediaan, noudata heidän toiveitaan.
7. Älä hyväksy tuntemattomia yhteydenottoyrityksiä verkostoosi äläkä napsauta vieraita, hämäräperäisiä linkkejä.
8. Älä keskustele työasioista muissa kuin työtehtäviin hyväksytyissä sosiaalisissa medioissa.
9. Ole erityisen huolellinen salassa pidettävän tiedon suhteen. Muista, että palvelun ylläpitäjät pääsevät teknisesti käsiksi kaikkeen palveluun talletettuun ja myös vain keskustelun osapuolten väliseksi tarkoitettuun tietoon.

Käytä työ sähköpostia vain työtehtäviesi hoitamiseen. Käytä muuhun kuin työtehtävien hoitamiseen vapaa-ajan sähköpostiasi. Käytä henkilökohtaisen postin lukemiseen henkilökohtaisia laitteita eikä työnantajan laitteita.

Lue työnantajan sähköpostia vain työnantajan antamilla laitteilla. Oman koneen käyttäminen ei ole sallittua tietoturvasyistä.

Työnantajan sähköpostiosoitteen saa luovuttaa vain sellaiseen internetpalveluun rekisteröidyttyessä, jolla on selkeä yhteys työtehtäviin.

Ole erityisen varovainen, jos saat vieraskielisen tai huonolla suomen kielellä kirjoitetun 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

Pyydä tarvittaessa kunnan tietohallintoa tutkimaan saamasi epäilyttävä liitetiedosto ennen sen avaamista.

Poista epäilyttävät sähköpostit, älä avaa niitä.

Kunnan sähköpostijärjestelmä ei lähetä automaattisesti kuittausta viestin lähettäjälle. Huolehdi sähköisen asiakirjan vastaanottamisesta ilmoittamisesta.

Työtehtävien keskeytymättömän hoitamisen vuoksi työntekijällä on velvollisuus käyttää sähköpostijärjestelmän automaattista vastaustoimintoa ilmoittaakseen poissaolostaan, sen kestosta ja siitä kuka hoitaa hänen tehtäviään poissaolon aikana.

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 jakelulistojen kautta.

Työsuhteen päättyessä sähköpostiosoite ja -laatikko poistetaan. Siirrä käsittelyä edellyttävä virkapostisi työnantajan käyttöön.

Etätyö

Etätyöllä tarkoitetaan työnantajan kanssa sovittua työnteon mallia, jossa työ tehdään joko osin tai kokonaan kotona tai sitten työnantajan eri toimipisteissä, työkohteissa, asiakkaan luona jne. Nämä elementit voivat sisältyä myös työhön, joka on liikkuvaa tai monipaikkaista.

Ammatillisiin tarkoituksiin käytettävien ohjelmistojen ja tietojen suojauksen on oltava etätyössä lähtökohtaisesti samaa tasoa kuin työnantajan tiloissa työskentelevillä.

Etätyössä käytetään vain työnantajan hankkimia laitteita.

Etäyhteyden suojaus edellyttää VPN-yhteyttä.

Työnantajan hankkimaa tietokonetta saa käyttää vain työntekijä ja työntekemiseen.

Tietoturvaan koskevat säännökset ovat samat, joita sovelletaan työnantajan tiloissa työskenteleviin.

Haastattelut, kyselyt, tutkimukset ja tietojen luovutus

Ohjaa haastattelu- ja kyselypyynnöt asian vastuuhenkilölle ja toimi organisaation viestintäpolitiikan mukaisesti. Pyydä tarvittaessa apua esihenkilöltäsi.

Varo antamasta viattomankin oloisten keskustelujen yhteydessä tietoa salassa pidettävistä tai yksityisyyden suojan piiriin kuuluvista tiedoista. Ole tarkka etenkin erilaisissa internetissä toimivissa sosiaalisen median palveluissa.

Ohjaa tietojen luovutus- ja tutkimuspyynnöt vastuuhenkilölle, jonka tehtävänä on varmistua tietojen luovutuksen perusteista ja mahdollisesta korvattavuudesta sekä päättää luovutuksesta. Ellet tiedä oikeaa tahoja, ota yhteys esihenkilösi.

Havaitsitko ongelman?

1. Jos huomaat tietoturvaongelman, velvollisuutesi on tarttua asiaan ja ilmoittaa siitä välittömästi esihenkilöllesi ellet itse pysty korjaamaan ongelmaa.
2. Ilmoita tietoturvallisuuteen liittyvistä ongelmista, uhkista tai suojauspuutteista organisaatiosi tietosuojavastaavalle tai esihenkilöllesi.
3. Jos huomaat tietoturvaongelman, velvollisuutesi on tarttua asiaan. Älä luota siihen, että joku muu ilmoittaa tai korjaa ongelman.
4. Ilmoita tietoturvallisuuteen liittyvistä ongelmista, uhkista tai suojauspuutteista esihenkilöllesi ja kunnan tietohallintoon. Heidän velvollisuutenaan on ryhtyä toimenpiteisiin.
5. Jos hallussasi oleva laite, kulkukortti, tunniste tms. katoaa tai varastetaan, ilmoita siitä välittömästi esihenkilöllesi, kunnan tietohallintoon tai päätelaitteen tukipalvelusta

vastaavalle toimittajalle mahdollisen vahingon pienentämiseksi ja oman vastuusi rajaamiseksi.

6. Jos epäilet päätelaitteeseesi tai käyttämäsi tietojärjestelmään liittyvää tietoturvaongelmaa tai haittaohjelmatartuntaa, ota yhteyttä Savon ICT:n palvelupisteeseen 017 272 3725.
7. Älä sulje päätelaitetta
8. Kerro mitä olit tekemässä, kun kone alkoi toimia odottamattomasti.
9. Toimi saamiesi ohjeiden mukaisesti.
10. Ilmoita asiasta myös esihenkilöllesi ja kunnan tietohallintoon.
11. Jos epäilet muuta tietoturvapoikkeamaa, ota yhteyttä kunnan tietohallintoon

Yhteystiedot poikkeamatilanteissa

hallintojohtaja Ulla Nikulainen 040 4883 211

ict-asiantuntija Kaarina Haapalainen 040 4883 042

Lisätietoa

<https://vm.fi/tiedonhallintalautakunta>

<https://www.suomidigi.fi/ohjeet-ja-tuki>

<https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet>

<https://www.suomidigi.fi/ohjeet-ja-tuki/jhs-suositukset-lakkautetut>

<https://vm.fi/julkisen-hallinnon-ict>