Keski-Pohjanmaan liiton Tietoturvaohje 2019

Sisältö

Käsitelty liiton toimistopalaverissa 16.4.2019

1. Yleisesti tietoturvasta

Tietoturvallisuus on osa organisaation toiminnan laatua, huolellinen henkilöstön jäsen pitää huolen sekä työtehtäviensä laadusta sekä huolehtii omasta ja samalla välillisesti muitten tietoturvasta. Vastuu tietoturvasta ja sen osaamisesta kuuluu jokaiselle organisaation työntekijälle.

Tietoturvajärjestelyjen tarkoituksena on varmistaa tietoaineistojen, tietojärjestelmien ja palveluiden asianmukainen suojaus siten, että niiden luottamuksellisuuteen ja saatavuuteen liittyvät riskit otetaan huomioon. Käytännössä tämä merkitsee mm. sitä, että tiedot ja tietojärjestelmät pidetään vain niiden käyttöön oikeutettujen henkilöiden saatavilla. Tietojen käsittelyyn oikeutetutkin saavat käyttää tietoja ja järjestelmiä vain asianmukaisesti työtehtävissään.

Tietokoneen, mobiililaitteiden sekä ohjelmistojen käyttö on isossa osassa työtehtäviä ja käyttäjän vastuulla niitten turvallinen käyttö.

Tällä ohjeella pyritään antamaan liiton henkilöstölle yhteneväiset toimintatavat, joiden mukaisesti ylläpidetään tietoturvaa sekä toimintaan tietoturvallisissa riskitilanteissa.

Ohjeiden tarkoitus on taata turvallinen ja tehokas työskentely kaikille.

Tämä ohje ei ota kantaa sosiaalisen median käyttöön. Sosiaalisen median käytöstä työssä ja vapaa-ajalla on annettu erillinen toimintaohje.

2 Julkisuuslaista ja henkilötietojen suojasta

Julkisuuslaki[1] määrittelee sen, että mikä tahansa asiakirja, joka on julkisen vallan viranomaisen hallussa, kuuluu julkisuuslain piiriin.

Asiakirja tulee julkiseksi, kun se valmistuu. Tämä tarkoittaa, että päätökset ja vastaavat tulevat julkisiksi antohetkellään. Tutkimukset ja tilastot ovat kuitenkin julkisia heti valmistuttuaan käyttökelpoiseen muotoon.

Jokaisella on oikeus saada tieto viranomaisen julkisesta asiakirjasta[2]. Asiakirja voi tarkoittaa mitä tahansa tallennetta esitysmuodosta riippumatta. Mikäli tallennetta ei voi käsitellä yleisesti käytössä olevin menetelmin, halukkaalle on annettava tilaisuus tutustua siihen viranomaisen laittein. Asiakirjan antamisesta katseltavaksi ja jäljennettäväksi ei saa periä maksua.

Julkisuuslaki ei estä tiedon antamista asiakirjoista, jotka keskeneräisyytensä vuoksi eivät vielä ole julkisia. Tällaisesta asiakirjasta voidaan antaa tieto, jos viranomainen niin päättää. Salaisesta asiakirjasta voidaan antaa julkiset osat.

On oltava erityisen varovainen salassa pidettävistä tiedoista sekä henkilötiedoista, joita ovat mm. liike- ja ammattisalaisuudet, terveydentilaa koskevat tiedot, poliittinen vakaumus (ei koske luottamushenkilöitä), yksityiselämää koskevat tiedot, pankkitiedot, sosiaaliturvatunnus ja palkkatiedot.

Salaista tietoa ei saa koskaan lähettää salaamattomana sähköpostilla vaan se tulee toimittaa vastaanottajalle kirjepostina. Sähköpostin voi myös salata erillisellä sovelluksella. Liitolla on käytössä salausohjelma, jota voi käyttää kirjaamon kautta. Tarvittaessa käytön aloittamisessa avustaa myös hallintopäällikkö.

Käsiteltäessä salassa pidettäviä tietoja on varmistettava ettei niihin kukaan pääse käsiksi (tallenna, tulosta, skannaa, kuljeta, lähetä ja tuhoa) eivätkä ne joudu ulkopuolisen tietoon.

[1] Laki viranomaisen toiminnan julkisuudesta 621/1999
[2] Suomen perustuslaki (731/1999) 2.luku 12§ *sananvapaus ja julkisuus*

3. Käytäntöä

3.1. Tiedon käsittely

Ulkoinen muisti

Ulkoisen muistin voi kiinnittää tietokoneeseen helpoiten USB-liitännän kautta. Käytettäessä muistitikkuja ei ole väliä onko tietokone päällä vai ei, muistiin voi tallentaa tiedostoja tai suoritettavia ohjelmia.

Ulkoisen muistin pitäminen ensisijaisena tai ainoana tallennuspaikkana tulee välttää.

Löydettäessä liiton tiloista muistitikku tai muun ulkoisen muistin media, joka ei kuulu löytäjälle se tulee toimittaa eteenpäin tutkimatta tai avaamatta sen sisältöä.

Talon ulkopuolelta tulleet suoritettavat ohjelmat ovat aina turvallisuusriski ja voivat sisältää haittaohjelmia.

Paperinen aineisto

Käsittelyssä tulee käyttää samaa huolellisuutta kuin sähköisen aineiston käsittelyssä.

M-Filesiin tallennetaan kaikki sähköinen aineisto. Työkappaleen voidaan ennen sen valmistumista tallentaa Z-asemalle. Tietokone tai sen työpöytä eivät ole säilytykseen käytettäviä paikkoja. Z-aseman ajoittaisen siivoamisen hoitaa jokainen henkilökohtaisesti

Tulostettaessa ja kopioitaessa tulee varmistaa, etteivät paperit jää kopiohuoneeseen asiattomien henkilöiden katseltaviksi. Etenkin salassa pidettävä materiaali on haettava välittömästi tulostuksen jälkeen pois koneesta. Ylimääräistä tulostamista ja kopiointia tulisi välttää sen tietoturvariskin sekä ympäristövaikutusten vuoksi.

Pysyvät ja pitkäaikaisesti säilytettävät asiakirjat arkistoidaan paperisesti. Dokumentin päälle kirjoitetaan arkistokappale ja toimitus arkistonhoitajalle. Liitossa ei ole käytössä sähköistä arkistointia.

M-Files

Asiakirjat tulee tallentaa M-Filesiin aina kun se on mahdollista. M-Files huolehtii asiakirjojen versioinnista ja näin saatavilla on asiakirjasta aina viimeisin versio ja tarvittaessa voidaan palata aiemmin tehtyihin versioihin. Muutoksien tekijät jäävät myös näkyviin. Muista palauttaa asiakirja muokkauksesta, mikäli se on luonteeltaan sellainen, että muutkin sitä työstävät esim. esityslistat ja yhteiset pohjat.

Käytettäessä poista-toimintoa tulee noudattaa varovaisuutta. Ohjelma kysyy varmistuksen tiedoston poistosta, poistaessa viestiä se tulisi lukea ja peruuttaa toiminto, jos et oikeasti haluta poistaa viestiä.

Jos asiakirjan tallentaminen M-Filesiin ei ole tarkoituksenmukaista tai mahdollista, talletetaan työ verkkolevylle, jonka varmuuskopioinnista tietohallinto huolehtii. Huom! työpöydällä olevat kuvakkeet, kansiot ja tiedostot eivät kuulu varmuuskopioinnin piiriin.

Tietojen hävittäminen

Paperiset asiakirjat, joissa on allekirjoitus tai salassa pidettäviä tietoja hävitetään aina tietosuoja-astiaan, joka sijaitsee liiton kellaritiloissa.

USB-muistit ja ulkoiset kiintolevyt tulee tyhjätä ennen niiden luovuttamista eteenpäin. Hävitettävät on toimitettava atk-tukeen.

3.2. Tietokoneen käyttö

Kannettava tietokone on henkilökohtainen työväline ja se on tarkoitettu vain henkilökohtaiseen käyttöön, omaa työkonetta ei saa antaa muitten henkilöiden käyttöön. Liiton palomuuri kerää lokia tietokoneen verkkoliikenteestä, käytöstä, käyttöajasta, latauksista sekä muista aktiviteeteista. Lokia käytetään vain uhkien löytämiseksi sekä haavoittuvuuksien paikkaamiseksi.

Matkustaessa ja etäkäytössä tulee tietoturvaan käyttää erityistä huomiota. Kannettavat työvälineet muodostavat suuremman riskin kuin pöytäkoneet. Niin vahingossa tapahtuvien kadottamisten kuin varkauksienkin näkökulmasta, parhaiten suojaudut pitämällä kannettavan aina mukanasi sekä lukitsemalla tietokoneesi aina kun et käytä sitä.

Työkonetta käytetään varovasti ulkopuolisessa verkossa. Älä yhdistä tietokonettasi julkiseen suojaamattomaan verkkoon. WPA (Wi-Fi protected acces) ei ole muualla aina yhtä kattava kuin liiton omassa verkossa. Liitä tietokoneesi vain luotettavaksi arvioituun verkkoon, äläkä liiku sivustoilla, joista epäilet saavasi haittaohjelmistoja.

Yleisen harhaluulon vastaisesti haittaohjelmat tai virukset eivät ilmoita käyttäjälle olemassaolostaan vaan pyrkivät levittäytymään mahdollisimman moneen tiedostosijaintiin, jolloin niitten poistaminen vaikeutuu. Jos tietokoneesi antaa virushälytyksen (huutomerkki tai punainen ruksi virustorjunnan pienoiskuvakkeen päällä), ota heti yhteys atk-tukeen. Tietoteknisiä työvälineitä ei koskaan saa jättää yksin ja laite tulee lukita, eikä niitä saa säilyttää pitkään esim. yön yli autossa.

Työkoneelle ei saa ladata työhön liittymättömiä sovelluksia.

Oma työkone on suoraan yhteydessä tärkeisiin tietojärjestelmiin ja siten sen turvallinen käyttö on olennainen osa tietoturvallisuuden kokonaisuutta. Tietokoneen turvallisen käytön

takaamiseksi tulisi noudattaa seuraavia ohjeita:

- Laitteen, käyttöjärjestelmän tai ohjelmiston turvallisuusasetusten muuttaminen on kiellettyä. Älä sammuta tietoturvaohjelmistoa tai sen osia.
- Käytä vain henkilökohtaista tunnustasi. Väärän tai toisen henkilön käyttäjä-tunnuksen käyttö on kiellettyä. Toisen käyttäjän tunnuksia käytetään vain erikoistilanteissa, jos työn toteuttaminen sitä ehdottomasti vaatii. Toisen henkilön sähköpostiin kirjautuminen luvatta on aina rikos.
- Vain luettavaksi tarkoitetut tiedostot luovutetaan organisaation ulkopuolelle pääsääntöisesti PDF-muodossa. Tästä voidaan poiketa, mikäli se on aineiston käsittelyn kannalta oleellista.
- Lukitse koneesi aina kun poistut työpisteeltä, kun lähdet pois työpaikalta pois tai sulje kone. Koneen sulkeminen on tärkeää myös päivitysten asentamisen ja asennusten viimeistelyn kannalta.

3.3. Internet

Internetin käyttö on sallittua pääsääntöisesti vain työtehtävien hoitamiseen. Internetistä haettu tieto tulee olla peräisin vain luotettavista lähteistä ja tietoon on suhtauduttava kriittisesti eikä sitä saa ottaa viranomaiskäyttöön ilman huolellista lähdeharkintaa.

Työkäyttöön tulevien ohjelmien ja ohjelmapäivitysten haku Internetistä on sallittu, muiden ohjelmien, pelien yms. imurointi ja asennus Internetistä on kielletty.

Internetissä oleville kauppapaikoille, postituslistoille ym. vastaaville tahoille on liiton yhteystietojen antaminen kielletty.

Internetin käyttö laittomaan toimintaan, kuten esimerkiksi luvattoman musiikin kopiointiin on ehdottomasti kielletty.

Verkkosivuille viedään tiedostot aina PDF-muodossa, jotta niitä ei niin helposti ulkopuoliset pääse muokkaamaan.

3.4. Sähköposti

Liiton antama sähköposti ei ole yksityisasioita varten. Liiton sähköpostiosoitteella tulisi välttää kaiken yksityisasioiden hoitoa.

Työtehtävien hoitoon tulee käyttää liiton sähköpostiosoitetta, ilmaisia sähköpostilaatikoita ei saa käyttää viranomaisliikenteessä eikä sähköpostia saa ohjata automaattisesti

viranomaisjärjestelmän ulkopuoliseen järjestelmään. Pidempien poissaolojen aikana on henkilön käytettävä poissaoloilmoitusta.

Sähköpostin käyttö ketjukirjeiden lähettämiseen on kielletty, samoin käyttö kaupallisiin tarkoituksiin, on kielletty. Älä avaa sähköpostin mukana tullutta liitetiedostoa, jollet ole varma viestin lähettäjästä ja liitetiedoston sisällöstä tai viestin tekstiosassa ei mainita liitetiedostosta mitään.

Sähköpostin käytössä tulee huomioida:

- Arkaluontoisten tai salassa pidettävien tietojen lähettäminen sähköpostin välityksellä on ehdottomasti kielletty
- Ole huolellinen kirjoittaessasi vastaanottajan nimeä. Automaattinen osoitteiden täyttöominaisuus voi tarjota sinulle väärää vastaanottajaa.
- Organisaation ulkopuolelle lähetettävissä dokumenteissa tulisi ensisijaisesti käyttää PDF-muotoa. Muita muotoja voidaan käyttää muokattavaksi tarkoitetuissa dokumenteissa.
- Varo kalasteluviestejä, joissa sinua pyydetään luovuttamaan tunnuksesi ja salasanasi tai kirjautumaan jollekin verkkosivulle.
- Sähköpostin lisäksi sinua voidaan yrittää harhauttaa myös muilla keinon, esimerkiksi puhelimessa tai sosiaalisessa mediassa. Varo yllättäviä laskuja ja tekaistuja viestejä ylläpidon nimissä.
- 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

Lähettäessä virallisia lausuntopyyntöjä, ilmoittautumisia, hakemuksia tai tarjouksia, pyydetään vastaukset viralliseen sähköpostiosoitteeseemme: kirjaamo@keski-pohjanmaa.fi. Näin toimien voidaan vastauksia hyödyntää aina, riippumatta siitä onko ko. henkilö paikalla.

Työnantaja voi hakea ja avata hänelle tarkoitetut sähköpostit työntekijän sähköpostista yksityisyyden suojasta työelämässä[3] annetun lain perusteella.

Työnantajalla on lupa toimia näin vasta kun työntekijään ei olla saatu yhteyttä ja on todennäköistä, että työntekijän sähköpostissa kiireellistä tietoa, joka ei voi odottaa.

[3] Laki yksityisyyden suojasta työelämässä 759/2004

3.5. Matkapuhelimet ja tablet-tietokoneet

Mobiililaitteisiin voidaan nykyään tallentaa valtavat määrät tietoa, usein matkapuhelimessa on tallessa satoja yhteystietoja ja sähköpostiosoitteita. Laitteiden pienen koon vuoksi riski niiden katoamiseen vahingon tai varkauden yhteydessä on suuri. Niiden käytössä noudatetaan seuraavia ohjeita ja tarvittaessa neuvoa voi kysyä atk-tuelta.

- Matkapuhelin tulee matkustaessa säilyttää taskussa, laukussa tai muutoin välittömässä läheisyydessä
- Älä puhu luottamuksellisista asioista julkisissa tiloissa tai kulkuvälineissä esim. odotustiloissa, junassa tai linja-autossa
- Suojaa mobiililaitteesi asettamalla suojakoodi sekä automaattinen lukitus päälle
- Sulje langattomat yhteydet (Bluetooth, WLAN ja NFC) aina kun et tarvitse niitä
- Jos laite katoaa, ilmoita katoamisesta välittömästi

3.6 Vierailijat

Vierailuiden tietoturvan varmistamiseksi on noudatettava seuraavia käytäntöjä:

- Toimiston ollessa suljettuna oven avaaja ilmoittaa vierailijasta isännälle, joka noutaa vieraan.
- Vierailut tulee ensisijaisesti järjestää neuvottelutiloissa.
- Neuvottelutilojen varaukset tehdään sähköiseen kalenteriin, jonka aikatauluja pyritään noudattamaan.
- Noudata "puhtaan pöydän" periaatetta, työpöydällä ei saa säilyttää salassa pidettävää tai ei-julkista tietoa.
- Toimistoajan ulkopuolella ei järjestetä kokouksia, ellei talon henkilökuntaan kuuluvaa henkilöä ole varmistamassa, ettei työhuoneissa käydä.
- Liitolla on käytössä kaksi verkkoa, "KPL-Guest" ja "KPL-Office". Nimensä mukaisesti KPL-Office on varattu vain liiton henkilöstölle. Henkilöt, jotka eivät kuulu liiton vakituiseen henkilökuntaan ohjataan käyttämään vierasverkkoa.

3.7. Käyttäjätunnukset ja salasanat

Käyttäjätunnukset ja salasanat ovat henkilökohtaisia. Käsiteltäessä salasanoja ja tunnuksia tulee toimia huolellisesti sekä seuraavia ohjeita noudattaen :

- Pidä salasana vain omana tietonasi.

- Jos pidät salasanaasi muistilapulla, säilytä sitä lukitussa tai muussa turvallisessa paikassa.
- Käytä riittävän vaikeaa salasanaa, mieluiten vähintään 8 merkkiä sisältäen isoja sekä pieniä kirjaimia, numeroita ja erikoismerkkejä
- Älä käytä samaa salasanaa mitä käytät yksityisillä tileilläsi
- Käytä salasanoja, jotka eivät ole yhdistettävissä sinuun. Huonoja salasanoja ovat esim. lemmikkien tai puolison nimi sekä syntymäajat.

4. Aiheeseen liittyvä lainsäädäntö

- Suomen perustuslaki (721/1999)[4] 2. luku 10 § ja 12 §
- Laki viranomaisen toiminnan julkisuudesta (621/1999)[5]
- Asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999)[6]
- Laki kunnallisesta viranhaltijasta (304/2003)[7]
- Työsopimuslaki (55/2001)[8]
- Arkistolaki (831/1994)[9]
- Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004)[10]
- Laki yksityisyyden suojasta työelämässä (759/2004)[11]
- Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)[12]
- Laki sähköisen viestinnän palveluista (914/2014)[13]
- Tietosuojalaki (1050/2018)[14]

Ulkoisten toimijoiden tekemät tietomurrot sekä liiton sisältä tietojen tahallinen vuoto täyttävät rikoksen tunnusmerkistön.

- Rikoslaki15 (39/1889) 34. luku 9 § ja 38. luku tieto- ja viestintärikoksista
- Euroopan parlamentin ja neuvoston direktiivi tietojärjestelmiin kohdistuvista hyökkäyksistä 2013/40/EU16

[4] Suomen perustuslaki (721/1999)
[5] Laki viranomaisen toiminnan julkisuudesta (621/1999)
[6] Asetus viranomaisen toiminnan julkisuudesta ja hyvästä hallintotavasta (1030/1999)
[7] Laki kunnallisesta viranhaltijasta (304/2003)
[8] Työsopimuslaki (55/2001)
[9] Arkistolaki (831/1994)
[10] Laki kansainvälisistä tietoturvavelvoitteista (588/2004)
[11] Laki yksityisyyden suojasta työelämässä (59/2004)
[12] Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)
[13] Laki sähköisen viestinnän palveluista (917/2014)
[14] Tietosuojalaki (1050/2018)
[15] Rikoslaki (39/1889)
[16] Euroopan parlamentin ja neuvoston direktiivi tietojärjestelmiin kohdistuvista hyökkäyksistä 2013/40/EU