



Alajärven kaupunki

Alajärvi – Aitoa elämää Aaltojen keskellä

Alajärven kaupunki

Tietosuoja-, tietoturva- ja salassapito-ohje

Ark.kohta 07 01 00

Hyv. henk.jaosto 10.4.2019 § 25
Voimaantulo 16.4.2019

Sisällysluettelo

Tietosuoja-, tietoturva- ja salassapito-ohje	2
1 Salassapito	2
2 Henkilökohtainen käyttäjätunnus ja salasanojen käyttö	3
3 Työaseman ja muiden sähköisten viestintävälineiden käyttö	3
4 Sähköpostin ja Internet-yhteyksien käyttö	5
5 Järjestelmäkohtaiset ohjeet	5
6 Seuraamukset	6
7 Ongelmista ilmoittaminen ja väärinkäyttöihin puuttuminen	6

Tietosuoja-, tietoturva- ja salassapito-ohje

Alajärven kaupungin hallinnon työasemiin, langalliseen/langattomaan tietoverkkoon ja atk-järjestelmiin saadut käyttöoikeudet velvoittavat käyttäjiä toimimaan tämän tietosuoja-, tietoturva- ja salassapito-ohjeen mukaisesti.

1 Salassapito

- Palvelussuhteen / muun työtehtävän aikana tai sen päätyttyä, työssä saatuja, sen toimintayksikköjä, asiakkaita, sopimuskumppaneita tai muita yhteistyötahoja koskevia luottamuksellisia tai salassa pidettäviä tietoja ei saa ilmaista ulkopuoliselle tai sivulliselle. Tällaisia ovat mm. arkaluontoiset henkilötiedot, potilastiedot, terveystiedot, sosiaalitoimen asiakastiedot, oppilastiedot, liike- ja ammattisalaisuudet sekä tiedot turvallisuus- ja valmiusjärjestelyistä.
- Rekisterien katselu- tai käyttöoikeutta ei saa olla muihin kuin omien työtehtävien edellyttämiin tietoihin. Esim. työtovereiden tai julkisuuden henkilöiden tietojen käsittely on kiellettyä, mikäli työtehtävät eivät sitä edellytä. Omien tietojen käsittely ja katselu ei ole sallittua edes työtehtävien puitteissa. Lähisukulaisten tietojen käsittely ei ole sallittua, paitsi sosiaali- ja terveyspalveluissa jos lähisukulaiseen on voimassa oleva hoitosuhde. Ohjeiden vastainen toiminta on ehdottomasti kiellettyä ja sellaisenaan rangaistavaa. Tietojen oikeudettomasta käytöstä voi seurata rikos-, työ- ja vahingonkorvausoikeudellisia seuraamuksia.
- Mikäli rikkeet ovat vakavia ja/tai toistuvia, voi työnantaja tarvittaessa päättää virka- tai työsuhteen.
- Käsittelyllä tarkoitetaan mm. tietojen katselua, tallentamista, käyttöä, siirtämistä, luovuttamista, säilyttämistä, muuttamista, yhdistämistä tai poistamista.
- Ilman rekisteristä vastaavan kirjallista lupaa ei ole sallittua luovuttaa tai siirtää salassa pidettäviä asiakas-, henkilö- tai potilastietoja tai muuta salassa pidettävää tietoa, eikä tallentaa niitä toisiin rekistereihin, työaseman kiintolevylle, levykkeelle tai muille talletuslaitteille, eikä tehdä niistä muita kuin työhön liittyviä muistiinpanoja. Salassa pidettävää tietoa ei saa käyttää omaksi tai toisen eduksi tai vahingoksi.
- Salassapito sekä tietojen ja tietojärjestelmien käyttö perustuvat lainsäädäntöön sekä normiohjaukseen. Kaikkia tietoja pitää käsitellä aina huolellisesti sekä hyvän hallintotavan mukaisesti.
- Salassapito on lähtökohta, mutta toisaalta on erityislainsäädäntöä, joka saattaa jopa velvoittaa tiedonvaihtoon. Salassapitovelvollisuudesta (asiakirjasalaisuus,

vaitiolovelvollisuus) ja viranomaisyhteistyöstä säädetään useissa laeissa, mm. julkisuuslaki, henkilötietolaki, lastensuojelulaki, perusopetuslaki, laki sosiaalihuollon asiakkaan asemasta ja oikeuksista.

- Tämä ohje koskee henkilökunnan lisäksi myös luottamushenkilöitä, opiskelijoita sekä muita henkilöitä jotka käsittelevät organisaation salassa pidettäviä tietoja.
- Lisätietoja tietosuojasta, tietoturvasta ja salassapidosta löytyy mm. kaupungin tietoturvapoliitikasta ja tietosuojaohjeistuksesta, nämä löytyvät kaupungin Intranetista ja yksiköiden esimiehiltä.

2 Henkilökohtainen käyttäjätunnus ja salasanojen käyttö

- Työasemaa saa käyttää vain omalla käyttäjätunnuksella ja salasanalla. Käyttäjätunnukset ovat henkilökohtaisia. Kukin vastaa käyttäjätunnuksellaan tehdyistä merkinnöistä ja niistä kirjautuvista lokitiedoista. Sama pätee kulunvalvontalaitteisiin rekisteröityneistä käyttäjäkirjauksista.
- Salasana on vaihdettava heti sen saamisen jälkeen ja myöhemmin tarvittaessa tai sovituin aikavälein.
- Käyttäjätunnus ja salasana on pidettävä salassa. Niitä ei saa antaa muiden tietoon.
- Salasanoja ei saa tallentaa työasemalle tai selaimen.
- Tietojärjestelmistä on kirjauduttava ulos ja työasema on lukittava välittömästi käytön jälkeen, ellei työasema ole käyttäjän valvonnassa.

3 Työaseman ja muiden sähköisten viestintävälineiden käyttö

- Työasemassa saa käyttää vain Alajärven kaupungin hyväksymiä ja lisensoituja ohjelmia, jotka ovat Järvinet Oy:n asentamia ja tukemia.
- Alajärven kaupungin hankkimia ohjelmia ei saa luvatta kopioida eikä käyttää työpaikan ulkopuolella.
- Työasemaa ei saa liittää **verkkoon luvatta**.
- Samoja levykkeitä tai muita tietovälineitä ei saa käyttää työpaikalla ja sen ulkopuolella, jollei ole varmistautunut niiden viruksettomuudesta.
- Työhön tai luottamustoimeen liittyviä salassa pidettäviä tietoa ei saa siirtää tai pitää säilytyksessä julkisissa pilvipalveluissa, kotilaitteissa tai muissa suojaamattomissa laitteissa.

- Jos kuitenkin muun kuin salassa pidettävän tiedon säilytyksessä ja käsittelyssä käytetään esim. julkisia pilvipalveluita, tulee noudattaa varovaisuutta tietoturvan suhteen ja laitteiden valvonnassa, ettei ulkopuoliset pääse tietoon käsiksi.
- Salassa pidettäviä tietoja ei saa tulostaa valvomattomaan tulostimeen. Käytä turvatulostusta tai tulostuskoodia jos ne ovat käytettävissä.
- Epäiltäessä työaseman olevan tietokoneviruksen saastuttama, työasemalla työskentely on lopetettava välittömästi. Tietokoneviruksista on aina ilmoitettava Alajärven kaupungin IT-tukeen.
- Työaseman käytössä on otettava huomioon tietoverkon ja palvelinlaitteiden rajoitettu kapasiteetti. Kuvia, grafiikkaa ja äänitiedostoja saa välittää verkossa tai tallentaa palvelimelle vain työtehtävien vaatiessa.
- Tarpeettomaksi käyneet tiedot ja muut tietosuojattavat materiaalit tulee hävittää asianmukaisesti, esim. tietosuojattavan jätteen hävityspöytäöihin. Kysy tarvittaessa lisätietoja esimieheltäsi tai tietosuojavastaavalta.
- Työasemaan talletettujen tiedostojen varmuuskopioimisesta vastaa kukin käyttäjä itse. Palvelimilla olevien tiedostojen varmistuskopiointi hoidetaan keskitetysti Järvinet Oy:n toimesta.
- Sähköisten viestintävälineiden (mm. sähköposti, kalenterit, pikaviestit, tabletit ja älypuhelimet) käytössä, tulee aina noudattaa velvoittavia ohjeita ja määräyksiä. Esim. tableteissa ja älypuhelimissa on AINA käytettävä lukituskoodia laitteen lukituksen avaamiseen.
- Työnantajan järjestelmien etäkäyttöön tulee saada lupa esimieheltä (asennettava erikseen). Käytettäessä työnantajan järjestelmiä työpaikan ulkopuolella, tulee varmistaa, että sivulliset kuten perheenjäsenet eivät näe tai kuule työtietoja, eivätkä käytä etätyölaitteita tai etäyhteyksiä.
- Turhien ja tarpeettomien käyttöäoikeuksien anominen on kielletty. Jos käyttöoikeudet jäävät tarpeettomiksi tai ovat vääränlaisista, ilmoita asiasta esimiehellesi tai Järvinet Oy:n ICT-asiantuntijoille. Työ- tai virkasuhteen päättyessä tai tehtävien muuttuessa, järjestelmistä ja tietokoneista tulee poistaa omat henkilökohtaiset tiedostot ja muut tarpeettomat tiedot. Työhön liittyvät tiedot pitää siirtää työnantajan saataville, jos ne ovat tallennettuna henkilökohtaiselle asemalle, jotta toiminta voi jatkua häiriöttä. Tietojärjestelmiin, työasemiin tai verkkolevyille tallennetut, työhön liittyvät tiedot ovat työnantajan omaisuutta ja niiden jatkokäyttö on työnantajan ratkaistavissa. Kun työ-/virkasuhde päättyy, käyttäjätunnukset (käyttäjätunnukset sekä sähköpostiosoite) poistetaan pikimmiten käytöstä.
- Työntekijä vastaa käytössään olevista tietokoneista tai muista laitteista niin, etteivät ne tai niissä olevat tiedot joudu väärin käsiin. Laitteiden vaihtuessa tulee vanhat laitteet palauttaa ohjeiden mukaisesti. Työsuhteen/luottamustoimen päättyessä laitteet palautetaan esimiehelle tai laitteen luovuttaneelle taholle.

4 Sähköpostin ja Internet-yhteyksien käyttö

- Sähköposti ja Internet-yhteydet on tarkoitettu työtehtävien hoitoon.
- Arkaluonteisia ja muita salassa pidettäviä tietoja ei saa lähettää normaalin sähköpostin välityksellä.
- Salattu sähköposti on käytössä, mikäli työtehtävien luonteen vuoksi sähköpostilla tulee lähettää arkaluontoista tietoa sisältävää postia.
- Virusriskin vuoksi ulkopuolelta tulevan sähköpostin liitetiedostoja ei saa avata, jos viesti tulee epämääräisestä lähteestä.
- Sähköpostiketjukirjeitä ja muuta roskapostia ei saa lähettää eikä välittää eteenpäin, vaan ne on tuhottava.
- Internetistä ei saa kopioida ohjelmia.
- Internet/WWW-selaimen käytöstä kertyy loki- ja varmistustietoa, josta tarvittaessa tehdään yhteenvetoraportteja käyttötilanteen seuraamiseksi.
- Järvinet Oy:n työntekijät, johtoryhmän henkilöt ja tietosuojavastaava saattavat järjestelmien ylläpitotehtävien suorittamiseksi tai tietoverkon väärinkäytösten selvittämiseksi (mm. tietoturva huolehtiminen, tekninen vika tai väärinkäytös-tilanne) tulla tietämään käyttäjien lähettämien tai vastaanottamien viestien lokitiedot (ei viestin sisältöä) lainsäädännön puitteissa.

5 Järjestelmäkohtaiset ohjeet

- Kunkin käyttäjän on tutustuttava Alajärven kaupungin tietoturvapoliittikkaan, tietoturvaohjeisiin sekä käyttämiensä tietojärjestelmien käyttöohjeisiin ja kyseisten rekistereiden tietosuojaselosteisiin.
- Tietojärjestelmien käytöstä kertyy lokitietoa ja käyttöä seurataan. Lokitietojen kerääminen ja käsittely suoritetaan kaupungin tietojärjestelmissä, joissa on henkilötietoja ja mahdollisuus kyseisten tietojen keräämiseen. Näiden tietojen keräämisen ja käsittelyn tarkoitus on varmistaa järjestelmien oikeanlainen käyttö ja toimivuus sekä selvittää mahdollisia väärinkäytöksiä. Tietojen kerääminen ja käsittely kuuluvat lakisääteiseen toimintaan suojata henkilötietoja. Lokitietoja seurataan ja analysoidaan säännöllisin väliajoin ja aina tarvittaessa jos on syytä epäillä väärinkäytöstä. Lokitietoja ei luovuteta ulkopuolisille paitsi jos laki näin velvoittaa. Lokitietoja analysoivat ja käsittelevät henkilöt ovat ennalta määrättyjä jotka ovat työnsä puolesta siihen oikeutettuja ja jotka osaavat niitä tulkita.
- Tämä ohjeen kautta käyttäjien tulee olla tietoisia siitä, että tietojärjestelmissä käyntejä ja siellä tehtyjä tapahtumia tallennetaan lokitietoihin, käyttöä valvotaan ja epäilyistä väärinkäytöstä raportoidaan esimiehelle tai viranomaiselle.

6 Seuraamukset

- Sääntöjen ja periaatteiden rikkomisesta käyttöoikeudet tietojärjestelmiin voidaan peruuttaa ja rikkomuksista tiedotetaan aina esimiehelle.
- Jos kyseessä on toistuva tai vakava rikkomus, ryhdytään tapauksen edellyttämiin jatkotoimiin. Mikäli rikkomuksesta aiheutuu välittömästi tai välillisesti taloudellisia menetyksiä, voidaan päätyä vahingonkorvausvaatimuksiin.
- Tietojen väärinkäyttö tai tahallinen ohjeiden vastainen toiminta voi johtaa muun ohella rikosoikeudellisiin seuraamuksiin.

7 Ongelmista ilmoittaminen ja väärinkäytöksiin puuttuminen

- Jos havaitset tietoturvaan, tietosuojaan tai tietojärjestelmiin liittyviä väärinkäytöksiä ja ongelmia, ilmoita niistä pikimmin tietosuojavastaavalle (teemu.karhunen(at)jarvinet.fi, puh. 040 757 5515) ja omalle esimiehellesi.
- Jos toimit esimiehenä, puutu tietojenkäsittelyn, tietojärjestelmien, tietoturvan ja tietosuojan väärinkäytöksiin, sekä ilmoita niistä tietosuojavastaavalle (teemu.karhunen(at)jarvinet.fi, puh. 040 757 5515).

Mikäli sinulla on epäselvyyttä tämän ohjeen sisällön tai merkityksen suhteen, selvitä asia ensi tilassa esimieheltäsi tai tietosuojavastaavalta. Noudattamalla annettuja ohjeita ja määräyksiä varmistetaan jokaisen oikeusturva.