

# MIKSI TIETOTURVALLISUUS ON TÄRKEÄÄ?

**Seinäjoen koulutuskuntayhtymässä käsitellään runsaasti erilaista luottamuksellista tietoa, esimerkiksi ihmisten henkilötietoja, taloustietoja ja opiskelijarekisteriä. Tieto ei saa joutua tahattomastikaan asiattomien käsiin. Myös julkista tietoa on käsiteltävä huolellisesti siten, että se on tarkoituksenmukaisesti saatavilla ja ettei sitä päästä luvottomasti muuttamaan.**

**Tietojärjestelmien luotettava toiminta on välttämätöntä Seinäjoen koulutuskuntayhtymän toiminnalle. Kuntayhtymästä ulospäin lähtevän tiedon on oltava luotettavaa. Paras suoja haittaohjelmia (virukset, madot ja troijalaiset), tietomurtoja ja tahatonta tai tahallista vahingontekoa vastaan on kaikkien tietojärjestelmien huolellinen ylläpito ja käyttö.**

**Suurimmat tietoturvallisuuden ongelmat liittyvät yleisesti huolimattomuuteen, ymmärtämättömyyteen ja osaamattomuuteen.**

**Tietoturvallisuus on juuri niin hyvää kuin sen heikoin lenkki — ei siis vain tekniikka vaan myös jokapäiväiset toimintatapamme ja asenteemme. Tietoturvallisuudesta huolehtiminen on jokaisen työskentelevän ja opiskelevan velvollisuus. Tietoturvallisuustoiminnan perusta on määritelty Seinäjoen koulutuskuntayhtymän tietoturvapoliitikassa. <http://www.epedu.fi/kayttosaannot/>**

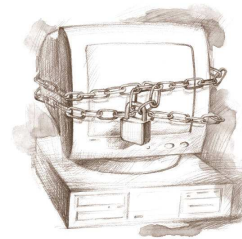
## TIETOKONEEN KÄYTTÄMINEN



- Vastaa käyttäjänä omasta koneestasi. Ole siis huolellinen - Tietokoneeltasi pääsee tietoihin, jotka ovat itse laitetta arvokkaampia.
- Vain atk-tuki saa asentaa laitteita verkkoon.
- Vain atk-tuki saa perustaa lähiverkkoon palvelimia.
- Atk-tuki vastaa asentamistaan ohjelmista.
- Älä muuta kansioiden ja levyjen käyttöoikeuksia, siten että atk-tuen ylläpito toiminta vaikeutuu.
- Estä asiaton pääsy tietojärjestelmiin lukitsemalla koneesi aina kun poistut huoneestasi (paina Ctrl-Alt+Del ja valitse "Lukitse tietokone") tai kirjaudu ulos koneelta.

## KÄYTTÖOIKEUDET JA SALASANAT

- Tietojärjestelmien käyttöön tarvitaan aina käyttöoikeus.
- Älä luovuta henkilökohtaisia käyttäjätunnuksia ja salasanojasi toisen henkilön käyttöön, ei edes atk-tuen edustajana esiintyvälle.
- Vaihda salasanasasi riittävän usein ja heti, jos epäilet niiden paljastuneen.
- Älä anna ulkopuolisen käyttää tietokonettasi, ellet pysty vastaamaan siitä kuin omasta käytöstäsi.
- Älä kirjoita salasanoja muistiin — ainakaan sellaiseen paikkaan mistä ne ovat helposti löydettävissä.



## TIETOJEN KÄSITTELEMINEN

- Käsittele tietoja huolellisesti välineestä riippumatta — olipa tiedon välittäjänä sitten tietokone, paperi, puhelin tai faksi.
- Tallenna tekemäsi työ palvelimelle, mistä tiedot voidaan varmistaa atk-tuen toimesta. Varmista yksittäinen atk-tuella, mikä on käytäntö yksityisten tiedostojen varmuuskopiointista. Käytäntö vaihtelee eri yksiköiden välillä. On huomioitava, että käyttäjä vastaa itse tiedostojensa suojauksesta sekä viime kädessä niiden varmuuskopiointista.

- Tarkista talon ulkopuolelta tuotu levyke, cd tai jokin muu muistiväline virustorjuntaohjelmalla. Atk-tuesta on saatavana virustorjuntaohjelmistot myös kotikoneisiin.
- Kuljeta matkoillasi mukana vain välttämätön määrä tietomateriaalia, älä koskaan jätä niitä vartiomatta esim. julkisissa kulkuneuvoissa.
- Tutustu tietojen luokittelusta ja käsittelystä annettuihin ohjeisiin, <http://www.epedu.fi/kayttosaannot/>
- Älä anna kenenkään nähdä tietokoneesi näyttöä tai näppäimistöä kun käsittelet arkaluontoista materiaalia tai syötät salasanoja.
- Hae tulosteesi verkkotulostimesta heti tulostuksen jälkeen.
- Käytä silppureita tai tietosuojajätteen keräilypisteitä luottamuksellisen ja arkaluontoisen materiaalin hävittämisessä.
- Mikäli joudut lähettämään luottamuksellista tietoa faksilla, varmista, että toisessa päässä on vastaanottaja paikalla ja että viesti on mennyt oikein perille.

## FYYSINEN TURVALLISUUS

- Tue osaltasi kuntayhtymän kulunvalvontaa. Ohjaa ystävällisesti vieraat ja "eksyneet" henkilöt oikeisiin paikkoihin.
- Älä päästä asiattomia henkilöitä kuntayhtymän tiloihin.
- Vastaa omista vieraistasi ja heidän kulkemisestaan kuntayhtymässä joko omakohtaisesti tai muun kuntayhtymän henkilökuntaan kuuluvan avustuksella.
- Säilytä tieto ja laitteet turvassa.
- Älä jätä kannettavaa tietokonetta tai matkapuhelinta ilman valvontaa. Säilytä laitetta lukitussa paikassa. Muista myös levykkeiden, paperitulosoiden ym. säilyttäminen niin, etteivät ne joudu väärin käsiin.



- Kannettavia tietokoneita tai matkapuhelimia ei saa jättää autoon näkyvälle paikalle, eikä niitä saa säilyttää autossa yön yli.
- Pidä työpöytä puhtaana. Älä jätä vierasta yksin tai valvonnatta työhuoneeseen tai muihin kuntayhtymän tiloihin.
- Jos käyttämäsi tallennusväline (levyke, cd-levy yms.) rikkoutuu, se on luotettavalla tavalla hävitettävä. Rikkoutuneet tallennusvälineet toimitetaan tietosuojajätteen keräilypisteeseen tai tuhotaan fyysisesti.

## OMAT TIEDOT JA YKSITYISYYS

- On huomioitava, että kuntayhtymän tietojärjestelmiin tallennetut yksityisetkin tiedostot voivat siirtyä myös varmuuskopioihin.
- Käyttäjä vastaa itse vastaanottamiensa henkilökohtaisten viestien käsittelystä.
- Järjestelmiin ja tietoverkon laitteisiin tallentuu yksityiskohtaista lokitietoa järjestelmien käytöstä. Tietoja käytetään ylläpidossa, vianmäärityksessä ja tietoturvallisuuden valvonnassa.
- Kaikki työntekijät ovat vaitiolovelvollisia tietoonsa tulleista yksityisistä viesteistä.

## INTERNET JA SÄHKÖPOSTI

- Internet ja sähköposti on tarkoitettu ensisijaisesti työ-/opiskelukäyttöön.
- Käytä vain sellaisia palveluja, joita pidät luotettavina.
- Muista, että esiinnyt tietoverkossa kuntayhtymän edustajana.
- Internetin kautta ei ole luvallista välittää luottamuksellista tietoa ilman asianmukaista salausta.
- Älä käytä tai asenna omatoimisesti kuntayhtymän tietokoneille Internetin tai muuta kautta saatavia ohjelmia. Vain atk-tuki saa asentaa ohjelmia kuntayhtymän tietokoneille.
- Työhön liittyvä sähköposti vastaanotetaan kuntayhtymän sähköpostijärjestelmään. Sitä ei saa omatoimisesti ohjata kuntayhtymän sähköpostijärjestelmän ulkopuolelle. Vain atk-tuki saa tehdä mahdollisen uudelleenohjauksen. Uudelleenohjauksessa tulee aina varmistua kopion jäämisestä kuntayhtymän palvelimelle. Muualle ohjautuneen sähköpostin tietoturva ja luottamuksellisuudesta vastaa käyttäjä itse.



- Liitetiedostot voivat sisältää haittaohjelmia (viruksia, matoja tai troijalaisia). Varo kaikkia epätavallisia sähköposteja ja varsinkin liitetiedostoja, älä avaa tuntemattomalta lähettäjältä tullutta liitetiedostoa. Ilmoita epäilystäsi aina atk-tukeen.



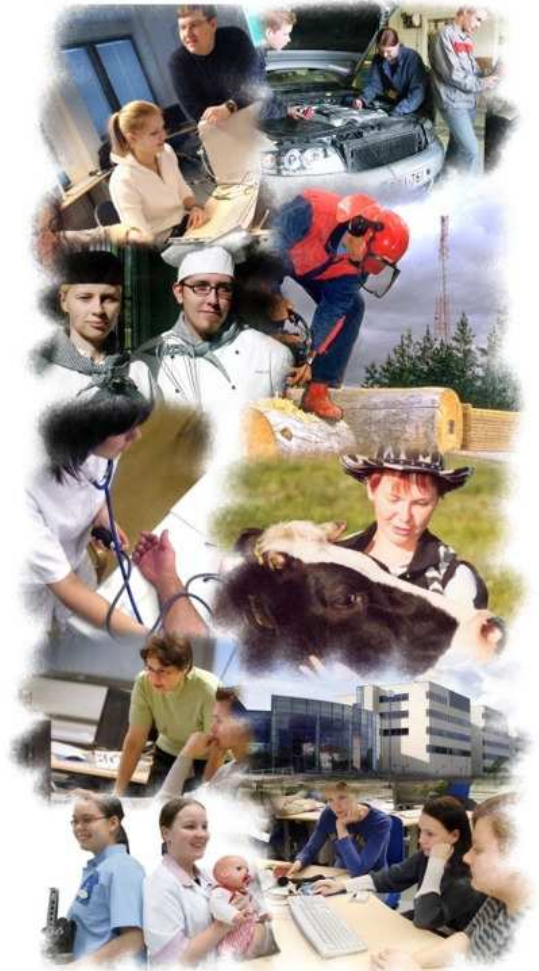
- Suhtaudu terveeseen epäluuloisesti sähköpostin luotettavuuteen; kuka tahansa voi lähettää sähköpostia toisen nimissä (myös virukset).
- Jakelulista on henkilöluettelo, jonka jokainen vastaanottaja saa tietoonsa. Käytä tarvittaessa piilokopio-toimintoa, jos haluat estää jakelulistan aiheettoman käytön. Jakelulistojen eteenpäin luovuttaminen on kiellettyä.
- Työsuhteen päättyessä sähköpostitunnus poistetaan. Siirrä virkapostisi työnantajan käyttöön ja poista mahdolliset henkilökohtaiset viestit.
- Myös opiskelijan sähköpostitunnus poistetaan opiskelun päättyessä. Poista mahdolliset henkilökohtaiset viestit.
- Sovi sähköpostisi käsittelystä pitkän poissaolon aikana.

## ILMOITUSVELVOLLISUUS

- Ilmoita aina haittaohjelmista (virukset, madot tai troijalaiset) ja muista tietoturvaan liittyvistä asioista välittömästi tietoturvavastaavalle, luokanvalvojalle, opettajalle, atk-tukeen tai esimiehellesi.
- Ilmoita aina myös muista turvallisuuteen liittyvistä asioista välittömästi turvallisuudesta vastaaville, luokanvalvojalle, vahtimestareille tai esimiehellesi.

## LISÄTIETOJA

Lisätietoa ja apua ongelmatilanteissa saat oman yksikkösi atk-tuelta.



SeAMKin ja SEDUn tietoturvasuohje