- 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 työhuoneeseesi tai muihin Sedun tiloihin.
- Jos käyttämäsi tallennusväline (USB-tikku, dvd-levy, cd-levy yms.) rikkoutuu, se on luotettavalla tavalla hävitettävä. Rikkoutuneet tallennusvälineet toimitetaan tietosuojajätteen keräilypisteeseen tai tuhotaan fyysisesti.

Omat tiedot ja yksityisyys

- On huomioitava, että Sedun 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.

Henkilötiedot

- Henkilötiedot on aina käsittelyn eri vaiheissa suojattava ulkopuolisilta lainsäädännön ja mahdollisten salassapitosäännösten edellyttämällä tavalla.
- Henkilötietoja sisältävistä rekistereistä on laadittava aina tietosuojaseloste, jonka tulee olla saatavilla Sedun www-sivulla.
- Jokaisella on oikeus pyytäessään saada nähtäväksi tietosuojaselosteet rekisterinpitäjien pitämistä henkilörekistereistä.

Internet ja sähköposti

- Internet ja sähköposti on tarkoitettu ensisijaisesti työ-/opiskelukäyttöön.
- Käytä vain sellaisia palveluja, joita pidät luotettavina.
- Muista, että esiinnyt tietoverkossa aina henkilökunta- tai opiskelijaroolissa Sedun edustajana.
- Internetin kautta ei ole luvallista välittää luottamuksellista tietoa, kuten henkilötietoja ilman asianmukaista salausta.
- Älä käytä tai asenna omatoimisesti Sedun tietokoneille Internetin tai muuta kautta saatavia ohjelmia. Vain IT-palvelut saa asentaa ohjelmia Sedun tietokoneille.
- Työhön liittyvä sähköposti vastaanotetaan Sedun sähköpostijärjestelmään. Sitä ei saa omatoimisesti ohjata Sedun sähköpostijärjestelmän ulkopuolelle. Vain **IT-tuki/Jelppari** saa tehdä mahdollisen uudelleenohjauksen. Uudelleenohjauksessa tulee aina varmistua kopion jäämisestä Sedun palvelimelle. Muualle ohjautuneen sähköpostin tietoturvasta 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 epäilyistäsi aina **Jelppariin.**

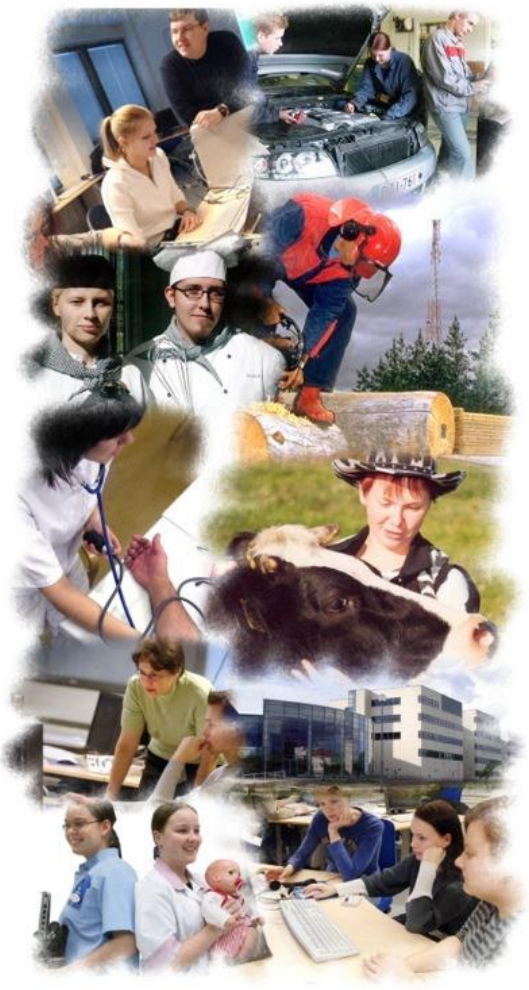
- Suhtaudu terveen epäluuloisesti sähköpostin luotettavuuteen; kuka tahansa voi lähettää sähköpostia toisen nimissä (myös virukset).
- Jakelulista on henkilöluettelo, jonka jokainen vastaanottaja saa tietoonsa. Käytä tarvittaessa piilokopio-toimintoa, jos haluat estää jakelulistan aiheettoman käytön. 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 myös pitkän poissaolon aikana.

Ilmoitusvelvollisuus

- Ilmoita aina haittaohjelmista (virukset, madot tai troijalaiset) ja muista tietoturvallisuuteen liittyvistä asioista välittömästi **Jelppariin.**
- Ilmoita aina myös muista turvallisuuteen liittyvistä asioista välittömästi turvallisuudesta vastaaville.

Lisätietoja

- Jelppari, jelppari@epedu.fi, puh. 020 124 5064



Seinäjoen koulutuskuntayhtymä
Sedun tietoturvallisuusohje

26.6.2019

Miksi tietoturvallisuus on tärkeää?

Seinäjoen koulutuskuntayhtymä Sedussa käsitellään runsaasti erilaista luottamuksellista tietoa, esimerkiksi 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 luvattomasti muuttamaan.

Tietojärjestelmien luotettava toiminta on välttämätöntä Sedun 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 tietoturvapolitiikassa.

Tietokoneen käyttäminen

- Vastaat käyttäjänä omasta koneestasi. Ole siis huolellinen - Tietokoneeltasi pääsee tietoihin, jotka ovat itse laitetta arvokkaampia.
- Vain IT-henkilöstö saa asentaa laitteita verkkoon.
- Vain IT-henkilöstö saa perustaa lähiverkkoon palvelimia.
- IT-palvelut vastaa asentamistaan ohjelmista.
- Älä muuta kansioiden ja levyjen käyttöoikeuksia, siten että IT-henkilöstön ylläpitotoiminta vaikeutuu.
- Estä asiaton pääsy tietojärjestelmiin lukitsemalla koneesi aina kun poistut huoneestasi (paina Ctrl-Alt+Del ja valitse “Lukitse”) tai kirjaudu ulos koneelta.

Käyttöoikeudet ja salasanat

- Tietojärjestelmien käyttöön tarvitaan aina käyttöoikeus.
- Älä luovuta henkilökohtaisia käyttäjätunnuksia ja salasanojasi toisen henkilön käyttöön, ei edes IT-tuen edustajana esiintyvälle.
- Vaihda salasanasi 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 tai puhelin.
- Tallenna tekemäsi työ palvelimelle (kotihakemistoon), mistä tiedot voidaan varmuuskopioida IT-tuen toimesta. Varmista yksikkösi IT-tuelta, mikä on käytäntö yksityisten tiedostojen varmuuskopioinnissa. Käytäntö vaihtelee eri yksikköjen välillä. On huomioitava, että käyttäjä vastaa itse tiedostojensa suojauksesta sekä viime kädessä niiden varmuuskopioinnista.
- Tarkista talon ulkopuolelta tuotu levyke, dvd, cd tai jokin muu muistiväline virustorjuntaohjelmalla.
- Kuljeta matkoillasi mukana vain välttämätön määrä tietomateriaalia, älä koskaan jätä niitä vartioimatta esim. julkisissa kulkuneuvoissa. Tutustu IT-palvelujen käyttösääntöihin sekä ohjeisiin.
- Älä anna kenenkään nähdä tietokoneesi näyttöä tai näppäimistöä, kun käsittelet arkaluontoista materiaalia tai syötät salasanoja. **Käytä kannettavissa tietokoneissa tietosuojakalvoa, jonka henkilökunta saa tilattua Jelpparin kautta.**
- Hae tulosteesi verkkotulostimesta heti tulostuksen jälkeen. Keskitetty tulostus on turvallisin. Henkilökunta saa **tarvittavan tulostuskortin Jelpparista.**
- Käytä silppureita tai tietosuojajätteen keräilypisteitä luottamuksellisen ja arkaluontoisen materiaalin hävittämisessä.

Fyysinen turvallisuus

- Tue osaltasi Sedun kulunvalvontaa. Ohjaa ystävällisesti vieraat ja “eksyneet” henkilöt oikeisiin paikkoihin.
- Älä päästä asiattomia henkilöitä Sedun tiloihin.

- Vastaat omista vieraistasi ja heidän kulkemisestaan Sedussa joko omakohtaisesti tai muun Sedun henkilökuntaan kuuluvan avustuksella.
- Säilytä tieto ja laitteet turvassa.
- Älä jätä kannettavaa tietokonetta tai matkapuhelinta ilman valvontaa. Säilytä laitetta lukitussa paikassa. Muista myös USB-tikkujen, paperitulosteiden yms. säilyttäminen niin, etteivät ne joudu väärin käsiin.