TIETOTURVALLISUUSOHJEET TIETOJÄRJESTELMIEN KÄYTTÄJILLE

TAVOITE

Tämän ohjeen tarkoituksena on toimia jokaisen Metropolian palveluksessa olevan henkilön yleisohjeena tietoturvallisuuden perusasioissa. Noudattamalla näitä ohjeita huolehdit osaltasi tunnuksesi, tietojesi ja käyttämiesi järjestelmien suojaamisessa väärinkäytöksiltä tai vahingoittumiselta.

Ohjeistuksen sisältö seuraa pääpiirteissään Valtiovarainministeriön julkaiseman valtion viranomaisen tietoturvallisuustyön yleisohjeen rakennetta ja voimassaolevaa lainsäädäntöä.

Metropolian tietoturvaohjeistus on jatkuvasti ylläpidettävä ja päivitettävä kokonaisuus, joka sisältää korkeakoulun ydintoiminnan tarpeista lähtevän pelkistetyn ohjeistusdokumentin sekä siihen liitettävät ohjeet, kaaviot ja ohjelmistot.

Ohjeistuksen avulla pyritään varmistamaan Metropolian elintärkeiden toimintojen jatkuvuutta tunnistamalla toimintaa uhkaavat riskit ja uhat sekä niiden vaikutukset suunnittelemalla etukäteen niiden eliminointi- tai vaikutuksen vähentämistoimenpiteet sekä toipumistoimenpiteet. Se sisältää tietoturvallisuuden johtamisen, toimenpiteet ja menettelyt seuraaville osa-alueille henkilöstöturvallisuus, ohjelmistoturvallisuus, tietoaineistoturvallisuus, käyttöturvallisuus, fyysinen tietoturvallisuus ja tietoliikenneturvallisuus sekä mm. olemassa olevien palvelujen riskien kartoituksen ja sen miten niihin on pyritty varautumaan.

http://tietohallinto.metropolia.fi sivustolta löytyy lisää tietoa tietohallinnon toiminnasta ja palveluista.

Tietoturvahuoneentaulu

(tulosta seinälle)

- Älä luota kaikkiin saamiisi sähköposteihin. Varsinkin jos lähettäjä on tuntematon.

- Älä välitä luottamuksellisia tietoja salaamatta internetissä.

- Talleta tärkeät tiedostot verkkolevylle.

- Älä ikinä missään tilanteessa kerro tunnustasi tai salasanaasi kenellekään.

- Salasana tulee olla vähintään 8 merkkiä pitkä, ja se sisältää isoja ja pieniä kirjaimia ja numeroita.

- Lukitse ruutu kun poistut koneelta.

- Älä asenna koneelle omia ohjelmia.

- Älä avaa ovia tuntemattomille.

- Sovi esimiehesi kanssa tiedostojen ja sähköpostien käsittelystä ollessasi kauan poissa.

- Luokkien ovia ei saa teljetä auki esim. roskakorilla. Ovissa on mahdollisesti sähkölukot tiloihin pääsyn hallinnan ja kulunvalvonnan vuoksi.

- http://tietohallinto.metropolia.fi sivustolta löytyy ajankohtaisia tiedotteita.

TILAT

- Lukitse työhuoneesi ovi poistuessasi huoneestasi. Älä jätä vierasta yksin tai ilman valvontaa työhuoneeseesi tai muihin tiloihin. Asiakaspalvelupisteessä tietokoneen näyttö ei saa näkyä asiakkaalle.
- Huolehdi ovien ja ikkunoiden lukituksesta, kun poistut viimeisenä paikalta. Atk-laitteita sisältävät tilat pidetään lukittuina.
- Selvitä itsellesi työpisteesi toiminta tulipalo- ja onnettomuustilanteessa.
- Työaseman luvattoman käytön estät lukitsemalla työaseman. Työasemissa tehdään ns. lukitus eli painetaan WINDOWS -näppäintä ja L -kirjainta. Sammuta tietokone, kun poistut työpaikaltasi. Jos käytössäsi on yhteiskäyttöinen kone, kirjaudu ulos, kun lopetat työskentelyn koneella.
- Säilytä tärkeät muistilaitteet, muistitikut, levykkeet, CD / DVD:t ja paperit lukituissa tiloissa.
- Hae verkkotulostimelta/kopiokoneelta tulosteet mahdollisimman pian.
- Koska opiskelijoiden käytössä ei ole näkyvillä pidettäviä henkilön tunnistavia kulkukortteja niin jokaisen henkilökuntaan kuuluvan velvollisuus on tarvittaessa tarkistaa tuntemattoman henkilön oikeus käyttää tiloja. Tieto harjoittelijoista pitäisi saada koko henkilökunnalle että tiedettäisiin keitä talossa liikkuu.
- Henkilökunnan tulee vastaanottaa vierailijat ja saattaa heidät ulos kiinteistön tiloista. Vierailijoiden valvontavastuu on kutsujalla.
- Opettaja tms. muu vastaava taho ei saa päästää omilla tunnuksillaan toista käyttäjää (esim. opiskelijaa) koneelle mikäli kyseinen käyttäjä ei muista salasanaansa tai tunnus ei muuten toimi.

TYÖASEMAT (pöytätietokoneet ja kannettavat tietokoneet)

- Muodosta salasanastasi riittävän pitkä ja vaikeasti arvattava (vähintään 8 merkkiä). Pidä salasana vain omassa tiedossasi, sillä vastaat itse omalla käyttäjätunnuksellasi tehdystä työstä. Vaihda salasanasi vähintään 4 kk:n välein, ellei järjestelmä itse vaadi salasanan uusintaa määräajoin. Yhteistunnusten käytöstä on vastuussa sitä käyttävä ryhmä.
- Muista, että ulkopuoliset henkilöt, joilla ei ole verkon käyttäjätunnusta, eivät saa käyttää työasemia tai muita tietotekniikkalaitteita.
- Käyttöoikeuden myöntäjä (esimies) vastaa siitä, että ohjelmiston saavat käyttöön oikeat henkilöt asianmukaisin käyttöoikeuksin. Pääkäyttäjä toteuttaa sovelluksen sisälle tarvittavat oikeudet silloin, kun ohjelmistoon sisältyy mahdollisuus rajata järjestelmän käyttöä esimerkiksi työtehtävien mukaan.
- Jos olet unohtanut salasanasi, on tietohallinnon varmennettava henkilöllisyytesi ennen uuden salasanan antamista.
- Salasanaa ei saa kertoa kenellekään puhelimessa eikä lähettää sähköpostissa helpdeskiin, kenenkään ylläpitäjän ei tarvitse tietää salasanaasi.
- Käyttöoikeudet ovat sidottu työsuhteeseen ja se lakkaa automaattisesti työsuhteen päättyessä.
- Omien ohjelmien asentaminen ja käyttö työasemassa ei ole toivottavaa. Tietohallinnolla on oikeus ja velvollisuus poistaa tai estää käyttäjän itse asentamien ohjelmien käyttö, mikäli ne haittaavat järjestelmän toimintaa, työasemassa informoimatta siitä käyttäjää.

- Varmista, että työasemassasi on asennettuna ja toiminnassa virustarkistusohjelma. Alla olevassa kuvasta selviää miten voi tarkistaa tunnistekuvauksien ajanmukaisuuden. Liikkeellä on haittaohjelmia, jotka rampauttavat tietoturvaohjelmistojen toimintaa.

    - Klikkaa oikeaa hiiren nappulaa sinisen kolmion päällä ja valitse ylimmäinen vaihtoehto.

    - Sitten valitset Automaattiset päivitykset/Automatic Updates –nappulan. Rengastetut päiväykset eivät saisi olla vanhempia kuin yksi viikko.

- Käytä kirjoitussuojaa, kun luet levykkeitäsi vieraalla tietokoneella. Sama koskee myös muistitikkuja, mikäli tikussa on sellainen toiminnallisuus.
- Hävitä tarpeettomat tiedostot omilta verkko- ja kiintolevyiltäsi.
- Siivoa sähköpostilaatikkoasi säännöllisesti poistaen sieltä turhat sähköpostiviestit.
- Laissa salaiseksi määrättyä tietoa saa säilyttää kovalevyllä tai muussa massamuistissa vain tietyn työtehtävän suorittamiseen tarvittavan ajan, jonka jälkeen tiedot on poistettava.
- Muista tallentaa työsi säännöllisesti kotihakemistoosi ja hyödynnä mahdollisia automaattitallennustoimintoja.
- Sulje avoimet ohjelmat poistuessasi pidemmäksi aikaa työpisteestäsi.
- Älä irrota sähköverkosta atk-verkkolaitteita työasemia lukuun ottamatta, kysymättä ensin neuvoa tietohallinnosta.
- Verkkolevyjen varmistus tapahtuu tietohallinnon toimesta. Työtiedostot tulee tallentaa omaan kotihakemistoon (Z:-asema). Työasemien kiintolevyille tallennettujen työtiedostojen osalta vastuu varmuuskopioinnista on käyttäjällä.
- Kaikki taloon tuleva ja talosta lähtevä sähköposti tarkistetaan virusten, roskapostin yms. varalta. Roskapostia pääsee suodatuksesta huolimatta läpi, johtuen uusista menetelmistä ja tavoista joita roskapostittajat käyttävät. Suodattamista kehitetään ja parannetaan kokoajan.
- Työasemiin on asennettu etähallintaa varten työaseman etäkäytön mahdollistava ohjelmisto. Etähallintaa käytettäessä käyttäjältä kysytään lupa ennen yhteyden muodostamista pois lukien opetustilat.

KANNETTAVIA TIETOKONEITA KOSKEVAT ERITYISOHJEET

- Laitteet ovat tarkoitetut ainoastaan oppilaitoksen palveluksessa olevien henkilöiden käyttöön työtehtäviä varten. Kannettavaa tietokonetta saavat käyttää vain henkilöt, joiden käyttöön se on luovutettu.
- Muita kuin oppilaitoksen hallinnoimia tietokoneita ei saa kytkeä langalliseen verkkoon. Langatonta verkkoa saa käyttää kaikilla laitteilla, mikäli sellainen WLAN-palvelu on saatavilla.
- Tietokoneen laite- tai ohjelmistokokoonpanoa taikka niihin liittyviä asetuksia ei saa muuttaa. Työaseman tietoturva-asetuksia ei saa muuttaa.
- Älä jätä kannettavaa tietokonetta autoon tai muuhun vartioimattomaan paikkaan näkyville edes lyhyeksi hetkeksi.
- Kannettava tietokone on liitettävä oppilaitoksen verkkoon säännöllisesti kahden viikon välein virustorjuntaohjelmistojen päivittämiseksi ja tietoturvapäivitysten asentamiseksi.
- Mikäli et tarvitse/käytä langattomia palveluita (WLAN ja bluetooth), niin poistakaa ne käytöstä (sammuta). Tämä sammutussääntö pätee myös puhelimiin, joissa on mahdollista käyttää langattomia palveluita. Nokian puhelimissa saa Bluetoothin sammutettua painamalla pitkään * -näppäintä.

INTERNET

- Internet -yhteys on tarkoitettu vain työtehtävien ja työnantajan kanssa sovittujen opintojen hoitamista varten.
- Yhteyden turvallisuutta valvotaan ns. palomuuriohjelmalla. Tietoliikennettä ja palvelinten lokitietoja seurataan sähköisen viestinnän tietosuojalain puitteissa palvelujen käytettävyyden ja niiden tietoturvan varmistamiseen, palveluiden käyttöä koskevien väärinkäytösten selvittämiseen sekä tekniseen kehittämiseen ja vianselvitykseen.
- Älä lataa internetistä ohjelmia tai työhön kuulumatonta materiaalia.
- Jos epäilet tietomurtoa tai mitä tahansa turvallisuusriskiä (myös muuta kuin internetiin liittyvää), ota heti yhteyttä tietohallintoon.
- Työnantajan luottokortin käyttö maksuvälineenä Internetissä on kielletty ilman erillistä sopimusta.
- Muista, että edustat työnantajaasi, kun käytät Internetiä. Tietokoneesi IP-osoite, joka näkyy internetissä, on rekisteröity ammattikorkeakoululle.
- Tyhjennä säännöllisesti Internet-selaimesi väliaikaistiedostot.
- Seuraavien sovellusten käyttö niiden sisältämien erityisen korkeiden tietoturvariskien tai muun haitan takia ei ole suotavaa mm. :
    - Musiikki- ja videotiedostojen lataamiseen tarkoitetut sovellukset esim. Napster, KaZaA, DC sekä vastaavat
    - Automaattiset näytönsäästäjät, jotka kuluttavat työaseman resursseja omaan toimintaansa esim. SETI@home (Search for Extra Terrestial Intelligence) tai vastaavat @home ohjelmat.
    - Kaikki käyttötarkoitukseltaan haitalliset, hyvän tavan vastaiset tai työtehtävien kanssa ristiriidassa olevat palvelut (esim. salauksen purku jo lain nojalla)

EI JULKISTEN TIETOJEN HÄVITTÄMINEN

- Henkilötietoja tai muita luottamuksellisia tietoja sisältävä paperi, levyke, muistitikku, CD, tms. on säilytettävä varmassa ja suojatussa paikassa.
- Luottamuksellisten papereiden hävittämistä varten kiinteistöistä löytyvät erikseen omat hävitysastiat.

TOIMINTA ONGELMATILANTEESSA

- Jos tietokone äkillisesti hidastuu tai muutoin käyttäytyy oudolla tavalla ilman, että olet tehnyt mitään erityistä toimintoa, toimi seuraavasti
    1. Älä hätiköi.
    2. Tietokonetta ei tarvitse sulkea.
    3. Kirjoita ylös havaintosi, tekemisesi sekä mitä mahdollisessa ilmoituksessa tai varoituksessa luki.
    4. Ota yhteyttä tietohallintoon ja/tai tietoturvavastaavaan.
    5. Toimi saamiesi ohjeiden mukaisesti.
    6. Auta tutkinnassa, kerro mitä olit tekemässä, kun kone alkoi toimia odottamattomasti.

SEURAAMUKSET

- Lakien, määräysten ja ohjeiden rikkomisesta tai laiminlyönnistä käyttöoikeudet tietojärjestelmiin voidaan peruuttaa. Näistä tiedotetaan aina esimiehelle.
- Mikäli rikkomuksista tai laiminlyönneistä aiheutuu taloudellisia menetyksiä, voidaan päätyä vahingonkorvausvaatimuksiin.
- Tietojen väärinkäyttö tai tahallinen tai huolimaton lakien, määräysten ja ohjeiden vastainen toiminta voi johtaa kurinpidollisiin seuraamuksiin, kuten irtisanomiseen ja/tai rikosoikeudellisiin seuraamuksiin.

MISTÄ SAA LISÄTIETOJA

- Käyttösääntö:
    - löytyy portaalista, kaikkien noudatettava
- Sähköpostin käsittelysääntö
    - löytyy http://tietohallinto.metropolia.fi, kaikkien noudatettava
- Valtiovarainministeriön ja VAHTIn ohjeet (www.vm.fi/vahti)
- Muut tietoturvallisuutta ohjeistavat ja säätelevät organisaatiot (esimerkiksi Viestintävirasto, Tietosuojavaltuutetun toimisto ja Arkistolaitos)
- Tietohallinto, esimies, työtoverit

LAIT JOTKA SÄÄTELEVÄT

- Henkilötietolaki(523/1999)
  - henkilötietojen käsittely
  - rekisteri-ilmoitus (Winha, palkkahallinto, kulunvalvonta)

- Sähköisen viestinnän tietosuojalaki (516/2004)
  - Metropolia on yhteisötilaaja, koska käsittelee tietoverkossaan käyttäjien luottamuksellisia tietoja ja viestejä
  - tunnistamistietoja saa käsitellä siinä määrin kuin on tarpeen verkkopalvelun, viestintäpalvelun tai lisäarvopalvelujen toteuttamiseksi ja käyttämiseksi sekä näiden tietoturvasta huolehtimiseksi
  - mahdollisuus estää roskaposteja ja poistaa haittaohjelmia jos palvelut vaarantuvat
  - ei saa kuitenkaan vaarantaa sananvapautta eikä luottamuksellisen viestin tai yksityisyyden suojaa enempää kuin on välttämätöntä viestinnän turvaamiseksi

- Laki yksityisyyden suojasta työelämässä (759/2004)
  - työnantajan on kerättävä työntekijää koskevat henkilötiedot ensisijaisesti työntekijältä itseltään
  - ohjeet työnantajalle kuuluvien sähköpostiviestien hakemisesta ja avaamisesta
  - ennen kuin voi avata posteja niin työnantajan hoidettava:
    - että työntekijä voi laittaa automaattisen poissaoloviestin ja ilmoittaa sijaisen tai
    - ohjata viestit sijaiselle tai käytössään olevaan toiseen osoitteeseen tai
    - antaa suostumuksen että työnantajan hyväksymä toinen henkilö voi lukea postia

- Tietyin edellytyksin (esim. jos työnantaja on huolehtinut edellisen kohdan toimenpiteistä ja työntekijän suostumusta ei ole mahdollista kohtuullisessa ajassa saada) työnantajan pääkäyttäjä voi ottaa selville onko työntekijälle poissaolon aikana tullut työnantajalle kuuluvia tärkeitä viestejä. Otsikkotietojen käsittelystä tehdään allekirjoitettu selvitys, joka on toimitettava työntekijälle. Avaamisesta on laadittava siihen osallistuneiden henkilöiden (ainakin pääkäyttäjä + toinen henkilö) allekirjoittama selvitys.

Vastuu henkilökunnan opastamisesta on kullakin esimiehellä omien alaistensa osalta.