

[YLIOPISTON] TIETOTURVAPOLITIikka

Hyväksytty [hallintoelin] [päiväys]

Sisällysluettelo:

| | | |
|---|--|----|
| 1 | Tavoitteet | 1 |
| 2 | Tietoturvan organisointi ja vastuut..... | 2 |
| 3 | Toteutuskeinot..... | 2 |
| 4 | Tiedottaminen | 3 |
| 5 | Tietoturvallisuuden seuranta ja ongelmatilanteiden käsittely..... | 3 |
| | LIITE 1: Määritelmät | 4 |
| | LIITE 2: Yliopiston tietoturvallisuutta ohjaavia säädöksiä, suosituksia ja ohjeita | 8 |
| | LIITE 3: Keskeiset yliopiston voimassa olevat tietoturvallisuuteen liittyvät säännöt ja ohjeet..... | 9 |
| | LIITE 4: Tampereen yliopiston tietoturvaperiaatteet, luku Vastuut (hyväksytty yliopiston hallituksessa 7.6.2002) | 9 |
| | LIITE 5: Tietoturvan organisointi ja vastuut..... | 10 |

Vastuu yliopiston toimivuudesta on sen ylimmällä johdolla. Yliopiston toiminta ja palvelut ovat yhä enenevässä määrin riippuvaisia tietotekniikkapalveluiden keskeytsettömästä saatavuudesta ja niiden turvallisesta toiminnasta. Tietotekniikan hyödyntäminen ja niin tietotekniikan kuin yleisempäänkin tietoturvallisuuteen panostaminen ovat johdon strategisia päätöksiä, joilla vaikutetaan yliopiston toimintakykyyn merkittävällä tavalla. Myös lainsäädäntö asettaa omat velvoitteensa tietoturvallisuudesta huolehtimiselle.

Tietoturvapolitiikka on [yliopiston] johdon kannanotto, joka määrittelee tietojen turvaamisen tavoitteet, vastuut ja toteutuskeinot yliopistossa. Tietoturvapolitiikka annetaan tiedoksi kaikille yliopistoyhteisön jäsenille ja heidän tulee toimia sen mukaisesti. Poliittikkaa tarkennetaan tietojen käsittelyn säännöissä ja ohjeissa.

Tiedon turvaaminen on oleellinen osa yliopiston toiminnan ja palveluiden laatua, kokonaisuutena ja yliopistossa tapahtuvaa päivittäistä tietojen käsittelyä. Tietoturvallisuuden hyvä hallinta edellyttää kaiken toiminnan jatkuvaa seuranta, pitkäjänteistä suunnittelua, varautumista erilaisiin uhkatilanteisiin, sovittujen toimintatapojen noudattamista, ohjeita, koulutusta ja viestintää. Tavoitteena on luoda ja ylläpitää luotettava ja turvallinen ympäristö niin yliopistoyhteisön omien kuin sen piirissä käsiteltävien sidosryhmienkin tietojen käsittelyyn.

1 Tavoitteet

Tietoturvallisuus koostuu tiedon luottamuksellisuudesta, eheydestä ja käytettävyydestä¹. Yliopiston tavoitteena on turvata riittävässä ja tarkoituksenmukaisella tasolla toiminnalleen tärkeiden tietojen, tietojärjestelmien, palveluiden ja tietoverkkojen toiminta, estää niiden valtuutetun käyttö sekä tahaton tai tahallinen tiedon tuhoutuminen ja vääristyminen.

Tietojen turvallisuudesta on huolehdittava niin manuaalisesti kuin tietotekniikankin avulla tapahtuvassa tiedon käsittelyssä, tiedon kaikissa olomuodoissa ja tiedon koko elinkaaren ajan. Yliopiston kunkin yksikön perusluonne ja mahdolliset tarpeet turvallisuuden tehostamiseen tulee ottaa huomioon. Tietojen turvaamisesta tulee erityisesti huolehtia yksiköissä, jotka käsittelevät runsaasti luottamuksellista tai muuten turvaluokiteltua tietoa. Tietojen turvaamisessa huomioidaan omina osa-alueinaan valtionhallinnon käytännön mukaan hallinnollinen, henkilöstö-, fyysinen, tietoaineisto-, tietoliikenne-, laitteisto-, ohjelmisto- ja käyttöturvallisuus.

¹ Katso tarkemmin LIITE 1: Määritelmät

Tietoturvallisuustyö on tietojen turvaamiseksi tehtävää jatkuvaa kehittämistä, suunnittelua, toteuttamista ja seuranta. Sillä pyritään ennalta ehkäisemään sisäisistä ja ulkoisista tietoon kohdistuvista uhkista aiheutuvat vahingot tai rajoittamaan ne hyväksyttävälle tasolle sekä varautumaan poikkeamatilanteista toipumiseen. Normaalijärjestyksen tietojen käsittelyn turvaamisen osana yliopisto varautuu myös häiriö- ja poikkeusoloihin siten, että toimintaa voidaan jatkaa mahdollisimman häiriöttömästi kaikissa olosuhteissa.

Yliopiston tietoturvallisuudesta huolehditaan kansallisten ja kansainvälisten tietoturvallisuutta koskevien säädösten mukaisesti sekä noudattaen valtionhallinnon tietoturvallisuudesta annettuja ohjeita ja suosituksia².

2 Tietoturvan organisointi ja vastuut

Tässä luvussa kuvataan keskeisimmät tietoturvallisuuteen liittyvät toimijat yliopistossa sekä heidän vastuunsa ja velvollisuutensa. Tarkempi vastuiden erittely kerrotaan tietoturvapoliittikan liitteessä 5. Johtuen kunkin yliopiston erilaisesta tehtävänjaosta, tulee tämä luku räätälöidä kuhunkin yliopistoon soveltuvaksi.

Luvussa tulee ottaa kantaa ainakin seuraaviin asioihin:

- Rehtori vastaa osana kokonaisvastuutaan tietoturvallisuudesta, sen toteuttamisesta, kehittämisestä ja tarvittavien edellytysten luomisesta (mm. resursoinnista) yliopistossa.
- Jokainen tietoja käsittelevä vastaa sen lisäksi **omalta osaltaan** tietojen turvallisuudesta ja on velvollinen noudattamaan siihen liittyviä yliopiston antamia sääntöjä ja ohjeita³.
- Tietoturvapoliittikasta päättäminen.
- Tietoturvallisuuden kehittämiseksi ja toteuttamiseksi yliopistossa voi olla erityisiä toimijoita kuten tietoturvallisuuden johtoryhmä, tekninen tietoturvaryhmä ja tietoturvapäällikkö.
- Huolehtimisvelvoitteet tietoturvallisuuden koulutuksesta ja tietoturvatietouden edistämisestä, tietoturvallisuutta koskevan lainsäädännön seuraamisesta, tietoturvallisuuden toteutuksen valvonnasta, raportoinnista, kehittämishankkeiden valmistelusta ja toteutuksesta, uusien ulkopuolisten uhkien seuraamisesta, fyysisestä tietoturvallisuudesta, tietoteknisestä tietoturvallisuudesta, ...
- Toimintavaltuudet tietoturvapoikkeamatilanteissa koko organisaation tasolla
- Jokaiselle yliopiston tiedolle ja niitä käsittelevälle tietojärjestelmällä tai tarvittaessa tietojärjestelmän osalle on nimettävä omistaja (laitos, yksikkö), jota edustaa viime kädessä yksikön esimies. Omistajalla on velvollisuus huolehtia tietojensa ja tietojärjestelmiensä suojaamisesta sekä lakien, hyvän ylläpitotavan ja yliopiston voimassa olevien sääntöjen ja politiikkojen noudattamisesta, vaikka tietojen käsittely tai tietojärjestelmien ylläpidon toteutus tapahtuisikin esimerkiksi [atk-yksikössä].⁴
- Erityisiä vastuita tietoturvallisuuden suhteen on myös hallintojohtajalla, hallituksella, tietohallinnolla/atk-yksiköllä, esimiehillä, luottamuksellista tietoa käsittelevillä sekä tietoteknisillä asiantuntijoilla ja tukihenkilöillä.
- Yliopiston yksiköt varautuvat oman ympäristönsä tietoturvallisuuden toteuttamisen kustannuksiin omissa toimintasuunnitelmissaan ja tietoturvallisuus on osa yksiköiden tuulosohjausta.

Esimerkkinä Liitteenä 4 on Tampereen yliopiston tietoturvaperiaatteet, luku Vastuut (hyväksytty yliopiston hallituksessa 7.6.2002).

3 Toteutuskeinot

Tietoturvallisuuden ylläpito ja kehittäminen on jatkuva prosessi, joka tapahtuu hallinnollisten, fyysisten ja tietoteknisten ratkaisujen avulla. Käyttäjien toimintaa ohjataan niihin sisältyvillä

² Katso tarkemmin LIITE 2: Yliopiston tietoturvallisuutta ohjaavia säädöksiä, suosituksia ja ohjeita

³ Katso tarkemmin LIITE 3: Keskeiset yliopiston voimassa olevat tietojärjestelmiin liittyvät säännöt ja ohjeet

⁴ Katso tarkemmin Ylläpitosääntö, luku2.

käytösäännöillä ja toimintaohjeilla sekä tietojen turvallisen käsittelyn koulutuksella ja tiedotuksella.

Tietojen turvallisesta käsittelystä solmitaan sopimukset myös yliopiston tietoja käsittelevien organisaatioiden sekä muiden yhteistyökumppanien kanssa.

Tarvittavan suojaustason (perustaso / tehostetut tasot) ja tarvittavien suojaustoimien määrittäminen tehdään riskikartoituksissa. Niissä kartoitetaan ja luokitellaan yliopiston ja yksiköiden merkittävät tietoaineistot ja tietojärjestelmät, näihin kohdistuvat uhat sekä arvioidaan menetyksen suuruus uhan toteutuessa. Riskikartoitukset toistetaan määräajoin ja muutosten yhteydessä.

Tietoturvapoliittikan ja riskikartoitusten pohjalta laaditaan yliopiston tietoturvasuunnitelma, jossa tietojenkäsittelyn perusturvallisuuden vaatimukset ja kehittämistarpeet kuvataan. Tietoturvaratkaisut ja toteutukset kuvataan kunkin käyttöympäristön, yksikön, palvelun, sovelluksen ja järjestelmän osalta tarvittaessa erillisissä suunnitelmissa. Suunnitelmissa otetaan kantaa, mitkä riskit edellyttävät toimenpiteitä ja mitkä taas ovat toiminnan ja lainsäädännön vaatimusten puitteissa hyväksyttäviä.

Tietoturvallisuus sisältyy yliopiston toimintaprosessien kehittämiseen ja toiminnan ja yksiköiden vuosisuunnitteluun. Perustaso määritellään [yliopiston tietoturvaohjeissa].

Henkilökunnalle jaetaan heidän työskentelyssään tarvitsemansa tietoturvasuunnitelmat. Opiskelijoille tiedotetaan tietoturvasuunnittelusta ja heitä koskevista säännöistä ja suosituksista.

Yleensäkin yliopistoyhteisön jäsenten tietoturvasuunnittelusta lisätään tiedottein ja kirjoituksin eri tiedotuskanavissa sekä järjestämällä koulutustilaisuuksia. [Yliopiston tietojenkäsittelyn ja tietojärjestelmien tietoturvasuunnittelun tasoa arvioidaan sisäisen tarkastuksen keinoin, tarvittaessa myös ulkoista tarkastusta käyttäen. Tietoturvasuunnittelun puutteet analysoidaan järjestelmien ylläpitäjien ja omistajien kanssa.]

4 Tiedottaminen

Yliopiston tietoturvasuunnittelusta koskevat asiat eivät ole aktiivisen ulkoisen tiedottamisen aihe. Julkisuuskuvan vuoksi, luottamuksen herättämiseksi asiointiin ja palveluun sekä käyttäjien opastamiseksi tiedotetaan yleisluontoisesti tietoturvasuunnittelumenettelyistä.

Yliopiston tietoturvasuunnittelun liittyvästä tiedottamisesta yliopiston ulkopuolelle ja yliopiston sisällä yleisellä tasolla vastaa ja huolehtii yliopiston tietoturvapääällikkö tietoturvasuunnittelman mukaisesti. Yksiköiden sisäiseen tiedottamiseen osallistuvat myös yksiköille nimetyt vastuuhenkilöt.

Yleisesti ottaen tietoteknisten yksityiskohtien varomaton kertominen voi vaarantaa tietoturvasuunnittelun, joten tiedotusvastuut on keskitettävä [kokonaisuudet hallitseville henkilöille].

5 Tietoturvasuunnittelun seuranta ja ongelmatilanteiden käsittely

Tietoturvasuunnittelun ylläpito edellyttää jatkuvaa seurantaan, johon kuuluvat tietoturvasuunnittelun valvonta sekä sen tason ja poikkeamien raportointi. Seuranta toteutetaan sekä automaattisesti teknisin keinoin että henkilöiden toimesta mm. osana esimiesvastuuta. Teknisestä seurannasta on erilliset ohjeensa. [Tietoturvapääällikkö] koordinoi tietoturvasuunnittelun seurantaan ja raportoi tietoturvasuunnittelusta yliopiston johdolle.

[Tietoturvapääälliköllä ja tietoturvasuunnittelun johtoryhmällä] on yliopiston ylimmän johdon antama valtuutus ja velvollisuus tehdä yliopiston tietojen käsittelyn turvallisuuteen liittyviä kartoituksia ja ryhtyä toimenpiteisiin havaittujen puutteiden korjaamiseksi.

Käyttäjien ja ylläpitäjien tulee ilmoittaa havaitsemistaan tietoturvasuunnittelun puutteista, tietoturvasuunnittelun liittyvistä väärinkäytöksistä tai epäilemistään tietoturvarikkomuksista yksikönsä [tietoturvahenkilölle tai] johtajalle sekä tietoturvapääällikölle, joka reagoi niihin erikseen määriteltävällä tavalla.

Tietoturvapoikkeamiin reagoimisesta ja tietoturvarikkomusten seuraamuksista on omat erilliset sääntönsä.

LIITE 1: Määritelmät**Eheys** (integrity)

- 1) Tietojen tai tietojärjestelmän aitous, väärentämättömyys, sisäinen ristiriidattomuus, kattavuus, ajantasaisuus, oikeellisuus ja käyttökelpoisuus,
- 2) Ominaisuus, että tietoa tai viestiä ei ole valtuudettomasti muutettu, ja että mahdolliset muutokset voidaan todentaa kirjausketjusta.

Fyysinen turvallisuus (physical security)

Henkilöiden, laitteiden, aineistojen, postilähetysten, toimitilojen ja varastojen suojaaminen tuhoja ja vahinkoja vastaan. Fyysinen turvallisuus sisältää muun muassa kulun- ja tilojen valvonnan, vartioinnin, palo-, vesi-, sähkö-, ilmastointi- ja murtovahinkojen torjunnan sekä kuriirien ja tietoaineistoja sisältävien lähetysten turvallisuuden.

Hallinnollinen tietoturvaluisuus (administrative and organizational information security)

Tietoturvaluuteen tähtäävät hallinnolliset keinot, kuten organisaatiojärjestelyt, tehtävien ja vastuiden määrittely sekä henkilöstön ohjeistus, koulutus ja valvonta.

Henkilöstöturvallisuus (personnel security)

Henkilöstöön liittyvien tietoturvariskien hallinta henkilöstön soveltuvuuden, toimenkuvien, sijaisuuksien, tiedonsaanti- ja käyttöoikeuksien, suojaamisen, turvallisuuskoulutuksen ja valvonnan osalta.

Henkilöturvallisuus

henkilöstöturvallisuus sekä henkilöstön että soveltuvin osin opiskelijain osalta.

Kokonaisturvallisuus

Yliopiston turvallisuus jaetaan yhdeksään eri osa-alueeseen: toiminnan turvallisuus, työturvallisuus, ympäristöturvallisuus, pelastustoiminta, valmiussuunnittelu, tietoturvaluisuus, henkilöturvallisuus, toimitilaturvaluisuus ja rikosturvallisuus.

Käytettävyyys (availability)

Ominaisuus, että tieto, tietojärjestelmä tai palvelu on siihen oikeutetuille saatavilla ja hyödynnettävissä haluttuna aikana ja vaaditulla tavalla.

Käyttöturvallisuus (operations security):

tietotekniikan käyttöön, käyttöympäristöön, tietojenkäsittelyyn ja sen jatkuvuuteen sekä tuki-, ylläpito-, kehittämis- ja huoltotoimintoihin liittyvät keinot tietoturvaluuden parantamiseksi.

Laitteistoturvaluisuus (computer security; facilities security)

tietojenkäsittely- ja tietoliikennelaitteiden ja tilojen käytettävyyteen, toimivuuteen, kokoonpanojen määrittelyyn ja pääsynvalvontaan sekä varaosien ja tarvikkeiden saatavuuteen liittyvät toimet tietoturvaluuden toteuttamiseksi.

Luottamuksellinen (confidential) **tieto**

Vain tietyn henkilön tai tiettyjen henkilöiden tietoon tarkoitettu.

Valtionhallinnon **turvaluokituksen** mukaan luottamuksellinen vastaa III turvaluokkaan kuuluvaa tietoa.

Luottamuksellisuus (confidentiality)

Tietojen säilyminen luottamuksellisina ja tietoihin, tietojenkäsittelyyn ja tietoliikenteeseen kohdistuvien oikeuksien säilyminen vaarantumiselta ja loukkaukselta.

Ohjelmistoturvallisuus (software security)

käyttöjärjestelmiin ja muihin ohjelmistoihin kohdistuvat toimet, kuten ohjelmistojen tunnistamis-, eristämisen-, pääsynvalvonta- ja varmistusmenettelyt, tarkkailu- ja paljastustoimet, lokimenettelyt ja laadunvarmistus sekä ohjelmistojen ylläpitoon ja päivitykseen liittyvät toimet tietoturvallisuuden parantamiseksi.

Perusturvallisuus (baseline security):

Vähimmäistoenpiteet, joilla varmistetaan tietojenkäsittelyn ja toimintaprosessien häiriötön toiminta normaalioloissa. (Tietoturvallisuuden taso, jossa järjestelmän omistaja on varautunut vastaamaan rutiininomaisin toimin normaalioloissa sattuviin vahinkoihin ja keskeytyksiin.)

Poikkeama, tietoturvapoikkeama (information security incident)

Tahallinen tai tahaton tapahtuma tai olotila, jonka seurauksena organisaation vastuulla olevien tietojen ja palvelujen käytettävyys ei ole suunnitellulla tasolla tai tietojen eheys tai luottamuksellisuus on vaarantunut..

Poikkeusolot (extraordinary circumstances)

Kansainvälisestä tilanteesta tai suuronnettomuudesta johtuva vakava vaara Suomen väestön toimeentulolle, talouselämälle, oikeusjärjestykselle, kansalaisten perusoikeuksille, maan alueelliselle koskemattomuudelle tai itsenäisyydelle.

Valmiuslain (1080/1991, muut. 198/2000) mukaan mahdollisia poikkeusoloja ovat mm.

Suomeen kohdistuva aseellinen hyökkäys, sota ja sodan jälkitila
alueellisen koskemattomuuden vakava loukkaus ja sodanuhka
vieraiden valtioiden välinen sota, josta on vaaraa Suomelle
tuonnin vaikeutumisesta aiheutuva vakava taloudellinen uhka
suuronnettomuus.

Poikkeustilanne (exceptional situation)

Organisaatiota kohtaava tilanne, joka voi esiintyä myös normaalioloissa, kuten tulipalo, sähkö- tai ilmastointihäiriö, tuhoisa rikos, lakko tai avainhenkilöstön menetys.

Tietoaineistojen luokitus (classification of data):

Tietojen jakaminen luokkiin tietojen omistajan asettamien perusteiden mukaisesti. Luokitusperusteena voi olla esimerkiksi tiedon luottamuksellisuus tai sen merkitys organisaation toiminnalle.

Valtionhallinnon turvaluokituksen perusteena on tietojen haavoittuvuus asiattomalle käsittelylle ja paljastumiselle sekä tästä yhteiskunnalle tai valtiolle aiheutuva menetys tai haitta.

Tietojen luokittelamisen perusteena voi olla esimerkiksi niiden suojaustarve, omistajuus tai tosiaikaisuusvaatimus.

Tietoaineistoturvallisuus (data security):

tietoturvallisuuteen tähtäävät toimet asiakirjojen, tiedostojen ja muiden tietoaineistojen käytettävyyden, eheyden ja luottamuksellisuuden ylläpitämiseksi keinoina muun muassa tietoaineistojen luettelointi ja luokitus sekä tietovälineiden ohjeistettu hallinta, käsittely, säilytys ja hävittäminen.

Tietoliikenneturvallisuus (telecommunications security)

- 1) tavoitetilä, jossa tietoturvaluullisuus on toteutettu tietoliikenteen laitteiden, järjestelmien ja niissä kulkevien tietojen osalta
- 2) lainsäädäntö, normit ja toimet, joilla pyritään aikaansaamaan tietoliikenteen turvallisuus. Tietoliikenneturvaluullisuuteen tähtääviä keinoja ovat mm. laitteistojen ja siirtoyhteyksien ylläpito ja niiden kokoonpanojen hallinta, verkonhallinta, pääsynvalvonta, tietoliikenteen käytön valvonta ja tarkkailu, ongelmatilanteiden kirjaaminen ja selvittäminen, viestinnän salausta ja varmistaminen sekä tietoliikenneohjelmien testaus ja hyväksyminen.

Tietotekniikan turvallisuus (IT security):

organisaation tietotekniikkaan kuten tietoliikenteeseen, laitteistoihin, ohjelmistoihin ja niiden käyttöön liittyvä tietoturvaluullisuus.

Tietoturvaluullisuus (information security):

- 1) tavoitetilä, jossa tiedot, tietojärjestelmät ja palvelut saavat asianmukaista suojausta niin, että niiden luottamuksellisuuteen, eheyteen ja käytettävyyteen kohdistuvat uhat eivät aiheuta merkittävää vahinkoa yhteiskunnalle ja sen jäsenille.
- 2) lainsäädäntö ja muut normit sekä toimenpiteet, joiden avulla pyritään varmistamaan tietoturvaluullisuus

(1) niin normaali- kuin poikkeusoloissa.

Tietoturvaluullisuuden toteuttamisessa on tapana erottaa kahdeksan toimenpidealuetta: hallinnollinen, henkilöstö-, fyysinen, tietoliikenne-, laitteisto-, ohjelmisto-, tietoaineisto- ja käyttöturvaluullisuus.

Tietoturvanormi (information security norm):

Säädös tai viranomaisen määräys, joka tähtää tietojen tai tietojenkäsittelyn luottamuksellisuuden, eheyden ja käytettävyyden turvaamiseen pyrkimällä torjumaan näihin kohdistuvia uhkia tai sääntelemällä tietoturvaluullisuuden kehittämistoimintaa tai sitä suorittavia organisaatioita.

Tietoturvaohjeisto (information security manual):

Yliopiston yhteinen, yksiköiden sisäinen ja palvelu- tai järjestelmäkohtainen ohjeistus tietojenkäsittelyn turvaamiseksi.

Tietoturvapoliittikka (information security policy) :

Sama kuin tietoturvastrategia (information security strategy).

Tietoturvalinjaukset, tietoturvaperiaatteet.

Organisaation tasolla johdon hyväksymä näkemys tietoturvaluullisuuden päämääristä, periaatteista ja toteutuksesta.

Tietoturvasuunnitelma (information security plan):

perusturvaluullisuuden toteutusta ja ylläpitoa normaalioloissa koskeva suunnitelma.

Suunnitelmassa esitetään organisaation tietoturvaluullisuustoiminnan tavoitteet, hallinto, tehtävät ja menettelyt, osoitetaan elintärkeät tietojärjestelmät ja määritellään niiden toipumisen edellyttämät toimet.

Tietoturvasuunnittelu (information security planning):

suunnitteluprosessi, johon kuuluu muun muassa uhka-analyysi, perusturvaluullisuuden määrittely sekä toipumisvalmiuden ja poikkeusolojen valmiussuunnittelu, ja jonka tuloksena on tietotur-

vasuunnitelmia,
-linjauksia ja -ohjeistoja.

Turvallisuus (security):

olotila, jossa tiedossa olevat uhat eivät merkitse sanottavaa riskiä ja ne voidaan hallita.

Turvaluokiteltu tieto, turvaluokitus (security classification)

luottamuksellisten asiakirjain ja tietojen jakaminen luokkiin salassapidettävyyden perusteella
Valtionhallinnon turvaluokitus sisältää seuraavat luokat:

- I turvaluokka - erittäin salainen: äärimmäisen arkaluonteista, salassa pidettävää tietoa, jota voi käsitellä vain sen vastaanottajaksi merkitty henkilö. Tietoa ei saa lähettää sähköpostissa.
- II turvaluokka - salainen: arkaluonteista, salassa pidettävää tietoa, jota voivat käsitellä vain ne, jotka on virastossa oikeutettu käsittelemään salassa pidettäviä asioita. Salaista tietoa voi lähettää sähköpostissa vain riittävän vahvasti salattuna.
- III turvaluokka - luottamuksellinen: salassa pidettävää tietoa, jota voivat käsitellä vain ne, jotka tehtävässään sitä tarvitsevat. Tietoa voi lähettää sähköpostissa riittävän vahvasti salattuna.
- IV turvaluokka - viranomaiskäyttö: Tiedon paljastuminen heikentäisi viranomaisen toimintaedellytyksiä.
- Valtionhallinnon turvaluokitus on tarkemmin selitetty valtiovarainministeriön ohjeessa VM 5/01/2000.

LIITE 2: Yliopiston tietoturvallisuutta ohjaavia säädöksiä, suosituksia ja ohjeita

Tietoturvallisuus perustuu viranomaisten toiminnan julkisuudesta annetun lain ja asetuksen lisäksi useisiin eri lakeihin. Yksityiselämän suoja ja julkisuusperiaate ovat jo perustuslaissa säädetyt perusoikeuksia. Eri lakeihin sisältyvien salassapitosäännösten lisäksi laeista tärkeimpiä ovat

- Perustuslaki (731/1999)
 - 10 § (Yksityiselämän suoja ja luottamuksellisen viestin salaisuus),
 - 12 § (Viranomaisten hallussa olevien asiakirjojen ja tallenteiden julkisuus)
- Laki viranomaisten toiminnan julkisuudesta (621/1999)
- Henkilötietolaki (523/1999) (Henkilötietojen käsittelyä koskevat yleiset periaatteet)
- Sähköisen viestinnän tietosuojalaki (516/2004)
- Laki yksityisyyden suojasta työelämässä (759/2004)
- Arkistolaki (831/1994) (Asiakirjojen laatiminen, säilyttäminen ja käyttö)
- Valtion virkamieslaki (750/1994) 17§ (Säädös valtion virkasuhteesta)
- Työsopimuslaki (55/2001)
- Rikoslaki (39/1889)
 - 28.luku 7-9 § (Luvaton käyttö)
 - 34.luku 9a § (Vaaran aiheuttaminen tietojenkäsittelylle)
 - 38.luku 1-9 § (Tieto- ja viestintärikokset)
 - 38.luku 2 § (Salassapitorikos)
 - 38.luku 3-4 § (Viestintäsalaisuuden loukkaus)
 - 38.luku 5-7 § (Tietoliikenteen häirintä)
 - 38.luku 8 § (Tietomurto)
 - 38.luku 9 § 1. kohta (Henkilörekisteririkos)
- Henkilötietolaki (523/1999) 48 § (Henkilörekisteririkkomus)
- Vahingonkorvauslaki (41/1974)

Valtioneuvoston periaatepäätökset

- Tietohallinto
- Tietoturvallisuus
- Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia

VM:n tietoturvaohjeita ja -julkaisuja: (www.vm.fi/vahti)

- Haittaohjelmista suojautumisen yleisohje, VAHTI 3/2004
- Tietoturvallisuus ja tulosohejaus, VAHTI 2/2004
- Valtionhallinnon tietoturvallisuuden kehitysohjelma 2004-2006, VAHTI 1/2004
- Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa, VAHTI 7/2003
- Opas julkishallinnon tietoturvakoulutuksen järjestämisestä, VAHTI 6/2003
- Käyttäjän tietoturvaohje, VAHTI 5/2003
- Valtionhallinnon tietoturvakäsitteistö, VAHTI 4/2003
- Tietoturvallisuuden hallintajärjestelmän arviointisuositus, VAHTI 3/2003
- Turvallinen etäkäyttö turvattomista verkoista, VAHTI 2/2003
- Valtion tietohallinnon Internet-tietoturvallisuusohje, VAHTI 1/2003
- Tunnistaminen valtionhallinnon verkkopalvelimissa, VM 6/01/2003
- Arkaluonteiset kansainväliset tietoaineistot, VAHTI 4/2002
- Valtionhallinnon etätyön tietoturvallisuusohje, VAHTI 3/2002

- Tietoteknisten laittilojen turvallisuussuositus, VAHTI 1/2002
- Toimet tietoturvaloukkaustilanteissa, VAHTI 7/2001
- Valtion tietotekniikkahankintojen tietoturvallisuuden tarkistuslista, VAHTI 6/2001
- Valtionhallinnon sähköpostien ja lokitietojen käsittelyohje, VAHTI 5/2001
- Sähköisten palveluiden ja asiointin tietoturvallisuuden yleisohje, VAHTI 4/2001
- Salauskäytäntöjä koskeva valtionhallinnon tietoturvaluussuositus, VAHTI 3/2001
- Valtionhallinnon lähiverkkojen tietoturvaluussuositus, VAHTI 2/2001
- Valtion viranomaisen tietoturvaluussyön yleisohje, VAHTI 1/2001
- Valtionhallinnon tietojärjestelmäkehityksen tietoturvaluussuositus, VAHTI 3/2000
- Valtionhallinnon tietoaineistojen käsittelyn tietoturvaluusohje, VAHTI 2/2000
- Tietojärjestelmäselosteen laadintasuositus, VM 17.2.2000
- Salassa pidettävien tietojen ja asiakirjojen turvaluokittelu- ja merkintäohje, VM 19.1.2000
- Valtion tietohallintotoimintojen ulkoistamisen tietoturvaluussuositus, VAHTI 2/1999
- Suositus toimitilaturvallisuudesta, VM 31.12.1998

Muita

Puolustustaloudellinen suunnittelukunta

- Tietotekniikan turvallisuus ja toiminnan varmistaminen, Tietojärjestelmäjaoston ohje 1/2002, http://www.nesa.fi/julk/VALMO_4=Kooste_web.pdf

LIITE 3: Keskeiset yliopiston voimassa olevat tietoturvaluuteen liittyvät säännöt ja ohjeet

- Tietoturvaluoliikka (määräys)
- Tietojärjestelmien käytön säännöt
- Tietotekniikkarikkomusten seuraamuskäytäntö (ohje)
- Sähköpostin käsittelysäännöt ja sen sovellusohjeet
- Sähköpostin suodatusohje
- Tietojärjestelmien ylläpitosäännöt
- Yliopistosta poistuvien henkilöiden tiedostojen käsittelysäännöt (kuolemantapauksen ja muun poistumisen osalta).
- Tietoturvaluopikkeamiin reagoiminen (ohje)
- Tiedottaminen poikkeamatilanteissa (ohje)
- Todistusaineiston suojausohje.

LIITE 4: Tampereen yliopiston tietoturvaluperiaatteet, luku Vastuut (hyväksytty yliopiston hallituksessa 7.6.2002)

Yleistä tietohallintoa johtaa yliopiston johtosäännön 13 §:n mukaan rehtori. Osana kokonaisvastuutaan rehtori ja yliopiston hallitus vastaavat tietoturvaluuden toteutumisesta ja tarvittavien edellytyksien luomisesta.

Rehtorin kolmivuotiskausiksi asettama tietoturvaluuden johtoryhmä valmistelee ja ohjaa yliopiston tietoturvaluuden käytännön toteutusta ja kehittämistoimenpiteitä sekä niihin liit-

tyvää riskienhallintaa hallituksen hyväksymän Tampereen yliopiston tietoturvaperiaatteiden mukaisesti.

Yliopistossa on rehtorin nimeämä tietohallintojohtajan alaisena toimiva tietoturvapäällikkö. Tietoturvapäällikkö vastaa tietoturvallisuuden seurannasta, raportoinnista ja kehittämishankkeiden toteutuksesta sekä valmistelelee niitä yhdessä tietoturvallisuuden johtoryhmän kanssa. Tietoteknisestä tietoturvasta yliopistossa vastaa tietokonekeskus.

Yksiköiden johtajat, tietojärjestelmien vastuuhenkilöt, yksiköiden atk-yhdyshenkilöt ja tietoturvavastaavat sekä tekniset asiantuntijat vastaavat kukin omalta osaltaan tietoturvan toteutumisesta yksiköissään ja tietojärjestelmissään.

Yliopiston yksiköt varautuvat oman ympäristönsä tietoturvallisuuden toteuttamisen kustannuksiin omissa toimintasuunnitelmissaan. Tietoturvallisuuden toteuttamista yksiköissä ja niiden tietojärjestelmissä ohjaa ja valvoo kullekin yksikölle nimettävä vastuuhenkilö.

Jokainen yliopiston tietoja käsittelevä on vastuussa tietoturvallisuuden toteuttamisesta omalta osaltaan.

LIITE 5: Tietoturvan organisointi ja vastuut

Tässä liitteessä on esimerkkinä tietoturvallisuuden organisoinnista ja siihen liittyvistä vastuiden erittelystä käytetty Tampereen yliopistossa vuonna 2002 tehtyä erittelyä, jossa käytettiin mallina VAHTI 1/2001 esitettyä jakoa. Johtuen kunkin yliopiston erilaisesta tehtävänjaosta, tulee tämä liite räätälöidä kokonaisuudessaan omaan yliopistoon soveltuvaksi.

[Tietoturvan organisointi ja vastuut Tampereen yliopistossa

Tietoturvallisuuden toteuttaminen on jatkuvaa laaja-alaista toimintaa, jota ei voida asettaa vain muutaman vastuuhenkilön kannettavaksi, vaan johon tarvitaan tiivistä ja rakentavaa yhteistyötä kaikkien yliopistoyhteisöön kuuluvien henkilöiden ja ryhmien kesken. Tietoturvallisuuden toteuttamiseen ja valvontaan osallistuu jokainen Tampereen yliopiston henkilökuntaan ja järjestelmien ja palveluiden käyttäjiin kuuluva osana omaa yleistä toimintavastuutaan. Tietoturvallisuuden ohjaustehtävissä ja kehittämisessä tarvitaan sen lisäksi erityisasiantuntemusta ja nimettyjä turvallisuusvastuuhenkilöitä.

Tietoturvallisuuden vastuujärjestelyn tulee seurata yliopiston toiminnan mahdollisia muutoksia. Monet alla mainituista vastuista voivat kuulua samankin henkilön tehtäviin ja vastuisiin. Olennaista on, että näiden tehtävien hoito on järjestetty, myös varamiesten osalta.

Rehtorin, hallintojohtajan ja/tai hallituksen vastuut

- tietoturvallisuuden toteutuminen osana kokonaisturvallisuutta
- tietoturvallisuuden resursointi ja organisointi
- tietoturvallisuuden päälinjaukset
- toimintojen tietoturvallisuuspriorisointi
- tietoturvallisuuden seuranta

Tietoturvallisuuden johtoryhmän tehtävänä on:

- valmistella ja ohjata yliopiston tietoturvallisuuden käytännön toteutusta ja kehittämistoimenpiteitä sekä niihin liittyvää riskienhallintaa hallituksen hyväksymän *Tampereen yliopiston tietoturvaperiaatteiden* mukaisesti yhdessä tietoturvapäällikön kanssa
- uudistaa tarvittaessa *Tampereen yliopiston tietoturvaperiaatteet*
- huolehtia, että yliopistolla on jatkuvuussuunnitelmat infrastruktuurin ja keskeisten järjestelmien osalta poikkeusoloja varten
- huolehtia riskianalyysin tekemisestä säännöllisesti
- edustaa yliopiston eri tahojen tietoturvallisuusnäkömymiä

- huolehtia henkilöstön turvallisuustietoisuuden lisäämisestä ja tietoturvaluususkoulutuksen suunnittelusta
- huolehtia tietoturvaluisuuden toteutumisesta ostetuissa atk-palveluissa ja
- raportoida ylimmälle johdolle tietoturvaluisuudesta
- tehdä rehtorille, hallintokeskukselle ja tietokonekeskuksen johtokunnalle yliopiston tietoturvaluisuutta koskevia ehdotuksia ja aloitteita sekä hallintokeskukselle tietoturvaluusuunnitelman edellyttämiä määrärahaesityksiä.

Tietoturvaluupäällikön tehtävänä on:

- valmistella tietoturvaluisuuden kehittämishankkeita yhdessä tietoturvaluisuuden johtoryhmän kanssa
- vastata tietoturvaluisuuden kehittämishankkeiden toteutuksesta
- vastata tietoturvaluususkoulutuksen järjestämisestä
- tiedottaa tietoturvaluusasioista ja -ongelmista
- osallistua turvallisuusperiaatteiden määrittelyyn
- avustaa johtoa ja yksiköitä tietoturvaluisuuden toimeenpanossa
- kehittää ehdotuksin tietoturvaluisuutta
- järjestää tietoturvaluisuutta koskeva seuranta
- raportoida ylimmälle johdolle tietoturvaluisuudesta
- toimia tietoturvaluisuuden johtoryhmän sihteerinä
- tehdä muut tietoturvaluisuuden johtoryhmän hänelle antamat tehtävät.

Tietokonekeskuksen tehtävänä on:

- huolehtia teknisestä tietoturvaluusta yliopistossa
- vastata yliopiston tietoliikenneverkon turvallisuudesta
- huolehtia yliopiston keskitetystä varmuus- ja suojakopioinnista
- järjestää tekniseen tietoturvaluuun liittyvää koulutusta ylläpitäjille
- neuvoa tekniseen tietoturvaluuun liittyvissä kysymyksissä.

Laitoksen / muun yksikön johtajan tehtävänä on:

- yksikkönsä tietoturvaluisuuden ja siihen liittyvien kehittämistoimenpiteiden resursointi ja toimeenpano asetettujen tietoturvaluustavoitteiden mukaisesti
- seurata yksikkönsä tietoturvaluisuuden ohjeiden noudattamista
- toimia yksikkönsä tietoturvaluisuuden yhteyshenkilönä tai nimetä yhteyshenkilö
- nimetä yksikkönsä omistamien tietojärjestelmien vastuuhenkilöt ja
- raportoida tietoturvaluisuudesta ja siihen kohdistuvista häiriöistä.

Tietoteknisten asiantuntijoiden (mm. järjestelmien ylläpitäjien, suunnittelijoiden, ohjelmoijien) tehtävänä on:

- soveltaa ja toteuttaa yliopiston tietoturvaluusperiaatteita omaa erikoisasiantuntemusta hyödyntäen
- vastata tietoturvaluustoimenpiteistä omalla alueellaan
- noudattaa hyvää tietoturvaluustapaa ja
- raportoida tietoturvaluisuudesta ja siihen kohdistuvista häiriöistä.

Tietopalveluista ja asiakirjahallinnosta vastaavien tehtävänä on:

- toimeenpanna tietoturvaluus tietopalveluissa ja asiakirjahallinnossa hyvän tiedonhallintatavan ja tietoturvaluustavan mukaisesti.

Tietojärjestelmän omistajan tehtävänä on:

- vastata henkilörekisteri- ja tietojärjestelmäselosteista

-
- vastata tietojärjestelmän ja sen tietojen suojauksesta, käyttöoikeuksista sekä varmuus- ja suojakopioinnista
 - toimeenpanna tietojärjestelmäänsä liittyvät turvallisuustoimenpiteet ja kehittää niitä
 - seurata tietoturvaluutta tietojärjestelmässä ja
 - raportoida tietoturvaluudesta ja siihen kohdistuvista häiriöistä.

Sovelluksen tai palvelun vastuuhenkilön/pääkäyttäjän tehtävänä on:

- ylläpitää henkilörekisteri- ja tietojärjestelmäselosteet ja pitää ne rekisterissä olevien saatavilla
- ylläpitää turvallisuusmenettelyt tietojärjestelmässä
- seurata järjestelmän toimintaa tietoturvaluuden kannalta
- varautua poikkeaviin tapahtumiin ja niiden vaatimiin vastatoimenpiteisiin ja
- raportoida turvallisuutta vaarantavista tapahtumista ja häiriöistä.

Yksiköiden atk-yhdyshenkilöiden ja tietoturvaluustavastavien tehtävänä on:

- ylläpitää ja valvoa vastuullaan olevien järjestelmien tietoturvaluutta yliopiston tietoturvaluuden yleisohjeistuksen mukaisesti ja
- raportoida tietoturvaluudesta ja siihen vaikuttavista tekijöistä

Loppukäyttäjien tehtävänä on:

- tuntee tietoturvaluudesta annetut ohjeet ja noudattaa niitä
- osallistua heille suunnattuun tietoturvaluokulutukseen sekä
- raportoida havaitsemistaan ongelmista, uhkista ja ohjeiden vastaisista menettelyistä.

Konsulttien ja palveluyritysten tehtävänä on:

- noudattaa hyvää tietojenkäsittely- ja tietoturvaluustapaa
- ylläpitää ja valvoa yliopistoon liittyvässä toiminnassaan valtiorhallinnon tietoturvaluuden yleisohjeistuksen mukaista ja ohjeistettua tietoturvaluutta sekä
- raportoida tietoturvaluudesta ja siihen vaikuttavista tekijöistä.

Tietoturvaluusvastuita on myös muilla keskeisillä henkilöryhmillä kuten

- hankintoja hoitavilla henkilöillä
- henkilörekisterien hoitajilla ja
- sopimus- ja kiinteistöhallinnon henkilöillä.

Yliopistossa suoritetaan Valtioralouden tarkastusviraston sekä omien sisäisten tarkastajien toimesta sisäistä tarkastusta mm. tietojenkäsittelyn, hallinnon järjestelmien ja yliopiston konnaistietoturvaluuden osalta.

]