Case-tutkimus: BS7799-vaatimusten, VAHTI-tietoturvaohjeiden ja ITIL-prosessikuvausten vertailusta ja yhdistämisestä

Lauri Hämäläinen

Tampereen yliopisto
Tietojenkäsittelytieteiden laitos
Tietojenkäsittelyoppi
Pro gradu -tutkielma
Ohjaaja: Pirkko Nykänen
Maaliskuu 2007

Tampereen yliopisto
Tietojenkäsittelytieteiden laitos
Tietojenkäsittelyoppi
Lauri Hämäläinen: Case-tutkimus: BS7799-vaatimusten, VAHTI-tietoturvaohjeiden ja ITIL-prosessikuvausten vertailusta ja yhdistämisestä
Pro gradu -tutkielma, 97 sivua, 103 liitesivua
Maaliskuu 2007

Tietoturvallisuuden hallintaan on olemassa lukuisia menetelmiä. Tässä tutkimuksessa käsiteltiin BS 7799 standardia, VAHTI-tietoturvaohjeita ja ITIL-prosessikuvauksia. Näissä ohjeissa puhutaan usein samoista asioista eri nimillä ja siksi eroja voi löytyä enemmän kuin niitä todellisuudessa on. Tutkimuksessa on selvitetty näiden ohjeistojen sisältöä, eroja ja sitä miten niitä voi yhdistää. Lisäksi on selvitetty miten nämä ohjeistot soveltuvat opetusorganisaatiolle. Tutkimuksen sisältö on jaoteltu BS 7799 päälukujen mukaan, sillä ne edustavat tietoturvan eri osa-alueita selkeästi. VAHTI-ohjeet ja ITIL- prosessikuvaukset on yhdistetty vastaaviin BS 7799 lukuihin.

Pelkällä teorialla kuitenkin harvoin saadaan muutoksia aikaan. Tietoturvallisuutta on siis paras tutkia käytännön esimerkin kautta, siksi tutkimuksen oleellisena osana on opetusorganisaatio Hämeen ammattikorkeakoulu. Käyn läpi tietoturvallisuuden teorioita ja hyviä käytäntöjä ja sovellan niitä tähän case-tapaukseen. Otan huomioon niin tekniikan kuin ihmisetkin, sillä tietoturva sisältää myös eettisiä kysymyksiä ja ihminen on usein tietoturvan heikoin osa. Tarkoituksena on parantaa tietoturvallisuustietoisuutta ja kouluttaa ihmisiä toimimaan oikein. Tähän vaaditaan kuitenkin resursseja ja ilman päteviä syitä ei panostusta tähän asiaan tapahdu. Kehittämispäätöksien lähteenä ovat HAMKille tehdyt riskianalyysit, joissa käydään kattavasti läpi organisaatiota uhkaavat tekijät. Tuloksina on konkreettisia ja perusteltuja parannusehdotuksia HAMKin tietoturvaan.

Avainsanat ja – sanonnat: tietoturvallisuus, riskienhallinta, BS 7799, ISO 17799, ITIL, VAHTI
CR-luokat: C.2, D.4.6 K.6.5

Kiitokset
Haluan erityisesti kiittää Jari Kivelää hänen antamastaan mahdollisuudesta tehdä tämä tutkimus HAMKin kanssa yhteistyössä. Kivelä uhrasi omaa aikaansa työkiireidensä lisäksi auttaakseen minua tämän tutkimuksen teossa. Toivon, että tämä tutkimus auttaa HAMKia.

SISÄLLYSLUETTELO

1 JOHDANTO 1

1.1 TAUSTA JA TUTKIMUSKYSYMYKSET 1
1.2 HÄMEEN AMMATTIKORKEAKOULUN ESITTELY 1
1.3 KESKEISET KÄSITTEET 3

2 TUTKIMUKSEN TAVOITTEET JA MENETELMÄT 6

2.1 TUTKIMUSKYSYMYKSET JA TUTKIMUKSEN RAJAUS 6
2.2 TUTKIMUKSEN MOTIIVIT 6
2.3 TUTKIMUSMENETELMÄT 6
2.4 AIKAISEMPI TUTKIMUS 8
2.5 ODOTETUT TULOKSET JA NIIDEN MERKITYS 9

3 TURVALLISUUSPOLITIIKKA 11

3.1 TIETOTURVALLISUUS JA TIETOSUOJA 12
3.2 TIETOTURVALLISUUSPOLITIIKKA 12
3.3 TIETOSUOJAPOLITIIKKA 13
3.4 TIETOTURVASTANDARDIT 13
3.5 TIETOTURVALLISUUDEN TOIMINTAOHJEET 14
3.6 RISKIEN HALLINTA JA RISKIKARTOITUKSET 14
3.7 TIETOTURVASUUNNITELMA 15
3.8 HAMKIN TIETOTURVAPOLITIIKKA 15

4 TIETOTURVALLISUUS 16

4.1 TIETOTURVALLISUUDEN HALLINTAJÄRJESTELMÄT JA NIIDEN KEHITTÄMINEN 16
4.2 TIETOTURVALLISUUDEN TAVOITTEET JA TULOSOHJAUS 18
4.3 TIETOTURVALLISUUDEN SEURANTA JA RAPORTOINTI 19
4.4 TIETOTURVALLISUUDEN JA -TOIMINNAN MITTAUS- JA ARVIOINTIMENETELMÄT JA NIIDEN TAVOITTEET 19
4.5 TIETOTURVATOIMINNAN MITTARIT 22
4.6 BS 7799, ITIL VAHTI JA PROSESSIMAISET TOIMINTAMALLIT 23
4.7 TIETOTURVALLISUUDEN PERUSRAKENNE 26
4.8 TURVAMENETTELYT SIVULLISEN PÄÄSYÄ VASTAAN 26
4.9 TIETOTURVAN ULKOISTAMINEN 27
4.10 HAMKIN TIETOTURVALLISUUDEN ORGANISOINTI, HALLINTA JA PROSESSIT 27

5 TIETORISKIEN JA – UHKIEN HALLINTA 30

5.1 RISKIEN HALLINTA 30
5.2 TIETORISKIEN ARVIOINTIMENETELMIÄ 33
5.2.1 Skenaarioanalyysi 33
5.2.2 Kyrölän menetelmä 34
5.2.3 Tarkistuslistat 35
5.2.4 Baseline 35
5.2.5 Courtneyn menetelmä 36
5.3 HAMKIN TIETORISKIEN IDEOINTI 36
5.4 HAMKIN TÄRKEÄT PALVELUT 37
5.5 HAMKIN RISKIANALYYSIT 39
5.6 HAMKIN TÄRKEIMPIEN PALVELUIDEN RISKIANALYYSIT 40
5.6.1 Prima – henkilöstöhallinto ja palkanmaksu 40
5.6.2 WinhaPro - opetushallinto 42
5.6.3 Nimipalvelut 44
5.6.4 Portaalijärjestelmä 46
5.7 RISKIANALYYSIEN TULOKSET 47

6 SUOJATTAVIEN KOHTEIDEN LUKITUS JA VALVONTA 50

6.1 VASTUU SUOJATTAVISTA KOHTEISTA 50
6.2 TIEDON LUOKITUS 50
6.3 HAMKIN SUOJATTAVIEN KOHTEIDEN LUKITUS JA VALVONTA 51

7 HENKILÖSTÖTURVALLISUUS 52

7.1 TIETOTURVALLISUUS TYÖTEHTÄVIEN MÄÄRITTELYSSÄ, RESURSOINNISSA JA YLLÄPIDON OHJEISTUKSESSA. 53
7.2 KÄYTTÄJIEN KOULUTUS 53
7.3 POIKKEUS- JA VIRHETILANTEISIIN REAGOIMINEN 55
7.4 HAMKIN HENKILÖSTÖTURVALLISUUS 55

8 FYYSINEN TURVALLISUUS JA YMPÄRISTÖN TURVALLISUUS 58

8.1 TURVA-ALUEET 58
8.2 LAITETURVALLISUUS 59
8.3 YLEISET TURVAMEKANISMIT 59
8.4 HAMKIN FYYSINEN JA YMPÄRISTÖN TURVALLISUUS 59

9 TIETOLIIKENTEEN JA KÄYTTÖTOIMINTOJEN HALLINTA 61

9.1 MENETTELYOHJEET JA VELVOLLISUUDET 61
9.2 JÄRJESTELMÄN SUUNNITTELU JA HYVÄKSYNTÄ 62
9.3 HAITALLISILTA OHJELMILTA SUOJAUTUMINEN 62
9.4 APUTOIMET 63
9.5 VERKON HALLINTA 63
9.6 TIETOVÄLINEIDEN KÄSITTELY JA TURVAAMINEN 63
9.7 TIETOJEN JA OHJELMIEN VAIHTO 63
9.8 HAMKIN TIETOLIIKENTEEN JA KÄYTTÖTOIMINTOJEN HALLINTA 64

10 PÄÄSY- JA KÄYTTÖOIKEUKSIEN VALVONTA 66

10.1 LIIKETOIMINNAN ASETTAMAT VAATIMUKSET PÄÄSYNVALVONNALLE 67
10.2 KÄYTTÖOIKEUKSIEN HALLINTA 67
10.3 KÄYTTÄJÄN VELVOLLISUUDET 67
10.4 VERKKOON PÄÄSYN VALVONTA 68
10.5 KÄYTTÖJÄRJESTELMÄÄN PÄÄSYN VALVONTA 68
10.6 SOVELLUKSEEN PÄÄSYN VALVONTA 68
10.7 JÄRJESTELMÄÄN PÄÄSYN JA KÄYTÖN TARKKAILU 68
10.8 TIETOKONEEN MATKAKÄYTTÖ JA ETÄTYÖSKENTELY 69
10.9 PÄÄSYOIKEUKSIEN VALVONTA HAMKISSA 69

11 JÄRJESTELMIEN KEHITTÄMINEN JA YLLÄPITO 71

11.1 JÄRJESTELMIEN TURVALLISUUSVAATIMUKSET 71
11.2 SOVELLUSTEN TURVAAMINEN 71
11.3 SALAKIRJOITUSMEKANISMIT 71
11.4 JÄRJESTELMÄTIEDOSTOJEN TURVALLISUUS 71
11.5 KEHITYS- JA TUKIPROSESSIEN TURVALLISUUS 72
11.6 HAMKIN JÄRJESTELMIEN KEHITTÄMINEN JA YLLÄPITO 72

12 LIIKETOIMINNAN JATKUVUUDEN HALLINTA 73

12.1 LIIKETOIMINNAN HALLINTAAN LIITTYVIÄ NÄKÖKOHTIA 73
12.2 HAMKIN TOIMINNAN JATKUVUUDEN HALLINTA 74

13 VAATIMUSTENMUKAISUUS 75

13.1 LAKISÄÄTEISTEN VAATIMUSTEN NOUDATTAMINEN 75
13.2 TURVALLISUUSPOLITIIKAN JA TEKNIIKAN VAATIMUSTENMUKAISUUDEN TARKISTUS 77
13.3 JÄRJESTELMÄN TARKASTUSNÄKÖKOHTIA 78
13.4 VAATIMUSTEN HUOMIOIMINEN JA TOTEUTTAMINEN HAMKISSA 78

14 TIETOTURVA JA ETIIKKA 79

14.1 ETIIKAN MÄÄRITELMÄ 79
14.2 TIETOTURVAETIIKAN ERI ROOLIT 80
14.3 TIETOTURVAETIIKAN TOTEUTUMINEN 82
14.4 HAMKIN TIETOTURVAKULTTUURI 84

15 YHTEENVETO 85

15.1 TUTKIMUSKYSYMYKSIIN VASTAAMINEN 85
15.2 HUOMIOITA TIETOTURVALLISUUDESTA JA TUTKIMUKSESTA 87
15.3 TULOKSET HAMKILLE 90

VIITELUETTELO 92

LIITE 1. HAMKIN RISKIEN ARVIOINTILOMAKE 98

LIITE 2. TIETOTEKNIIKKARIKKOMUSTEN SEURAAMUSKÄYNTÄNTÖ 130

LIITE 3. TIETOJÄRJESTELMIEN KÄYTTÖSÄÄNNÖT 133

LIITE 4. SÄHKÖPOSTIN KÄSITTELYSÄÄNNÖT 136

LIITE 5. TIETOJÄRJESTELMIEN YLLÄPITOSÄÄNNÖT 142

LIITE 6 TIETOTURVAPOIKKEAMIIN REAGOIMINEN 150

LIITE 7. TIEDOTTAMINEN POIKKEAMATILANTEISSA 163

LIITE 8. HÄMEEN AMMATILLISEN KORKEAKOULUTUKSEN KUNTAYHTYMÄN TIETOTURVAPOLITIIKKA 167

LIITE 9. HÄMEEN AMMATILLISEN KORKEAKOULUTUKSEN KUNTAYHTYMÄN TIETOTEKNIIKKAPALVELUIDEN KÄYTTÖSÄÄNNÖT 171

LIITE 10. HAMKIN TYÖNTEKIJÖIDEN KÄYTTÄJÄTUNNUSHALLINTO 176

LIITE 11. MALLI TIETOSUOJAPOLITIIKAKSI 179

LIITE 12. TIETOTURVALLIUUSPOLITIIKAN MALLI 183

1 Johdanto

1.1 Tausta ja tutkimuskysymykset

Tutkimuksen aiheena on case-tutkimus British Standards Instituten 7799 standardin vaatimusten, VAHTI-tietoturvaohjeiden ja the IT Infrastructure Libraryn prosessikuvausten vertailusta ja yhdistämisestä. Tutkimuksen kohde on Hämeen ammattikorkeakoulu (HAMK) ja HAMKin Kehittämisyksikkö. Tälle kokonaisuudelle tehdään riskianalyysit, tietoturvan kartoitus ja -kehittämissuunnitelma käyttäen apuna yllämainittuja lähteitä. Yhteyshenkilönäni HAMKissa on tutkimuksen teon aikana ollut tietojärjestelmäpäällikkö Jari Kivelä.

Kohdeorganisaation omat tarpeet määrittävät tutkimukseen otettavat tietoturvan osa-alueet, joten yhteistyö HAMKin henkilökunnan kanssa on erityisen tärkeää. Opetusorganisaation erityispiirteet tekevät tutkimuksesta mielenkiintoisen ja on hyvä käytännössä nähdä, miten tietoturvan organisoiminen onnistuu tällaisessa ympäristössä, jossa erilaiset käyttäjäryhmät vaativat erilaisia menetelmiä tietoturvallisuuden kokonaisvaltaiselle hallinnalle. Tietoturvallisuuden kehityksessä on eri kypsyysvaiheita ja tarkoitukseni on selvittää, millä tasolla HAMK on tällä hetkellä ja mille tasolle olisi realistista pyrkiä.

Järvisen sanoin tieto on yrityksen voimavara ja menestystekijä [2002, s. 21 ja 34]. Vaikka HAMK ei ole yritys, sen fyysistä omaisuutta, työntekijöitä ja mainetta on syytä suojella. Myös opetusorganisaatiossa käsitellään arvokkaita tietoja ja tietoturvan painotusten on oltava erilaista kuin yrityksissä. Tietoturvan onnistuneelle toteuttamiselle on olemassa valitettavasti lukuisia esteitä. Suurimpina ovat resurssien ja motivaation puute, koulutuksen puuttuminen tai riittämättömyys ja muutosvastarinta työntekijöiden keskuudessa. Jatkuva työn tehokkuuden korostaminen ja tulosvastuullisuus saattavat vähentää tietoturvan huomioimista, sillä tietoturva vaatii aina ajallista ja rahallista panostusta. Tietoturvatyön tavoite on kuitenkin tukea arkityötä, jolloin jo pienillä lisäpanostuksilla koulutukseen ja teknisiin suojaratkaisuihin voidaan ehkäistä tietoriskejä ja varautua niiden vaikutuksiin tehokkaasti. Tässä tutkimuksessa tutkittu tietoturvallisuus on vain yksi osa yritysturvallisuutta ja se ei ole eristetty muista osa-alueista.

1.2 Hämeen ammattikorkeakoulun esittely

HAMK on valtakunnallista tunnustusta saanut kouluttaja ja aluekehittäjä. HAMK toimii seitsemällä koulutusalalla, koulutusohjelmia on 24. HAMK tarjoaa opiskelijoilleen monialaisen, elinkeinoelämän kanssa verkottuneen

oppimisympäristön. Verkko-opetuksen ja digitaalisten opetustoteutusten kehittämiseen on HAMKissa panostettu verkkosivujen mukaan merkittävästi [HAMKin verkkosivut, 2007]. Valmistuneiden työllistymisaste on maan korkeimpia, samoin yrittäjiksi ryhtyvien osuus. Yrittäjyyttä edistetään mm. starttihautomoilla, joita on kaikissa HAMKin toimipaikoissa. HAMK toimii seitsemällä paikkakunnalla ja palvelee kahden miljoonan asukkaan työssäkäyntialuetta. HAMK tekee soveltavaa tutkimusta ja kehitysprojekteja yritysten ja yhteisöjen kanssa. Keskeisenä tavoitteena on laaja-alaisen ja kansainvälisesti laadukkaan tiedon sekä osaamisen kehittäminen ja välittäminen alueen elinkeinoelämälle ja julkiselle sektorille [HAMKin verkkosivut, 2007].

HAMKin tietojärjestelmillä on noin 8000 käyttäjää. Henkilökuntaan kuuluvat opetushenkilöt, tukitoimintojen ja yleishallinnon henkilöt, tietotekniikkapalveluiden henkilöt. Opiskelijoita ovat omat opiskelijat, vaihto-opiskelijat (ulkomaalaiset) ja täydennyskoulutuksen opiskelijat.

Yhteistyökumppaneihin kuuluu yritysten henkilöstöä, vierailijoita (opettajia, yritysten edustajia), luottamushenkilöitä (esim. HAMK:n hallituksen).

HAMK:n tietotekniikka on organisoitu siten, että toimipaikkojen (n. 12 kpl) tietotekniikkahenkilöstö (kaikkiaan vähän yli 20 henkilöä) vastaa paikallisen tietotekniikan toimivuudesta ja paikallisesta tietotekniikkatuesta. Toimipaikoissa on ns. tietotekniikkavastaavat, jotka viime kädessä ovat vastuussa paikallisista tietotekniikkapalveluista. Toimipaikkojen tietotekniikkahenkilöt osallistuvat nykyään jonkin verran yhteisten tietotekniikkapalveluiden ylläpitoon (yhteiset sovellukset ja palvelimet). Kehittämisyksikön tietotekniikkahenkilöstö (7 henkilöä) vastaa yhteisten järjestelmien hankinnasta (ml. vaatimusmäärittelyt) ja ylläpidosta (sekä ohjelmistot että laitteet).

Kehittämisyksikkö tuottaa koko kuntayhtymän (HAMK ja HAMI yhdessä) käyttöön seuraavia palveluita: talous- ja henkilöstöhallinto, kaupallinen täydennyskoulutustoiminta, opiskelijahallinto, (ml. avoin AMK ja ylemmät AMK-tutkinnot), hankkeiden hallinnoinnin, tukeminen, tietotekniikkapalvelut, viestintä- ja julkaisutoiminta, informaatio- ja kirjastopalvelut, tutkimus- ja kehittämistoiminnan kehittäminen, koulutuksen kehittäminen (ml. etäopetustoiminta) ja yleishallinto. Kehittämisyksikkö tuottaa siis toisaalta ns. peruspalveluita ja toisaalta toimii koko HAMKin kehittämistoiminnan moottorina. Talous-, henkilöstö- ja opiskelijahallinto ovat riippuvaisia tietotekniikkapalveluista.

Tietoverkkoja ovat toimipaikat yhdistävä alueverkko (yhteyksien nopeudet 10–100 Mbps, tähtimäinen rakenne, keskellä reititys), toimipaikkojen lähiverkot (reititystä tapahtuu myös lähiverkon sisällä) ja Internet-yhteys (Funet-liittymä).

1.3 Keskeiset käsitteet

Tietoturva, valtiohallinnon tietoturvakäsitteistön mukaan tietoturva merkitsee tavoitetilaa, jossa tiedot ja järjestelmät ovat asianmukaisesti suojattu [VAHTI 4/2003, s. 51]. Asianmukainen ei tarkoita mitään tiettyä vakiotasoa, vaan se määritetään tarpeiden mukaan. Tutkimuksen näkökulma tietoturvaan on laaja, sillä tarkoitus on syventyä moniin tietoturvan eri osa-alueisiin ja pystyä toteuttamaan, arvioimaan ja kehittämään organisaationsa tietoturvaa. Tiivistetysti tieturva on prosesseja, joilla taataan tiedon luottamuksellisuus, eheys ja käytettävyys. Määrittelyssä on tiettyjä vaikeuksia, sillä kaikki tietoturvallisuuteen liityviä asioitaei voida pelkästään näillä kolmella käsitteellä kuvata.

Järvinen esittää tietoturvan ulottuvuudet luottamuksellisuutena, eheytenä, saatavuutena sekä todentamisena, pääsynvalvontana ja kiistämättömyytenä [2002]. Perinteisten ulottuvuuksien rinnalle on esitetty muitakin ulottuvuuksia kuten Miettisen ehdottamat aitous, hyödyllisyys ja hallussapito [1999]. On selvää, että Miettinen ja Järvinen tarkoittavat samoja asioita, mutta käyttävät vain hieman erilaisia termejä. Heidän kuvauksiensa asiasisältö on silti sama.

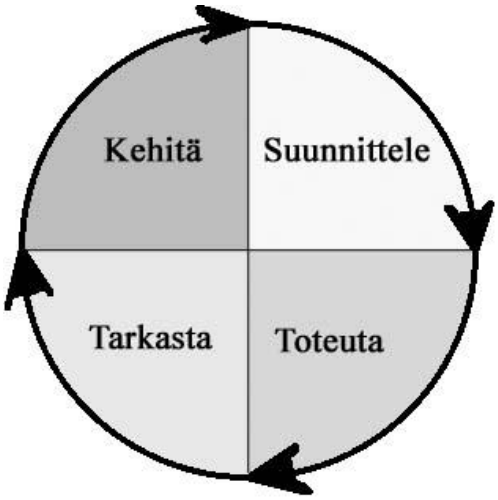
Tietoturvan ulottuvuuksia voidaan painottaa eri tavoilla. Tietojen tärkeydellä on väliä, kun pohditaan, minkälaisia vaatimuksia niitä suojamaan asetetaan. Esimerkkinä pankkitietojen täytyy olla täysin eheitä, sillä väärä tilinumero tai saldosta puuttuva nolla tekevät tiedosta käyttökelvotonta. Sarjakuvan puhekuplasta puuttuva merkki ei kuitenkaan tee yhtä paljon vahinkoa tiedolle. Näissä molemmissa tapauksissa tietojen eheys on vaikkapa 99,99 %, mutta tulkitsijan virheensietokyky erilainen, jolloin eheyden käytännön vaatimukset ovat erilaiset. Henkilötietojen käsittelyssä luottamuksellisuus toteutuu, kun tietoja pääsee käsittelemään vain siihen oikeudet omaava henkilö. Yksityisyys voi kuitenkin olla vaarassa, jos henkilötietoja on kerätty ilman lupaa. Tässä tapauksessa tarvitaan yksinkertaistettuna kaksi erityyppistä käsitettä henkilötietojen käsittelyyn turvallisesti. Tietoja käsittelevää henkilöä ohjaavat yksityisyyden käsittelyä koskevat määräykset ja tietojärjestelmän data on suojattu luottamuksellisuuden vaatimilla salasanoilla. Mietittäessä tätä tapausta laajemmin huomataan, että tarvitaan lisäksi muitakin tietoturvallisuuden periaatteita, jotta voidaan turvata henkilötietoja mahdollisimman hyvin.

Tietoturvan perustavoitteita ei voi toteuttaa, jos ei määritetä mitä kukin tavoite tarkalleen pitää sisällään ja millä tarkkuudella tavoite voidaan

todellisuudessa toteuttaa. Tutkimuksessa pyrin ottamaan huomioon tietoturvallisuuden sekä sosiaaliset että tekniset näkökulmat huomioon.

Tietoriski, tietoturvariski, tietoturvauhka, tietoturvaselkkaus ja tietorikos ovat termejä, joiden tarkoitus on kuvata tietoturvaan liittyviä mahdollisia ja toteutuneita tapahtumia.

Britannian standardointilaitos BSI on julkaissut tietoturvastandardin BS 7799/ISO 17799. BS 7799:n osasta 1 Tietoturvallisuuden hallinnan menettelyohje on lukuisten päivitysten jälkeen luotu ISO 17799 [BS 7799-1:fi, 2000]. Osa 2 on nimeltään tietoturvallisuuden hallintajärjestelmät [BS 7799-2:fi, 2003]. Menettelyohje on eräs normisto, jota voidaan käyttää tietoturvallisuuden hallintajärjestelmän tehokkuuden arvioinnin perustana. BS 7799 tarkastelee tietoturvallisuuden johtamista kymmeneltä eri kannalta. Standardi soveltuu myös voittoa tavoittelemattoman organisaation käyttöön. Standardi kannustaa ottamaan käyttöön prosessimallin organisaation tietoturvallisuusjärjestelmää kehitettäessä, toteutettaessa, käytettäessä, valvottaessa, ylläpidettäessä ja parannettaessa sen vaikuttavuutta. Nykyiseen versioon on otettu käyttöön PDCA-malli (PLAN- DO-CHECK-ACT) [Kuva 1].

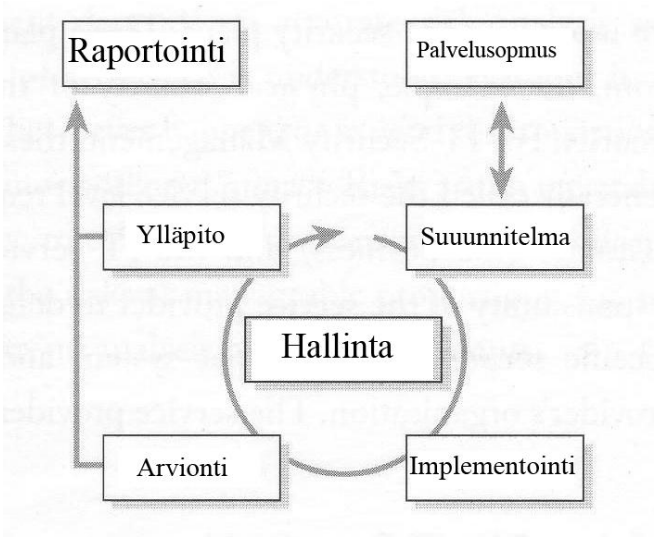


Kuva 1. PDCA-malli

Valtiovarainministeriö asettama valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI on tietoturvallisuuden asiantuntemusta laajapohjaisesti edustava ryhmä, jonka kehittämät ohjeistukset kattavat kaikki tietoturvallisuuden osa-alueet [VAHTI].

Tietosuojan yleislaki on henkilötietolaki. Tietosuojaan kuuluvat ihmisten yksityiselämän suoja ja muut sitä turvaavat oikeudet henkilötietoja käsiteltäessä. Tietosuojan tarkoitus on estää tietojen valtuuttamaton saanti ja käyttö. Tietoturva on menetelmiä, joilla tietosuoja toteutetaan.

ITIL, Information Libararyn kirjoihin sisältyvä Security Management esittää ITIL-käytäntöjen mukaisten tietoturvaprosessien mallit [ITIL, 2004]. ITIL:ssä on kyse parhaiden käytäntöjen kokoelmista. Kyse on myös aina näiden parhaiden käytäntöjen soveltamisesta kussakin organisaatiossa. ITIL turvallisuudenhallintaprosessi on erillinen prosessi, joka pyritään liittämään muihin prosesseihin. Hallinta voi reagoida tarkasti vain silloin, kun se toimii kehämallin periaatteen mukaan. Palvelutasosopimuksista lähtien on tietotuvallisuuden takaamiseksi suoritettava turvatoimia. Turvallisuudenhallinta mahdollistaa ja takaa, että menetelmät muuttuvia tilanteita varten implementoidaan ja ylläpidetään, tietoturvaselkkaukset selvitetään, auditointien tulokset kertovat menetelmien riittävyyden ja tietoturvallisuuden tasosta tuotetaan raportteja. Prosessien kehittämisessä on käytössä suljettu kehämalli aivan kuten BS 7799:ssa [Kuva 2].



Kuva 2. Tietoturvallisuuden hallintaprosessi [ITIL, 2004, s. 16]

2 Tutkimuksen tavoitteet ja menetelmät

2.1 Tutkimuskysymykset ja tutkimuksen rajaus

Haluan selvittää seuraaviin kysymyksiin vastaukset:

- Voidaanko BS7799 tietoturvastandardi, ITIL-prosessit ja VAHTI ohjeet yhdistää?
- Mitä edellä mainitut standardit pitävät sisällään?
- Miten ne soveltuvat opetusorganisaation tarpeisiin?
- Mikä on HAMKin tietoturvallisuuden tila ja miten sitä voi parantaa?

Tutkimus on pääosin rajattu BS 7799/ISO 17799 standardiin, ITILiin ja VAHTI-ohjeisiin, mutta tukena on myös muu alan tutkimus ja kirjallisuus. Kohteena HAMK Kehittämisyksikkö ja Hattelmalan yksikkö, FUNET ulkoisena osapuolena vaatimuksineen, HAMKin taloushallinto sisältäen kirjanpidon, henkilöstöhallinnan ja opintotoimisto sisältäen opintohallintojärjestelmän.

2.2 Tutkimuksen motiivit

Haluan selvittää, miten BS 7799 tietoturvastandardia, VAHTI-tietoturvaohjeita ja ITILin hyviä käytäntöjä voidaan yhdistää opetusorganisaation tietoturvaturvan kehityksessä. Motiiveinani ovat kiinnostus alaa kohtaan ja oman koulutuksen ja tietämyksen soveltaminen käytännön tietoturvatutkimuksessa. Tietoturvatyössä tarvitaan suurta määrää erilaisia käsitteitä, ja pelkästään niiden ulkoa opettelu ei johda mihinkään. Näiden käsitteiden sisällön ymmärtäminen vaatii tutkimusta ja kokemusta, jota tässä tutkimuksessa lähden tavoittelemaan. Erilaisten työkalujen, lähdemateriaalin ja kirjallisuuden hyödyntäminen ja soveltaminen tietoturvatyössä todelliseen esimerkkitapaukseen on haastavaa ja samalla palkitsevaa. Yksinkertaisiin ongelmiin on hyvä olla yksinkertaiset ratkaisut. Tietoturva realisoituu käytössä olevien prosessien kautta, eikä pelkästään suunnittelemalla ja dokumentoimalla. Tietoturva on myös asennekasvatusta parempaan. Oikealla asenteella ihmiset voivat oppia soveltamaan tietoturva-asioita ja monet ongelmat voidaan tehokkaasti ehkäistä. Tahdon poistaa turhaa mystiikkaa tietoturvasta ja yrittää esittää sen roolin työtä tukevana prosessina eikä vain pakollisena kiusana, kuten monet ajattelevat sen olevan.

2.3 Tutkimusmenetelmät

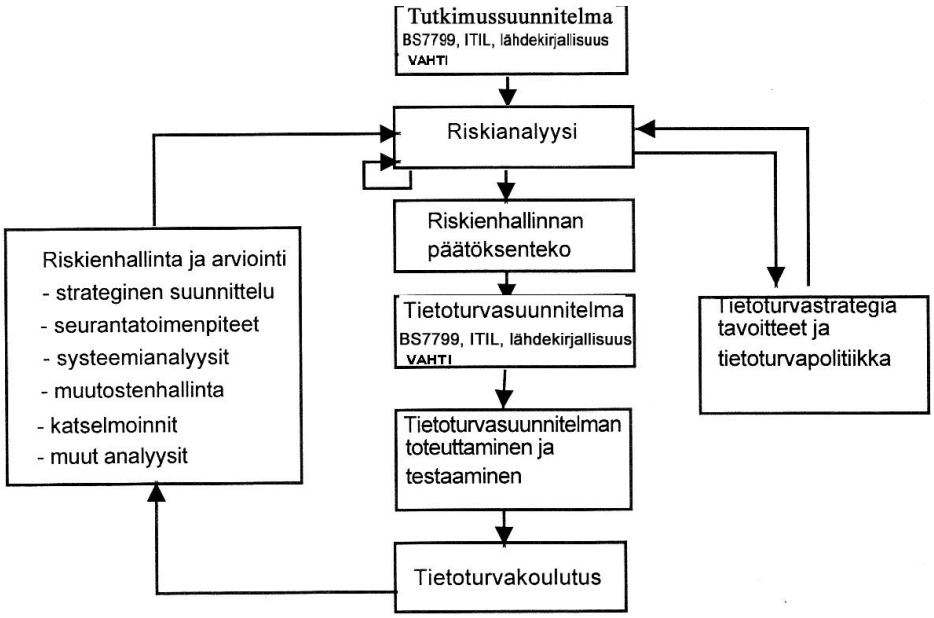
Tutkimusprosessin tukena ja – metodin valinnassa olen käyttänyt Pertti ja Annikki Järvisen kirjaa Tutkimustyön metodeista [Järvinen ja Järvinen, 2000]. Tutkimus on tyypiltään case-tutkimus, jossa olen ottanut mallia Jenkinsin tutkimusprosessista [Järvinen ja Järvinen, 2000]. Case-tutkimuksessa tutkimuskysymyksissä kysytään miten ja miksi, joten olen muotoillut omat tutkimuskysymykseni tällä tavoin. Case-tutkimus on sidoksissa nykyhetken

tapahtumiin ja oma tutkimukseni kuvastaa tätä hyvin, sillä haluan selvittää, miten HAMKin tietoturvan nykytilannetta kuvataan ja miten sitä voitaisiin parantaa.

Teorioita testaava case-tutkimus soveltuu tutkimuksessa käytettäväksi hyvin, sillä aion selvittää olemassa olevien tietoturvallisuusstandardien soveltuvuutta opetusorganisaation vaatimuksiin ja ominaisuuksiin. Perusolettamuksena minulla on se, että tietoturvastandardeja ja hyviä tietoturvakäytäntöjä voidaan käyttää opetusorganisaatiossa, mutta tarvitaan räätälöintiä ja kohdealueen tuntemista. Esimerkkinä tästä ovat VAHTI ohjeet, jotka tietyiltä osin ovat tarpeettoman tiukat HAMKia ajatellen, jolloin ne eivät suoraan sovellu sellaisinaan kaikilta osin.

Pyrin selittämään syy-seuraussuhteita, jotka ovat tietoturvallisuudessa tärkeitä. Uhkien ja riskien selvittämisessä tutkimus on sekä arvioivaa että kuvailevaa.

Organisaation tietoturvaa käydään kohta kohdalta läpi sovittujen BS 7799:n vaatimusten mukaan. Käyttökelpoisimpia ITIL-prosesseja soveltamalla voidaan tukea tietoturvaprosesseja. Tukena käytetään myös muuta tietoturvallisuuskirjallisuutta. Periaatteena on esittää tapauskohtaisesti tämänhetkinen tilanne ja esittää parannusehdotuksia. Tutkimus etenee kuvan 3 mukaisesti tietoturvasuunnitelmaan asti. Siitä eteenpäin HAMKin on tarkoitus itse jatkaa tietoturvan kehittämistä [Kuva 3.]. Kuvaa on muokattu lisäämällä siihen uusina osina tutkimussuunnitelma ja tietoturvasuunnitelmaan käyttämäni tietoturvastandardit ja muut lähteet tutkimukselle.



Kuva 3. Tutkimuksen eteneminen, muokattu Paavilaisen kuvasta [1999, s. 50].

Tietoturvallisuustason mittauksessa tarvitaan mittareita, joilta vaaditaan luotettavuutta, soveltuvuutta, yksiselitteisyyttä, helppolukuisuutta, oikea-aikaisuutta ja olennaisuutta. Käytännössä tärkein ominaisuus mittarille on olennaisuus, jotta sillä voidaan mitata juuri niitä asioita, jotka ovat organisaation tietoturvalle tärkeitä. Mittarit voidaan jakaa laadullisiin ja määrällisiin. Laadullisessa mittaamisessa käytetään sanallisia arvioita kuten ”joka päivä” tai ”tyydyttävästi” tai ”ei ole otettu huomioon”. Määrällisessä mittaamisessa mitataan numeerisia arvoja ja apuna käytetään tilastomatematiikka ja todennäköisyyslaskelmia. On syytä kuitenkin huomioida, että tietoturvaa voi mitata monin eri tavoin ja tulokset ovat usein suuntaa antavia. Mitattujen tulosten pohjalta voidaan tehdä kuitenkin päätelmiä, eikä tarvitse turvautua arvailuihin ja pelkästään subjektiivisiin arvioihin toteaa Miettinen [1999]. Riskinanalyyseissä tulen pohtimaan tällaisten mittareiden avulla miten uhkia luokitellaan.

2.4 Vastaavat aikaisemmat tutkimukset opetusorganisaatioiden tietoturvallisuudesta

Aikaisempia opetusorganiaatioiden tietoturvaan kantaaottavia tutkimuksia ovat Tietoyhteiskunnan rakenteet oppilaitoksissa. Vuoden 2004 kartoitusten tulokset ja vuosien 2000 - 2004 yhteenveto [Opetusministeriö, 2005] ja Information Security in Academic Institutions Emerging Issues and Remediation Strategies [Burd et al., 2005]. En löytänyt kuitenkaan yllämainittujen lisäksi tutkimuksia, joissa tutkittaisiin erityisesti opetusorganisaatioiden tietoturvallisuutta ja sen kehittämistä. Tutkimistani tietoturvastandardeista on toki olemassa useita tutkimuksia, esimerkiksi ACM:n tietokannasta löytyy 71 kappaletta BS 7799 standardiin liittyvää tutkimusta [ACM]. Uskon, että Jussi Saarisen pro gradu – tutkielma ”Valtionhallinnon tietoturvaohjeiden soveltuvuus luotaessa pk-yritykselle BS 7799/ISO 19977 -standardin mukaista tietoturvaa” on kaikkein lähinnä omaa tutkimustani [Saarinen, 2006]. En ole tutustunut Saarisen tutkimukseen, joten sisältöön en voi ottaa kantaa. Uskoisin kuitenkin, että pk-yritys ja opetusorganisaatio eroavat toisistaan tietoturva-asioiden hoitamisessa. Voiton tavoittelu ja opetustoiminnan turvaaminen ovat lähtökohdiltaan niin erilaisia tavoitteita, että täysin samankaltaiset tietoturvaratkaisut eivät voi päteä. Lisäksi käyttäjäryhmät ovat näissä kahdessa tapauksessa erilaisia. Molemmissa organisaatioissa on palkattuja työntekijöitä, mutta HAMKissa on lisäksi opiskelijoita.

Tietoturvasta ja sen eri osa alueista on olemassa tietokantahakujeni ja kirjallisuuskartoitukseni perusteella suuri määrä lähdemateriaalia. Suomenkielisen materiaalin määrä ja laatu on myös kasvamaan päin.

Lähdekartoituksen tarkoituksena on löytää oleellisimmat asiat monelta eri näkökannalta katsottuna, standardien näkökulma ei kuitenkaan anna tähän paljoa mahdollisuuksia. Tärkeimpinä lähteinä tutkimukselleni haluan mainita BS7799 standardin molemmat osat [BS 7799-1:fi, 2000][BS 7799-2:fi, 2003], ITILin [ITIL, 2004] ja valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) ohjeet ja määräykset [VAHTI], tietoturvallisuuden hallintaa ja toteuttamista koskevia kirjoja kuten Tietoturvallisuuden johtaminen – näin suojaat yrityksesi toiminnan [Miettinen, 1999] ja esimies ja tietoriskien hallinta [Kyrölä, 2001] sekä HAMKin omat julkaisut, tutkimukset, pohjat ja säännöt sekä Suomen perustuslait ja säädökset ja viranomaisten muut ohjeet. Yliopistojen tietoturvasivuille on koottu yliopistojen yhteistyönä tuottamia tietoturvapoliitikkoja ja käyttösääntöjä [Yliopistojen tietoturvasivusto 2006]. Näitä kokoelmia voidaan hyvin käyttää pohjana luotaessa HAMKille päivitettyjä käyttösääntöjä, sillä niiden käyttö on hyväksytty ammattikorkeakoulujen kesken ARENEn päätöksellä.

2.5 Odotetut tulokset ja niiden merkitys

Uskon, että HAMKista löytyy tietoturvaongelmia ja odotan korjaamisella olevan positiivinen vaikutus organisaation tietoturvan tasoon. Tutkimuksessa syntyvää dokumentaatiota voidaan parhaimmassa tapauksessa käyttää sellaisenaan ohjeina ja käytäntöinä tietoturvalle. Organisaation puolesta Kivelä odottaa tutkimuksen antavan pohjan tietoturvan kehittämiselle kokonaisuutena. Tietoturvan hallintaprosessi ei ole koskaan valmis, vaan sitä pitää ylläpitää, seurata ja kehittää. Tutkimus kertoo arvion kohdeorganisaation tietoturvasta kokonaisuutena ja miten työ on onnistunut minulta. Kaikki tutkimuksessa esille tulleet huomiot dokumentoidaan, jotta saataisiin mahdollisimman suuri hyöty jatkoa ajatellen.

Tutkimustulosten avulla pyritään parantamaan organisaation tietoturvaa ja luomaan tietoturvaa parantavia käytäntöjä ja ohjeistuksia. Yhtenä tutkimustuloksena on myös tulos BS 7799:n ITILin ja VAHTI-ohjeiden soveltumisesta opetusorganisaation tarpeisiin ja vaatimuksiin. Suomessa on paljon opetusorganisaatioita ja tietoturvan huomioiminen on mielenkiintoinen tutkimusaihe.

Tuija Kyrölä on todennut kirjassaan Esimies ja tietoriskien hallinta [Kyrölä, 2001], että 80 % tietoriskien hallinnasta saavutetaan ihmisten toiminnalla. Tällä tutkimuksella voidaan siis osoittaa organisaation ja sen johdon tietoturvatahdon olemassaolo. Tämä tahto pitää myös osoittaa käytännön toimilla tietoturvan parantamiseksi, muuten selvityksellä ei ole mitään hyötyä. Kun organisaation johto ymmärtää tietoturvatyön merkityksen ja ottaa vastuun siitä, voidaan vaatia myös työntekijöitä sitoutumaan siihen. Toivon, että

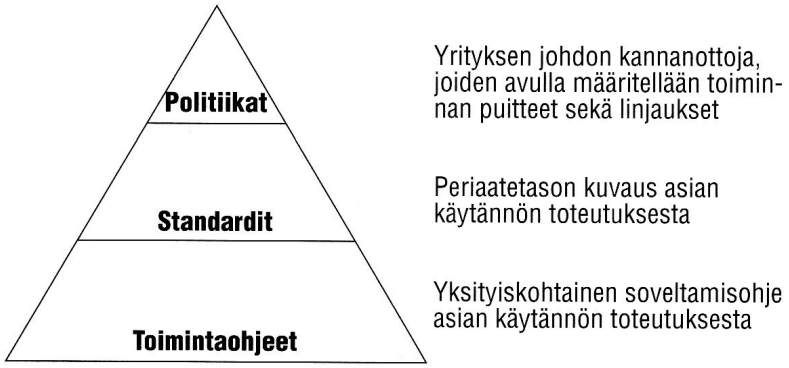
tutkimukseni perusteella organisaation tietoturvaa kehitetään tasolle, jossa sitä kehitetään jatkuvasti kehämallin periaatteella. Käytössä ovat johdon hyväksymät tietoturvapolitiikat, ohjeet ja säännöt ja henkilökunta kokee nämä omaa työtään tukeviksi ja he myös käyttävät näitä työssään.

3 Turvallisuuspolitiikka

ITILin mukaan kaikille erityyppisille organisaatioille koosta välittämättä on elintärkeää olla turvallisuuspolitiikka [ITIL, 2004]. Tämä politiikka sanelee, mitä ollaan suojelemassa ja miksi, sekä kuka suojelee. Tärkeä kysymys on, kuinka paljon halutaan sijoittaa resursseja tavoitellun turvallisuuden hallintaan. Tärkeimmät osa-alueet, jotka jokaisessa organisaatiossa täytyy ottaa huomioon turvallisuusasioissa BS 7799:n mukaan ovat henkilöstö, organisaatio, kirjanpito, raha-asiat, rakennus- ja yleiset asiat (kuten sähkö, tuli, vesi jne.) [BS 7799-1:fi, 2000]. Organisaatiolle tärkeät asiat riippuvat aina sen ominaisuuksista, toimialasta ja vaatimuksista. Yleisen turvallisuuspolitiikan on oltava kunnossa ennen tietoturvapolitiikan luontia, sillä tietoturvapolitiikan on oltava yhteensopiva turvallisuuspolitiikan kanssa. Jos näin ei ole, saattaa näissä kahdessa olla ristiriitaisuuksia ja ne eivät tue toisiaan.

Miettinen kuvaa yritysturvallisuuden keskeiset osa-alueet seuraavasti: yritysturvallisuuden johtaminen, vakuutustoiminta, riskien hallinta, tuotannon ja toiminnan turvallisuus, työsuojelu, pelastustoiminta, poikkeusoloihin varautuminen, henkilöstöturvallisuus, toimitilaturvallisuus, turvallisuus ulkomaan toiminnoissa ja rikosturvallisuus [1999]. Nämä mainitut aihealueet on myös otettu huomioon BS 7799:ssä. Tietoturvallisuus on vain yksi osa-alue, jolla on siis paljon riippuvuuksia muihin yritysturvallisuuden osiin.

Organisaation käyttämä tietoturvaohjeisto ei saa olla hajanainen kokoelma ohjeita, vaan selkeä ja looginen kokonaisuus. Kokonaisuuden saa muodostettua tietoturvallisuuspolitiikoista, -standardeista sekä tietoturvallisuuteen liittyvistä toimintaohjeista [Kuva 4]. Tämän pyramidin kolme kerrosta eivät saa olla ristiriidassa keskenään. Organisaation politiikat kuvaavat, mihin pyritään ja minkälaisia arvoja halutaan toteuttaa. Standardien sisältämien määritelmien avulla voidaan järjestelmällisesti ja tarkasti kuvata, mitä halutaan tehdä. Toimintaohjeilla voidaan kuvata, miten halutut asiat on tehtävä. Näistä kolmesta tasosta käy hyvin ilmi niiden keskinäinen riippuvuus. Jonkin tason puuttuminen tekee kokonaisuuden toimimisen mahdottomaksi. Politiikan puuttuminen merkitsee tavoitteiden ja suunnan puuttumista, standardien puuttuminen järjestelmällisyyden puuttumista ja toteuttamisohjeiden puuttuminen käytännön toteutuksen ongelmia, sillä haluttua toimintaa ei voida viestittää henkilöstölle. Usein kuitenkin unohdetaan käytännön ohjeistus ja koulutus henkilöstölle.



Kuva 4. Yrityksen tietoturvallisuuden tasot [Miettinen, 1999, s. 104]

3.1 Tietoturvallisuus ja tietosuoja

Tietosuoja sisältää tietoturvallisuuden keskeisimmät ulottuvuudet, mutta lisäksi tietosuojaan kuuluu monia asioita, joihin tietoturvallisuus ei ota kantaa. Vastaavasti tietoturvallisuus sisältää lukuisia osatekijöitä, jotka vain välillisesti vaikuttavat tietosuojaan. Tietoturvallisuus ja tietosuoja käsitteinä liittyvät läheisesti toisiinsa, mutta ne eivät ole synonyymeja. Niihin sisältyy samoja asioita ja ne ovat osin päällekkäisiä, mutta molempiin kuuluu myös asioita, jotka eivät sisälly toiseen käsitteeseen [VAHTI CD, 2004]. Käsitän edellä olevan määritelmän niin, että tietoturvallisuuden toimenpiteillä varmistetaan tietosuojan toteutuminen, mutta lisäksi tarvitaan tietosuojan toimintaohjeita ja vaatimuksia, jotka saattavat jo sisältyä tietoturvallisuuteen. Tietosuojaan kuuluvat yksityisasiat, henkilökohtaisen viestinnän- ja henkilötietojen suoja. Kyrölä puhuu yksityisyyden, tietosuojan ja oikeusturvan vaarantumissta, kun ihmisten yksityistietoihin päästään asiattomasti käsiksi [2001, s. 96]. Tutkimalla Kyrölän listaa vaaraa aiheuttavista tilanteista selviää, että tavalliset arkipäivän tilanteet ja huolimattomuus niissä ovat suurimpia riskien aiheuttajia.

3.2 Tietoturvallisuuspolitiikka

Yrityksen tietoturvan kulmakivi on Järvisen mukaan tietoturvapolitiikka [2002]. Tähän politiikkaan on kiteytetty yrityksen tai organisaation tietoturvatyön tavoitteet, vastuut ja asenne. Tietoturvapolitiikka voidaan määritellä salaiseksi, jos se sisältää arkaluonteista tietoa. Käytännön ohjeilla voidaan toteuttaa määritettyä politiikkaa. Tietoturvallisuuspolitiikka sisältää johdon luoman koko organisaatiota koskevan tietoturvallisuuspolitiikan ja sen ylläpidon, tietoturvallisuuspolitiikan määrittelyasiakirjat, tarkastukset ja arvioinnit. Tavoite on määrittää organisaation johdon antama tietoturvallisuutta koskeva ohjaus ja tuki. Käytettäessä ITILin parhaita käytäntöjä oletetaan, että tietoturvallisuuspolitiikka on annettu valmiiksi. ITIL esittää lähtökohdiksi

politiikalle tavoitteeksi olla selkeä suunta tietoturvatyölle ja johdon täytyy osoittaa tukensa tämän saavuttamiseksi.

Yhteenvetona menetelmiksi BS 7799:ssä esitetään luonnollisesti tietoturvapolitiikan kehitys ja implementointi [BS 7799-1:fi, 2000]. Tarvittavat dokumentit on luotava sisältäen tavoitteet ja laajuudet, tietoturvallisuuden merkitys organisaatiolle, yleiset vastuualueet johdolle, työntekijöille ja erityisvastuut, tietoturvahäiriöiden raportointi ja perusperiaatteet liiketoimintaprosessien jatkuvuuden hallinnasta. Riippuvuudet muihin poliitikkoihin (kuten henkilöstöpolitiikka liittyen koulutukseen ja määräaikaisiin tarkastuksiin) ja ulkoisiin vaatimuksiin (lakisääteiset velvoitteet ja sopimukset) on myös selvitettävä. Lisäksi on oltava olemassa turvallisuuspolitiikan vastuuhenkilö, joka vastaa, miten usein on päivityksiä tehtävä ja millä tavoilla.

Tietoturvapolitiikan on oltava kaikkien tietoturvasta vastaavien organisaation työntekijöiden saatavissa. Tarkoituksena on luoda näiden ehtojen perusteella sopiva ja ajan tasalla oleva tietoturvallisuuspolitiikka ja siitä tiivistetyn dokumentin voi luoda Miettisen kirjassa olevan mallin mukaan [1999].

3.3 Tietosuojapolitiikka

Tietosuojalla tarkoitetaan hyvän tietojenkäsittelytavan aikaansaamista henkilötietojen käsittelyssä. Hyvä tietosuojapolitiikan malli on esitelty Stakesin sosiaali- ja terveyshuollon tietoturvaa ja tietosuojaa koskevassa raportissa [Tammisalo, 2005]. Olen liittänyt tämän mallin tutkimuksen liitteeksi, sillä sitä voi hyödyntää kun nykyistä HAMKin tietosuojapolitiikkaa päivitetään.

Tietosuoja toteutuu, kun

- henkilötietoja käsitellään vain säädetyin edellytyksin
- henkilötietoja käytetään vain ennalta määriteltyyn tarkoitukseen
- tietojen tarpeellisuus ja virheettömyys varmistetaan
- tietojen suojaamisesta huolehditaan kaikissa käsittelyvaiheissa,
- henkilötietojen käsittelyyn liittyvistä rekisteröityjen oikeuksista huolehditaan
- henkilörekisteristä laadittu rekisteriseloste on kaikkien saatavilla

[Vahti CD, 2004]

3.4 Tietoturvastandardit

Organisaatiossa käytettävien tietoturvapolitiikkojen ja toimintaohjeiden välissä ovat tietoturvallisuusstandardit. Niissä on kuvauksia ja toimintamalleja siitä, miten organisaatio voi toteuttaa suojauksensa. Yleensä tietoturvastandardit sisältävät tarkkoja kuvauksia suojauksien toteutuksesta, jolloin niiden

valmistelu, ylläpito ja päivittäminen ovat eri alojen teknisten asiantuntijoiden vastuulla. Standardit voivat olla teknisiä tai ei-teknisiä Miettisen mukaan [1999]. Tutkimuksessa käytettävä tietoturvastandardi BS 7799 on tekninen standardi ja ITIL edustaa ei-teknistä mallia, jossa keskitytään tietoturvan huomioimiseen organisaation toimintaprosessien suojauksia luotaessa.

3.5 Tietoturvallisuuden toimintaohjeet

Toimintaohjeet koskevat jokapäiväistä työtä ja jokaista organisaation palveluksessa olevaa. Toimintaohjeita voidaan päivittää tarvittaessa ja nopeasti. Toimintaohjeita ovat esimerkiksi toiminta haittaohjelmia havaittaessa, etätyön vaatimukset ja palosuojelu. Toimintaohjeiden on oltava selkeitä ja helposti saatavilla ja ne vaikuttavat vasta kun ne on koulutettu henkilöstölle. Ohjeita on syytä testata käytännössä, jotta voidaan vakuuttua niiden toimivuudesta. VAHTI-ohjeet sisältävät paljon suosituksia ja menettelyohjeita.

3.6 Riskien hallinta ja riskikartoitukset

Tietoturvariskien hallinta on osa organisaation yleistä riskienhallintaa. Hallinta edellyttää aktiivista yhteistyötä tietoturvallisuuden ja muiden riskien hallinnan asiantuntijoiden välillä. Palvelun tai toiminnon hyöty on kyseenalainen, jos sen riskejä ei aktiivisesti hallita. Ennen tietoturvapolitiikan luomista on suoritettava riskikartoituksia, jotta tiedetään, mitä vastaan joudutaan ja halutaan suojautua. Tämä alue on käsitelty tarkemmin luvussa 5. Riskikartoituksen tulee olla mukana palveluiden ja toimintojen suunnittelusta lähtien. Sisäisen tarkastuksen tulee valvoa kriittisten järjestelmien riskienhallintaa. Riskikartoitusten avulla organisaatio muodostaa kuvan tietoturvallisuutensa nykytasosta. Tavoitteena on löytää uhkatekijät sekä arvioida uhkien todennäköisyys ja niiden seurausten vakavuus. Kartoituksia on tarpeen tehdä säännöllisesti ja monella tasolla: koko organisaatio, osastot tai muut yksiköt, toimintaprosessit, erilaiset tietojärjestelmät, palvelimet tai muut laitteistokokonaisuudet [VAHTI 3/2005].

Standardi tarjoaa mallin tietoturvallisuuden hallintajärjestelmän rakentamiseen ja hallintaan. Standardin mukaan organisaation turvallisuusvaatimusten tunnistamisessa ensimmäinen lähde on riskianalyysi, jonka avulla tunnistetaan suojattaviin kohteisiin kohdistuvat uhat sekä arvioidaan alttius vahingoille, vahingon todennäköisyys ja vahingon mahdolliset vaikutukset. Luotaessa standardin kuten BS 7799 mukaista tietoturvallisuuden hallintajärjestelmää organisaation tulee määritellä hallintajärjestelmän kattavuus ja systemaattinen riskien arvioinnin menettelytapa, tunnistaa ja arvioida riskit, tunnistaa ja arvioida riskien käsittelyn vaihtoehdot, valita valvontatavoitteet ja turvamekanismit riskien

käsittelyyn sekä valmistella soveltamissuunnitelma, tässä tutkimuksessa puhun tietoturvasuunnitelmasta [VAHTI 7/2003].

3.7 Tietoturvasuunnitelma

Organisaation tietoturvasuunnitelman on pohjauduttava riskikartoituksiin ja tietoturvapolitiikkaan. Tämän tutkimuksen on tarkoitus olla pohjana HAMKin tietoturvasuunnitelmalle. Tietoturvasuunnitelmat ja jotkin osat tietoturvaohjeistuksista eivät ole julkisia tietoja, joten suunnitelmien tekemisessä, säilyttämisessä ja jakelussa on syytä noudattaa huolellisuutta.

3.8 HAMKin tietoturvapolitiikka

Tässä käydään läpi tämän hetkinen käytössä oleva tietoturvapolitiikka ja päivitetään sitä ajan tasalle. Hämeen Ammatillisen Korkeakoulutuksen Kuntayhtymän Tietoturvapolitiikka nykyinen versio on päivätty 29.8.2003 [Liite 8]. Korjattu tietoturvapolitiikka tulee hyväksyttää HAMKin johdolla, jotta siitä tulisi virallinen ja se voitaisiin ottaa käyttöön

HAMKin tietoturvapolitiikka sisältää tarvittavat asiat ja ongelma ei ole niinkään sisällössä ja sen laajuudessa vaan siinä, miten määritetyt asiat on toteutettu käytännössä. Tietoturvapolitiikan tulisi olla toteutettuna, pelkkä dokumentti on itsessään arvoton, sillä siinä on vain kirjattu organisaation arvot, vastuut ja tehtävät tietoturvan kannalta.

Käytännössä on selvinnyt, että kaikki työntekijät eivät oikein tunne vastuutansa tietoturva-asioissa. Tietoturvallisuuden seuranta ja ongelmatilanteiden käsittely on myös vaihtelevaa. Tietoturvapolitiikan pohjalta ei ole laadittu kuntayhtymän tietoturvaa koskevia suunnitelmia ja käyttösäännöstöjä valmiiksi asti, henkilökunnan saatavissa ei ole sekä www-palvelun kautta, eikä kirjallisessa muodossa heidän toimissaan tarvitsemansa tietoturvallisuusohjeita. Opiskelijoille ei ole tiedotettu tietoturvallisuudesta ja heitä koskevista säännöistä ja suosituksista tarpeeksi. Kuntayhtymän jäsenten tietoturvallisuustietoisuutta ei ole juurikaan lisätty eri tavoin tiedottamalla ja koulutustilaisuuksia järjestämällä. Kuntayhtymän tietojenkäsittelyn ja tietojärjestelmien tietoturvallisuuden tasoa ei ole arvioitu sisäisen tarkastuksen keinoin tai tarvittaessa myös ulkoista tarkastusta käyttäen. Tietoturvallisuustason määrittämiseksi kuntayhtymän tietoaineistoja ja tietojärjestelmiä ei ole luokiteltu.

Uudistetun tietoturvapolitiikan mallina voi käyttää Yliopistojen U-CIRT – työryhmän Tietoturvapolitiikka -dokumenttipohjaa [Yliopistojen U-CIRT, 2005]. Dokumentti sisältää tietoturvapolitiikan tavoitteet, organisoinnin ja vastuut, toteutuskeinot, tiedottamisen, tietoturvallisuuden seurannan ja ongelmatilanteiden käsittelyn ja tarvittavat liitteet. Riskien hallinta ja riskikartoitukset käsitellään tässä tutkimuksessa omassa luvussaan.

4 Tietoturvallisuus

Vahva tietoturvallisuus ei synny itsestään. Sen luomiseksi organisaatioon on luotava hallintarakenne, joka tekee aloitteita ja hallitsee turvallisuutta. Käytettävissä on useita erialaisia ratkaisuja. BS 7799 -standardin mukaisen hallintarakenteen on tarkoitus valmistella, hyväksyä ja implementoida tietoturvapolitiikka, jakaa vastuut ja käytännössä implementoida turvatoimet sekä luoda tarvittavat työpaikat tietoturva-asiantuntijoille [BS 7799-1:fi, 2000]. VAHTI-ohjeissa sama asia ilmaistaan viitekehyksenä, jossa johtamis- ja hallintajärjestelmä on muokattu organisaation toimintastrategian mukaiseksi ottamalla huomioon tietoturvan nykyinen kehitysvaihe ja juuri organisaatiota koskevat tietoturvariskit [VAHTI, 6/2006]. ITILin tavoitteena on tietoturvallisuuden hallinnan varmistaminen, eikä siinä esitetä varsinaisen hallintajärjestelmän rakennetta tai ohjetta [ITIL, 2004]. Kuten VAHTI-ohjeissa todetaan, standardeja voidaan käyttää apuna tietoturvan hallinnassa, vaikka ei aktiivisesti pyritä sertifioimaan niiden mukaista tietoturvaa. Tietoturvastandardit sisältävät tutkittuja ja hyväksi koettuja menetelmiä tietoturvan hallitsemiseen ja niiden seuraaminen ja toteuttaminen parantavat organisaation tietoturvaa.

4.1 Tietoturvallisuuden hallintajärjestelmät ja niiden kehittäminen

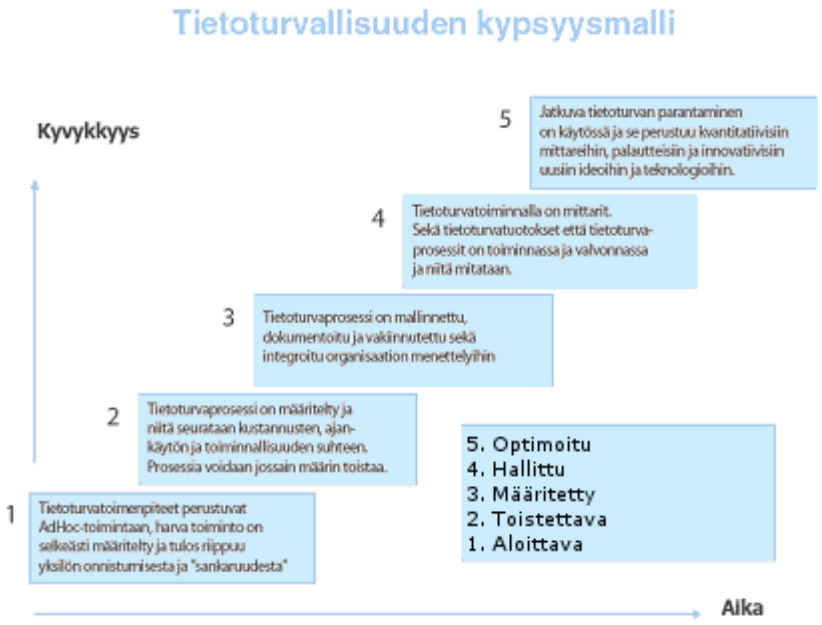
BS 7799:ssä esitettyjä hallintajärjestelmän toteutusmenetelmiä ovat tietoturvallisuuden hallinnollisen foorumin perustaminen, jossa ajoittain tietoturvan vastuuhenkilöt kokoontuvat ja keskustelevat tietoturvan suunnasta, tietoturvapolitiikkojen ja turvamenetelmien muutoksista, hyväksyvät suunnitelmia ylläpitävät vastuita ja seuraavat muuttuvia uhkia ja tilanteita. Tietoturvallisuuden koordinoinnilla tarkoitetaan suunnitelmien ja menetelmien käyttöä. Koordinoinnilla erilaiset roolit ja niiden väliset vastuut määritetään tietoturvallisuuden kannalta. Johdon vaikutusvaltaa ja vastuuta korostavat myös Miettinen [1999, s. 98] kirjoittamalla tietoturvallisuuden johtamisesta ja johtamisjärjestelmistä ja Kyrölä tietoriskien hallinnan ja turvallisuuden johtoryhmästä [2001, s. 142]. Organisoinnin tueksi voidaan hyväksyä esimerkiksi koulutusohjelma tietoturvallisuustietoisuuden nostamiseksi, riskianalyysien teko ja saman luokittelujärjestelmän käyttö koko organisaatiossa [BS 7799-1:fi, 2000].

Tietoturvallisuusvastuiden jakamiseen kuuluvat selkeästi määritellyt vastuut. Tiedon suojaamiseen, tietojärjestelmien ja turvamenetelmien implementointiin tarvitaan vastuuhenkilöitä. Tietotekniikkatilojen turvallisuus täytyy tarkastaa ja testata ennen käyttöönottoa. Asiantuntija-avun käyttämistä suositellaan erikoistilanteiden ja riskien selvittämisessä, varsinkin jos osaavaa henkilöstöä ei ole omassa organisaatiossa ollenkaan saatavilla.

Organisaatioiden välinen yhteistyö ja tiedonvälitys uusista suojakeinoista ja uhkista on hyvä käytäntö. Tietoturvallisuuden tason riippumaton arviointi on suoritettava säännöllisesti sisäisen tai ulkoisen auditoijan tekemänä. Kolmansien osapuolten pääsyn riskit on tunnistettava ja kolmansien osapuolten kanssa tehtävien sopimuksien on sisällettävä turvallisuusehtoja.

VAHTI-ohjeiden mukainen tietoturvallisuuden hallintajärjestelmä sisältää aiemmin mainitun organisaatiokohtaisen toimintastrategian lisäksi laajan riskienhallinnan [VAHTI, 6/2006]. Asetettuja tavoitteita tuetaan ja epävarmuustekijöitä pyritään hallitsemaan tehokkaasti ja systemaattisesti. VAHTI-ohjeiden mukainen tietoturvallisuudenhallintajärjestelmä koostuu tietoturvariskien hallintasuunnitelmaan sisältyvistä toimintamalleista ja dokumenteista. Nämä sisältävät tietoturvapolitiikan ja – strategian, tietoturvallisuuden kehittämissuunnitelman, voimassaolevien tietoturvakäytäntöjen tietoturvasuunnitelma, tietoturvallisuuden perusohjeistus ja lisäohjeistus, tietoturva-arkkitehtuurit (topologia- ja periaateratkaisujen kuvaukset), tietoturvaraportointi johdolle, jatkuvuussuunnitelmat, poikkeusolojen tietojenkäsittelyn valmiussuunnitelmat, toimintaan liittyvät tietoturvaprosessit ja auditointisuunnitelma. Nämä osa-alueet ovat erittäin selkeitä verrattuna BS 7799 standardin vastaaviin. VAHTI-ohjeiden vahvuus onkin niiden antamat ohjeet, miten käytännössä järjestelmiä ja prosesseja voidaan luoda ja ylläpitää.

Tietoturvallisuuden hallitsemiseen tarvitaan siis jokin järjestelmä, jolla tietoturva-asiat pysyvät hallinnassa. Tällainen järjestelmä ei voi olla täydellinen ja muuttumaton. Ihmiset voivat erehtyä ja laitteisiin voi tulla vikoja, tekniikan kehitys ja toimintaympäristön muutokset luovat uusia riskejä tietoturvallisuudelle. Jostain on kuitenkin aloitettava ja kehitys alkaa luonnollisesti perusasioista. VAHTI-ohjeissa käytetään termejä hallintojärjestelmän kypsyysaste ja evoluutioprosessi [VAHTI, 6/2006]. Kuvassa 5 esitetystä prosessien kypsyysarviointimallista (CMM) ovat nähtävissä eri kehitysasteet. Askeleelta seuraavalle siirtyminen vie aikaa, sillä nykyinen taso on hallittava ensin perusteellisesti. Kehitysprosessin alku on varmasti vaikeaa, sillä ensimmäisellä tasolla olevilla organisaatioilla ei välttämättä ole minkäänlaista tietoturvaan liittyvää hallintajärjestelmää. Kehitysprosessi tulee jatkumaan vaikka tietty kehitysvaihe olisi saavutettu, sillä nykyisen aseman ylläpitäminen vaatii resursseja. Tietoturvakehitys voi helposti taantua, jos sitä ei ylläpidetä riittävästi. Organisaatiolla tulee olla tavoitteita tietoturvan suhteen ja nämä tavoitteet on liitettävä tulosohjaukseen.



Kuva 5. Tietoturvallisuuden kypsyysmalli (CMM) [VAHTI, 6/2006, s. 19]

4.2 Tietoturvallisuuden tavoitteet ja tulosohjaus

Tietoturvallisuuden parantamiseksi organisaatiossa on oltava selkeitä tavoitteita. Näiden tavoitteiden täytyy olla sellaisia, että niihin kannattaa ja on mahdollista pyrkiä. Organisaation johdon on siis luotava tietoturvatavoitteita, jotka tukevat organisaation toimintaprosesseja ja tärkeimpiä palveluja. Esimerkiksi HAMKin tärkein toiminto on opetustoiminnan tuottaminen. Tulosohjauksella otetaan vastuu siitä, että tietoturva-asiat sidotaan organisaation tuloksiin ja talouteen. Tavoitteena on tasapaino resurssien ja niillä saavutettavien tulosten välille.

Tietoturvallisuuteen panostamalla täytyy organisaation kokonaistoiminnan muuttua turvallisemmaksi ja uhkien ja riskien todennäköisyydet ja vaikutukset pienentyä. Tietoturvatyöhön kulutettuja varoja ja niiden vaikutuksia on voitava mitata ja selvittää miten asetettuihin tavoitteisiin on päästy. Organisaation tietoturvapolitiikassa on hyvä määrittää mitä tavoitteet ovat, jotta ne voidaan välittää kaikille organisaatiossa työskenteleville. VAHTI-ohjeissa on tiivistetty vuositavoitteet tietoturvallisuuden kehittämiseen sekä tavoiteltavaan ja mitattavissa olevaan tietoturvatasoon [VAHTI, 2006].

Tietoturvatyötä ja sen vaatimia kustannuksia ja menoja on budjetoitava huolellisesti. Tietoturvamenoja voidaan jakaa muuttuviin ja kiinteisiin menoihin sekä riskivarauksiin [VAHTI, 2006]. Kustannukset eivät saa ylittää niistä saatavaa hyötyä, vaikeutena tässä on kuitenkin sellaisten asioiden arvottaminen, joita ei voi mitata rahassa. Tällaisia ovat varsinkin henkilötiedot..Kiinteitä menoja ovat esimerkiksi ihmisten palkat ja ylläpitokulut

laitteistoille. Muuttuvia menoja ovat kehittämiskulut, kuten hankinnat. Riskien toteutumisen varalle tehtäviä varauksia ovat esimerkiksi erilaiset vahinkovakuutukset ja varalaitteistot.

4.3 Tietoturvallisuuden seuranta ja raportointi

VAHTI-ohjeissa kerrotaan asetettujen tavoitteiden, toiminnan laadun ja kustannuksien olevan tärkeimpiä seurantakohteita tulosohjaukselle [VAHTI, 6/2006]. Tulosohjauksessa käytetään apuna erilaisia laadullisia ja määrällisiä mittareita. Mittauksen kohde määrittää miten sitä voidaan mitata, ominaisuuksia voi arvioida matemaattisesti tai arvioida laadullisesti. Nämä mittaukset ja arvioinnit antavat mahdollisuuden tehdä perusteltuja ohjauspäätöksiä. Ohjauspäätöksillä hallitaan ja ohjataan tietoturvaa ja sen kehitystä paremmiksi. VAHTI-ohjeissa ohjeissa jaetaan organisaation johdolle tehtävä raportointi kahteen osaan, tietoturvatoimintaa kuvaaviin raportteihin ja normatiiviseen käytäntöön. Ensimmäisessä osassa ovat organisaatioille sopiviksi muokatut kausiraportit ja häiriöiden poikkeamisraportit. Organisaation omat tarpeet määrittävät siis minkälaisia raportteja tarvitaan. Toisessa osassa ovat sääntöjen ja määräysten mukainen raportointi organisaation johdolle riskienhallinnan asianmukaisuudesta ja riittävyydestä toimintakertomusta varten.

Muita VAHTI-ohjeissa esitettyjä tietoturvan raportointia tukevia menetelmiä ovat tietoturvatilan selvitykset, tarkastukset, auditoinnit ja arvioinnit. Raportoinnin tulee olla VAHTI-ohjeiden mukaan jatkuvaa. Raporttien sisältö ja laatu ovat tärkeitä, mutta on seurattava myös itse raportointimenettelyitä, jotta raportteja tuotetaan riittävän usein ja yhdenmukaisilla tavoilla. Tällaisia raportteja tuskin voidaan tehdä koskaan liikaa, sillä mahdollisimman ajan tasalla oleva raportointi parantaa tietoturvallisuuden hallintamahdollisuuksia kun muutoksiin voidaan reagoida mahdollisimman nopeasti. Pikemminkin niitä tehdään liian vähän kuten HAMKin tapauksessa. VAHTI-ohjeissa tarjotaan hyviä esimerkkejä raportointien tekoon [VAHTI, 6/2006].

4.4 Tietoturvallisuuden ja -toiminnan mittaus- ja arviointimenetelmät ja niiden tavoitteet

VAHTI-ohjeissa kuvataan arviointien kuuluvan oleellisesti tietoturvallisuuden hallintajärjestelmän toimintamalliin. Näitä voidaan käyttää myös mittareina. [VAHTI, 6/2006]. Tällaisen mittarin tärkein ominaisuus on kertoa luotettavasti juuri haluttu suure tietystä kohteesta. Laadulliset mittarit ovat arvioita ja raportoidut tapahtumat ja määrälliset mittarit systemaattisia mittausmenetelmiä. Arviointien hyöty perustuu niiden jatkuvaan tekemiseen ja

tulosten analysointiin. Vertaamalla tuloksia tavoitteisiin voidaan kehittää omaa tietoturvaa ja löytää heikkouksia ja vahvuuksia. VAHTI-ohjeissa kuvataan muutamia arviointityyppejä, jotka eivät ole toisiaan poissulkevia.
Itsearvionti on systemaattinen kehittämismenetelmä. Itsearvionnissa verrataan tasaisin väliajoin ja systemaattisesti organisaation toimintoja ja tuloksia johonkin malliin, kuten esimerkiksi EFQM-arviointimalliin [EFQM]. Holistisen mallin, kuten EFQM, käytöllä voidaan mitata miten pitkällä organisaatio on matkalla erinomaisuuteen, mitä ongelmia sen saavuttamiselle on ja millaisia ratkaisuja täytyy tehdä ongelmien voittamiseksi. Itsearvionti voi perustua VAHTI-ohjeisiin tai ISO 17799 / BS 7799 -standardiin tai muuhun sopivaan menetelmään.

Ulkoisessa arvioinnissa hyödynnetään ulkopuolista ja puolueetonta osapuolta tietoturvan arvioinnissa. Ulkoisen osapuolen tekemänä arviointiin on vaikeampi vaikuttaa organisaation sisältä. Kokeneita ja ammattitaitoisia ulkoiseen arviointiin erikoistuneita yrityksiä käyttämällä voidaan suorittaa arviointi, jos organisaation sisällä ei ole siihen mahdollisuuksia.

Benchmarking on oman organisaation vertaamista sopiviin esikuviin eli sellaisiin organisaatioihin, jotka ovat edelläkävijöitä tietoturvassa. Näillä esikuvilla on käytössään toimivia menetelmiä tietoturvan hoitoon. Tällaisten esikuvien on hyvä olla samalla sektorilla ja toimialalla kuin vertailua käyttävä organisaatio. Vertailua käyttävän organisaation on mietittävä, miten muiden organisaatioiden hyviä käytäntöjä voidaan soveltaa heille itselleen ja mitä muutoksia tarvitaan.

Laadullinen mittaaminen on toiminnan onnistumisen mittaamista. Toiminnoille tai asioiden tiloille voidaan antaa sanallisia määreitä, esimerkiksi kuinka usein tai kuinka tarkasti jokin asia suoritetaan tai millainen on eri osastojen asenne tietoturvaan.

Määrällinen mittaaminen on sellaisten arvojen mittaamista, joiden arvo voi vaihdella. Mittauksessa mitataan yksiköitä, esimerkiksi työaikaa, kustannuksia tai tietoturvapoikkeuksien lukumäärää.

Tietoturvatoiminnan tuloksellisuuden arviointi ja mittaus on VAHTI-ohjeiden mukaan mahdollista, kun käytetään asetettujen tavoitteiden ja toiminnan tilan seurantaa koskevia mittareita. Tietoturvallisuuden hallintajärjestelmän kehitysvaihe määrittää millaisia tavoitteita tietoturvallisuustyölle on asetettu [VAHTI, 6/2006]. Kehitysvaiheet on esitetty kuvassa 6. Kuvasta nähdään, että VAHTI-ohjeita voidaan hyödyntää useassa kehitysvaiheessa, mutta esimerkiksi jonkin tietoturvastandardin kuten BS 7799:n implementointiin kannattaa ryhtyä vasta kun on saavutettu hallittu kehitysvaihe tietoturvallisuuden kehitystyössä.

Tietoturvallisuuden kehitystyön kypsyysvaihe ja niihin soveltuvat arviointimenetelmät				
1. Aloittava	2. Toistettava	3. Määritelty	4. Hallittu	5. Optimoituva
Riskienhallinta COSO-ERM malli[3] (ks liite, lähde 11) Ohje riskien arvioinnista tietoturvallisuuden kehittämiseksi valtionhallinnossa. VAHTI 7/2003.	Arvioinnit tietoturvallisuuden osa-alueittain, esim. Valtion keskeisten tietojärjestelmien turvaaminen. VAHTI 5/2004.	Hallintajärjestelmä dokumentoitu. Tietoturvallisuuden hallintajärjestelmän-arviointisuositus. VAHTI 3/2003.	Toiminalle on asetettu tulosmittarit ja tietoturvastandardeja sovelletaan vakiintuneesti.	Toiminnanjatkuva sisäinen ja ulkoinen arviointi ja mittaaminen. Benchmarking.
Ohje tietoturvallisuuden arvioinnista valtionhallinnossa. VAHTI ohje, 2006.				
Muutos ja tietoturvallisuus. VAHTI -ohje, 2006.				

Kuva 6. Tietoturvallisuuden arviointi eri kypsyysvaiheissa [VAHTI, 6/2006, s. 33]

Mittausprosessi on siis olennainen osa tietoturvallisuuden hallintaprosessia. VAHTI-ohjeissa todetaan prosessimuotoisen ja kehittyvän mittauksen parantavan tietoturvallisuutta. Sitä mitä ei voi mitata, ei voi tuntea ja mitä ei tunneta, ei voida hallita.

Toiminnan ohjaus jaetaan omistajaohjaukseen, organisaation johtoon ja tietoturvallisuuden toiminnan johtoon. Eri tasoilla mitataan onnistumista ja tavoitteiden toteutumista eri tavoilla. Luonnollisesti eri tasoilla tarvitaan erilaisia mittareita. Ylemmän tason mittarit ovat strategisia ja niitä on vähän, operatiivisen tasolla niitä on enemmän ja ne ovat tarkempia. On syytä muistaa, että tasoja on sitä vähemmän, mitä nuorempi organisaation tietoturvakehitys on. Toisaalta liian suuri tasojen määrä voi hidastaa tiedon kulkua.

Tulosohjauksen kannalta merkittävät tietoturvallisuuden arviointikohteet ovat [VAHTI, 6/2006]:

- Toteutuvatko toiminnan riskien hallintaan liittyvät tietoturvatavoitteet?
- Mikä on tietoturvallisuuden nykytaso suhteessa asetettuun tavoitetasoon, ja mitkä ovat edellytykset tietoturvatavoitteiden toteuttamiseen (osaaminen, resurssit)?
- Mikä on tietoturvallisuuden hallintajärjestelmän kehittyneisyys ja laatu?
- Mitä tietoturvariskejä on tunnistettu ja miten tunnistettuja riskejä hallitaan?
- Onko verkko- ja järjestelmätason tietoturvaratkaisujen (tietoturva-arkkitehtuuri) tavoitetila määritelty ja toteutettu?
- Miten eri aikaväleille asetetut tavoitteet ovat toteutuneet?
- Seurataanko tietoturvatoiminnan kustannuksia ja tehdäänkö ohjauspäätöksiä niiden perusteella?
- Onko säädösperusteinen tietoturvataso toteutunut?

4.5 Tietoturvatoiminnan mittarit

VAHTI-ohjeissa on listattu Väestörekisterikeskuksen ja Poliisin käyttämiä tietoturvatason mittareita [VAHTI, 6/2006]. Alla olevasta luettelosta huomataan, että mitattavia kohteita ja mittareita on paljon. On siis valikoitava ne mittarit, jotka parhaiten kertovat haluttuja tuloksia. Ei ole mielekästä ylläpitää suurta määrää mittareita, jos mittaustuloksia ei tehdä tarpeeksi usein ja tarkasti. Valittuja mittareita on käytettävä tehokkaasti ja niiden tuottamia tuloksia on seurattava ja tehtävä ohjauspäätöksiä niiden perusteella. Toisaalta mitä enemmän mittareita käytetään, sitä enemmän saadaan tietoa organisaation tietoturvatasosta, toisaalta mitä vähemmän mittareita on, sitä enemmän niihin jokaiseen voi keskittyä. Ihannetapauksessa resursseja on niin paljon käytössä, että kaikki halutut ja tarvittavat mittarit voidaan toteuttaa ja seurata niitä aktiivisesti.

Tapahtuneet tietoturvapoikkeamat. Tavoitteena on seurata ja mitata toiminnalle aiheutuvaa haittaa ja hankkia tietoa tietoturvatoimenpiteiden suunnittelua varten.

- Ilmoitetut/tietoon tulleet toimenpiteitä vaatineiden tietoturvatapahtumien lukumäärä
- Vahinkojen määrä (esim. sähköposti- ja tietoliikennepalvelujen ja muiden toiminnalle)
- Kriittisten järjestelmien keskeytysten pituudet ja lukumäärä
- Virus- ja muut haittaohjelmavahingot ja torjuntaprosentti
- Tietoverkon poikkeukselliset kuormitustilanteet
- Raportoitujen tietoturvarikkomusten luonne ja määrä
- Varkauksien lukumäärä.

Tietoturvapoikkeamien hallinta. Tavoitteena on seurata toteutettujen tietoturvatoimenpiteiden tehokkuutta.

- Havaitut virus- ja muut haittaohjelmat
- Havaitut (esim. palomuuriin pysähtyvät) tunkeutumisyritykset
- Havaitut palveluksen estohyökkäykset
- Roskapostitilanne
- Toteutetut torjuntaohjelmien päivitykset
- Toteutetut tietoturvapäivitykset
- Tietoliikenneyhteyksien kapasiteetti ja käytettävyys
- Epäonnistuneiden tunkeutumisyritysten lukumäärä järjestelmiin.

Tietoturvatoimintaa kuvaavia mittareita. Tavoitteena on arvioida tietoturvatoiminnan tehokkuutta seuraamalla suoritteita ja käytettyjä panoksia.

- Tietoturvatoiminnan kustannukset (kehittäminen, operatiivinen toiminta, investoinnit)
- Tietoturvallisuustyön työtunnit tai henkilötyöpäivät
- Tietoturvaryhmän kokousten lukumäärä
- Tietoturvakoulutuksen koulutuspäivien ja/tai opetustuntien määrä, osallistujalukumäärä
- Henkilöstölle suunnattujen tiedotteiden lukumäärä
- Tietoturvasopimusten lukumäärä ja luonne
- Tietoturvakatselmointien lukumäärä kohteittain
- Tietojärjestelmien tietoturvasuunnitelmat (toipumissuunnitelmat)
- Henkilöstöturvallisuus
- Käyttöoikeudet
- Tietoaineistot (suojaus, varmistukset, laatu)
- Operaattorin palvelut Tietoturvariskien hallinta...
- Toimitilat
- Tietoliikenne ja verkot
- Laitteet
- Määriteltyjen prosessien mukainen toiminta
- Suunnitelmat ja ohjeet ml. jatkuvuus- ja valmiussuunnitelmat
- Vastuut, delegoinnit
- Tietoturvasopimukset
- Riskikartoituksen ajantasaisuus

4.6 BS 7799, ITIL VAHTI ja prosessimaiset toimintamallit

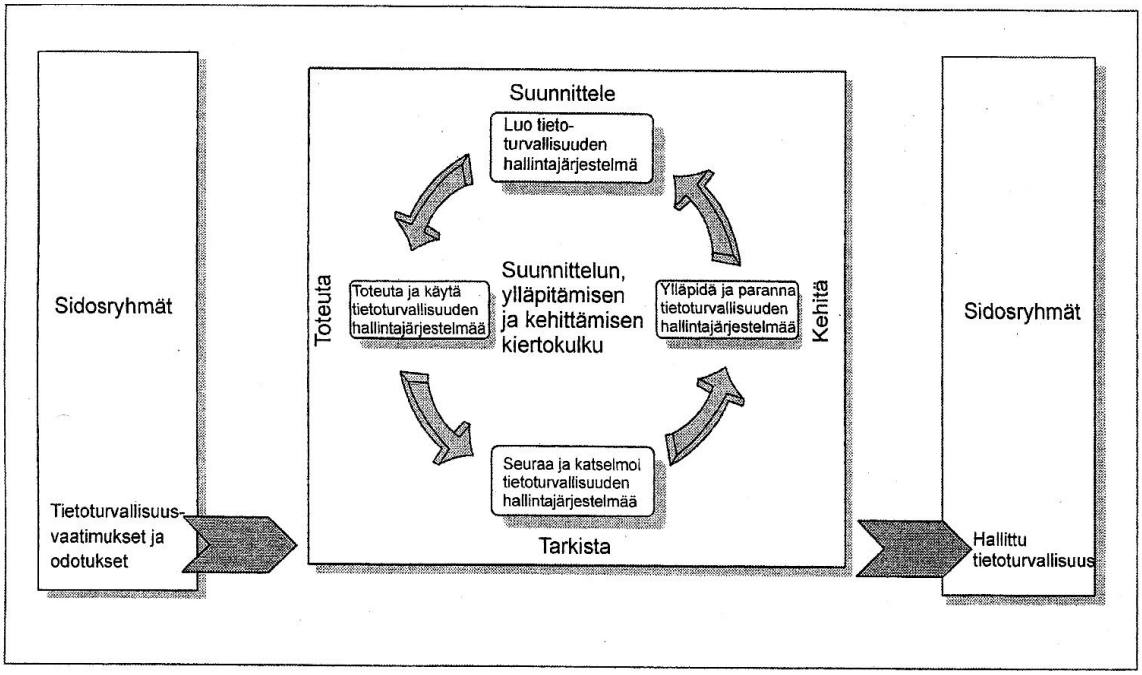
BS 7799:2 sovellusohjeen mukaan organisaation tulee tunnistaa ja johtaa monia toimintoja toimiakseen vaikuttavasti. Prosessiksi voidaan kutsua toimintaa, jossa käytetään resursseja ja jota johdetaan siten, että panokset muutetaan tuotoksi. Usein yhden prosessin tuotos on suoraan panos toiselle prosessille. Prosessimaiset toimintamallit ovat johtamista, jossa prosessijärjestelmiä sovelletaan organisaatiossa, prosessien ja niiden vuorovaikutusten tunnistamista ja prosessien johtamista [BS 7799:2].

BS 7799:2 korostaa, että prosessimaisen toimintamallin käytöllä painotetaan seuraavien asioiden tärkeyttä: liiketoimintavaatimusten ymmärtäminen ja tietoturvallisuuspolitiikan ja tietoturvallisuustavoitteiden määrittäminen, valvontamekanismien luominen ja käyttö organisaation yleisten toimintariskien hallintaan, tietoturvallisuuden hallintajärjestelmän valvonta ja sen suorituskyvyn ja vaikuttavuuden katselmointi ja objektiiviseen mittaamiseen perustuva jatkuva parantaminen.

ITILissä ja BS 7799:ssa käytetään avoimen kehän periaatetta, jossa prosessia kehitetään ja seurataan ja siihen vaikutetaan ulkopuolelta ja se myös vaikuttaa

ulkopuolelle. Turvallisuustietoisuus, vastuullisuus, vastatoimet, riskien arviointi, turvallisuuden suunnittelu ja toimeenpano, turvallisuuden hallinta ja uudelleenarviointi ovat mallien osa-alueita. Näiden prosessikehien pyörimisen voima tulee syötteistä ja palautteesta, ilman niitä sitä ei voi hallita tehokkaasti. Prosessin hallinnalla voidaan tarkkailla eri vaiheita ohjata prosessia haluttuun suuntaan.

BS 7799:n soveltamisessa tarvittava PDCA-malli koostuu suunnittelusta, jossa luodaan tietoturvallisuuden hallintajärjestelmä. Seuraava vaihe on toteuttaminen, jossa toteutetaan ja käytetään luotua hallintajärjestelmää. Tarkistamisvaiheessa seurataan ja katselmoidaan tietoturvallisuuden hallintajärjestelmää. Viimeinen vaihe on kehittäminen, jossa ylläpidetään ja parannetaan tätä tietoturvallisuuden kehittämisjärjestelmää. Sidosryhmät antavat ja ottavat vastaan syötteitä [Kuva 7].



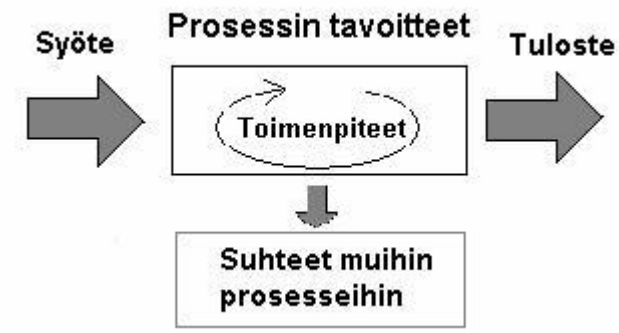
Kuva 7. PDCA-malli sovellettuna tietoturvallisuuden hallintajärjestelmän prosesseihin [BS 7799-2:fi, 2003, s. 10].

Käsiteltävä ITIL Security Management [ITIL, 2004] on vain yksi prosessi ITILin yhdeksästä prosessista. ITILin käsittelemät prosessit suoritetaan osana it:n hallintaa. ITIL keskittyy hallinnan parhaisiin käytäntöihin ja tietotekniikkainfrastruktuurin hyödyntämiseen. ITIL on luotu käytännön kokemusten myötä ja tämä tekee siitä tehokkaan. Kokemus on myös osoittanut ITILin käytön parantavan tietotekniikkapalveluiden laatua.

ITILin vahvuuksia ovat keskittyminen olemassa olevaan työympäristöön, sen hallintaan ja muutosten toteuttamiseen. ITILin esittelemiä menetelmiä ei voi

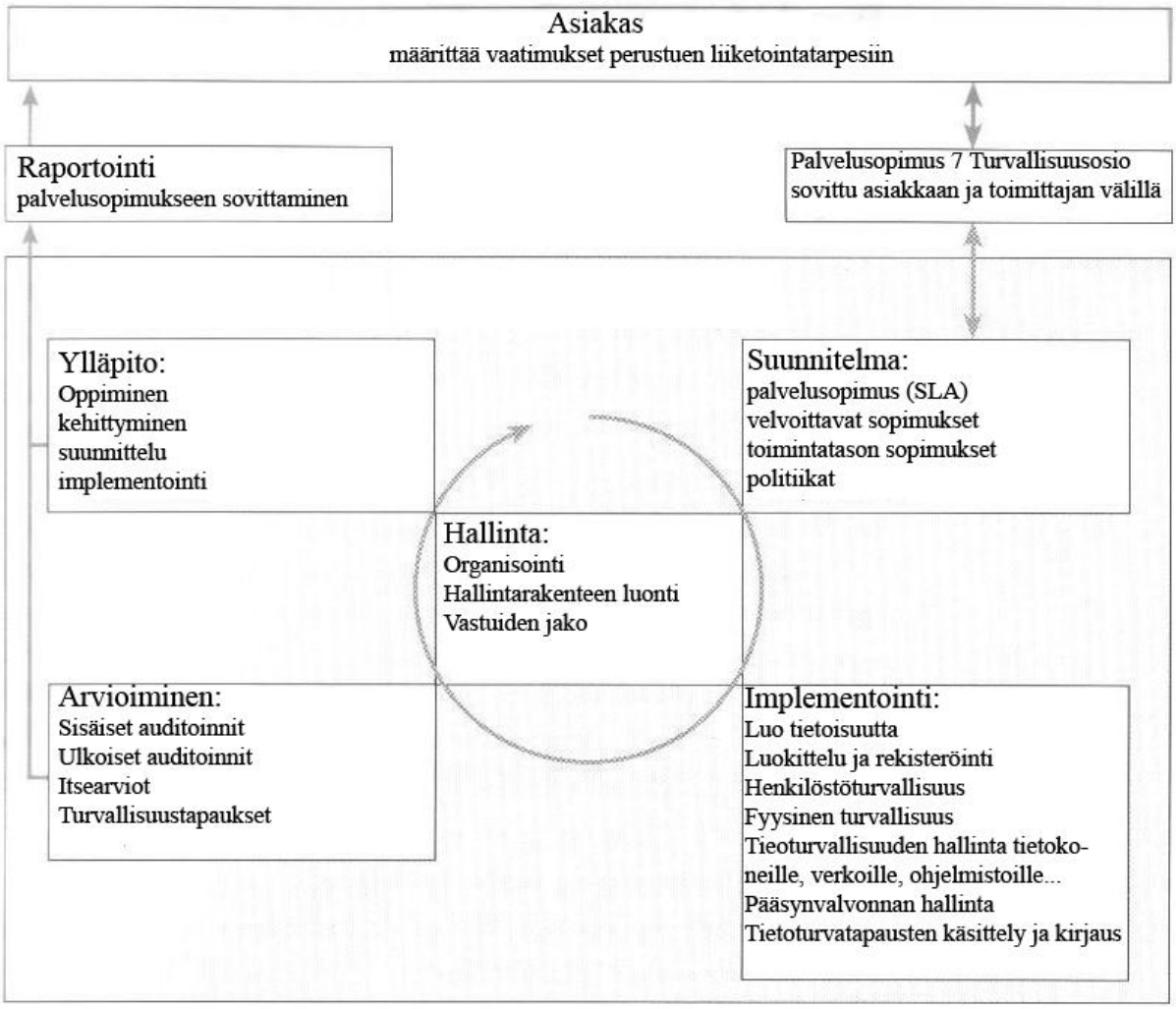
käyttää sellaisinaan, vaan on valittava omaan organisaatioon parhaiten sopivat ja muokattava niitä vielä tarvittaessa.

ITIL lähestyy hallintaa täysin prosessipohjaisesti [Kuva 8]. Yksinkertaistettuna jokainen ITIL prosessi on olemassa tiettyä tavoitetta varten. Tavoite saavutetaan suorittamalla tietty joukko toimintoja. Syötteet tälle prosessille ovat ne erityiset vaatimukset, jotka vaaditaan tavoitteiden toteuttamiseksi. Tuloste tälle prosessille on vaatimusten toteuttamisen laatu. Suhteet muihin prosesseihin ovat mahdollisia.



Kuva 8. ITILin prosessipohjainen lähestymistapa [2004, s. 22]

ITIL korostaa tietoturvallisuuden hallintaprosessin olevan suljettu kehä, jossa tietoturvallisuutta on hallittava, suunniteltava, implementoitava, arvioitava ja ylläpidettävä [Kuva 9]. VAHTI-ohjeet soveltavat myös PDCA-mallia, näin todetaan esimerkiksi valtionhallinnon tietoturvallisuussuosituksessa [VAHTI, 3/2000].



Kuva 9. ITILin tietoturvallisuuden hallintaprosessi [2004, s. 15].

4.7 Tietoturvallisuuden perusrakenne

Tavoite BS 7799:n mukaan on organisaation tietoturvallisuuden hallinnan toteuttaminen. Tietoturvallisuuden toteuttamisen aloittamiseen ja valvontaan tulee luoda perusrakenne. Perusrakennetta varten on luotava johtoryhmä.

Toteuttamismenettelyitä ovat tietoturvallisuutta koskeva yritysjohdon työryhmätietoturvallisuuden koordinointi, tietoturvallisuutta koskevien vastuiden jako, tietojenkäsittelypalveluja koskeva hyväksymisprosessi, tietoturvallisuutta koskeva asiantuntija-apu, organisaatioiden välinen yhteistoiminta ja tietoturvallisuuden riippumaton arviointi.

4.8 Turvamenettelyt sivullisen pääsyä vastaan

Tavoite on organisaation tietojenkäsittelypalvelujen ja tietoaineistojen suojaaminen sivullisen tunkeutumista vastaan ja ulkopuolisten pääsyn valvonta. On tarpeellista selvittää, sallitaanko ulkopuolisten pääsy tietyillä ehdoilla.

Kohtaan kuuluvat ulkopuolisten pääsyoikeuksiin liittyvien riskien tunnistaminen, pääsyoikeustyyppien määritys, pääsyoikeuksien perusteet, yrityksen tiloissa työskentelevät toimittajat (ylläpito- ja tukihenkilöstö, siivoojat, opiskelijat jne.) ja ulkopuolisten sopimusten turvaehdot.

4.9 Tietoturvan ulkoistaminen

Ulkoistaminen on organisaation jonkin osan tai toiminnan antamista toisen yrityksen tai organisaation tehtäväksi. Organisaatio maksaa tälle toiselle osapuolelle tästä hyvästä. Ulkoistamalla organisaatio voi keskittyä siihen, mitä se osaa parhaiten. Tietoturvapalvelut ovat vain yksi ulkoistamisen kohteista. Tietoturva vaatii kuitenkin erikoisosaamista, joten se on monesti luonnollinen kohde ulkoistamiselle.

BS 7799 standardin tavoite ulkoistamisen osalta on tietoturvallisuuden tehokas ylläpito tilanteessa, jossa tietojenkäsittelypalvelu on annettu ulkopuolisen organisaation hoidettavaksi. Ulkoistamisjärjestelyiden sopimuksista tulee ilmetä riskit, turvamekanismit sekä ohjeet tietoverkoista ja -järjestelmistä eri osapuolille [BS 7799-1:fi, 2000].

Ulkoistamissopimuksen turvavaatimuksissa määritetään lakivaatimukset esimerkiksi tietosuojalain perusteella, vastuut, liiketoimintamallien eheyden ja luottamuksellisuuden varmistaminen ja testaus, fyysiset ja loogiset turvanmekanismit informaation rajauksessa valtuutetuille käyttäjille, palvelujen saatavuuden takaaminen äkillisissä ongelmatilanteissa, ulkoistettujen laitteiden fyysinen turvallisuus ja tarkastusoikeudet. Järvinen [2002, s. 114] muistuttaa ulkoistamisen olevan aina riski, sillä organisaatiolta häviää tällöin suora kontrolli. Lisäksi ulkoistajan ja asiakkaan välillä liikkuu tietoliikennettä, jota pitää erityisesti suojata. Ulkoistamisen on tuotava huomattavia etuja, jotta se olisi kannattavaa.

4.10 HAMKin tietoturvallisuuden organisointi, hallinta ja prosessit

Olen koonnut tähän kappaleeseen HAMKin suunnitelmissa olevia tietoturvallisuuden organisointiin liittyviä asioita. Suunnitelmat ovat olleet hyvässä vaiheessa, mutta käytännön toteutus on jäänyt kesken. Yleiset periaatteet ovat kunnossa, samoin vastuiden jakaminen.

Tietoturvallisuusprosessin kehittämisen lähtökohtina HAMKissa ovat valtionhallinnon ja kunnallishallinnon antamat ohjeet ja suositukset, hyvä tiedonhallintatapa sekä muu lainsäädäntö. Tietoturvallisuuden kehittämisen päämääränä ovat kuntayhtymän tärkeiden palveluiden ja niitä tukevien tietoteknisten järjestelmien tietoaineistojen ja toimintojen turvaaminen.

Tietoturvallisuusprosessiin kuuluvat tietoturvapolitiikka, jossa todetaan kehittämisen yleisperiaatteet ja vastuut:

- tietoturvasuunnitelma, jossa määritellään tietoturvatoimenpiteiden periaatteet ja toimintatavat sekä joka tarkistetaan vuosittain
- tietoturvan toteuttamisen ohjeet, jotka liittyvät turvattaviin toimintoihin ja henkilöiden toimintaan
- tietoturvallisuuden toteuttaminen ja jatkuva valvonta
- tietoturvallisuutta koskevien tapahtumien ja toimenpiteiden raportointi vuosittain

Tietoturvallisuustilanteen merkittävimmät muutokset kirjataan vuosittain tietohallintostrategiaan, jossa määritetään tarvittavat toimenpiteet, toteutustavat ja resurssitarpeet. Tällaisia muutoksia aiheuttavat erityisesti uusien tietotekniikkapalveluiden käyttöönotot, organisaatiomuutokset sekä peruslinjausten muutokset.

Tietoturvallisuussuunnitelman tehtävänä on (VAHTI 1/2001)

- luoda puitteet tietoturvallisuustoimenpiteille, määrittelemällä ylläpidettävät toimenpiteet ja niiden taso sekä toteutustapa
- määritellä varsinaisen toiminnan, sitä tukevan tietotekniikan sekä kehittämishankkeiden seuranta tietoturvallisuustoimenpiteiden toteuttamiseksi niiden yhteydessä
- ohjata varautumistoimenpiteitä ja valmiutta, joilla huolehditaan tarvittaessa toiminnan varmistamisesta

Tietoturvallisuussuunnitelman tavoitteena on huolehtia tietoaineistojen suojaamisesta, oikeasta käsittelystä ja salassapidosta sekä tietotekniikan turvaamisesta laitevioilta, ohjelmavirheiltä, haittaohjelmilta, tietomurroilta ja väärinkäytöksiltä sekä valvoa ja raportoida turvallisuudesta. Suunnitelman keskeisiä tulee testata osana käytännön tieturvallisuustyötä.

Vakavien toiminnan keskeytyksien, kuten palvelintietokoneet sisältävän konesalin tuhoutumisen, varalle on laadittava erillinen *toipumissuunnitelma*, jota seuraten voidaan palata vähitellen normaaliin toimintaan.

Tietojärjestelmä:

- järjestelmän omistaja vastaa palvelutasovaatimuksen määrittelystä ja tietoturvan toteuttamisen edellytysten luomisesta (esim. resurssit)
- ylläpidon vastuuhenkilö huolehtii tietoturvan teknisestä toteuttamisesta ja valvonnasta

Toimipaikan työasemat, palvelimet ja lähiverkko:

- tietoturvavastaava huolehtii tietoturvan teknisestä toteuttamisesta ja valvonnasta

Organisaatioyksikkö:

- yksikön johtaja vastaa yksikön omistamien tietojärjestelmien tietoturvasta ja riittävästä tietoturvaan resursoinnista
- yksikön työntekijät vastaavat työtehtäviensä tietoturvasta

Kuntayhtymä:

- ylin vastuu tietoturvasta on kuntayhtymän hallituksella ja rehtorilla
- tietotekniikasta vastaava johtaja vastaa tietoturvasta ja sen kehittämisestä
- tietojärjestelmäpäällikkö koordinoi tietoturvan kehittämistä ja teknistä toteuttamista

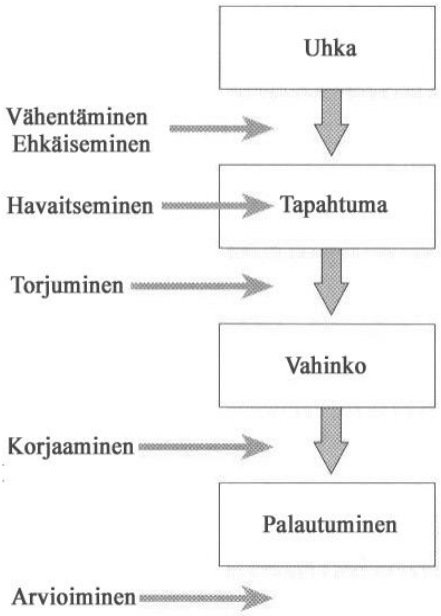
HAMKissa käyttäjähallinto jakaa käyttäjätunnukset. Pääryhmät ovat henkilökunta, opiskelijat ja yhteistyökumppanit.

HAMKille olisi erityisen tärkeää perustaa tietototurvaryhmä ja tietoturvallisuuden hallintajärjestelmä. Tietoturvaryhmä hallinnoisi tietoturva-asioita ja kokoontuisi päättämään toimenpiteistä. Tietoturvaryhmän jäseniä voisivat olla tietohallintojohtaja, tietojärjestelmäpäällikkö, tietojärjestelmähankkeiden vetäjä, opetusprosessista vastaava henkilö, tietoturvan teknisestä toteutuksesta vastaava henkilö, henkilöstöpäällikkö, tutkimustoiminnasta vastaava. Tietoturvaryhmän tehtävä on suunnitella ja toteuttaa tietoturvallisuuden hallintajärjestelmä, joka toimii PDCA-prosessimallilla. Tietoturvallisuuden hallintavaihe on tällöin aloittava, mutta PDCA-prosessia toistamalla hallinta kypsyy ja kehittyy. Yksinkertainen, mutta hyvin suunniteltu ja toimiva hallintajärjestelmä on helpompi ottaa käyttöön, kuin monimutkainen ja byrokraattisesti raskas. Tärkeätä on toiminnan jatkuminen ja kehittyminen paremmaksi. Tässä tutkimuksessa on käytyaikaisemmin läpi hallintajärjestelmän periaatteita ja tavoitteita, joten niihin perehtymisestä on hyvä aloittaa.

5 Tietoriskien ja – uhkien hallinta

5.1 Riskien hallinta

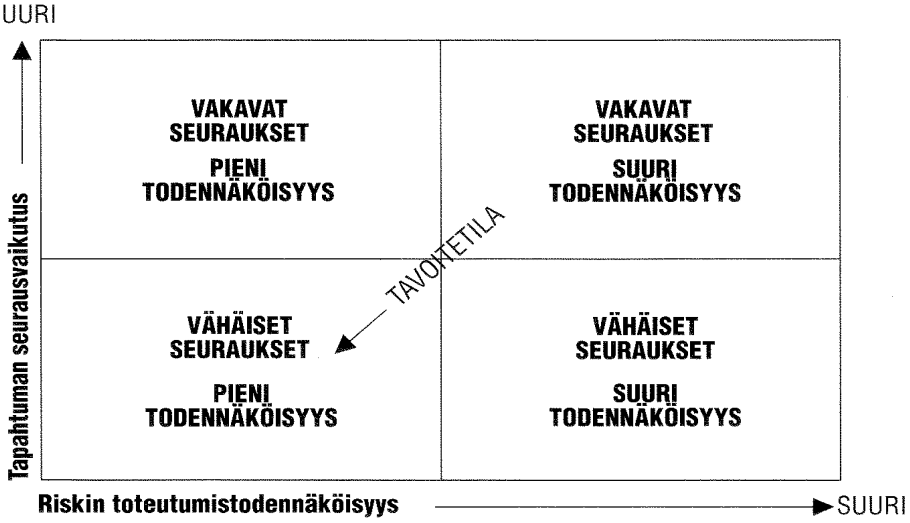
Riski on jonkin vahingollisen tapahtuman todennäköisyyden ja seurausten tulo. Riskejä on olemassa lukemattomia ja niiden seuraukset voivat olla mitättömistä aina korvaamattomiin asti. Todennäköisyyksien laskeminenkaan ei ole yksinkertaista, joten epävarmuutta ei voi täysin poistaa. Riskejä voidaan kuitenkin hallita ja ymmärtää, kun ne tunnetaan. Teoriassa kaikilta riskeiltä voidaan suojautua: tarvitaan vain tarpeeksi resursseja. Käytännössä resurssit ovat rajatut, jolloin on tarpeen määritellä riittävä riskitaso, priorisoida tärkeimmät riskit ja tyytyä tiettyjen riskien olemassa oloon ilman suojausta. Riskiketju on tunnettava niin hyvin, että se hallitaan aina palautumiseen asti, kuten kuvassa 10 on esitetty [Kuva 10].



Kuva 10. Uhkasta palautumiseen ITILin tavoin [2004, s. 11]

Riskien hallinnassa ja tietoturvallisuudessa on yhtymäkohtia, joten näitä kahta ei tule erottaa. Organisaation päivittäisessä toiminnassa on tärkeää, että nämä molemmat osa-alueet tukevat toisiaan. Organisaation turvallisuusvaatimusten tunnistamisen ensimmäinen vaihe on riskianalyysien tekeminen, jossa tunnistetaan suojattavat kohteet, niihin mahdollisesti kohdistuvat uhkat, alttius vahingoille, todennäköisyys vahingoille ja mahdolliset vaikutukset. Tutkimus aloitetaan riskianalyyseilla, joissa selvitetään mahdollisimman tarkasti uhkat HAMKille. Nykyistä tilannetta tutkittaessa käydään läpi voimassa olevat käyttösäännöt ja ohjeet. Apuna käytetään tarkistuslistoja.

Riskien ideoinnissa käytetään menetelminä lähdekirjallisuutta, aivoriihiä, esimerkkejä riskianalyyseistä, tarkistuslistoja ja haastatteluita. Näistä mainituista valitaan parhaiten tutkimukseen sopivat menetelmät ja niiden käyttö kirjataan omiin alalukuihinsa. Ideoinnissa syntyviä riskejä ja uhkia verrataan tarkistuslistojen vastauksiin ja yhdessä niistä kootaan riskianalyysien pohjaksi halutut riskit. Löydetystä riskeistä tehdään riskianalyysit ja kaikkein tärkeimmistä riskeistä tehdään erittäin yksityiskohtaiset analyysit. Lopuksi tehdään yhteenveto riskianalyysien tuloksista. Tulosten perusteella on syytä esittää tarpeellisia toimenpiteitä, jotta riskien hallinnassa päästäisiin Miettisen kuvan esittämään tavoitetilaan [Kuva 11].



Kuva 6 Tietoturvallisuusriskien hallinnan tavoitetila

Kuva 11. Tietoturvallisuusriskien hallinnan tavoitetila [Miettinen 1999, s. 58]

Haavoittuvuus erilaisille tietoriskeille ja uhkille on väistämätöntä, jos ei tiedosteta uhkien olemassaoloa ja varauduta niihin. Vaarana tästä tietämättömyydestä on harhaanjohtava turvallisuuskäsitys, jos organisaatiossa tuntuu kaikki olevan kunnossa ja mitään tavallisesta poikkeavaa ei ole tapahtunut. Tunne ei korvaa tietoa ja turvallisuuden todentamiseksi on tehtävä töitä ja selvitettävä todellinen tilanne. Kyrölän mukaan tietoriskityön koordinoijan rooli on tärkeä, mutta mielestäni tällaisen roolin olemassa olo ei vielä takaa mitään [2001, s. 142]. Mielestäni vastuun ottaminen on hyvä alku. On erittäin tärkeää, että tiedostetaan ero tiedettyjen asioiden ja luultujen asioiden välillä.

Kaikki riskit ja uhkat eivät ole koskaan samanarvoisia. On resurssien ja varojen tuhlausta panostaa vääriin kohteisiin ja vääränlaisiin suojausmenetelmiin. On myös resurssien tuhlausta jos suojausten arvo on suurempi kuin suojattavien kohteiden. Tietoturvasuunnitelman tekemistä

varten on siis selvitettävä, mitä halutaan suojata ja millaisilta uhkilta. Riskien hallinta ei ole ilmaista ja se vaatii budjetin, jonka avulla sitä suoritetaan ja toteutetaan. Tietoturvasuunnitelman voidaan katsoa olevan arvoton, jos siinä ei oteta huomioon organisaation erityisluonnetta ja tilannetta. Geneerinen tietoturvasuunnitelma voi näyttää paperilla hyvältä ja laajalta, mutta itse sisältö ei sovellu organisaatiolle tarpeeksi hyvin ollakseen käyttökelpoinen tai kukaan ei ota vastuuta siinä mainituista velvollisuuksista. Eri organisaatioilla on erilaista tietoa ja erilaiset prioriteetit niiden suojelemiselle. Valmiita ratkaisuja riskien hallinnalle ei ole olemassa, sillä riskien selvittäminen vaatii asioihin paneutumista pintapuolista syvemmälle. On kuitenkin hyvä käyttää työn tukena valmiita hyväksi tunnettuja pohjia rakenteen selkeyttämiseksi, mutta ei liikaa tukeutua valmiiseen materiaaliin.

Kyrölä [2001, s. 147] esittää yleisen uskomuksen, että tietoriskien hallinta ei ole tuottavaa työtä ja yrittää samalla perustella miksi tämä käsitys on väärä. On totta, että on vaikea näyttää rahallinen hyöty tietoriskityön tuottavuudesta. Tämä pätee jokaiseen yrityksen prosessiin ja palveluun. Yksistään niitä ei kuitenkaan olisi olemassa ja vasta, kun ne kaikki toimivat yhteen, saadaan tuloksia. Tietoriskien hallinnalla tuetaan näitä muita toimintoja ja palveluita ja taataan näiden sujuva toiminta. Usein kuitenkin mietitään tietoturvallisuutta ja riskejä vasta, kun jotain on jo tapahtunut eli reagoidaan. Tietoriskien hallinnalla ei odoteta jotain vain tapahtuvan, vaan aktiivisesti pyritään pysymään tilanteen tasalla ja ennakoidaan, estetään ja varaudutaan tapahtumiin. Tietoriskien hallinta on onnistunutta, kun sillä ennakoidaan ja estetään pahimmat uhkat ja riskit ja minimoidaan toteutuneiden uhkien seuraukset.

Työ on hyvä aloittaa pohtimalla mitä nämä tietoriskit ja – uhkat ovat. Tietoriskiä voi määritellä Miettisen mukaan kolmella tavalla: määritetään uhka, epävarmuus ja mahdollisuus [1999, s.50]. Riskianalyyseilla ja -arvioinneilla muodostetaan kuva siitä, mitä riskejä organisaation toimintaan kohdistuu ja millaisia vaikutuksia niillä on organisaation toimintaan. Nämä toimenpiteet kuuluvat oleellisina osina organisaation tietoturvakartoitukseen ja niitä on suoritettava riittävän usein ja varsinkin olosuhteiden muuttuessa.

Riskien hallinnalla tarkoitetaan Miettisen [1999, s. 50] tulkinnan perusteella organisaation toimintaan kohdistuvien riskien eli epätoivottujen tapahtuminen luonteen, merkityksen ja laajuuden ymmärtämistä, hyväksyttävän riskitason määrittämistä ja sekä olemassa olevien riskien alentamista hyväksyttävälle tasolle. Tutkimuksessa keskitytään erityisesti tietoturvariskeihin, joten riskien hallinta jaetaan sen mukaisesti eri osa-alueisiin. Riskien hallinta suoritetaan erilaisilla tietoriskien arvioinneilla, joissa selvitetään riskien seurauksia organisaatiolle. Riskien hallitsemisen mahdollisia toteutuskeinoja ovat riskin poistaminen, riskin pienentäminen, riskin siirto ja riskin hyväksyminen.

Paavilaisen [1998, s. 26] ja Miettisen [1999, s. 92] mukaan samalla on hyvä toteuttaa suojeltavien kohteiden luettelointia, sillä on tiedettävä mitä on suojeltava.

5.2 Tietoriskien arviointimenetelmiä

Riskianalyysi tarkoittaa Miettisen [1999, s. 51] sanoin ”Yksityiskohtaista teknistä tutkintaprosessia, jossa selvitetään kohteena olevaan organisaatioon kohdistuvat ei-toivotut tapahtumat”. Hän ei kuitenkaan mainitse, mitä yksityiskohtainen tarkkaan ottaen tarkoittaa. Löydettyjen riskien jälkeen voidaan niille suorittaa arviointi, jossa selvitetään seurausvaikutukset kyseisen riskin toteutuessa. Paavilainen [1998, s. 60] on todennut kaikkien riskianalyysimenetelmien pohjautuvan pääosin seitsemään toimenpiteeseen: tunnista tietoarvot, määrittele arvot, tunnista uhkat, tunnista haavoittuvuus, arvioi riskien todennäköisyys, valitse ja toteuta turvallisuustoimenpiteet, korjaa ja seuraa tietoturvallisuusohjelman toteuttamista. Uhkatekijöitä voi tunnistaa käyttämällä järjestelmällisiä lähestymistapoja tai arvaamalla. Arvaamisen parempi termi voisi olla ennustaminen tai aivoriihi, jossa ideoidaan tajunnanvirran mieleen tuomia asioita ja luotetaan intuitioon, joskus tällainen lähestymistapa voi tuoda yllättäviä tuloksia, joita ei perinteisillä järjestelmällisillä tavoilla välttämättä löydetä. Ennustamiselle ja arvaamiselle ei ideointia voi kuitenkaan pelkästään perustaa.

Riskianalyyseja voidaan suorittaa kvantitatiivisilla ja kvalitatiivisilla menetelmillä. VAHTI ohjeissa [VAHTI] korostetaan, että menetelmien valinnassa on otettava huomioon tiedon keruu ja tarvittavat kysymykset, menetelmän ominaisuudet ja sopivuus käyttökohteeseen, tulosten esitystapa ja kattavuus sekä selkeys ja yksiselitteisyys, käytön helppous, menetelmän omat turvaominaisuudet ja raportointimahdollisuudet. On syytä ottaa riskien tutkimisprosessiin mukaan useita asiantuntevia ihmisiä, jotta saadaan mahdollisimman monipuolisia mielipiteitä ja ideoita. Pelkkien asiatuntijoiden suorittamista arvioista voi puuttua täysin käytännön työn tekijöiden asenne ja kokemukset. Työtä ei tehdä asiantuntijoita varten vaan tulosten on oltava sidoksissa todenmukaiseen työilmapiiriin ja – olosuhteisiin. Toisten tekemää työtä ei voi arvioida kuulematta itse tekijöitä. Esittelen seuraavaksi muutamia tietoriskien arviointimenetelmiä, joita voi käyttää tutkimuksen teossa apuna.

5.2.1 Skenaarioanalyysi

Yksi yleisimmin käytetyistä tietoturvallisuuden uhkien tunnistamisen kvalitatiivisista menetelmistä on skenaarioanalyysi. Skenaario on pieni kertomus jossa kuvataan uhkatilanne ja jälkiseuraamukset organisaatiolle mahdollisimman tarkasti. HAMKin tapauksessa voimme ideoida Kivelän kanssa mahdollisia tapauksia yhdessä ja erikseen, tärkeätä on pitää mielessä

käytännöllinen näkökulma. Ei ole tarkoitus liioitella tai vähätellä erilaisia skenaarioita, vaan ideoidaan ja esitetään juuri HAMKiin kohdistuvat tapaukset. Mitä enemmän ihmisiä on tekemässä skenaarioanalyysejä, sitä vähemmän jää asioita pimentoon.

Jokaisen skenaarion kohdalla tehdään arviointi todennäköisyydestä ja seurauksista. On tärkeää, että prosessia jatketaan kunnes kaikki osallistuvat osapuolet ovat varmistuneita työn laajuuden riittävyydestä ja oleellisten uhkien löytymisestä. Arvioituja uhkaskenaarioita voidaan asettaa tavoitteiden mukaan erilaisiin tärkeysjärjestyksiin, esimerkiksi taloudellisten seuraamusten tai todennäköisyyden perusteella. Jokaiselle skenaariolle on mietittävä torjunta- ja suojausmenetelmät. Skenaariotekniikan yksinkertaisuuden takia katson sen olevan helpoin tapa tehdä yksittäisten tietoturvauhkien arviointi. Paavilaisen lista on yksi esimerkki skenaariotekniikan sisällöstä [1999].

1. Tapahtumien kuvaus
2. Turvallisuustoimenpiteiden kuvaus
3. Puutteiden ja heikkouksien erittely
4. Tapahtumien seurausten kuvaus
5. Tapahtumien todennäköisyysarvio
6. Arvio tarvittavista toimenpiteistä
7. Ehdotus tarvittavista toimenpiteistä

5.2.2 Kyrölän menetelmä

Kyrölä esittää tietoriskien kartoitukseen seuraavanlaista toteutustapaa, joka vastaa skenaariotekniikkaa [2001, s. 168]. Tämä tapa kertoo toiminnan kokonaisuudessaan eri vaiheiden kautta. Tällä hallintamenetelmällä pyritään myös kehittämään tietoturvallisuutta esittämällä kehityssuunnitelma riskien vähentämiseksi ja poistamiseksi.

1. Tunnista toimintayksikön suojattavat kohteet
2. Tunnista toimintayksikössä noudattavat käytännöt
3. Tunnista sidosryhmät ja muut yhteydet
4. Arvioi sidosryhmien käytäntöjä
5. Arvioi millaisia tilanteita voi tapahtua
6. Arvioi mitä vahinkoja voi aiheutua asiakkaille, sidosryhmille ja toimintayksiköille
7. Käy läpi kehittämisaloitteet ja häiriöilmoitukset
8. Arvioi toimintayksikön käytäntöjen riittävyys
9. Vertailu vahinko- ja kehittämistarpeiden kustannuksia
10. Tee lausunto tietoriskien hallinnan tilasta
11. Esittele kehittämissuunnitelma johdolle.

5.2.3 Tarkistuslistat

Hyväksi koettuja ja tarpeellisia tietoturvallisuuden tutkimiseen liittyviä kysymyksiä on koottu tarkastuslistoihin. Tarkistuslistat koostuvat kysymyssarjoista, joissa selvitetään olemassa olevien suojausten ja uhkien tunnistamista ja identifiointia. Tarkoituksena on saada yleiskuva tietoturvallisuuden tasosta organisaatiossa. Käymällä kohta kohdalta läpi kysymyksiä ja vastaamalla niihin voidaan helposti havaita puutteita ja virheitä olemassa olevissa suojauksissa. Uhkien löytämiseen sopii paremmin skenaariotekniikka. Tarkistuslistojen käytön helppous on myös niiden suurin vaara, sillä on houkuttelevaa vain vastata ylimalkaisesti kysymyksiin. Itse kysymyksetkin voivat olla epätarkkoja tai riittämättömiä. Tarkistuslistan laajuus ja sopivuus voivat olla myös epäsopivia ja vääränlaiset listat antavat harhauttavan kuvan organisaation tietoturvasta. Täytetty tarkistuslista ei takaa vielä mitään. Tarkistuslistat toimivat huonosti olemassa olevien suojausmenetelmien arvioimisessa, sillä ne eivät ole tietoturvallisuuden mittareita, sillä kysymyksiin vastaan yleensä kyllä, ei tai en tiedä. Suojausmenetelmien riittävyyden arviointiin on olemassa omat menetelmänsä [Paavilainen, 1998] [Miettinen, 1999]. On tärkeää käyttää asiantuntijoiden hyväksymiä ja luotettavia lähteitä tarkistuslistoille, kuten valtiovarainministeriön julkaisuja ja ammattikirjallisuutta. HAMKin ominaisuuksien mukaan on käytettävä sopivia tarkistuslistoja. Tarkistuslistat eivät sovi ainoaksi lähestymistavaksi. Tarkoituksena on soveltaa lähdekirjallisuuden ja VAHTI -tarkistuslistoja.

5.2.4 Baseline

Baseline-tekniikassa ei varsinaisesti tunnisteta uhkatekijöitä vaan käytetään hyväksi joukkoa hyväksi katsottuja tietoturvallisuuden parantamisen perusmenetelmiä. Paavilainen kertoo, että nämä asianmukaisesti hyväksytyt suojakeinot ja asianmukaisen huolellisuuden noudattaminen ovat saaneet *de facto* aseman maailmalla [1998, s. 61]. Peruskontrollit on kuvattu alla ja ne noudattavat samanlaista kaavaa kuin aikaisemmin Paavilaisen [1998, s. 60] ja Miettisen [1999, s. 149] esittämät skenaarioanalyysimenetelmät.

1. suojeltavan kohteen tunnistaminen
2. olemassa olevien suojausten tunnistaminen
3. peruskontrollien valinta yleisimpien uhkien torjumiseksi
4. kontrollien toteuttaminen
5. erityisuhkien tunnistaminen
6. uhkien ja riskien analysointi
7. lisäkontrollien valinta
8. lisäkontrollien toteutus
9. turvallisuuden säännöllinen seuranta

5.2.5 Courtneyn menetelmä

Eräs mainittu kvantitatiivinen menetelmä Paavilaisen [1998, s. 63] ja Miettisen [1999, s. 150] kirjoissa on Courtneyn menetelmä, jossa keskitytään uhkien ja riskien todennäköisyyksiin. Mitä suuremmat vahinkojen odotusarvot ovat, sitä pahempi riski on kyseessä. Menetelmän luotettavuus on verrannollinen lähtöarvojen tarkkuuteen. Tuloksiin on siis syytä suhtautua varauksella ja lähtöarvoille on asetettava arvio luotettavuudesta ja virhemarginaalin suuruudesta. Riskien odotusarvojen mukaan voidaan määritellä tärkeysjärjestys eri kohteiden suojauksille. On syytä miettiä, onko tämä menetelmä käyttökelpoinen tutkimuksessa. Alla olevan kuvan kaavaan [Kuva 12] sijoitetaan muuttujat.

E = P x A

Jossa E = vahingon odotusarvo,

P = Vahingon todennäköisyys ja

A = odotetun vahingon suuruus rahayksikössä

Kuva 12. Courtneyn menetelmä [Miettinen, 1999, s. 150]

5.3 HAMKin tietoriskien ideointi

Olen ideoinut yhdessä HAMKin tietojärjestelmäpäällikön Jari Kivelän kanssa mahdollisia tietoriskejä. Riskien löytämisessä on käytetty apuna VAHTI-ohjetta riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa [Vahti 7/2003]. Tässä ohjeessa ollut riskianalyysilomake valittiin käytettäväksi sen selkeyden ja riskien lajittelun takia ja siksi, että siihen oli sisällytetty alla vaaditut asiat. Samoja asioita käytiin läpi myös Miettisen [1999, s. 160, 176, 186, 198, 225, 229, 240, 248 ja 250] ja Kyrölän [2001, s. 247-301] kirjojen tarkistuslistoissa, mutta VAHTI-tarkistuslistan kokonaisuus oli laajempi ja yksikohtaisempi. Näistä kahdesta jälkimmäisestä sain kuitenkin lisää ideoita mahdollisiksi HAMKia koskeviksi tietoriskeiksi. HAMKin riskianalyyseissä oli tarkoitus selvittää vähintään seuraavat asiat:

Hallinnolliset tietoturvariskit

- Johdon sitoutumattomuus tietoturvallisuuden toteuttamiseen ja ylläpitoon
- Tietoturvakoulutuksen puutteet
- Tietoturvan seurannan puutteellisuus
- Tietoturvaprosessin jatkuvuus
- Suurimpien riskien tunnistaminen

Henkilöstötietoriskit

- Avaintyöntekijän menettäminen
- Oman tietoturvallisuuden laiminlyönti
- ATK-käyttösääntöjen tahallinen / tahaton rikkominen
- Tietojen vuoto ulkopuolisille, henkilötiedot tms.
- Työntekijän puutteellinen tietoturvakoulutus

Toimintaympäristöön kohdistuvat tietoriskit

- Vesivahingot
- Sähkökatkot
- Tulipalot

Asiattomien pääsy kiinteistöön ja siellä oleviin toimitiloihin

Tietojärjestelmiin kohdistuvat tietoriskit

- Tunkeutuminen tietojärjestelmään / Hakkerointi
- Kapasiteetin riittämättömyys normaalissa työskentelyssä
- Tietokonevirukset, haittaohjelmat
- Tietojärjestelmän käyttö estyy
- palkkatietojen myöhästyminen
- opiskelijatietojen myöhästyminen
- Tietojen tuhoutuminen
- Tietojen korruptoituminen

Opetustoiminnan riskit

- Oppilaiden tuomien laitteiden ja lataamien ohjelmien riskit
- Tekijänoikeuksien rikkominen
- Ilkivalta laitteistolle / tiedoille

5.4 HAMKin tärkeät palvelut

HAMKin toimintaan kuuluu lukuisia palveluita, joiden kriittisyys vaihtelee. Taulukon 1 pohjana on käytetty päivitettyjä HAMKin tärkeiden palvelujen riskianalyyseja. Taulukosta nähdään, että kaikkein kriittisimmät kohteet sietävät vain muutaman tunnin katkoksia. Taulukosta nähdään suojattava tietojärjestelmä sekä sen sisältämien tietojen vaikuttavuus muihin järjestelmiin ja toimintoihin sekä riippuvuudetn muista järjestelmistä.

Taulukko 1. HAMKin tärkeiden palvelujen riskianalyysit [HAMK]

Tietojärjestelmä	**Tietojen vaikuttavuus**	**Toiminnan kriittisyys, pisin siedettävä palvelukatko**	**Riippuvuudet**
Henkilöstöhallinto			
Prima, henkilöstöhallinto ja palkanmaksu	Koko henkilöstön palkanmaksu	Erittäin kriittinen, 1 pv	Maksuliikenne (Analyste) Kirjanpito (Wintime) Tietoliikenneyhteydet, palomuuri
eHRMinfo, henkilöstöraportit	Henkilöstöhallinnon raportit mm.	Melko kriittinen, 5 pv	Henkilöstöhallinto (Prima) Tietoliikenneyhteydet,

	tilinpäätökseen		palomuuri
Taloushallinto			
Wintime, kirjanpito ja reskontra	Kaikki laskutus- ja maksuliikenne, tilinpäätöstiedot	Erittäin kriittinen, 1 pv	Maksuliikenne (Analyste) Tietoliikenneyhteydet, palomuuri
Analyste, maksuliikenne	Maksuliikenteen toimivuus	Erittäin kriittinen, 1 pv	Tietoliikenneyhteydet, palomuuri
Basware IP, ostolaskujen kierrätys	Kaikkien ostolaskujen asiatarkastus ja hyväksyminen	Erittäin kriittinen, 1 pv	Tietoliikenneyhteydet, palomuuri
Travelman, matkalaskut	Henkilöstön matkasuunnitelmat ja -laskut	Erittäin kriittinen, 1 pv	Tietoliikenneyhteydet, palomuuri
Opetushallinto			
WinhaPro, opetushallinto	Opintotarjonta, ilmoittautuminen, suoritukset, todistukset	Kriittinen, 2 pv	Tietoliikenneyhteydet, palomuuri
WinhaWille, opiskelijaliittymä	Opiskelijoiden ilmoittautuminen	Kriittinen, 2 pv	Opetushallinto (WinhaPro) Tietoliikenneyhteydet
WinhaWiivi, opettajaliittymä	Opintosuoritusten kirjaaminen (osittain)	Kriittinen, 2 pv	Opetushallinto (WinhaPro) Tietoliikenneyhteydet
InterDocs, kansainvälinen vaihto	Kv-vaihdon tietojen kirjaus, tilastot ja tiedot	Melko kriittinen, 5 pv	Tietoliikenneyhteydet
Opetustoiminta			
Moodle etäopetusjärjestelmä	Etäopetustoiminta (paljon)	Kriittinen, 2 pv	Tietoliikenneyhteydet
Optima, etäopetusjärjestelmä (ostopalvelu)	Etäopetustoiminta (vähän)	Kriittinen, 2 pv	Tietoliikenneyhteydet
Voyager, kirjastojärjestelmä (ulkoistettu)	Koko lainaustoiminta, luettelointi	Kriittinen, 1 pv	Tietoliikenneyhteydet, Funet-yhteys
Opetuksen ohjelmistot (työasemissa ja palvelimissa kuten Word ja Excel)	Päivittäinen lähiopetus	Erittäin kriittinen, 2 h	Tietoliikenneyhteydet, lähiverkko
Viestintä			
Groupwise, sähköposti- ja kalenterijärjestelmä	Henkilökunnan ja opiskelijoiden viestintä	Erittäin kriittinen, 4 h	Tietoliikenneyhteydet
Portaali, tukee opiskelua, työntekoa ja kumppaneita	Henkilökunnan, opiskelijoiden ja kumppaneiden päivittäinen työskentely	Erittäin kriittinen, 2 h	Tietoliikenneyhteydet Perusjärjestelmät (integroidut)
Web-sivustot, useilla palvelimilla, pääasiassa portaalissa	Kaikkien tiedonsaanti, erit. potentiaaliset asiakkaat	Kriittinen, 1 pv	Tietoliikeyhteydet Portaali
Palvelutoiminta			
Täydennyskoulutuksen tietojärjestelmä	Täydennyskoulutuksen työntekijät ja kaikki asiakkaat	Kriittinen, 1 pv	Tietoliikenneyhteydet Portaali (käyttöliittymä)
Kassa-järjestelmä	Kassajärjestelmän asiakkaat, esim. ruokala	Erittäin kriittinen, 2 h	Tietoliikenneyhteydet
Varausjärjestelmät (esim. golf)	Varausjärjestelmän asiakkaat, esim. Lepaa golf	Erittäin kriittinen, 2 h	Tietoliikenneyhteydet
Verkkokauppa (esim. julkaisut)	Viestinnän työntekijät ja asiakkaat	Kriittinen, 1 pv	Tietoliikenneyhteydet
Infrastruktuuripalvelut			
Tietoliikenneyhteydet	Koko kuntayhtymä, kumppanit, asiakkaat, potentiaaliset asiakkaat	Erittäin kriittinen, 2-4 h	Alueverkkoyhteydet Funet-yhteys Nimipalvelut
Nimipalvelut (keskitetyt, sisäiset)	Koko kuntayhtymä	Erittäin kriittinen, 2 h	Alueverkkoyhteydet Palvelintietokoneet

Etäyhteyspalvelut, HAMK-adsl, VPN	Henkilöstön osa (aktiiviset käyttäjät)	Kriittinen, 2 pv	Alueverkkoyhteydet Nimipalvelut
Lähiverkon palvelut, levyt ja tulostimet	Koko toimipaikka	Erittäin kriittinen, 2 h	Lähiverkkokytkimet Palvelintietokoneet
Langattomat lähiverkkoyhteydet, public-wlan ulos	Koko toimipaikka	Erittäin kriittinen, 2 h	WLAN-autentikointipalvelut/ VPN-yhteys Lähiverkkoyhteydet Alueverkkoyhteydet
Kirjautumispalvelut, mm. eDirectory ja LDAP, OID	Kyseisen palvelun käyttäjät, esim. intranet, portaali	Erittäin kriittinen, 2 h	Alueverkkoyhteydet Palvelintietokoneet Nimipalvelut
Ohjausjärjestelmät Kulunvalvonta	Ohjattavan järjestelmän kohde, esim. kasvihuone tai rakennus	Erittäin kriittinen, 2 h	Alueverkkoyhteydet Palvelintietokoneet Lähiverkkoyhteydet

5.5 HAMKin riskianalyysit

VAHTI-ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa [Vahti 7/2003] on ollut pohjana kun olen rakentanut yksityiskohtaisemman lomakkeen [Liite 1, HAMKin tietoriskien arviointilomake] HAMKin tietoriskien arvioimiseksi. Riskien arviointi on jaettu VAHTI-ohjeiden mallin mukaisiin lukuihin ja lisäksi jokaiseen arvioitavaan kohtaan on lisätty vaaditut tarkennukset. Tämä lomake täyttää aikaisemmin asetetut vaatimukset sille, mitä asioita riskinanalyyseihin pitää vähintään sisällyttää. Käsiteltävistä riskeistä tehdään yksilöidyt riskianalyysit, joissa selvitetään:

1. Vaaraa tai uhkaa aiheuttava tilanne
2. Arvio tilanteen hallinnasta
3. Seurausten selvittäminen
4. Riskin arviointi
5. Nykyinen varautuminen
6. Toimenpide-ehdotukset, lisäkysymykset tai ehdotus tarvittavista toimenpiteistä

Riskit on määritelty käyttämällä apuna VAHTI-ohjeiden taulukkoja [Vahti 7/2003]. Uhkan todennäköisyyden olemme arvioineet yhdessä Jari Kivelän kanssa. Seurausten vakavuuden luokittelussa on sovellettu kuvan 13 taulukkoa. Riskin suuruus on saatu kuvan 14 taulukosta, jossa uhkan todennäköisyyden ja seurausten vakavuuden leikkauskohdassa on riskin suuruus.

Erittäin vakavat	3	• Seuraukset koskevat kaikkia tietojen tai palveluiden käyttäjiä • Uhkan toteutuminen aiheuttaa välittömiä toimenpiteitä • Uhkan toteutuminen aiheuttaa raportoinnin ministeriölle ja tiedotusvälineille • Uhkan toteutuminen aiheuttaa toiminnan keskeytymisen tunneista useisiin päiviin • Uhkan toteutuminen aiheuttaa suuria taloudellisia kustannuksia • Uhkan toteutuminen aiheuttaa vakavan häiriön organisaation toiminnassa (useiden avainhenkilöiden menetys) • Uhkan toteutuminen aiheuttaa luottamuksellisuuden menetyksen • Toiminta on lainsäädännön velvoitteiden vastaista.
Vakavat	2	• Seurauksilla on vaikutuksia organisaation sisällä, esimerkiksi yksittäisten työntekijöiden työmäärät kasvavat (avainhenkilön menetys) • Seuraukset koskevat useita tietojen tai palveluiden käyttäjiä • Seurauksilla on vaikutus organisaation toimintaan (saatava kuntoon tunneissa) • Uhkan toteutuminen aiheuttaa tiedotteen tekemisen • Uhkan toteutuminen aiheuttaa merkittäviä taloudellisia kustannuksia
Vähäiset	1	• Seuraukset koskevat muutamia tietojen tai palveluiden käyttäjiä • Uhkan toteutuminen ei aiheuta välittömästi toimenpiteitä • Uhkan toteutuminen aiheuttaa sisäisen raportoinnin • Uhkan toteutuminen aiheuttaa vähäisiä taloudellisia kustannuksia • Toiminnan keskeytyminen on muutaman minuutin pituinen

Kuva 13. Seurausten vakavuuden luokittelu [Vahti 7/2003, s. 42]

Kriittisyys		Seurausten vakavuus		
		Vähäinen (1)	Vakava (2)	Erittäin vakava (3)
Uhkan toden-näköi-syys	Korkea (3)	3. Kohtalainen riski	4. Merkittävä riski	5. Sietämätön riski
	Keskimääräinen (2)	2. Vähäinen riski	3. Kohtalainen riski	4. Merkittävä riski
	Alhainen (1)	1.Merkityksetön riski	2. Vähäinen riski	3. Kohtalainen riski

Kuva 14. Riskitaulukko [Vahti 7/2003, s. 43]

5.6 HAMKin tärkeimpien palveluiden riskianalyysit

HAMKin kaikkein kriittisimmät palvelut vaativat erityisen huolellista tarkastelua. Seuraavaksi tarkastelen näitä tärkeitä palveluita.

5.6.1 Prima – henkilöstöhallinto ja palkanmaksu

Prima-järjestelmän avulla huolehditaan palkanmaksutietojen ja henkilöstön työsuhdetietojen ylläpidosta. Priman käyttäjiä on henkilöstöhallinnossa 7 henkilöä. Prima-palvelin on palomuurin takana ja siihen on pääsy Priman käyttäjien työasemista sekä muutamasta muusta työasemasta. Prima toimii Digitalin/HP:n Alphaserver -palvelimessa, jossa on Tru64Unix-käyttöjärjestelmä ja Oraclen tietokanta. Priman palvelintietokone on sijoitettu lukittuun laitehuoneeseen, jonne vain rajatulla henkilöjoukolla on pääsy.

Uhkat ja vahingot

Laitevika eli palvelintietokoneen jonkin komponentin vikaantuminen aiheuttaa toimintakatkon, joka kestää sen aikaa, kunnes uusi komponentti on saatu asennettua. Lisäksi saatetaan joutua palauttamaan tietoja varmistuksista, jos tiedostoja on hävinnyt vian seurauksena. Laiteviat ovat niin todennäköisiä, että niihin pitää varautua. Ohjelmistovika voi estää Priman käytön tai korruptoida tietokannan sisällön. Ohjelmistoviat ovat niin todennäköisiä, että niihin pitää varautua.

Merkittävin uhka on vikaantuminen juuri ennen kuin palkkatiedot pitäisi toimittaa pankkiin. Toimitus tapahtuu noin neljää päivää ennen maksupäivää. Tällöin yli kahden päivän käyttökatko saattaa aiheuttaa palkanmaksun viivästymisen. Uhka on niin vakava, että siihen pitää varautua. Vakavassa vikatilanteessa kaikki tiedot ovat tuhoutuneet ja palvelin joudutaan asentamaan uudelleen.

Asiantuntijan puute aiheuttaa viivästystä vioista toipumiseen sekä jonkin Priman päivityksen tai ajon tekemiseen, jos tarvittavan asiantuntemuksen omaavaa henkilö ei ole saatavilla (esim. hän on lomalla). Uhka on todennäköinen ja siihen on varauduttava.

Riippuvuudet muista tietojärjestelmistä voivat aiheuttaa Priman käyttökatkoja tai estää palkanmaksutietojentoimituksen pankkiin. Tietoliikennepalveluiden häiriöt ja kirjanpito- tai maksuliikenneohjelmistojen toimintahäiriöt ovat uhkia, joihin pitää varautua.

Priman käyttäjän työaseman voi joutua vääriin käsiin, jos työasema tai työhuoneen ovi jätetään auki, kun Priman käyttäjä on poissa työhuoneesta. Tämä antaa tunkeutujalle mahdollisuuden käyttää luvatta Primaa ja muuttaa järjestelmän sisältämiä arkaluonteisia tietoja. Uhka on todennäköinen ja siihen on varauduttava.

Uhkiin varautuminen

Laitevikoihin varaudutaan ottamalla laitteistolle huoltopalvelusopimus, joka kattaa kaikki palvelintietokoneen laiteviat. Laiteviat pitää korjata tai ainakin aloittaa korjaus samana arkipäivänä (esim. neljän tunnin vasteaika). Tuhoutuneiden tietojen palauttamiseksi tiedot varmistetaan jokaisen työpäivän päätteeksi, jolloin vain yhden työpäivän tiedot voivat tuhoutua.

Ohjelmistovikoihin varaudutaan varmistamalla tiedot jokaisen työpäivän päätteeksi, jolloin vain yhden työpäivän tiedot voivat tuhoutua. Vanhoja varmistuksia säilytetään viimeiseltä viideltä työpäivältä, neljältä edellisen viikon perjantailta ja kahden edellisen kuun lopulta. Varmistusten avulla voidaan tarvittaessa palata taaksepäin tietokantaan, jonka tiedot eivät olleet korruptoituneita.

Merkittävintä uhkaa voidaan pienentää tai poistaa kokonaan toimittamalla palkkatiedot pankkiin hyvissä ajoin ennen palkanmaksupäivää. Toimitusten ja maksupäivän väliin pitäisi jäädä niin monta päivää, että vakavimmankin häiriön hoitamiseen jää kolme päivää aikaa.

Asiantuntijan puutteeseen varaudutaan riittävän tarkalla dokumentoinnilla ja varahenkilöjärjestelyillä. Jonkun Priman ylläpitotoimenpiteitä osaavan pitää olla aina tavoitettavissa joko työpaikalta tai ääritapauksessa kotoa.

Riippuvuudet muista järjestelmistä aiheuttavat käyttökatkoja, joiden pituus ei saa aiheuttaa palkanmaksujen viivästymistä. Tietoliikennepalveluiden, kirjanpito- tai maksuliikenneohjelmistojen pisin käyttökatko ei saa olla yhtä päivää pidempi.

Priman käyttäjän työasema pitää aina lukita (käyttöjärjestelmän avulla), kun Priman käyttäjä poistuu työhuoneestaan. Pidemmän poissaolon ajaksi työhuoneen ovi on lukittava.

Palvelutasovaatimus

Palkanmaksutietojen toimittaminen pankkiin viivästyy korkeintaan kolme päivää, vaikka kyseessä olisi vakava vikatapaus. Käyttökatkon pituus muissa vikatilanteissa on enintään yksi päivä.

Korkeintaan yhden työpäivän aikana syötetyt tiedot voivat hävitä tietokannasta. Vanhoja tietoja on saatavissa noin kuukauden ajalta.

Priman käyttäjän työasemaa eivät muut henkilöt voi luvatta käyttää.

Vastuu tietoturvasta

Priman palvelimen tietoturvasta vastaa nimetty kehittämisyksikön atk-suunnittelija. Priman työasemien tietoturvasta vastaavat työasemien käyttäjän ja paikallinen tietotekniikkavastaava. Priman palvelutasovaatimuksen määrittelystä vastaa henkilöosastolta nimetty henkilö.

5.6.2 WinhaPro - opetushallinto

WinhaPro-järjestelmän avulla huolehditaan opetushallinnon tietojen ylläpidosta. WinPron käyttäjiä ovat opintosihteerit ja jotkut opettajat. WinhaPron tietokantapalvelin on palomuurin takana ja siihen pääsy WinhaPron käyttäjien työasemista sekä web-liittymien palvelimista. Sovellus toimii tavallisessa Intel-palvelimessa, jossa on Windows-käyttöjärjestelmä ja Solidin tietokanta. WinhaPron palvelintietokone on sijoitettu lukittuun laitehuoneeseen, jonne on pääsy vain rajatulla henkilöjoukolla.

Uhkat ja vahingot

Laitevika eli palvelintietokoneen jonkin komponentin vikaantuminen aiheuttaa toimintakatkon, joka kestää sen aikaa, kunnes uusi komponentti on saatu asennettua. Lisäksi saatetaan joutua palauttamaan tietoja varmistuksista, jos tiedostoja on hävinnyt vian seurauksena. Laiteviat ovat niin todennäköisiä, että niihin pitää varautua.

Ohjelmistovika voi estää WinhaPron käytön tai korruptoida tietokannan sisällön. Ohjelmistoviat ovat niin todennäköisiä, että niihin pitää varautua.

Merkittävin uhka on vikaantuminen juuri opiskelijavalintojen tai kursseille ilmoittautumisten aikaan. Tällöin usean päivän käyttökatko aiheuttaa suurta haitta opetushallinnon toiminnalle. Uhka on niin vakava, että siihen pitää varautua. Vakavassa vikatilanteessa kaikki tiedot ovat tuhoutuneet ja palvelin joudutaan asentamaan uudelleen.

Vioista toipuminen sekä jonkin WinhaPron päivityksen tai ajon tekeminen voi viivästyä, jos tarvittavaa asiantuntijaa ei ole saatavilla (esim. hän on lomalla). Uhka on todennäköinen ja siihen on varauduttava.

Riippuvuudet muista tietojärjestelmistä voivat aiheuttaa WinhaPron käyttökatkoja tai estää palkanmaksutietojentoimituksen pankkiin. Tietoliikennepalveluiden häiriöihin pitää varautua.

WinhaPron käyttäjän työaseman voi joutua vääriin käsiin, jos työasema tai työhuoneen ovi jätetään auki, kun Winhapron käyttäjä on poissa työhuoneesta. Tämä antaa tunkeutujalle mahdollisuuden käyttää luvatta Winhaprota ja muuttaa järjestelmän sisältämiä arkaluonteisia tietoja. Uhka on todennäköinen ja siihen on varauduttava.

Uhkiin varautuminen

Laitevikoihin varaudutaan ottamalla laitteistolle huoltopalvelusopimus, joka kattaa kaikki palvelintietokoneen laiteviat. Laiteviat pitää korjata tai ainakin aloittaa korjaus samana arkipäivänä (esim. neljän tunnin vasteaika). Tuhoutuneiden tietojen palauttamiseksi tiedot varmistetaan jokaisen työpäivän päätteeksi, jolloin vain yhden työpäivän tiedot voivat tuhoutua.

Ohjelmistovikoihin varaudutaan varmistamalla tiedot jokaisen työpäivän päätteeksi, jolloin vain yhden työpäivän tiedot voivat tuhoutua. Vanhoja varmistuksia säilytetään viimeiseltä viideltä työpäivältä, neljältä edellisen viikon perjantailta ja kahden edellisen kuun lopulta. Varmistusten avulla voidaan tarvittaessa palata taaksepäin tietokantaan, jonka tiedot eivät olleet korruptoituneita.

Merkittävintä uhkaa voidaan pienentää laatimalla ohjeet palvelinohjelmiston, tietokantaohjelmiston ja Winha-tietokannan uudelleenasennuksesta.

Asiantuntijan puutteeseen varaudutaan riittävän tarkalla dokumentoinnilla ja varahenkilöjärjestelyillä. Jonkun WinhaPron ylläpitotoimenpiteitä osaavan pitää olla kahden päivän varoitusajalla tavoitettavissa joko työpaikalta tai ääritapauksessa kotoa.

Riippuvuudet muista järjestelmistä aiheuttavat käyttökatkoja, Tietoliikennepalveluiden pisin käyttökatko ei saa olla yhtä päivää pidempi.

Winhapron käyttäjän työasema pitää aina lukita (käyttöjärjestelmän avulla), kun WinhaPron käyttäjä poistuu työhuoneestaan. Pidemmän poissaolon ajaksi työhuoneen ovi on lukittava.

Palvelutasovaatimus

Opetushallinnon järjestelmän käyttökatko on korkeintaan kaksi päivää, vaikka kyseessä olisi vakava vikatapaus. Käyttökatkot pituus muissa vikatilanteissa on enintään yksi päivä.

Korkeintaan yhden työpäivän aikana syötetyt tiedot voivat hävitä tietokannasta. Vanhoja tietoja on saatavissa noin kuukauden ajalta. WinhaPron käyttäjän työasemaa eivät muut henkilöt voi luvatta käyttää.

Vastuu tietoturvasta

WinhaPron palvelimen tietoturvasta vastaa nimetty kehittämisyksikön atk-suunnittelija. WinhaPron työasemien tietoturvasta vastaavat työasemien käyttäjät ja paikallinen tietotekniikkavastaava. WinhaPron palvelu-tasovaatimuksen määrittelystä vastaa opintotoimistosta nimetty henkilö.

5.6.3 Nimipalvelut

Nimipalvelu on tietoliikenneverkkojen ydinpalveluihin kuuluva palvelu, joka muuttaa koneiden IP-osoitteet numeromuodosta ymmärrettävämpään tekstimuotoon ja päinvastoin. Suuri osa palveluista on määritelty käyttämään tekstimuotoa joustavuuden ja palveluiden siirrettävyyden takia. Samoin käyttäjät suosivat poikkeuksetta tekstimuotoisia osoitteita. Nimipalvelua hyödynnetään myös osoite-pohjaisessa autentikoinnissa, joissa esimerkiksi tietyt palvelut rajataan vain hamk.fi–osoitteiden käyttöön. Kun nimipalvelu ei ole käytettävissä, Internet-tekniikoin toteutettujen palveluiden käyttö ei käytännössä onnistu.

Ulkoinen nimipalvelu on toteutettu kahdella Dell PE1550 1U-räkkipalvelimella, jotka on kytketty pieneen HP ProCurve 400 – sarjan kytkimeen. Sisäinen nimipalvelu on toteutettu kahdella Dell PE2550 2U – räkkipalvelimella, jotka on kytketty HP ProCurve 4000 –sarjan kytkimeen. palvelimissa on käyttöjärjestelmänä Redhat Linux ja nimipalvelinohjelmistona Bind.

Uhkat ja vahingot

Ulkoisen nimipalvelun käyttökatkon aikana palvelimille ei voi kohdistaa nimipalvelukyselyjä julkisesta Internet–verkosta. Sähköposti ei löydä perille, koska tietoa postia kuljettavista palvelimista (mx) ei ole käytettävissä. Lyhyet käyttökatkot eivät juuri näy suurimmalle osalle käyttäjiä, koska muut nimipalvelimet tallentavat välimuistiin jo tehdyt nimipalvelukyselyt. Siihen, kuinka kauan tietoa säilytetään ja saadaan säilyttää, vaikutetaan TTL-määrityksellä. Nimipalvelimissa minimum-arvo on yksi vuorokausi ja expire-arvo on seitsemän vuorokautta.

Sisäisen nimipalvelun aikana suurin osa alueverkon palveluista ei ole käytettävissä, työasemille kirjautuminen on normaalia hitaampaa sekä Internet-yhteydet eivät käytännössä toimi. Nimipalvelun käyttökatkot vaikuttavat hidastavasti työasemien kirjautumiseen, sillä Novell asiakasohjelmien SLP-määrityksissä Directory Agent –asetukset on tehty käyttäen palvelimien DNS-nimeä eikä IP-soitetta. Tämä on tehty palveluiden siirrettävyyden takia, näin voidaan esimerkiksi päivityksen yhteydessä tai ongelmatilanteessa vaihtaa DA-palvelu toiselle palvelimelle käyttäjän sitä havaitsematta.

Uhkiin varautuminen

Sähkönsyöttövikoihin on pyritty varautumaan sijoittamalla palvelimet UPS-laitteiston taakse. Sisäisiä nimipalvelimissa on vikasietoinen virtalähde.

Laitteistovikoihin on varauduttu ostamalla laadukas palvelinlaitteisto, jossa on kolmen vuoden takuu. levyrikkoihin on varauduttu joko peilaamalla järjestelmälevyjä tai käyttämällä RAID 5 -levyjärjestelmää.

Ohjelmistovikoihin pyritään varautumaan asentamalla palvelimen käyttöjärjestelmään julkaisemat päivitykset säännöllisin väliajoin (1-2 viikkoa). Käytännössä melkein kaikki X-Window -ympäristöön liittymättömät julkaistut päivitykset ovat kuitenkin tietoturvapäivityksiä. Sen sijaan nimipalvelinohjelmistoon päivitetään valmistajan julkaisemat toiminnallisuuteen vaikuttavat korjaukset vain tarvittaessa, ei kuitenkaan välittömästi uuden version julkaisemisen jälkeen. Ylläpitovirheen aiheuttamia vikoja pyritään välttämään dokumentoimalla tehdyt toimenpiteet ja muutokset.

Nimipalvelimille murtautuminen ja niiden väärinkäyttö on pyritty estämään asentamalla käyttöjärjestelmästä ainoastaan tarpeelliset komponentit ja poistamalla kaikki turhat palvelut käytöstä. Suoraan julkiseen Internetiin liitetyillä ulkoisilla nimipalvelimilla on käytössä paikallinen palomuuri (iptables), joka sallii ainoastaan nimipalvelukyselyt. Nimipalvelinohjelmistoa ajetaan ns. chrootatutussa tilassa, joten nimipalveluohjelmistossa oleva mahdollinen tietoturva-aukko ei mahdollista koneen hyödyntämistä kovinkaan

helposti. Mahdollinen murtautuja näkisi ainoastaan tietyn määrätyn osan levyjärjestelmästä normaalikäyttäjän oikeuksin. Ulkoisille nimipalvelimille ei voi myöskään kirjautua lainkaan verkon kautta, vaan ainoastaan palvelimen konsolilta. Palvelimien käyttöjärjestelmään päivitetään valmistajan julkaisemat tietoturvapäivitykset säännöllisin väliajoin (1-2 viikkoa) tai heti kriittisestä tietoturva-aukosta tiedottamisen jälkeen. Nimipalvelinohjelmisto päivitetään valmistajan tietoturvakorjauksilla heti mahdollisen ilmoituksen jälkeen.

Palvelinhuoneen sisällä mahdollisesti tapahtuviin verkkovikoihin on varauduttava varalaitteistoilla. Ulkoisia nimipalvelimia varten on olemassa erillinen varakytkin, joka voidaan vaihtaa rikkoutuneen laitteen tilalle. Sisäiset nimipalvelimet voidaan yksinkertaisesti kytkeä toiseen kytkimeen (kehikossa on kolme mahdollista kytkintä).

5.6.4 Portaalijärjestelmä

Nykyinen järjestelmä on portaali, jonka sisälle on rakennettu aikaisemmin hajallaan olleet www-palvelut uudestaan. Portaali-järjestelmässä on toteutettu sisällönhallinta ja käyttöoikeuksien hallinta. Intranet sivusto korvautuu myös portaalilla. Portaaliympäristö on toteutettu Oracle 10 G -tekniikalla ja kaikki toiminnot ja laitteet on kahdennettu. Palvelinhierarkia on kolmetasoinen.

Erilaiset uhkat ja niihin varautuminen

Sähkönsyöttövikoihin on pyritty varautumaan sijoittamalla palvelimet UPS-laitteiston taakse. Laitteistovikoihin on varauduttu ostamalla laadukas palvelinlaitteisto, jossa on kolmen vuoden takuu. levyrikkoihin on varauduttu joko peilaamalla levyjärjestelmälevyjä tai käyttämällä RAID 5 -levyjärjestelmää.

Ohjelmistovikoihin pyritään varautumaan asentamalla palvelimen käyttöjärjestelmään julkaisemat päivitykset säännöllisin väliajoin (1-2 viikkoa). Käytännössä melkein kaikki X-ympäristöön liittymättömät julkaistut päivitykset ovat tietoturvapäivityksiä. WWW-palvelinalustan (Apache, MySQL, PHP, Tomcat) julkaistut päivitykset testataan ensin testiympäristössä, minkä jälkeen päivitykset suoritetaan tuotantoympäristöön.

Ylläpitovirheen aiheuttamia vikoja pyritään välttämään dokumentoimalla tehdyt toimenpiteet ja muutokset. Ylläpitovirheitä voi myös aiheutua tahattomasti päivitysten yhteydessä, kun esimerkiksi uusi versio PHP-skriptikielestä toimiikin hieman eri tavalla kuin edellinen versio.

WWW-palvelimelle murtautuminen ja sen väärinkäyttö on pyritty estämään asentamalla käyttöjärjestelmästä ainoastaan tarpeelliset komponentit ja poistamalla kaikki turhat palvelut käytöstä. Palvelimelle asennetaan useita ns. shell-käyttäjiä: henkilökuntaa (kehy, tietojenkäsittely), opiskelijoita (julkaisun harjoittelijat, automaint) sekä yrityksiä (Ambientia, Paperjam). Shell-käyttäjiä varten palvelimelle on toteutettu chroot-ympäristö, jossa WWW-sivustoja

ylläpitävät henkilöt näkevät vain tietyn, rajatun alueen palvelimen levyjärjestelmästä. Erilaiset ylläpitotyökalut (esim. PHPMyAdmin, jolla hallinnoidaan MySQL-kantoja) on toteutettu niin, että kukin käyttäjä pääsee käsiksi vain omiin kantoihinsa.

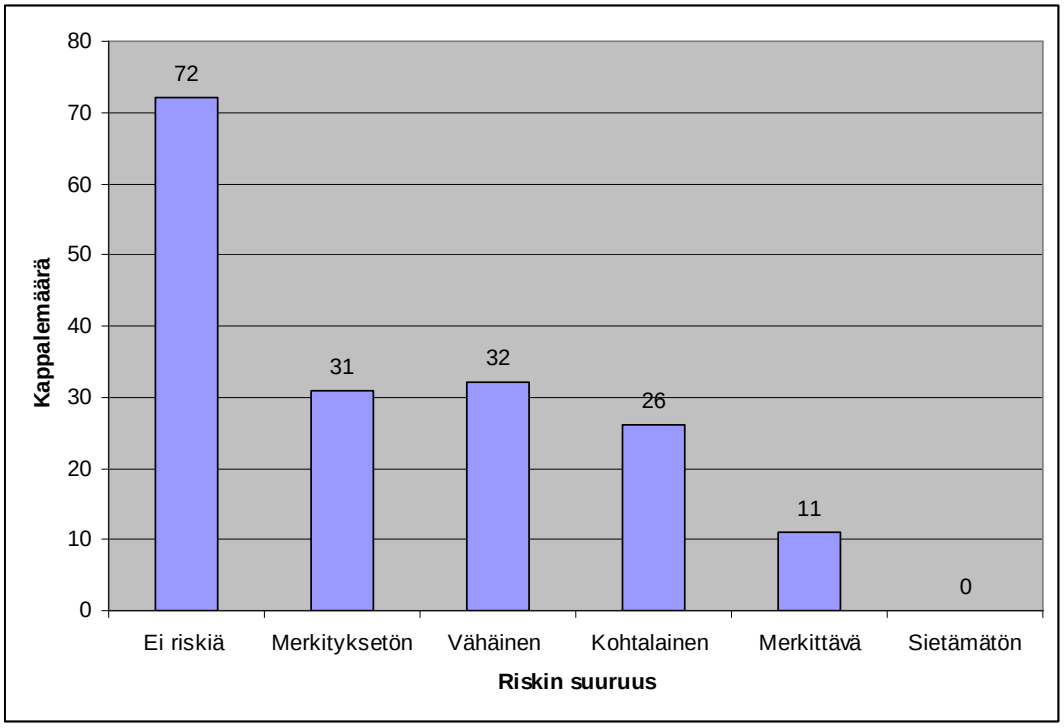
Verkkoon liitetään ainoastaan palvelimia, joilla on nimetty ylläpitäjä. Ylläpitäjä huolehtii palvelimen tietoturvasta, siihen liittyvistä asetuksista ja päivityksistä. Lähiverkkojen turvallisuutta voidaan tarkastella säännöllisesti skannausohjelmistolla, joka etsii tunnettuja tietoturva-aukkoja ja virheellisiä määrityksiä. Skannausohjelmisto voisi olla esim. Nessus keskitetysti Funetin tyyliin:

- Nessus-palvelin kehyssä (huolehditaan ajantasaisista versioista ja ”sormenjälkitiedoista”)
- Nessus-client yksiköissä ja kehyssä (palvelinta käytetään clientin kautta)
- Funtilla on myös Nessus-server, jolle voidaan määrittää 1-2 käyttäjää HAMK-verkosta. Tämän avulla voidaan tarkastella tietoturvaa HAMK-verkon ulkopuolelta

5.7 Riskianalyysien tulokset

Riskianalyysien tavoitteena oli löytää HAMKiin kohdistuvat riskit. Tulokset kertovat tietoturvallisuuden tasosta ja siitä, miten tietoturvallisuutta hoidetaan. Riskien pienentämisellä tai poistamisella on suuri vaikutus tietoturvaan. Kuva 15 kertoo löydettyjen riskien määrästä. Jokaiselta riskianalyysien osa-alueelta löytyi jotain korjattavaa, sillä riskejä oli lukumääräisesti runsaasti. Ilahduttavaa oli huomata, että sietämättömiä riskejä ei havaittu yhtään ja suurin määrä riskeistä oli pieniä. Merkittäviä riskejä oli 11 kappaletta. On kuitenkin muistettava, että osa riskeistä saattoi jäädä pimentoon, sillä niitä ei yksinkertaisesti vielä tunnistettu. Kaikkien tärkeimmät palvelut oli kuitenkin suojattu hyvin, mutta vain muutaman tuntien katkoksien sieto tarkoittaa sitä, että ongelmien sattuessa korjaustoimenpiteiden on oltava todella nopeita ja ennalta suunniteltuja.

Riskien hoitaminen tulee aloittaa suurimmista, sillä niiden seuraukset ovat vakavimmat. On syytä myös huomioida pienemmät riskit, sillä niiden korjaaminen voi olla nopeaa ja yksinkertaista.



Riskin suuruus	*Ei riskiä*	*Merkityksetön*	*Vähäinen*	*Kohtalainen*	*Merkittävä*	*Sietämätön*
Löydettyjen määrä	**72**	**31**	**32**	**26**	**11**	**0**

Kuva 15. Löydetyt riskit

Suurimpia riskejä olivat: organisaation omaisuutta ja tietoja ei ole konkretisoitu tietoturvapolitiikassa ja säännöissä, tietoturvapolitiikan keskeneräisyys, tietoturvasuunnitelman puuttuminen, tietojenkäsittelytapojen ja turvajärjestelyjen arvioinnin puutteellisuus, tietoturvaperiaatteiden puuttuminen, suullisen viestinnän ja paperidokumenttien käsittelyn ohjeistuksen puuttuminen, henkilöstön puutteellinen tietoturvakoulutus, tietoturva-asiat eivät ole mukana työntekijöiden työhön perehdyttämisessä, tietoturvapolitiikan merkitystä ei selvitetä uusille ja väliaikaisille työntekijöille, työntekijät eivät kirjoita erillistä sitoumusta tietojen ja järjestelmien käytöstä, tärkeitä laitetiloja ei ole sijoiteltu pois viemärien ja putkistojen läheisyydestä, laitetilat ovat alttiita lämpötilan vaihteluille. Merkittävistä riskeistä voidaan päätellä HAMKilla olevan vakavia puutteita:

- Tietoturvallisuuden hallinnan johtamisessa,
- Henkilöstön koulutuksessa
- Laitetilojen suojaamisessa.

Uhkat ovat HAMKille todellisia. Tätä kuvaavat esimerkiksi HAMKin historiassa tapahtuneet tietomurto ulkoistetulle palvelimelle palvelunestohyökkäyksen järjestämiseksi vuonna 2004 ja työtapavirheestä johtunut eräiden ohjelmistojen tahaton jakaminen ulkopuolisille suojamattomassa intranetissä 2002.

Riskien hallinta tulee vastuuttaa ja riskien jatkokäsittelylle asettaa suunnitelmat. Riskianalyysejä on tarkoitus suorittaa tarpeeksi usein ja uudistaa riskien määrittelyitä ja lisätä uusia uhkia, jotta pysytään ajan tasalla riskienhallinnassa. Ajan kuluessa ja olosuhteiden muuttuessa aiemmin riskitön tai merkityksetön riski saattaa kasvaa suuremmaksi. Riskejä selvittämällä organisaation johto ja tietoturvallisuudenhallintajärjestelmän ylläpitäjät saavat arvokasta tietoa siitä, mitä organisaatiossa on suojeltava. Tulokset on huomioitava tietoturvapolitiikassa ja tietoturvallisuuden kehittämisessä.

6 Suojattavien kohteiden lukitus ja valvonta

ITILin tavoitteena on luoda lähestymistapa turvallisuusmenetelmien implementoimiselle ja organisaation omaisuuden suojauksien ylläpitoon [ITIL, 2004].

Yhteenvetona tarvittavista menetelmistä BS 7799:ssä ovat vastuuvelvollisuuksien määrittäminen omaisuudelle, kuten tärkeimmille tietolähteille ja järjestelmille ja kaikille tietovarannoille. Muita tietovarantoja ovat ohjelmistot ja sovellukset, laitteistot, dokumentaatiot ja menetelmät. Tiedot on luokiteltava ja on tarpeellista erottaa luottamuksellisuus, eheys ja saatavuus luokittelussa. On kiinnitettävä huomiota luokittelun suorittamisen sääntöihin, jolloin on päätettävä, miten implementoidaan, kuka on vastuussa implementoinnista, käytetäänkö fyysisiä merkintöjä ja kuinka kauan luokitus on voimassa [BS 7799-1:fi, 2000].

6.1 Vastuu suojattavista kohteista

Tavoite on pitää yllä organisaation suojattavien kohteiden riittävää suojausta. Kaikki merkittävät suojattavat kohteet pitää luetteloida ja määritellä niille omistajat. Turvamekanismien toteuttamisvelvollisuudet voidaan jakaa, vaikka vastuun tulee pysyä kohteen nimetyllä omistajalla [BS 7799-1:fi, 2000].

ITIL käsittelee vastuita seuraavilla määritelmillä. Prosessin on tarkoitus kontrolloida kaikkia atk-infrastruktuurin komponentteja ja niihin liittyviä käytäntöjä ja dokumentaatioita tukemalla muita prosesseja, jotta voitaisiin tarjota korkealaatuisia palveluja oikeutetuilla kustannuksilla alati muuttuvien käyttäjävaatimusten keskellä [ITIL, 2004].

Suojattavat kohteet on luetteloitava, jotta varmistetaan kohteiden suojauksen tehokkuus. Suojattavia kohteita voivat olla tietoaineistot kuten tietokannat ja tiedostot, ohjelmistot, fyysiset kohteet, kuten tietolaitteet ja toimitilat ja palvelut, kuten tietojenkäsittely ja -tietoliikennepalvelut sekä yleishyödylliset palvelut kuten lämmitys ja valaistus.

6.2 Tiedon luokitus

Tavoite on varmistaa, että suojattavilla kohteilla on riittävä suojaus. Turvaluokitusta tulee käyttää turvallisuussuojauksen tarpeen ja tärkeysjärjestyksen ilmaisemiseen [BS 7799-1:fi, 2000].

Kohtaan kuuluvat luokitusohjeet ja -kategoriat, tiedon merkitseminen ja käsittely sisältäen kopioimisen, tallentamisen, tiedonvälityksen postitse, faksilla ja sähköpostitse, tiedonvälitys puhutussa muodossa, matkapuhelimet, ääniposti ja vastaajat mukaan luettuna, sekä tiedon hävittäminen. ITILissä on mainittu esimerkkinä erilaisia luokitustyyppejä ja korostetaan, että luokitusjärjestelmä on aina räätälöitävä kohdeorganisaation mukaan. On suositeltavaa käyttää vain

yhtä luokitusjärjestelmää koko organisaatiossa. Esimerkkejä luokitteluista on alla [ITIL, 2004].

Luottamuksellisuus:
Korkea = Henkilötietoja, terveystietoja, strategista tietoa, HAMKissa esim. ”rahaa per opiskelija”
Keskisuuri = Sisäinen, ei saa päästä organisaation ulkopuolelle, HAMKissa esim. työilmapiiritutkimus
Matala = Ulkoinen, kaikki mille sallitaan pääsy organisaation ulkopuolelle

Eheys:
Korkea = Rahaliikenne, pankkiliikenne, ohjelmisto, henkilötiedot
Keskisuuri = Mittausdata, nimi ja osoitetiedot
Matala = Ei vaatimuksia

Saatavuus:
Korkea = 24 tuntia päivässä, 99,5 %, HAMKissa esim. lukitusjärjestelmä
Keskisuuri = 07:00–19:00, 99 %
Matala = Ei takeita

Viralliset: Salainen, luottamuksellinen, rajoitettu, luokittelematon
NATO: Cosmic Top Secret, NATO Secret, NATO Confidential, NATO Restricted, NATO Unclassified

6.3 HAMKin suojattavien kohteiden lukitus ja valvonta

HAMKin suojattavien kohteiden lukitus ja valvonta ovat kunnossa. Tämä voidaan perustella riskianalyysien tulosten perusteella. Valvonta- ja lukitusmenettelyt ovat sopivaa tasoa HAMKin tyyppiselle julkiselle organisaatiolle. Rikosturvallisuudesta on huolehdittu asianmukaisilla hälytys- ja murtosuojauksilla sekä vartioinnilla.

Parannusehdotuksena olisi kuitenkin suojattavien kohteiden luettelointi, jossa olisi kuvattu myös kohteista vastaavat henkilöt ja lukitus- ja valvontamenetelmät. Tiedon luokitteluun ei HAMKissa ole tarvetta, sillä suojattavia tietoja kuten henkilötietoja käytetään asianmukaisesti. Ei olisi kuitenkaan haitaksi, jos luokittelu otettaisiin käyttöön.

7 Henkilöstöturvallisuus

Mikään yritys tai organisaatio ei toimi ilman työntekijöitä. Henkilöstön osuus tietoturvasta on erittäin suuri, sillä toisin kuin tekniset tietoturvaratkaisut voidaan ostaa helpostikin rahalla, pätevää ja motivoitunutta henkilöstöä ei voi ostaa kaupan hyllyltä. On tärkeää, että henkilöstö otetaan kokonaisvaltaisesti tietoturvan kehittämisprosessissa huomioon. Tietoturva toimii vain silloin, kun sen suunnittelussa, toteutuksessa ja koulutuksessa otetaan henkilöstöturvallisuus huomioon ja henkilöstö puolestaan ymmärtää omat vastuunsa ja on motivoitunut toimimaan turvallisesti.

Peruskäyttäjää lähinnä ovat arkipäivän työrutiinit. Työntekijän vastuulla ovat myös hänelle kuuluvat, eri muodoissa olevat tiedot kuten mapit, muistiot ja tiedostot ja työvälineet kuten tietokoneet sekä matkapuhelimet. Tavoite ITILin mukaan on työntekijöiden käyttäminen parhaimmalla mahdollisella tavalla sekä ylläpitää tarvittavaa tietämystä ja kokemusta tietoturvallisuuden takaamiseksi [ITIL, 2004]. Näin voidaan myös vähentää riskejä, joita voi syntyä tahattomista ja tarkoituksellisista toimista. Työntekijöille tärkeimpiä ovat tietoturvan perusasiat, jolloin vaativammat asiat voidaan hyvin jättää asiantuntijoiden vastuulle, kunhan on olemassa hyviksi todettuja käytäntöjä ja toimintaohjeita monimutkaisempien tilanteiden varalle. Järvinen [2002, s. 17 ja 34] toteaakin arkipäiväisten uhkien olevan suurin uhka tavalliselle käyttäjälle. Työntekijä sitoutuu useisiin organisaation vaatimuksiin allekirjoittaessaan työsopimuksensa. Näitä ovat esimerkiksi vaitiolovelvollisuus ja tietotekniikkaan liittyvät käyttösäännöt. Ongelmia kuitenkin aiheuttavat tällaisten sopimusten puuttuminen ja koulutuksen sekä ohjeistuksien puutteellisuudet.

Yhteenvetona BS 7799:ssä henkilöstöturvallisuuden menetelmistä ovat työnkuvien määrittely, työntekijöiden seulonta, koko henkilöstön koulutus, tietoturvahäiriöihin reagoiminen, tietoturvahäiriöiden raportoinnin rohkaiseminen, kurinpitotoimet ja yhtenä tärkeimmistä tietoturvatietoisuuden lisääminen [BS 7799-1:fi, 2000].

On työntekijöiden aliarvioimista, jos oletetaan, etteivät he tiedä tietoturvasta mitään. On olemassa työntekijöitä, jotka ovat ajan tasalla tietoturvasta omien harrastusten, aikaisemman koulutuksen tai työtehtävien vuoksi. Järvinen [2002, s. 120] onkin sitä mieltä, että osaaminen voi olla myös vaaraksi: on helppo alkaa kokeilla ja säätää omin luvin kun osaa. Lisäksi muita valvovien työntekijöiden ja ylläpitohenkilöstön työetiikan on oltava oikealla tasolla. Tietoturvallisuus on yhteinen asia ja yksikään työntekijä tai johtaja ei voi asettua sen ulkopuolelle työstään tai asemastaan huolimatta. Lait ja säädökset määräävät viime kädessä, mitä saa tehdä ja mitä ei, mutta määräysten toteutuminen vaatii valvontaa.

Tietoturvaa ei kuitenkaan hallita lakien avulla. Luvussa 14 käsitellään tarkemmin tietoturvaa ja etiikkaa.

7.1 Tietoturvallisuus työtehtävien määrittelyssä, resursoinnissa ja ylläpidon ohjeistuksessa.

Tietoturvallisuuden parantamisen tavoitteet työtehtäviin liittyen ovat vähentää suojattavien aineistoihin kohdistuvaa inhimillisen (henkilön aiheuttaman) virheen riskiä sekä varkaus-, petos- ja väärinkäytösriskejä.

Henkilöstöturvallisuuteen kuuluvia menetelmiä ovat turvallisuuden huomioiminen työtehtävien kuvauksessa, sopivan henkilöstön valinta ja toimintaperiaatteet palkkauksessa ja rekrytoinnissa, salassapitositoumusten käyttö ja työsopimuksen ehdot. Ylläpidon ohjeistuksilla ja säännöillä pidetään huoli myös ylläpidon toiminnasta ja periaatteista.

Valvojiakin on valvottava, sillä ylläpidolla on erityisasema tietoturvallisuudessa. Yliopistojen tietoturvasivuilla olevilla tietojärjestelmien ylläpitosäännöillä otetaan kattavasti kantaa tietojärjestelmien ylläpitäjien erilaisiin velvollisuuksiin ja valtuuksiin. Valtuuksien ja vastuiden lisäksi määritellään toimintaperiaatteet toimintakäytäntöjä, sääntöjen valvonta sekä lainsäädännön vaatimuksia edellä mainituille.

7.2 Käyttäjien koulutus

Tavoite on varmistaa, että käyttäjät ovat tietoisia tietoturvallisuuteen kohdistuvista uhkista ja niiden merkityksestä ja että heillä on keinot tukea organisaation turvallisuuspolitiikkaa tehdessään normaalia työtään toimimalla toimintaohjeiden mukaan. Kaikille työntekijöille on annettava perustiedot tietoturvasta ja otettava huomioon eri kohderyhmien tarpeet koulutusta suunniteltaessa. Yksi suurimmista haasteista Järvisen mukaan on saada työntekijät ymmärtämään miksi rajoitukset ja ohjeet ovat heidän oman etunsa vuoksi olemassa [2002, s. 122]. Järvinen myös toteaa myös kieltojen luettelemisen olevan paljon huonompi tapa kouluttaa kuin näyttää käytännön esimerkkejä.

Käyttäjät tulee kouluttaa toimimaan turvallisuusohjeiden mukaan ja käyttämään tietojenkäsittelypalveluja oikein mahdollisten turvallisuusriskien minimoimiseksi. Tietoturvallisuuskoulutuksella ja -harjoittelulla annetaan organisaation työntekijöille tarvittava koulutus. Miettinen ehdottaa [1999, s. 158] peruskoulutuspakettiin kuuluviksi seuraavia asioita: tietoturvallisuuden merkitys organisaation liiketoiminnalle, tietoturvallisuuden peruskäsitteet, tietoturvallisuuden osa-alueet, tietoturvallisuusasioiden vastuut organisaatiossa, tietoturvallisuuden erityispiirteet organisaation toimialalla, tietoturvallisuus työntekijän lähiympäristössä (työasemien suojaaminen,

tietokonevirusten torjuminen, etätyö ja tietoturvallisuus työmatkoilla, tietoaineiston luokittelu ja käsittely (henkilötiedot, sisäiset asiakirjat), tietoturvallisuusongelmien ja väärinkäyttötapausten raportointi, tietoturvallisuuden yhteyshenkilöt organisaatiossa ja lisätietojen hankinnassa. Koulutuksen järjestäminen on vasta ensimmäinen askel henkilöstön tietoturvatietoisuuden lisäämisessä. Koulutuksen sisällön on oltava kiinnostavaa ja selkeää, jotta siitä oikeasti jäisi jotain muistiin. Lisää koulutusasioita on VAHTI Internet-tietoturvallisuusohjeessa [VAHTI, 1/2003].

Tietoturvan yleisiä periaatteita

1. Yleisiä periaatteita
2. Mukavuus * tietoturva = vakio
3. Toisto on turvallisuuden vihollinen
4. Vahingon torjunta on halvempaa kuin vahingon korjaaminen
5. Tiedolla on taipumus levitä
6. Usko hyvästä tietoturvasta on vaarallisempaa kuin tieto huonosta
7. Käyttäjä itse on puolustuksen ensimmäinen lenkki
8. Ainoa täysin turvallinen järjestelmä on sellainen jossa ei ole yhtään käyttäjää
9. Todellista tietoturvaa ei voi ostaa kaupasta
10. Tietoturva on 20 % tekniikka ja 80 % psykologiaa
11. Haluamme lisää valvontaa muille ja lisää yksityisyyttä itsellemme
12. Yksityisyyden voi menettää vain kerran

Järvisen mielestä [2002] seuraavat alueet tulisi ohjeistaa:

- Tietokoneet
- Internetin käyttö
- Sähköposti
- Yrityksen (organisaation) verkkosivut
- Arkipäivän toiminta
- Etätyö

Ohjeistamista ei pidä ajatella pelkästään tietoturvan kannalta, ohjeita tarvitaan myös perusasioiden opettamiseen. Tietotekniikasta ei voi saada kaikkea irti, jos jokaisen työntekijän pitää omin avuin selvittää, miten kukin ohjelma tai laite toimii. Perusasioiden ohjeistamisella vähennetään turhautumisen ja virheiden aiheuttamia ongelmia. Uusien työntekijöiden perehdyttämisessä on hyvä ottaa tietoturva-asiat opetukseen mukaan luonnollisena osana.

7.3 Poikkeus- ja virhetilanteisiin reagoiminen

Tavoite on minimoida poikkeustilanteiden ja toimintahäiriöiden aiheuttamat vahingot, tarkkailla kyseisiä tilanteita ja ottaa niistä oppia. Poikkeustilanteista tulee raportoida mahdollisimman nopeasti. Odottamia tapahtumia ja häiriöitä varten täytyy olla menettelytapoja, joilla asiat voidaan ratkaista. Jos johto ja tietoturva-asioista vastaavat eivät saa tietoa tapahtumista, on vaikea hallita ja tietää tietoturvan todellinen taso.

Reagoimiseen kuuluvat poikkeustilanteista raportoiminen, turvallisuuden heikkouksista raportoiminen, ohjelmistojen toimintahäiriöistä raportoiminen, poikkeustilanteista oppiminen ja sanktiomenettelyt. Tähän sopii vielä esimerkiksi malli erikoistilanteiden toimintaohjeista. Käyttäjien koulutuksella mahdollistetaan se, että haluttu reagointi on edes mahdollista.

7.4 HAMKin henkilöstöturvallisuus

HAMKissa ei ole henkilöstöntasolla huomioitu tietoturvallisuutta yleisesti. Tietoturvakoulutusta ei ole järjestetty. Muutamia ohjeita on henkilöstölle toimitettu ja uhkien, erityisesti virusepidemioiden, aikana heitä on ohjeistettu vielä erikseen. Työntekijöiden tietoturvallisuustietoisuus on varsin vaihtelevaa. Tietyissä toiminnoissa kuten talous-, henkilöstö- ja opiskelijahallinnossa tietoturvallisuustietoisuus on melko hyvä. Tietoturvataitojen kehittäminen on selvästi tarpeellista. Tietoturvaongelmista on ollut haittaa työntekijöille, sillä muutama virusepidemia on aiheuttanut tietoliikenneongelmia ja muutamia saastuneita koneita on suljettu muutamaksi päiväksi. Varsinkin virusepidemioita voitaisiin estää, jos henkilökunta osaisi toimia oikein.

Yleisellä tasolla HAMKin henkilöstöturvallisuuden parantamiseksi on luotava ja päivitettävä ohjeita päivittäiseen työskentelyyn ja tietoturva-asioihin. Näiden edellä mainittujen ohjeistamisessa käytän apuna yliopistojen yhteisen U-CIRT –työryhmän tekemiä Yliopistojen tietoturvasivuilla olevia mallipohjia [Yliopistojentt, 2006]. Vuoden 2007 tammikuussa HAMKissa on aloittanut työnsä uusi henkilöstöpäällikkö, joten hänellä on mahdollisuus ottaa tietoturva-asiat huomioon henkilöstön johtamisessa.

Tietoturvapoikkeamisen ohjeistus voidaan tehdä yliopistojen tietoturvasivuilla olevan tietoturvan poikkeamiin reagointi-ohjeen [Liite 6] mukaan. Tämä ohjeistus tarjoaa kattavan tietoturvapoikkeamien reagointisuunnitelman tarkoituksen ja soveltamisalan, tietoturvapoikkeamien käsittelyn, organisaation roolin, reagoimisen tietoturvapoikkeamiin sisältäen poikkeamien vakavuuden arvioinnin, vastatoimien laajentamisen, toimintavastuut, viranomaisilmoitukset, tietoturvapoikkeaman jälkeisen toiminnan, tiedottamisen ja ohjeen päivittämisen.

Ohjeessa ehdotettua periaatetta ”suunnittele, kouluta ja harjoittele” on hyvä miettiä tarkemmin. Suunnitteluvaiheessa mietitään mitä, miten, kenelle ja milloin koulutetaan. Koulutusvaiheessa valitut asiat koulutetaan työntekijöille. Viimeinen vaihe on myös tärkeä, sillä opitut asiat on harjoiteltava, jotta voidaan varmistua, että opetus on mennyt perille ja toiminta on halutun laista. Liian monimutkaiset tai vastaavasti liian suppeat ohjeet eivät hyödytä työntekijöitä.

Poikkeamatilanteiden ohjeistus voidaan tehdä yliopistojen tietoturvasivuilla olevan mallin [Liite 7] mukaan. Tiedottamisen tulee olla informoivaa, ohjaava, ohjeistavaa ja rauhoittavaa ja sen perustarkoituksena on ylläpitää tietoisuutta tosiasioista ja toimenpiteistä. Tiedottamisen tulee ehtiä väärien tietojen edelle. Vastuun tiedottamisesta tulee pysyä yksissä käsissä. Kaikista toimista informoidaan ainakin niitä henkilöitä, joiden toimintaan ne vaikuttavat. Ohjeessa käydään läpi menetelmät poikkeamisesta tiedottamiseen, tiedotuskanavat ja toimenpiteet poikkeaman jatkuessa sekä annetaan esimerkkejä tiedotteiden sisällöstä.

Sähköpostin käytön ohjeistamisessa voidaan käyttää mallina yliopistojen tietoturvasivuilla olevaa sähköpostin käsittelysäännöt -ohjetta [Liite 4]. Näissä ohjeissa määritellään sähköpostiviestit ja –osoitteet sekä niiden käsittely, käsitellään erikoistoimenpiteitä vaativat viestit, sähköpostin käsittely erikoistilanteissa, sähköpostin salaus ja todentaminen, sähköpostin käytön valvonta sekä lokitietojen kerääminen ja säilyttäminen ja sääntöjen valvonta.

Tietojärjestelmien käytön ohjeistus voidaan tehdä yliopistojen tietoturvasivuilla olevan tietojärjestelmien käyttösäännöt -ohjeen mukaisiksi. Kyseisissä ohjeissa käydään läpi sääntöjen tarkoitus, käytön periaatteet, käyttöoikeudet ja käyttäjätunnukset, käyttöoikeuden voimassaolo ja tietojärjestelmien ylläpito.

Tietotekniikkarikkomusten käsittelyä voidaan ohjeistaa lisää yliopistojen tietoturvasivuilla olevan tietotekniikkarikkomusten käsittelysääntöjen [Liite 2] mukaan. Ohjeissa käydään läpi käyttöoikeuksien rajoittaminen selvitystyön ajaksi ja esitellään eritasoisia seuraamuksia rangaistusmenetelmiksi. Nykyiset rikkomusmenettelyt löytyvät Hämeen ammatillisen korkeakoulutuksen kuntayhtymän tietotekniikkapalveluiden käyttösäännöistä [Liite 9].

HAMKissa tulisi lisätä tietoturvakoulutuksen määrää. Tietoturvallisuuden yleisten asioiden peruskoulutuspaketti voisi kestää noin puoli päivää ja jokaisella työntekijällä tulisi olla mahdollisuus vähintään näiden perusasioiden koulutukseen. HAMKin verkkosivuja voidaan käyttää materiaalin itseopiskeluun, mutta sillä ei voi täysin korvata koko koulutusta. Koulutusta varten olisi hyvä luoda koulutussuunnitelma, josta selviää minkälaista koulutusta ja kenelle sitä annetaan, millä aikataululla koulutus järjestetään sekä muutama yksinkertainen koulutussuunnitelman pohja. VAHTIn tietoturva

2004 cd:ssä on koulutus- ja opetusmateriaalia, jota voidaan muokata HAMKille sopivaksi [Vahti CD, 2004]. HAMKin portaaliin on luotava keskitetty paikka, jonne kerätään tietoturvaohjeita ja –tiedotuksia. Tällaisista tietoturvasivustoista on kerrottava myös työntekijöille.

8 Fyysinen turvallisuus ja ympäristön turvallisuus

Fyysinen turvallisuus vaatii Järvisen [2002, s. 50] mukaan lukkoja ja salasanoja. Näillä keinoilla voidaan parhaiten suojata pääsyä eri kohteisiin. ITILin fyysisen turvallisuuden tavoitteena on estää luvaton tai tarpeeton fyysinen pääsy tietoon ja tietojärjestelmiin [2004]. Näin pyritään estämään tietojen luvaton tutkiminen, tuhoaminen, varkaus ja tietojärjestelmien häiritseminen ja vahingoittuminen. Osana tavoitteita on myös luoda ympäristö, joka edesauttaa tietojen ja tietojärjestelmien turvallista käyttöä.

Yhteenvetona BS 7799:ssä fyysisen turvallisuuden menetelmistä ovat turva-alueet, jotka mahdollistavat tietotekniikkatilojen käytön kriittisten tai arkaluonteisten liiketoimintatoimintojen suorittamiseen. Fyysinen turvallisuus tarkoittaa niiden tilojen määrittämistä, jotka pitää fyysisesti suojata. Erityisen tärkeää on suojata tietokonetilat. Saatavuuden fyysisellä kontrolloinnilla suojellaan turva-alueille ja tiloihin pääsyä käyttämällä sopivia kulunvalvontakeinoja, kuten kulkukortteja ja avaimia. Tavaroiden ja ihmisten tuomis- ja viemisalueiden on oltava eristettyjä. Työntekijän tasolla puhtaan työpöydän periaatteella ei pidetä tietoja turhaan esillä ja korjataan paperit pois, kun työskentely lopetetaan. Samoin istuntojen ja tietokonelaitteiden fyysisestä ja sähköisestä turvallisuudesta on pidettävä huolta [BS 7799-1:fi, 2000].

Organisaation (vanhentuneiden) varojen tuonti ja vienti on määriteltävä ja tämä koskee myös poistettavaa laitteistoa. Laitteistoja on suojattava fyysisesti, tämä koskee myös laitteita, joita käytetään organisaation ulkopuolella. Tärkeimpien laitteiden virransyöttö on turvattava. Kaapeloinnin turvallisuudessa on huomioitava, että puhelin-, sähkö- ja verkkokaapeloinnit on tehty turvallisesti ja niiden kuntoa voidaan tarkkailla silmämääräisesti vikojen sekä salakuuntelun selvittämiseksi. Laitteiston ylläpito on hoidettava sekä otettava huomioon, kuka saa huoltaa ja mitä huollettavien laitteiden tietosisällöille tehdään ennen huoltoa.

8.1 Turva-alueet

Turva-alueiden käytön tarkoituksena on estää luvaton tunkeutuminen organisaation toimitiloihin ja tietoaineistoihin sekä estää niiden vahingoittuminen ja toiminnan häiriintyminen.

Liiketoiminnan kannalta kriittisten tai arkaluontoisten tietojenkäsittelylaitteistojen ja toimintojen tulee olla suojattu. Tämä toteutetaan fyysisillä turva-alueilla, kulunvalvonnalla, toimistojen, tilojen ja laitteistojen suojauksilla, turva-alueilla työskentelyn määrittämisellä sekä eristetyillä toimitus- ja kuormausalueilla. Suojausjärjestelyt tulee mitoittaa tunnettujen riskien mukaan. Puhtaan työpöydän ja puhtaan kuvaruudun periaatteen

noudattaminen on suositeltavaa, jotta vähennettäisiin luvattoman tunkeutumisen tai vahinkojen riskiä.

8.2 Laiteturvallisuus

Laiteturvallisuuden huomioimisen tarkoituksena on estää omaisuuden häviäminen, vahingoittuminen tai vaarantuminen sekä liiketoiminnan keskeytyminen. Laitteet tulee suojata fyysisesti turvallisuusuhkia ja ympäristön uhkia vastaan. Erityisiä riskejä aiheuttavat tilat, joita ei ole varta vasten suunniteltu käyttötarkoitukseen, kuten esimerkiksi palvelinten sijoittaminen vesiputkien läheisyyteen tai tiloihin, joissa ei ole vaadittavaa jäähdytystä.

Laiteturvallisuus sisältää laitteiden sijoituksen ja suojauksen (pääsy, tietojen luvaton näkyminen, eristäminen, turvamekanismit, tuli, vesi, varkaudet, syöminen laitteiden läheisyydessä, onnettomuudet jne.) virransyöttökaapeloinnin turvallisuuden, laitteiden huollon ja toimitilojen ulkopuolelle vietyjen laitteiden turvallisuuden, laitteistojen turvallisen käytöstä poistamisen ja kierrättämisen. Asianmukaisilla asennuksilla ja käyttötarkoituksiin soveltuvilla tiloilla voidaan jo suojautua yleisimmiltä uhkatekijöiltä ja ympäristön aiheuttamilla uhkilla. Turvallisuuden ylläpitämiseen vaaditaan laitteiden ja tilojen ylläpitoa ja huoltoa sekä lukituksien valvontaa. Jos ja kun ongelmia ilmenee, on oltava luotuna ja testattuna jatkuvuussuunnitelmat ja mahdolliset varalaitteistot toiminnan katkeamattomuuden takaamiseksi. Laitevalmistajat määrittävät laitteidensa käytölle ja käyttöolosuhteille vaatimuksia, joilla taataan laitteiden toimivuus ja käyttöturvallisuus. Nämä vaatimukset pitää huomioida laiteturvallisuudessa.

8.3 Yleiset turvamekanismit

Yleisten turvamekanismien tavoite on estää informaation ja tietojenkäsittelypalvelujen vaarantuminen tai varkaus. Organisaatio voi käyttää tarpeidensa mukaan monia erilaisia turvamekanismeja varmistamaan haluttuja asioita.

Informaatio ja tietojenkäsittelypalvelut tulee suojata, jotta ne eivät paljastu ulkopuolisille ja jotta sivulliset eivät voi muuttaa tai varastaa niitä. Suojamekanismit tulee toteuttaa menetysten tai vahinkojen minimoimiseksi. Turvamekanismeja ovat esimerkiksi puhtaan pöydän ja puhtaan näytön politiikka ja suojattavien kohteiden siirtäminen pois työpaikalta, kuten kannettavat tietokoneet.

8.4 HAMKin fyysinen ja ympäristön turvallisuus

Samat vastaukset pätevät tähän kuin luvussa 6.3, jossa käytiin vastaavia asioita läpi. HAMKissa ei ole käytössä erityisiä turva-alueita. Suojattavat tilat on lukittu asianmukaisesti. Laiteturvallisuudesta pidetään huolta ja laitteiden

kuntoa seurataan. Käytössä olevat yleiset turvamekanismit selviävät riskinanalyyseistä.

9 Tietoliikenteen ja käyttötoimintojen hallinta

ITILin tietoliikenteen ja käyttötoimintojen hallinnan tavoitteet ovat tietotekniikkaresurssien asianmukaisen, oikean ja turvallisen käytön turvaaminen [ITL, 2004]. Tietokoneiden hallinnan täsmällinen muoto riippuu paljon organisaatiosta, tietojärjestelmien merkityksestä erilaisille liiketoimintaprosesseille ja liiketoimintasovellusten luonteesta sekä herkkyydestä.

Yhteenveto BS 7799:n menetelmistä sisältää operationaaliset prosessit ja vastuut, jotta varmistutaan, että kaikille tietotekniikkaresursseille ja infrastruktuureille on määritetty vastuut. Toimintaprosessit on dokumentoitava ja niissä luodaan menetelmät operaatioiden hallintaan. Erityistä huomiota on kiinnitettävä töiden eriyttämiseen ja turvallisuustapausten käsittelyyn. Turvatapausten hallintaprosesseilla luodaan menetelmiä ja vastuita turvatapausten käsittelylle. Tähän kuuluu myös niiden raportointi. Työtehtävien eriyttämisellä eriytetään työtehtäviä eri ihmisten tehtäviksi. Näin vähennetään tahattomien virheiden ja tarkoituksellisten väärinkäytösten riskiä. Tuotanto ja kehitys ovat pidettävä erillään, jotta ei tapahtuisi häiriöitä ja kehitystyökaluja ei voitaisi väärinkäyttää tuotantoympäristössä [BS 7799-1:fi, 2000].

Ulkoisten toimintojen hallitsemisella otetaan huomioon, mitä muutoksia saattaa ilmetä, kun ulkoiset toiminnot ovat kolmannen osapuolen käytössä. Organisaation tietovarantoja suojellaan varmistamalla tietovälineiden suojaus ja oikea käsittely, ottamalla huomioon siirrettävien tietovälineiden turvallisuus ja hallinta, luomalla ohjeet käsittelylle ja käytölle, huomioimalla järjestelmien dokumentoinnin turvallisuus, vanhojen tietovälineiden uudelleenkäyttö ja käytöstä poisto sekä käyttämällä sopimuksia kolmansien osapuolien kanssa siitä, mitä tietoa vaihdetaan säännöllisesti.

9.1 Menettelyohjeet ja velvollisuudet

Tavoitteena on varmistaa tietojenkäsittelypalvelujen asianmukainen ja turvallinen käyttö. Kaikki tietojenkäsittelypalvelujen hallintaan ja käyttötoimintaan tarvittavat ohjeet tulee luoda ja määritellä velvollisuudet. Tämä sisältää operointi- ja häiriötilanteiden ohjeet.

Tarvittavia ohjeita ovat kirjalliset menettelyohjeet ja niiden dokumentointi ja ylläpito, käyttötoimintojen muutosten hallinta, poikkeustilanteiden käsittelytavat (tietojärjestelmien häiriöt, palvelujen katkeamiset ja estymiset, tietovuodot ja epätäydellisistä tai virheellisistä liiketoimintatiedoista aiheutuvat virheet), odottamattomien tilanteiden varasuunnitelmat, jäljitysketjut ja vastaavat todisteet, turvallisuusrikkomuksien ja järjestelmän toimintahäiriöistä palautumisen toimenpiteitä on valvottava, tehtävien eriyttäminen, kehitettävien

ja tuotannossa olevien palvelujen erottaminen sekä ulkopuolisten palvelujen hallinta.

ITIL olettaa että menettelyohjeet ja velvollisuudet selvitetään palvelutason SLA–sopimuksissa (Service Level Agreement).

9.2 Järjestelmän suunnittelu ja hyväksyntä

Tavoite on järjestelmien häiriöiden riskien minimointi. Etukäteissuunnittelu- ja valmistelu on tarpeen riittävän kapasiteetin ja resurssien käytettävyyden takaamiseksi.

Kapasiteetin suunnittelulla ja järjestelmän hyväksynnällä estetään järjestelmä ylikuormittumisen riskiä ja voidaan ennakoida ja arvioida tulevaisuuden kapasiteettivaatimuksia. ITIL käsittelee järjestelmien hyväksyntää ja kapasiteetin suunnittelua kohdassa omassa luvussaan [ITIL, 2004].

9.3 Haitallisilta ohjelmilta suojautuminen

Tavoite on ohjelmien ja tietojen eheyden turvaaminen. Haitallisten ohjelmien käyttöönoton estäminen ja havaitseminen edellyttää varotoimia.

Ohjelmisto- ja tietojenkäsittelypalveluita voidaan haavoittaa monilla haitallisilla ohjelmilla, kuten tietokoneviruksilla, troijalaisilla, verkkomadoilla, mainos – ja vakoiluohjelmilla, haitallisilla työkaluilla ja pilailuohjelmilla. Turvamekanismeilla jäljitetään kyseisiä ohjelmia ja estetään niiden käyttö. Käyttäjiä pitää opettaa haitallisten ohjelmien vaaroista. Turvamekanismeja haitallisten ohjelmien torjunnassa ovat mm. ohjelmalisenssien noudattaminen ja luvattomien ohjelmien käytön estäminen, virustentorjunta- ja korjausohjelmat, kriittisiä liiketoimintaprosesseja tukevien järjestelmien ohjelma- ja tietosisällön tarkastus, tiedostojen liitetiedostojen virustarkastus, johdon menettelyohjeet ja vastuut virustorjunnassa ja -koulutuksessa, liiketoiminnan jatkuvuussuunnitelmat ja vahingollisiin ohjelmiin liittyvän informaation varmentaminen.

Organisaation on määritettävä yllä mainittujen haittaohjelmien lisäksi, mitkä muut ohjelmat luokitellaan haitallisiksi. Esimerkiksi Internet-radiot, tiedostonvaihto-ohjelmat ja erilaiset pelit eivät ole haittaohjelmia, mutta ne voivat olla haitallisia esimerkiksi kuluttamalla tiedonsiirtokapasiteettia, niiden käyttö voi vähentää varsinaiseen työhön kulutettavaa aikaa ja niiden avulla voidaan levittää tekijänoikeuksien suojattua materiaalia. Ohjelman käyttötarkoitus voi siis määrittää, aiheuttaako se haittaa käyttäjälle itselleen tai muille. Jos käyttäjän on mahdollista asentaa itse omalle työkoneelleen mainittuja ohjelmia, niiden käyttö voi jäädä ylläpidolta huomaamatta.

Tällaisten ohjelmien käytöllä voidaan aiheuttaa tahattomia tai tahallisia haittoja muille järjestelmille.

9.4 Aputoimet

Tavoite on tietotekniikka- ja tietoliikennepalvelujen eheyden ja käytettävyyden säilyttäminen. Aputoimia ovat tietojen varmuuskopiointi, operaattorin suorittamat kirjaukset ja häiriöiden kirjaus. Näihin tehtäviin tulee luoda rutiinitoimenpiteet ja menetelmiä pitää testata.

ITIL ei perehdy näihin tarkemmin, varmuuskopiointi liittyy saatavuuden hallintaan, lokitietojen käyttö ja virheiden kirjaaminen ovat osa häiriöidenhallintaa ja tukipalveluita, ympäristön tarkkailu on ITILin laajuuden ulkopuolella ja sopimukset tietojen vaihdosta on määritetty SLA-sopimuksissa.

9.5 Verkon hallinta

Tavoite on verkossa kulkevan tiedon turvaaminen ja niiden tukena olevan perusrakenteen suojauksen varmistaminen. Organisaatiorajojen yli mahdollisesti ulottuvien tietokoneverkkojen turvallisuuden hallinta vaatii erityistä huomiota.

Verkon turvamekanismeja ovat verkkoja koskevan vastuun erottaminen tietokoneiden operoinnista, etälaitteiden hallinnanvelvollisuuksien määrittely ja menettelyohjeiden luonti, erityismekanismit julkisissa verkoissa kulkevan tiedon luottamuksellisuuden ja eheyden suojaaminen sekä tietokoneiden ja verkon hallinnan toimien koordinointi keskenään sekä liiketoimintapalvelujen optimoinnin että turvatoimien soveltamisen yhdenmukaisuuden varmistamiseksi kaikissa hankituissa tietotekniikan peruspalveluissa.

9.6 Tietovälineiden käsittely ja turvaaminen

Tavoite on suojattavien kohteiden vahingoittumisen ja liiketoiminnan keskeytymisen estäminen. Asianmukaiset käytössäpito-ohjeet tulee luoda tietovälineille, syöttö/tulostustietojen ja järjestelmän dokumentoinnin suojaamiseen vahingoittumiselta, varkaudelta ja luvattomalta käytöltä.

Tietovälineitä tulee valvoa ja suojata fyysisesti. Keinoja ovat siirrettävien tietovälineiden hallinta, tietovälineiden poistaminen käytöstä, tietojen käsittelyohjeet ja järjestelmän dokumentoinnin turvaaminen.

9.7 Tietojen ja ohjelmien vaihto

Tavoite on organisaatioiden välillä vaihdettavan tiedon katoamisen, muuttumisen ja väärinkäytön estäminen. Organisaatioiden välistä tietojen ja ohjelmien vaihtoa tulee valvoa ja vaihdossa tulee noudattaa asiankuuluvaa lainsäädäntöä. Asiaan liittyvät tietojen ja ohjelmien vaihtoa koskevat sopimukset, tietovälineiden turvaaminen kuljetuksen aikana, sähköisen

asioinnin turvallisuus, sähköpostin turvallisuus, elektronisten toimistojärjestelmien turvaus, julkiset järjestelmät ja muut informaation vaihdon muodot. ITIL olettaa että menettelyohjeet ja velvollisuudet selvitetään SLA-sopimuksissa.

9.8 HAMKin tietoliikenteen ja käyttötoimintojen hallinta

Tietotekniikan turvallisuus

Autentikointia vaativissa palveluissa käytetään tietoliikenteen salausta. Esimerkiksi autentikointia vaativissa WWW-palveluissa ei sallita http-yhteyksiä, vaan käytetään SSL-salattua HTTPS-yhteyttä. Tällöin yhteys asiakkaan ja WWW-palvelimen välillä on salattu eikä käyttäjätunnuksia ja salasanoja saada selville verkkoliikenteestä. WWW-palvelimen ja mahdollisen LDAP-palvelimen välinen yhteys toteutetaan suojattuna.

Tietoliikenteessä on muutamia ongelmia. Tällä hetkellä WWW-palvelimien ja LDAP-palvelimien yhteyttä ei ole salattu, koska toiminto on testaamatta. WAP/GPRS-yhteydet vaativat HTTP-yhteyden webmail-palvelimiin. Salausvaatimus tuntuu aina unohtuvan tilaajilta, kun kyse on esim. räätälöidystä WWW-palvelusta, joka ostetaan ulkopuoliselta tai teetetään opiskelijoilla.

Autentikoituja FTP-yhteyksiä ei sallita Internet-verkosta alueverkkoon. Alueverkon sisälläkään ei sallita FPT-kirjautumista NDS-hakemistosta LDAPin välityksellä, koska on vaarana, että tunnus salasanoineen joutuu vääriin käsiin myös alueverkon sisällä. FTP-palvelun sijaan käytetään SFTP/SSH-palvelua.

Tunnuksia ja salasanoja ei lähetetä käyttäjille suojaamattoman sähköpostin välityksellä. Tietoliikenteen salausmahdollisuus on huomioitava järjestelmiä hankittaessa. Jälkikäteen tilannetta on usein kallista ja vaikeaa parantaa. Jos tietokoneille, kämmenmikroihin tai puhelimiin tallennetaan järjestelmien admin-salasanoja tai muuta vastaavaa ”vaarallista vääriin käsiin joutuneena” –tietoa, niin on käytettävä salausohjelmistoa.

Palomuurit, tunkeutumisen esto ja internet

Tietokone- ja tietoliikennelaboratoriot eristetään alueverkosta kokonaan. Laboratorioista sallitaan tarvittaessa Proxy-palvelimen välityksellä WWW-yhteydet Internet-verkkoon.

Palomuurien perussäännöt:

- Internetistä alueverkkoon kaikki liikenne on oletuksena kielletty
- alueverkosta Internetiin on sallittu oletuksena kaikki portit, poikkeuksena SMTP, Windows-portit ja P2P-ohjelmistojen portit

Viruksilta suojaudutaan seuraavilla keinoilla:

- käyttäjien koulutus, opastus ja muistuttelu

- kaikki alueverkosta tai alueverkkoon lähtevät ja tulevat sähköpostit kulkevat virustorjuntaan tarkoitetun yhdyskäytävän (gateway) läpi
- sähköpostiliikenteen sallimisessa käytetään hyväksi harmaita ja valkoisia listoja
    - tiettyjä liitetiedostoja ei sallita lainkaan
    - käytetään hyväksi viestien header-tietoja, kun on mahdollista
- verkkopalvelimille asennetaan virustorjuntaohjelmisto, joka päivittyy automaattisesti
    - automaattipäivityksen toimintaa seurataan säännöllisesti
- työasemille asennetaan virustorjuntaohjelmisto, joka päivittyy automaattisesti
    - automaattipäivityksen toimintaa seurataan säännöllisesti
    - ongelmana ovat kannettavat tietokoneet, ratkaisuna käyttäjille annetaan oikeus tehdä ja opastetaan tekemään manuaalinen virustunnistepäivitys
    - ongelmana kotikoneet, etäkäyttäjille jaetaan systemaattisesti virustorjuntaohjelmisto
- palvelimien ja työasemien käyttöjärjestelmäpäivitykset automatisoidaan mahdollisimman pitkälle
    - Windows-työasemille käytetään SUS-palvelua ja vakioidaan Windows XP, jotta palvelu saadaan käyttöön

Varsinkin WWW-sivujen ja Internetistä ladattavien ohjelmien avulla leviävät haittaohjelmat (mainosohjelmat, vakoiluohjelmat) aiheuttavat turhaa verkkoliikennettä sekä erilaisia korruptoitumisongelmia Windows-käyttäjäprofiilien kanssa. Haittaohjelmat heikentävät tietosuojaa ja pahimmillaan saavat käyttäjän luovuttamaan kiintolevynsä sisällön kolmannen osapuolen tutkittavaksi. Haittaohjelmilta suojaudutaan seuraavilla keinoilla:

- käyttäjien koulutus, opastus ja muistuttelu
- käytetään Progkill-ohjelmistoa sulkemaan työasemilla pyörivät haittaohjelmaprosessit
    - säännöllisen ylläpidon tarve
- käytetään Ad-Aware- ja Spybot-ohjelmistoja

Parannusehdotuksia ovat. Palomuurijärjestelmät on syytä miettiä uusiksi., koska nykyinen ratkaisu ei ole kovin joustava. Työasemille voisi asentaa omat palomuurit, joiden avulla voitaisiin suojautua sekä viruksilta että haittaohjelmilta. Haittaohjelmien toimintaa voisi estää kieltämällä esim. Proxy–palvelimella tiettyjä haittaohjelmien käyttämiä WWW-sivustoja.

10 Pääsy- ja käyttöoikeuksien valvonta

Tavoite on ITILin mukaan [ITIL, 2004] estää luvaton pääsy tietoon ja tietojärjestelmiin, jotta voidaan suojella tiedon luottamuksellisuutta, estää luvattomia ja epätoivottuja muutoksia, tiedon tai ohjelmiston vahinkoja tai tuhoutumista sekä estää häiriöitä normaaleissa tuotantovaiheissa. Pääsyoikeuksia tarkastellessa erotetaan pääsy tietoverkkoihin, tietokoneisiin ja ohjelmistoihin.

Yhteenvetona BS 7799:ssa esitetään menetelmät pääsynvalvonnan ylläpidon tehokkuus, jolla varmistetaan että käyttäjien, tilien, oikeuksien, idenfiointien ja autentikointien (salasanojen) hallinta ja ajan tasalla oleminen. Loppukäyttäjien vastuut, loppukäyttäjien on oltava tietoisia omista vastuistaan ja oikeuksistaan, tietoturvatietoisuuden lisäämisellä parannetaan vastuiden noudattamista. Tietoverkkojen pääsynvalvonnassa käytetään erilaisia turvamenetelmiä tilanteen mukaan. Tärkeimpiä ovat käyttöoikeuksien valvonta ulkoisille ja sisäisille käyttäjille, kuten ulkoisille ja sisäisille palveluille. Lisäksi käyttäjät tulee aina autentikoida. Tietoverkkoja voidaan eriyttää ja jakaa osiin ja luoda tarvittaessa reittejä verkkojen välille. Tietoverkoissa olevat tietokonejärjestelmät ja työasemat on autentikoitava niin hyvin kuin teknisesti on mahdollista. Kolmansien osapuolten verkkopalveluiden turvallisuusvaatimukset ja uhkat on tunnistettava. Tietokoneiden pääsynvalvonta perustuu pitkälti siihen millaisia identifiointi- ja autentikointimenetelmiä on mahdollista toteuttaa [BS 7799-1:fi, 2000].

Tärkeimpiä valvontamenetelmiä ovat kaikkien työasemien ja päätteiden identifiointi ja autentikointi, pakotettu kirjautumismenettely jossa kirjautumisen kohteesta annetaan mahdollisimman vähän tietoa kirjautujalle, loppukäyttäjän identifiointi ja autentikointi, jotta aina voidaan jäljittää tekijä, painostushälytyksen käyttö, automaattinen aikakatkaisu istunnoille, aikarajat käytölle, epäonnistuneiden kirjautumisyritysten jälkeinen lukitus, pääsyoikeuksien lisätarkistus tarkistussoitoilla, kysymys-vastaus mekanismeilla jne., ohjelmistojen pääsynvalvonta, virustentorjuntaohjelmien käytön politiikka eli mitä käytetään ja miten päivitetään, lisenssien hallinta, tietojärjestelmien käytön valvonta, pääsyn valvonta ja tarkastaminen, luvattoman pääsyn estämiseksi on talletettava jäljitysketjuja virheistä, epäilyttävistä ja epätavallisista tapahtumista, joita voidaan yhdistellä ja antaa turvallisuusvastaavalle, ja järjestelmien käytön valvonta. Automaattisia varoituksiaen täytyy syntyä, kun tietyt rajat ylitetään Seurantajärjestelmien ajanmittaus on synkronisoitava. Virushyökkäysten raportointi ja korjaustoimenpiteet on luotava.

Tulevaisuuden pääsyoikeuksien hallinnassa on monia uusia mahdollisuuksia tunnistaa käyttäjä luotettavasti. Biometriikka mahdollistaa

lukuisia ihmisen fyysisiin ominaisuuksiin perustuvia tunnistautumistapoja. Näitä uusia tapoja voidaan yhdistää vanhempiin menetelmiin. Käyttäjä voidaan tunnistaa hänen hallussa , tiedossa tai omistuksessa olevaan asiaan [1998, s.98]. Asia voi olla fyysinen esine kuten USB-avain tai kulkukortti, tietona oleva salasana tai jokin käyttäjän yksilöivä ominaisuus kuten sormenjälki tai iiris.

10.1 Liiketoiminnan asettamat vaatimukset pääsynvalvonnalle

Tavoite on tietoihin käsiksi pääsyn valvonta. Tietoon ja liiketoimintaprosesseihin pääsyä tulee valvoa turvallisuus- ja liiketoimintavaatimusten mukaisesti. ITIL ei käsittele tätä osa-aluetta.

Tietojen levitystä ja saantioikeuksia koskevat periaatteet tulee ottaa huomioon. Näkökohtia ovat pääsyn valvonnan toimintaperiaatteet, liiketoiminnalliset vaatimukset ja pääsyoikeuksien valvonnan säännöt.

10.2 Käyttöoikeuksien hallinta

Tavoite on estää luvaton pääsy tietojärjestelmään. Tietojärjestelmien ja tietojenkäsittelypalveluiden käyttöoikeuksien myöntämisen valvontaan tulee olla määrämuotoiset ohjeet.

Ohjeiden tulee kattaa käyttöoikeuksien elinkaaren kaikki vaiheet. Tutkittavia kohteita ovat käyttäjien rekisteröinti, pääkäyttäjän oikeuksien hallinta, käyttäjän salasanojen hallinta ja käyttöoikeuksien uudelleenarviointi.

Turvallisen salasanan luontiin on olemassa paljon ohjeita. Järvinen [2002, s. 340] luettelee hyvän salasanan ominaisuudet: riittävän pitkä, ei johdettavissa, ei sisällä henkilökohtaista tietoa, sisältää tarpeeksi erilaisia merkkejä ja vaihdetaan tarpeeksi usein. Samaa salasanaa ei kannata käyttää monessa eri paikassa ja palvelussa. Liian pitkä ja vaikeasti muistettava salasana kirjoitetaan helposti muistilapulle, jolloin salasanan tuoma etu käytännössä häviää, jos tunkeutuja pääsee kirjoitettuun versioon käsiksi.

10.3 Käyttäjän velvollisuudet

Tavoite on luvattoman käytön estäminen. Luvallisten käyttäjien yhteistyö on tehokkaan tietoturvallisuuden kannalta olennaisen tärkeää, sillä salasanojen vuotamisen havaitseminen ja muiden tällaisten riskitekijöiden ja ongelmien raportointi muille käyttäjille vähentää uhkien toteutumismahdollisuuksia. Mitä nopeammin tieto saadaan kulkemaan, sitä nopeammin voidaan reagoida.

Käyttäjille tulee kertoa, että heidän velvollisuutensa on pitää yllä tehokasta pääsyn valvontaa, erityisesti salasanojen käytön ja käyttäjälaitteiden turvallisuuden kannalta.

Tämä osio on pääasiassa ITILin laajuuden ulkopuolella. Kuitenkin esitetään seuraavia näkökohtia todeten, että lista ei ole täydellinen: käyttäjän vastuu salasanoistaan, käyttäjän vastuu käyttämistään aktiivisista istunnoista,

laitteistosta ja tietovälineistä, käyttäjän vastuu tuonti ja vientisäännöistä, käyttäjän vastuu ulkoisen kommunikaation ja palvelujen käytössä, käyttäjän vastuu tietoturvallisuushäiriöiden sattuessa.

10.4 Verkkoon pääsyn valvonta

Tavoite on verkkopalvelujen suojaus. Pääsyä sekä sisäisiin että ulkoisiin verkkopalveluihin tulee valvoa. Valvonnan sisältönä ovat verkkopalvelujen käytön periaatteet, ohjattu reititys, ulkopuolisia yhteyksiä käyttävien henkilöiden todentaminen, etätietokoneen todentaminen, huoltoyhteyksien suojaus, verkkojen looginen jaottelu, verkkoyhteyden valvonta, verkon reitityksen valvonta ja verkkopalvelujen turvaaminen.

10.5 Käyttöjärjestelmään pääsyn valvonta

Tavoiteena on estää luvaton pääsy tietokoneeseen. Käyttöjärjestelmän tasoisia turvallisuuspalveluja tulee käyttää tietokoneen resurssien käyttöoikeuksien rajoittamiseen. Menetelmiä ovat automaattinen työasemien tunnistus, työasemayhteyden luontimenetelmät, käyttäjien tunnistaminen ja todentaminen, salasanojen hallintajärjestelmäjärjestelmine apuohjelmien käyttö, painostushälytys käyttäjien turvaamiseksi, työasemayhteyden aikakatkaisu ja yhteysajan rajoittaminen

10.6 Sovellukseen pääsyn valvonta

Tavoitteena on estää luvaton pääsy tietokonejärjestelmissä säilytettäviin tietoihin. Tulee toteuttaa turvallisuustoimenpiteet, joilla rajoitetaan tietojärjestelmiin pääsyä. Looginen pääsy tietokoneohjelmiin ja -tietoihin tulee rajoittaa luvallisiin käyttäjiin.

Keinoja ovat tietojen käytön rajoittaminen (pääsy-, luku-, kirjoitus ja poisto-, ja suoritusoikeudet) sekä arkaluontoisen sovelluksen eristäminen.

10.7 Järjestelmään pääsyn ja käytön tarkkailu

Tavoite on luvattomien toimintojen havaitseminen. Järjestelmää tulee tarkkailla siltä varalta, että käytönvalvontaperiaatteista poiketaan. Lisäksi havaitut tapahtumat tulee tallentaa todistusaineistoksi.

Menetelmiä ovat tapahtumien kirjaaminen, järjestelmien käytön tarkkailu, menettelytavat ja riskialueet, riskitekijät, tapahtumien kirjaaminen ja tutkinta sekä kellojen synkronointi.

Työnantajan suorittama työntekijöiden valvonta ei ole yksiselitteistä. Laki suojaa työntekijöiden yksityisyyttä. Järvinen mielestä valvonnasta olisi hyvä kertoa etukäteen työntekijöille [2002, s. 129]. Näin voidaan ennalta ehkäistä ongelmien syntymistä, kun jo pelkkä tieto valvonnasta saattaa estää kiellettyä toimintaa. Tekniikka mahdollistaa työntekijöiden sähköpostin, puheluiden ja

Internetin käytön seurannan. Valvontaa voidaan oikeuttaa työn tuottavuuden perusteella, koska työntekijän kuuluu tehdä työtä josta hänelle maksetaan. Kuitenkin on toimittava sovituissa rajoissa ja huomioitava, että luvaton seuranta on rikos. Työntekijän yksityisasiat eivät kuulu työnantajalle, joten seuranta ei saa olla liian tarkkaa.

10.8 Tietokoneen matkakäyttö ja etätyöskentely

Tavoitteena on varmistaa tietojen turvallisuus tietokoneiden matkakäytössä ja etätyöskentelyssä. Aihe sisältää tietokoneen matkakäytölle ja etätyöskentelylle asetetut vaatimukset ja suojaukset.

Etätyöskentelyn edellytyksenä on sopivien työvälineiden käyttö. Työntekijä voi työskennellä kotoaan käsin omalla tietokoneellaan. Hänelle on voitu hankkia tätä tarkoitusta varten kannettava tietokone tai mobiililaite. Järvinen [2002, s. 79]. toteaa matkamikrojen olevan alttiita uhkille paljon kiinteästi sijoitettuja tietokoneita enemmän Matkamikrojen liikkuvuudella on hintansa, koska ne voidaan helpommin varastaa tai hukata, niiden korjaaminen on vaikeampaa ja varmistusten tekeminen on monimutkaisempaa. Matkamikron omistajan on tiedettävä, mihin kaikkeen varautua. Matkamikron rahallinen arvo on yleensä paljon pienempi kuin mikron sisältämän tiedon arvo. Sen sisältämät tiedot voivat salaamattomina muiden käsissä aiheuttaa rahallisia tai muita tappioita. Pelkästään omien työtiedostojen katoaminen voi aiheuttaa ajanmenetystä tai kuluja, kun niitä yritetään palauttaa.

Etätyöskentelyn turvallisuutta voidaan parantaa käyttämällä suojattuja tietoyhteyksiä ja suojaamalla käytetyt työvälineet ja niiden sisältämät tiedot. Tietojärjestelmiä suojausmenetelmiä ovat tietojen salaus ja pääsynvalvonta salasanoja käyttämällä. Tietoliikenteen suojaamisessa voidaan käyttää VPN-yhteyksiä. Fyysisiä turvamenetelmiä ovat erilaiset lukot kuten Kensington-lukko, jolla voidaan lukita tietokone vaijerilla johonkin kiinteästi ja usb-avaimet, joita ilman tietokonetta ei voi käyttää.

10.9 Pääsyoikeuksien valvonta HAMKissa

Verkkoon pääsyn valvonta on tärkeä osa-alue HAMKille. HAMKissa on erityiskysymyksenä langattomien verkkojen käyttö henkilökunnalla, opiskelijoilla ja vierailijoilla. HAMKissa järjestelmien pääkäyttäjillä on oikeudet järjestelmien hallintaan. Käyttäjätunnusten hallinto on hoidettu HAMKissa hyvin, sillä sen toiminta on dokumentoitu ja prosessi määritelty omassa dokumentissaan [Liite 10].

Etätyöskentely järjestetään HAMKissa salattujen VPN-yhteyksien avulla, jolloin etätyöskentely verkon kautta ei aiheuta riskejä. Kannettavilla tietokoneilla ei pitäisi olla henkilötietoja, mutta niitä saattaa kuitenkin niissä

olla. Pääosin näillä tietokoneilla on hallinnon budjetteja ja taulukoita. Pieniä ongelmia on kuitenkin aiheuttanut laskujen kierrätysohjelma BasWare Invoice Processing. On hyvä kuitenkin luoda ohjeistus etätyöskentelyyn, mallina voisi olla Valtionhallinnon etätyön tietoturvallisuusohje [VAHTI, 3/2002].

11 Järjestelmien kehittäminen ja ylläpito

Tavoite on taata tietojärjestelmien turvallisuus koko niiden elinkaaren ajan. ITILIssä on käsitelty tietojärjestelmien kehittämistä ja ylläpitoa kirjassa Software Lifecycle Support and the Business Perspective Set. Seuraavien kohtien aloituskohtien käyttöä suositellaan: ohjelmistojen turvallisuus, uusien ja vanhojen järjestelmäresurssien testaus, hyväksyntä, esittely ja turvallisuus, kehitys- ja tuotantoympäristöjen turvallisuus, käyttöjärjestelmien muutokset sekä ohjelmistopakkausten muutokset. Valtionhallinnon tietojärjestelmä-kehityksen tietoturvallisuussuositusta voidaan käyttää apuna tämän osion tekemisessä [VAHTI, 3/2000].

11.1 Järjestelmien turvallisuusvaatimukset

Tavoitteena on varmistaa, että tietojärjestelmät kehitetään turvallisiksi.

ITIL 4.2 käsittelee tätä aihetta, alakohdat on esitetty aikaisemmissa kohdissa. Menetelmiä ovat turvallisuusvaatimusten analyysi ja määrittelysovellusten turvaaminen, syöttötietojen oikeellisuuden tarkistus, sisäisen käsittelyn valvonta, riskialueet, tarkastukset ja turvamekanismit, viestin todentaminen, ja tulostustietojen oikeellisuuden tarkistus,

11.2 Sovellusten turvaaminen

Tavoitteena on estää käyttäjien tietojen katoaminen, muuttuminen ja väärinkäyttö sovelluksissa. Menetelmiä ovat syöttötietojen oikeellisuuden tarkistus, sisäisen käsittelyn valvonta, riskialueet, tarkastukset ja turvamekanismit, viestin todentaminen ja tulostustietojen oikeellisuuden tarkistus.

11.3 Salakirjoitusmekanismit

Tavoite on suojata tiedon luottamuksellisuus, alkuperäisyys ja eheys. Toteutustapoja mietittäessä on otettava huomioon salakirjoitusmekanismien käytön periaatteet, salaus, digitaaliset allekirjoitukset, kiistämättömyyspalvelut, salausavainten hallinta, salakirjoitusavainten suojaus ja salasanojen talletus.

11.4 Järjestelmätiedostojen turvallisuus

Tavoitteena on varmistaa, että tietotekniikkahankkeet ja niiden tukitoiminnot suoritetaan turvallisella tavalla. Pääsyä tietojärjestelmätietoihin tulee valvoa. Järjestelmän eheyden säilyttämisen tulee olla sen käyttötoiminta- tai kehitysryhmän vastuulla, jolle sovellusjärjestelmä tai -ohjelmisto kuuluu.

Osa-alueita ovat tuotannossa olevan ohjelmiston valvonta, järjestelmän testiaineiston suojaus ja ohjelmien lähdekirjastoon pääsyn valvonta.

11.5 Kehitys- ja tukiprosessien turvallisuus

Tavoite on sovellusjärjestelmän ohjelmien ja tietojen turvallisuuden ylläpito. Läpikäytäviä asioita ovat muutosten valvontamenetelmät, käyttöjärjestelmän muutosten tekninen tarkastus, ohjelmistopakettien muutoksia koskevat rajoitukset, ohjelmiin piilotettu tahallinen haitallinen koodi ja ulkoistettu ohjelmistokehitys.

11.6 HAMKin järjestelmien kehittäminen ja ylläpito

HAMKissa käytetään järjestelmien kehittämissä ja ylläpidossa edellä mainittuja perusperiaatteita. Salakirjoitusmenetelmiä ei ole käytössä. HAMKin kehitys- ja tukiprosessien turvallisuudessa huomioidaan esimerkiksi se, että testipuolella ei saa käyttää tuotannon tunnuksia. Järjestelmien turvallisuutta voidaan parantaa dokumentoimalla vaatimuksia ja ylläpitoa paremmin. Lisäksi tärkeätä olisi saada ulkopuolisilta tilattavien järjestelmien tarjouspyyntöihin liitteeksi turvallisuusvaatimukset.

12 Liiketoiminnan jatkuvuuden hallinta

ITIL käsittelee jatkuvuuden hallintaa erillisessä kirjassa Service Delivery kohdassa Contingency / Planning, joten sitä ei Security Management kirjassa tarkasti käsitellä. Tiivistettynä esitetään, että tavoitteena on tehdä jatkuvuussuunnitelmia suurien odottamattomien häiriöiden tai katastrofien varalle. Tämä onnistuu, kun luodaan prosesseja jatkuvuussuunnitelmien kehitykselle, ylläpidolle ja päivitykselle ja aloitetaan kaikkein kriittisimmistä liiketoiminnoista. On varmistettava, että käytössä on yhdenmukainen rakenne liiketoiminnan jatkuvuuden suunnittelulle koko organisaatiossa.

Jatkuvuussuunnittelun on sisällettävä BS 7799:n mukaan vähintään menetelmät hätätilanteita varten. Näitä ovat ovat vastuumäärittelyt ja toiminta, joka täytyy suorittaa välittömästi häiriöiden jälkeen, varmistusmenettelyt, joilla voidaan jatkaa kriittisten prosessien suorittamista vaihtoehtoisilla tavoilla tai palauttaa alkuperäiset prosessit mahdollisimman nopeasti kuntoon. On kuvattava lisäksi toipumismenettelyt, joilla palautetaan alkuperäinen tilanne ja testausaikataulut jatkuvuussuunnitelmien säännölliseen testaamisen ja harjoittelemiseen varsinkin suurten muutosten jälkeen [BS 7799-1:fi, 2000].

12.1 Liiketoiminnan hallintaan liittyviä näkökohtia

Tavoite on ehkäistä liiketoiminnan keskeytyminen ja suojata kriittisiä liiketoimintoprosesseja merkittävien häiriöiden ja onnettomuuksien vaikutuksilta. Viranomaisilta on olemassa erilaisia suosituksia, joita pitää noudattaa.

Liiketoiminnan jatkuvuuden hallintaan tulee sisältyä turvamekanismit riskien havaitsemiseen ja vähentämiseen. Niillä tulee rajoittaa uhkan mahdollisen toteutumisen aiheuttamia seurauksia ja niillä tulee varmistaa olennaisen tärkeiden toimintojen nopea palautuminen. Näihin liiketoiminnan jatkuvuuden hallintaprosesseihin kuuluvat liiketoiminnanjatkuvuus- ja vaikutusanalyysit, jatkuvuussuunnitelmien laatiminen ja toteuttaminen, liiketoiminnan jatkuvuussuunnittelun puitteet, suunnitelmien testaus, ylläpito ja uudelleenarviointi. Jatkuvuussuunnittelun voidaan katsoa olevan onnistunutta, kun tietoturvaselkkausten aiheuttamat haitat organisaatiolle jäävät vähäisiksi [Vahti 3/2005]. Korjauksen onnistumista voidaan tarkastella seuraavan kaavan avulla [Kuva 16]:

$$\text{Korjauksen onnistuminen} = \frac{(\text{toipumisen} + \text{menetetyn mahdollisuuden kustannus})}{(\text{häiriön aiheuttama kustannus organisaatiolle})}$$

Kuva 16. Korjauksen onnistumisen kaava [Vahti 3/2005, s. 75]

12.2 HAMKin toiminnan jatkuvuuden hallinta

HAMKiin kohdistuvia suuria uhkia ovat isot tulipalot ja vesivahingot, etäopetuksen ongelmat ja palvelinten tai tietoliikenneyhteyksien viat. Näihin on myös varauduttu riskianalyysien mukaan. Parannusehdotuksina toiminnan jatkuvuuden suunnitelmia tulisi tarkistaa ja harjoitella toimintaa tarpeeksi usein. Suunnitelmat tulisi myös kouluttaa henkilökunnalle, jotta häiriöt lamaannuttaisivat toimintaa mahdollisimman vähän ja vaihtoehtoiset menettelyt ja laitteet voidaan ottaa kitkattomasti käyttöön. Riittävät varmistusmenettelyt on turvattava tärkeimmille kohteille. HAMKin tärkeimmät palvelut ja niiden pisimmät siedettävät palvelukatkot määräävät, mille palveluille on asetettava parhaimmat varmuusmenettelyt.

13 Vaatimustenmukaisuus

Organisaatioiden toiminta ei voi olla mielivaltaista. Niiden tulee noudattaa lukuisia lakeja ja muita vaatimuksia. Vaatimustenmukaisuutta käsitellään ITILIssä [ITIL, 2004] ja tavoitteena on yhtenevyys asiakkaiden organisaation tietoturvapolitiikan ja sovittujen standardien kanssa. Tämän vuoksi vaaditaan säännöllisiä tietojärjestelmien tarkastuksia.

BS 7799:n mukaisia menetelmiä ovat tietojärjestelmien asiattoman käytön estäminen, yhtäpitävyys turvallisuuspolitiikkojen ja –standardien kanssa, yhtäpitävyys lakien kanssa mukaan luettuina luvattoman kopioimisen estäminen, tietojärjestelmien säännöllinen tarkastus niin, että tarkastukset häiritsevät mahdollisimman vähän tuotantoa ja ne suoritetaan asianmukaisesti ja testaustyökalujen antaminen vain valtuutetuille käyttäjille. Peruskäyttäjille vaatimustenmukaisuus ilmenee työsopimuksessa esitettyjen vaatimusten toteuttamisella ja vaitiolovelvollisuuden, viestintäsalaisuuden ja yksityisyyden suojan kunnioittamisessa. Henkilökunnan, ylläpidon ja yhteistyökumppaneiden on allekirjoitettava edellä mainitut sopimukset, sillä näin heidät velvoitetaan noudattamaan niitä [BS 7799-1:fi, 2000].

13.1 Lakisääteisten vaatimusten noudattaminen

ITIL ei erityisesti käsittele lakisäätöisiä ja sopimuksellisia vaatimuksia. Tavoitteina ovat organisaation turvallisuuspolitiikan vertaaminen voimassa oleviin sopiviin standardeihin ja estää myös rikkomukset lakisääteisiä ja sopimuksellisia vaatimuksia kohtaan. On kuitenkin kiinnitettävä huomiota seuraaviin kohtiin: tekijänoikeuksien suojaaminen, organisationaaliset dokumentit ja henkilötiedot. On selvitettävä, minkälainen on koko organisaation turvallisuuspolitiikka ja miten siinä otetaan lakisääteiset vaatimukset huomioon.

Tavoite on kaikkien rikos- ja siviilioikeuden sekä asetusten, säännösten ja sopimusten velvoitteiden ja kaikkien turvallisuusvaatimusten noudattaminen. Tämä saattaa kuulostaa vaativalta, mutta arkityössä tulee harvoin esiin tilanteita, joissa olisi mahdollista toimia lakien vastaisesti. Tietyt työtehtävät sisältävät mahdollisuuden käsitellä arkaluonteista tietoa kuten henkilötietoja ja rahaliikennettä. Jos voidaan olettaa ja tiedetään, että jossain työtehtävässä vaaditaan tietoutta voimassaolevista laeista ja vaatimuksista, työntekijän on ymmärrettävä ja osattava tulkita näitä asioita.

Erityisiä laillisuusvaatimuksia koskevaa tietoa tulee kysyä organisaation lakimiehiltä tai asianajajilta. Näkökohtia ovat sovellettavan lainsäädännön tunnistaminen, aineettomat oikeudet, ohjelmistojen tekijänoikeudet, organisaation tallenteiden turvaaminen, tietosuoja ja henkilötietojen yksityisyys, tietojenkäsittelypalvelujen väärinkäytön estäminen,

salakirjoitusmekanismeja koskevat säädökset, todisteiden kokoaminen, turvallisuuspolitiikan ja tekniikan vaatimustenmukaisuuden tarkastus.

Suomessa ei ole yhtenäistä tietoturvalainsäädäntöä. Tietoturvallisuuden järjestämistä koskevia säännöksiä sisältyy useisiin lakeihin ja asetuksiin. Lainsäädännöstä on tiedostettava organisaation toiminnan perusteita koskevat säännökset, kuten tietojen salassa pidettävyyttä sekä tietojen ja aineistojen käsittelyä koskevat säännökset. Valtion säädöstietopankissa FINLEXissa on koottu ajan tasalla olevat säädökset [FINLEX, 2006]. Tietojen luottamuksellisuuden, eheyden ja käytettävyyden turvaamiseen sekä tietoturvarikkomusten käsittelyyn otetaan kantaa seuraavissa tietoturvalaeissa [Yliopistojen tietoturvasivut, 2006]:

- Tietoturvasäädökset - viestintäviraston linkit
- Tietoturvaa käsitteleviä otteita rikoslaista
- 39/1889 - Rikoslaki (38. luku Tieto-ja viestintärikoksista)
- 731/1999 - Suomen perustuslaki (10 §)
- 1080/1991 - Valmiuslaki
- 393/2003 - Viestintämarkkinalaki
- 565/1999 - Laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta - Mitä se tarkoittaa
- 523/1999 - Henkilötietolaki
- 621/1999 - Laki viranomaisten toiminnan julkisuudesta
    - 1030/1999 - Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta
- 1117/2001 - Laki eräiden suojauksen purkujärjestelmien kieltämisestä
- 282/2002 - Laki tietoyhteiskunnan palvelujen tarjoamisesta
- 458/2002 - Laki yksityisistä turvallisuuspalveluista
- 738/2002 - Työturvallisuuslaki
- 13/2003 - Laki sähköisestä asioinnista viranomaistoiminnassa
- 14/2003 - Laki sähköisistä allekirjoituksista
- 228/2003 - Verkkotunnuslaki
- 516/2004 - Sähköisen viestinnän tietosuojalaki
- 759/2004 - Laki yksityisyyden suojasta työelämässä

Laki viranomaisen toiminnan julkisuudesta (621/1999)

Viranomaisen on hyvän tiedonhallintatavan luomiseksi ja toteuttamiseksi huolehdittava asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen asianmukaisesta saatavuudesta, käytettävyydestä ja suojaamisesta sekä eheydestä ja muusta tietojen laatuun vaikuttavista tekijöistä. Viranomaisen on suunniteltava ja toteutettava asiakirja- ja tietohallintonsa samoin kuin ylläpitämänsä tietojärjestelmät ja tietojenkäsittelyt niin, että asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen suoja, eheys ja laatu turvataan asianmukaisin menettelytavoin ja tietoturvallisuusjärjestelyin ottaen huomioon tietojen merkitys ja käyttötarkoitus sekä asiakirjoihin ja tietojärjestelmiin kohdistuvat uhkatekijät ja tietoturvallisuustoimenpiteistä aiheutuvat kustannukset.

Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999)

Hyvän tiedonhallintatavan toteuttamiseksi viranomaisen on selvitettävä ja arvioitava tietojen saatavuuteen, käytettävyyteen, laatuun ja suojaan sekä tietojärjestelmien turvallisuuteen vaikuttavat uhat sekä niiden vähentämiseksi ja poistamiseksi käytettävissä olevat keinot ja niiden kustannukset sekä muut vaikutukset.

Henkilötietolaki (523/1999)

Rekisterinpitäjän on toteutettava tarpeelliset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä tai muulta laittomalta käsittelyltä. Toimenpiteiden toteuttamisessa on otettava huomioon käytettävissä olevat tekniset mahdollisuudet, toimenpiteiden aiheuttamat kustannukset, käsiteltävien tietojen laatu, määrä ja ikä sekä käsittelyn merkitys yksityisyyden suojan kannalta.

Valmiuslaki (1080/1991)

Valtioneuvoston, valtion hallintoviranomaisten, valtion liikelaitosten ja muiden valtion viranomaisten sekä kuntien on valmiussuunnitelmin ja poikkeusoloissa tapahtuvan toiminnan etukäteisvalmisteluin sekä muin toimenpitein varmistettava tehtäviensä mahdollisimman häiriötön hoitaminen myös poikkeusoloissa.

13.2 Turvallisuuspolitiikan ja tekniikan vaatimustenmukaisuuden tarkistus

Tavoite on varmistaa, että järjestelmät toimivat organisaation turvallisuuspolitiikan ja -standardien mukaisesti. Tietoturvapolitiikan on oltava linjassa yleisen turvallisuuspolitiikan kanssa.

Tarkistuskohtia ovat turvallisuuspolitiikan noudattaminen ja teknisen kelpoisuuden tarkistus. Tarkastuksia ja auditointeja tulee suorittaa riittävän usein, käytännössä ainakin kerran vuodessa ja olosuhdemuutoksien jälkeen. Tietoturvapolitiikkaa ja ohjeita on päivitettävä, jos tapahtuu muutoksia.

13.3 Järjestelmän tarkastusnäkökohtia

Tavoite on maksimoida järjestelmän tarkastusprosessin tehokkuus ja minimoida järjestelmän tarkastusprosessista tai -prosessiin aiheutuvat häiriöt.

Järjestelmän tarkastusmekanismit sisältävät tarkastusvaatimuksia ja -toimintoja. Myös järjestelmän tarkastusvälineiden suojaus on huomioitava, jotta voidaan valvoa niiden eheyttä ja väärinkäyttöä. Tarkistustoimenpiteet pitää suunnitella niin, että niistä ei aiheudu haittaa tai vahinkoja organisaation toiminnalle. Tarkastuksien sisältö ja tulokset on dokumentoitava yhdenmukaisesti aikaisempien tarkastusten kanssa, jotta tuloksia ja mittareiden arvoja voidaan verrata.

13.4 Vaatimusten huomioiminen ja toteuttaminen HAMKissa

HAMKia koskevat yllä mainitut lakisääteiset vaatimukset. Käytännössä tärkeimmät ovat opetusorganisaatioiden erityisvaatimukset ja sähköpostisäädäntö ja työelämän lainsäädäntö. Koulutuspuolella ei ole erityisiä vaatimuksia.

Turvallisuuspolitiikan ja tekniikan vaatimustenmukaisuuden noudattaminen ja järjestelmien tarkastaminen HAMKissa tulisi selvittää. Käytännössä tämän suorittaa HAMKin ohjausryhmä. Organisaation johto saadaan ottamaan kantaa asioihin, kun selvitetään onko kaikista vaatimuksista suoriuduttu.

14 Tietoturva ja etiikka

Tietoturvaa ei voi tarkastella pelkästään standardien ja lakien valossa, sillä lain mukaan oikea ja moraalisesti oikea eivät tarkoita samaa asiaa. Ihmiset toimivat myös moraalinsa mukaan, eivätkä aina noudata lakia pilkuntarkasti. Etiikka on moraalia tutkiva filosofian haara. Normatiivisessa etiikassa pyritään selvittämään, mitä eettisiä sääntöjä ihmisen tulisi noudattaa, jotta hän olisi hyvä ihminen. Tietotekniikkaa varten on ollut tarpeen luoda uusia eettisiä sääntöjä, sillä aihe on nostattanut esiin lukuisia kysymyksiä, joihin perinteiset eettiset säännöt soveltuvat huonosti.

14.1 Etiikan määritelmä

Käsittelen tietoturvallisuutta tässä yhteydessä tietotekniikan yhtenä osa-alueena. Tietojenkäsittely sisältää eri osa-alueita, jaottelua voidaan tehdä monin eri tavoin ja moni asia on päällekkäin, sillä kaikkia kohteita ei voi rajata vain tiettyihin lokeroihin. Olen kerännyt eri lähteistä jaotteluita, esitän tässä Gehringerin tieoturvallisuuden jaottelun [2005]. Jaottelusta huomaa, että etiikan voi ulottaa koko tietojenkäsittelyn laajuudelle ja tietoturva on olennainen osa eettisiä kysymyksiä. Tietoturvatyön etiikka ei ole tietoteknisten etujen tavoittelua ja sääntöjen seuraamista, sillä aina on oltava valinnan mahdollisuus. Lukuisia eettisiä normistoja on luotu eri ammattijärjestöjen toimesta, arvostetuimpien joukossa ovat Association for Computing Machinery [ACM] ja Institute of Electrical and Electronics Engineers [IEEE]. Näiden järjestöjen jäsenien tulee hyväksyä ja noudattaa näitä normeja työssään.

Tietoturvallisuuden eettiset kysymykset

- Sananvapaus: ketjukirjeet, sähköpostin yksityisyys, käyttäytymiskoodit internetissä (netiketti)
- Tietokoneiden väärinkäyttö: hakkerointi, virukset, madot, haittaohjelmat
- Kaupallisuus: petokset, vapaa kauppa, verotus, uhkapeluu, kilpailun vääristäminen
- Yksityisyys: yksityisyys verkossa, anonyymiys, kryptaus, roskaposti
- Tietojenkäsittelyn riskit: ohjelmistojen luotettavuus, tekoälykysymykset, tietoverkkojen turvallisuus, ohjelmistojen turvallisuus, lisensointi
- Sosiaalis-oikeudelliset kysymykset: tietokoneaikakauden epäkohdat, pääsyn tasapuolisuus, työpaikan kysymykset
- Henkisen ja aineettoman pääoman suojaus: patentti- ja tekijänoikeuskysymykset, elektroniset tekijänoikeudet, ohjelmistopiratismi, plagiointi

Gehringerin jaottelu tietoturvallisuudesta[2005]

Suomen korkeakoulujen ja tutkimuksen tietoverkko Funet määrittelee tietoverkkojen käyttöetiikan kieltävän käyttäjien ja ylläpitäjien yhteistä etua haittaavan toiminnan [2006]. Normaalien laissa kiellettyjen toimien lisäksi Funet ottaa kantaa myös huonoon käytökseen ja epäeettiseen käytökseen, joka ei suoranaisesti ole lainvastaista. Tällaista toimintaa ovat esimerkiksi resurssien tahallinen tuhlaaminen ja oman tietoturvan laiminlyönti. Nämä Funetin periaatteet korostavat käyttäjän vastuuntuntoa, sillä kaikkea ei voi erikseen kieltää. Vastuuntuntoinen käyttäjä osaa omatoimisesti tehdä hyviä eettisiä päätöksiä kun säännöt ja ohjeet eivät riitä.

Mitä hyvän ihmisen käsite tarkoittaa puhuttaessa tietoturva-asiantuntijasta? Tällaisen ihmisen on toteutettava tiettyjä moraalisia ihanteita ja perustettava toimintansa ja päätöksensä niiden perusteella. Motivaation on oltava aitoa, sillä ihmisen on uskottava aidosti periaatteisiin, jotta voidaan olettaa hänen toimivan niiden mukaan. Tietoturvaetiikka on johdettava yleisemmistä etiikoista, jotta ei syntyisi ristiriitaisuuksia. Esimerkkeinä ihanteista voidaan ottaa rehellisyys, luotettavuus ja muiden vahingoittamisen välttäminen. Tietoturva-asiantuntijana voi olla myös ilman hyviä ja yleisesti hyväksyttyjä eettisiä periaatteita, mutta tällöin kyseistä henkilön arvomaailma ei toteuta alan ihanteita.

14.2 Tietoturvaetiikan eri roolit

Tietoturva-asiantuntijoilla tulee olla ammattietiikka aivan kuten muiden alojen ammattilaisillakin. Asiantuntijuus tuo mukanaan vastuun, sillä työssä on mahdollisuus vaikuttaa moneen eri asiaan ja päästä käsiksi tietoihin työnkuvan vuoksi. Alla olevassa Bynumin taulukossa [Kuva 17] on listattu mahdollisia rooleja tietoturva-asiantuntijalle [Bynum]. Eri rooleihin sisältyy erilaisia tavoitteita ja etuja, jotka voivat olla keskenään ristiriidassa. Tarkoitus on tiedostaa mahdolliset ristiriidat ja välttää niitä. Roolit eivät sulje toisiaan pois, vaan tietoturva-asiantuntija toimii monessa roolissa samaan aikaan.

Työnantaja - Työntekijä
Asiakas - Asiantuntija
Asiantuntija - Asiantuntija
Yhteiskunta - Asiantuntija

Kuva 17. Tietoturva-asiantuntijan roolit [Bynum]

Tietoturva-asiantuntijat saavat elantonsa tietoturvaongelmien takia, sillä työ sisältää ongelmien ja niiden seurausten käsittelyä. Tämä ristiriita on aina syytä muistaa ja nähdä asiat kokonaisuutena. Tietoturvatyö ei ole kuitenkaan pelkkää ongelmien ratkontaa, työhön sisältyy myös suunnittelua ja toteutusta. Tarkoituksena on ylläpitää, korjata ja parantaa tietoturvallisuutta ja siihen liittyviä asioita. Epäeettinen toiminta voisi olla sellaista, että korjataan vain oireita, mutta jätetään itse syyt korjaamatta tai pelotellaan aiheettomasti uhkakuvilla. Liiallinen oireiden pintapuolinen korjailu vahingoittaa alan uskottavuutta ja jatkuva kilpailu johtaa lopulta tilanteeseen, jossa epäeettisesti toimivat työntekijät korvataan paremmilla. Tietoturva-asiantuntijoiden ja työntekijöiden tavoitteena tulee olla tietoturvan kokonaisvaltainen parantaminen yhteistyötä tekemällä Pelkästään taloudellisten tai muiden henkilökohtaisten syiden mukaan toimimista ei sinänsä voida lukea eettiseksi. Pitkällä aikavälillä voidaan nähdä asiantuntijan todellinen arvo, sillä asiantuntijan on opeteltava oma toimintaympäristönsä ja organisaation erityspiirteet. Organisaation tietoturvan parantaminen ei onnistu ilman asiantuntijoiden apua.

Tietokoneilla ja tietojärjestelmillä on kasvava rooli yhteiskunnassa. Tämän vuoksi tietoturvaetiikan olemassa olo on tärkeää ja välttämätöntä. Tietokoneita voidaan käyttää hyviin ja pahoihin tarkoituksiin. Yritysten ja organisaatioiden tietoturvapolitiikan ja ohjeiden tulee toteuttaa hyvää tietojenkäsittelyn etiikkaa aivan samalla tavalla kuin ihmisten on noudatettava sitä.

Tietoturvasäännöt voidaan tehdä hyvinkin selkeiksi määrittelemällä kaiken mikä on sallittua tai kiellettyä. Etiikka kuitenkin neuvoo ja ohjaa tilanteissa, joissa ohjeet ovat riittämättömät tai ristiriitoja esiintyy. Tämä on kuitenkin harvoin mahdollista ja usein keskitytään päälinjauksiin, joista voidaan johtaa tarkemmat yksityiskohdat. Laki ja asetukset määrittävät vain osan vaatimuksista ja usein nämä vaatimukset eivät ole luonteeltaan eettisiä. Laki ja moraali voivat olla ristiriidassa, siksi eettisiin säännöstöihin on otettava tämä huomioon.

Helenius pohtii moraalin merkitystä osana tietoturvallisuutta [2005, s. 6]. Hänen mielestään, jos tietoturvan parantuminen jatkuu toivottuun suuntaan, niin jatkossa tarvitaan yhä vähemmän nykyisen kaltaista tietoturvan ylläpitoa, kehitystä, tutkimusta ja koulutusta. Tähän on kuitenkin vielä paljon matkaa. Tietoturva-asiantuntijan vastuulle voi jäädä turvallisuuden arvioiminen ja objektiivisuuden saavuttaminen tässä asiassa on vaikeaa, toisessa ääripäässä houkuttimena on raha ja toisessa arvot. Niin kauan kun on ongelmia, töitä riittää ja ongelmien täydellinen korjaus ei ole yhtä tuottavaa kuin vähittäinen korjaus. Tämä ajatusmalli on arveluttava ja epäeettinen. Asiantuntija ei saa hyödyntää asemaansa liikaa ja tuloksia pitää syntyä. Helenius ehdottaa

ratkaisuksi, että tietoturvan riippumatonta tutkimusta on tuettava, jotta positiivinen kehitys ei pysähdy pelkästään hyödyn tavoittelun vuoksi. Puolueeton taloudellinen tukeminen takaa omalta osaltaan vaihtoehtoisten tutkimuksen, jonka tuloksina voi tulla erilaisia tuloksia kuin tulosrahoitteisilla tutkimuksilla.

14.3 Tietoturvaetiikan toteutuminen

Etiikasta on syytä erottaa palkitseminen ja rankaiseminen. Joskus halutun toiminnan edesauttamiseksi tai pakottamiseksi voidaan asettaa kiihokkeita tai rangaistuksia. Eettiset periaatteet perustuvat kuitenkin valinnan mahdollisuuteen. Silloin kun nämä palkinnot ja rangaistukset nousevat määräävämmiksi kuin eettiset periaatteet, tietoturvakäsitys on vääristynyt. Tietoturvallisuuteen liittyvien virheiden ja epäkohtien esiintuomiseksi saattaa olla tarpeen palkita vakavien virheiden ja ongelmien löytämisestä. Paradoksaalista tässä on se, että henkilö voi joutua käyttämään epäeettisiä menetelmiä löytääkseen tai todistaakseen epäkohtien olemassaolon. Tästä on esimerkkinä virusten levittäminen tai tietoturva-aukkojen paljastaminen hyökkäyksillä. Tarkoitukset voivat olla hyvät, mutta niihin pääsemiseksi on toimittava eettisiä periaatteita vastaan. Tällainen toiminta on kuitenkin yleisesti kielletty tietoturvan ja tietojenkäsittelyn eettisissä normistoissa.

Tietoturvallisuus on ihmisten keskinäisellä tasolla myös sosiaalista toimintaa. Väärinkäytösten tai rikosten selvittämisessä vaarana voi olla se, että teon paljastajan maine kärsii. Työilmapiiri voi muuttua rennosta epämiellyttäväksi, jos aletaan vaalia tiukkaa valvontakulttuuria, jossa pienimmästäkin virheestä rangaistaan. Luottamusta vaaditaan puolin ja toisin. Järvinen [2002, s. 294] varoittaa tulehtuneesta työilmapiiristä, jossa työntekijät alkavat rikkoa sääntöjä ja toimia yrityksen etua vastaan. Tietoturvan liittyvien ongelmien selvittämisessä on toimittava lakien mukaan ja hyviä tapoja noudattaen. Tyytymättömyys tai vastaava kauna voi olla syynä tilanteeseen, jossa organisaation oma työntekijä alkaa tehdä tihutöitä. Järvinen [2002, s. 124] käsittelee hyvin hakkerin ja omaan henkilökuntaan kuuluvan tietoja ja motiiveja tietoturvahyökkäystapauksissa [Kuva 18]. Kaikkein vaarallisin yhdistelmä syntyy, kun hakkeri ja henkilökuntaan kuuluva yhdistävät voimansa. Uhka voi siis tulla ulkopuolelta ja sisäpuolelta.

Hakkerit	Oma henkilökunta
uteliaisuus	selkeä päämäärä
kokeilunhalu	hyötymistarkoitus
ei tiedä mitä hakee	tietää mitä hakee
monta kohdetta	yksi kohde
ei tunne turvajärjestelyjä	tuntee turvajärjestelmät
paljon julkisuutta	vähän julkisuutta

Kuva 18. Järvisen taulukko vihollisista [2002, s. 124]

Liiallinen ihmisten palkitseminen, kehuminen, rankaisemin tai valvonta ei palvele tietoturvallisuuden etua. Oikeanlaisen asenteen syntymisen pohjana pitää olla ymmärrys siitä, että vahva tietoturva on kaikkien etujen mukaista ja jokainen voi vaikuttaa omalla panoksellaan. Yleisimpiä väärinkäsityksiä tietoturvasta ovat että se on vain johdon ylhäältä pakotettua toimintaa tai asiantuntijoiden propagandaa oman tärkeytensä pönkittämiseksi.

Ihminen toimii aina joko tahallisesti tai tahattomasti. Näiden kahden tavan erottaminen voi olla ulkopuolisesta vaikeaa. Joskus ihminen itse ei osaa sanoa tarkasti mihin hänen oma toimintansa on perustunut, onko se ollut tietoa, tunnetta vai jotain muuta. Kokemuksen tuoma osaaminen iskostuu usein alitajuiseksi toiminnaksi ja ihmisen tarvitsee yhä vähemmän turvautua ohjeisiin ja muiden ihmisten apuun. Rangaistuksilla ja sanktioilla voidaan määrittää mitä seuraamuksia kielletystä tai haitallisesta toiminnasta halutaan antaa. Turha tietoturvan vaarantaminen on erityisen vaarallista. Tahallinen toiminta yhdistettynä luottamusaseman tai työtehtävän hyväksikäyttöön omien etujen ajamiseksi on selvä merkki ammattietiikan matalasta tasosta.

Tietokoneilla ei ole moraalia tai tunteita. Kuitenkin puhutaan vihamielisistä ohjelmista. Ihmiset käyttävät tietokoneita työvälineinä omia tarkoitusperiään varten. Haittaohjelmia, viruksia, mainos- ja vakoojaohjelmia, tietoturva-aukkoja ja muuta haitallista ohjelmakoodia käytetään pahantahtoiseen toimintaan. Hyvä tietoturvaetiikka on tällaista toimintaa vastaan. Ihmisiä voidaan huiputtaa ja suostutella paljastamaan tietoja. Tietokoneita varten pitää käyttää hyväksi suunnitteluvirheitä ja aukkoja suojauksissa. Ihmisiä hyväksikäyttämällä eli sosiaalisella houkuttelulla voidaan päästä käsiksi tietokoneiden sisältämään tietoon esimerkiksi houkuttelemalla käyttäjiä kertomaan salasanojaan ja vakoiluohjelmia voidaan käyttää esimerkiksi salasanojen kaappaamiseen käyttäjän näppäillessä ne näppäimistöllä. Kaikkien näiden erilaisten haittaohjelmien luomiseen tarvitaan tietoturva-asiantuntijuutta. Haittaohjelmien käyttäminen voi kuitenkin olla helppoa, mutta itse ohjelmien tekeminen vaatii taitoa.

Tietoturvallisuusasioista on tiedotettava ja koulutettava ne ihmisille, jotta ei voida vedota tietämättömyyteen. Osaamattomuuden tunnustaminen on paljon hyväksyttävämpää kuin omien taitojen ja tietojen liioittelu. Tätä kuitenkin tapahtuu kun ei haluta olla huonompia kuin muut tai pelätään että tietämättömyys on jotenkin häpeällistä. Siksi on tärkeää että tietoturvasuunnitelmissa, -kartoituksissa ja -koulutuksessa otetaan huomioon tämä. Ei voi olettaa automaattisesti, että kaikki tietävät kaiken, vaan pitää selvittää ensin mitä kukin tietää ja mitä ei. Vasta tämän perusteella voidaan suunnitella koulutusta ja selvittää epäkohtia. Koska tietoturva-ala kehittyy nopeasti, voi jopa asiantuntijoilla olla vanhentuneita tai vääriä käsityksiä tietoturvasta. Kaikkien osapuolten kannalta on hyvä että jokaiselle kohdennetaan kykyjä ja työtehtäviä vastaavaa koulutusta. Tietoturvallisuus on yhtä vahva kuin sen heikoin lenkki. Tätä heikointa osaa voidaan kuitenkin vahvistaa monin tavoin.

14.4 HAMKin tietoturvakulttuuri

HAMKissa sekä johto, että henkilökunta suhtautuvat suotuisasti tietoturva-asioihin Jari Kivelän lausunnon mukaan. Mutta asian tärkeyttä ei tiedosteta riittävästi eikä huomata pientenkin asioiden vaikuttavan tietoturvaan. Asenteita pitäisi parantaa niin, että jokainen ottaisi omissa työtavoissaan tietoturvan paremmin huomioon. Muutosvastarintaa ei HAMKissa laajemmin ole. Alituiset kirjautumiset moniin järjestelmiin aiheuttavat vaivaa, josta valitetaan. Työntekijät eivät ota aktiivisesti kantaa tietoturva-asioihin, sillä asia nähdään vielä liian tietoteknisenä. Työntekijöille tiedotetaan aika ajoin tietoturvasta, kun tehdään muutoksia järjestelmiin (esim. salasanojen laadusta) ja virusepidemioiden aikana. Johdon ja työntekijöiden vastuut tietoturvasta ovat periaatteessa tiedossa, mutta näkökulman teknisyydestä johtuen omien toimintatapojen merkitystä tietoturvaan ei nähdä. Vastuuta ei tässä mielessä tunneta riittävästi. Paras lääke tietoturvan tunnetuksi tuomiseen on johdon vastuun ottaminen ja tiedottamisen ja ohjeistamisen lisääminen. Tuntematon tietoturva jää etäiseksi asiaksi ja siitä ei voi ottaa vastuuta, kun ei oikein tiedä mistä vastuu pitäisi ottaa.

15 Yhteenveto

Olen jakanut tutkimukseni tulokset kolmeen osaan yhteenvedon selkeyttämiseksi. Ensimmäisessä osassa esitän vastaukset tutkimuskysymyksiin ja perustelut niille. Toisessa osassa selvitän tutkimuksen aikana heränneitä ajatuksia, ja mitä uutta opin tutkiessani tietoturvallisuutta. Kolmannessa osassa tiivistän tietoturvaselvityksen tulokset ja parannusehdotukset HAMKille.

15.1 Tutkimuskysymyksiin vastaaminen

Ensimmäisenä tutkimuskysymyksenä oli, voidaanko BS 7799 tietoturvastandardi, ITIL-prosessit ja VAHTI-ohjeet yhdistää ja toisena oli selvittää näiden sisältöä. Sisältöä on käyty tämän tutkimuksen aikana läpi omissa luvuissaan ja näin vastattu kysymykseen. Tämän selvitystyön kautta pystyn vastaamaan ensimmäiseen kysymykseen myönteisesti, sillä olen poiminut kaikista kolmesta hyviksi katsomiani osia. Kaikissa kolmessa käytetään hallintajärjestelmä tärkeänä osana tietoturvaa. Lisäksi jokaiseen näistä kolmesta ohjeistosta kuuluu oleellisena osana sen annettujen ohjeiden ja suositusten soveltaminen tapauskohtaisesti. Katson että tekemäni yhdistely on juuri tällaista soveltamista. Vastaukset tutkimuskysymyksiin ”miten yllämainitut soveltuvat opetusorganisaation tarpeisiin?” ja ”mikä on HAMKin tietoturvallisuuden tila ja miten sitä voi parantaa” kehittyivät yhdessä tutkimuksen edetessä. Käytin kaikkia kolmea ohjeistoa HAMKin tietoturvallisuuden selvitystyössä, joten sain hyvän kuvan niiden käytännön soveltuvuudesta. Osa asioista oli HAMKin tapauksessa soveltumattomia ja osa sopi sellaisenaan hyvin. Selväksi kävi kuitenkin, että opetusorganisaatiolla on omia erityistarpeita, joita ei voi täydellisesti huomioida pelkällä yksittäisen ohjeiston soveltamisella. Soveltaminen on tässä tapauksessa paras termi kuvaamaan toimintaa, sillä orjallisesti seuraaminen tekee toiminnasta kankeaa ja todellisuudessa huonosti soveltuvaa.

Mitään tietoturvastandardia tai ohjeistusta ei voi siis suoraan lähteä toteuttamaan tuntematta ensin omaa organisaatiota ja sen erityispiirteitä riittävän hyvin. Esimerkiksi BS 7799:n ensimmäistä osaa tietoturvallisuuden hallinnasta ei kannata lähteä toteuttamaan, jos toisen osan mukaista tietoturvallisuuden hallintajärjestelmää ei ole ohjeen mukaisesti järjestetty. On toki mahdollista aloittaa tietoturvan parantaminen ilman hallintajärjestelmää, mutta työ on tehotonta ja työn tuloksien pysyvyydelle ei ole takeita.

Tietoturvakehityksen aloitusvaihe on raskas ja siksi suosittelen VAHTI-ohjeilla aloittamista. Niissä otetaan huomioon aloittava tietoturvaorganisaatio hyvin ja luodaan edellytyksiä standardien myöhemmälle seuraamiselle paremmin kuin BS 7799:ssä.

Käsittelen seuraavaksi ohjeistojen sisältöä ja perusperiaatteita tarkemmin. BS 7799 ja ITIL käyttävät molemmat kehämallia prosessissaan. Niitä ei voi kuitenkaan verrata suoraan keskenään, sillä ne ovat erilaisia luonteeltaan. ITILin avulla voidaan luoda tietoturvaprosesseja ja BS 7799:n avulla tarkistaa niiden turvallisuus standardin mukaisiksi. ITILIä ja VAHTIa on helppo lukea ymmärtää, BS 7799 on paljon teknisemmin kirjoitettu.

ITIL ei esittele kontrolleja, jolloin BS 7799 kontrolleja tarvitaan kun halutaan toteuttaa kontrolleja. ITILiä ei voi sertifioida, BS 7799:n voi sertifioida virallisesti. ITILissä on esitetty vastaavuus BS 7799ään sisältöön. Useat BS 7799 asiat ylittävät kuitenkin ITILin laajuuden ja tämä selvisi myös tutkimuksen aikana verrattaessa lähteiden sisältöä vastaavissa kohdissa, kun ITILissä ohitettiin jokin BS 7799:ssä käsitelty asia kokonaan tai se vain pintapuolisesti esiteltiin. ITILissä todetaan, että BS 7799 on selkeästi määritelty tietoturvallisuuden standardi, jonka suosituksia tulisi noudattaa tietoturvallisuuden hallinnassa.

VAHTI-ohjeiden vahvuuksina ovat esimerkit ja ohjeet käytännön toiminnan tekemiseen. Ohjeiden jakaminen erillisiin dokumentteihin on käytännönläheistä. Näin voidaan tarvittaessa kehittää yksittäisiä osa-alueita ja tarvittava tieto löytyy nopeasti. Ohjeet ovat suomenkielisiä ja ne ovat varta vasten suunniteltu suomalaisten organisaatioiden käyttöön, vaikkakin valtionhallinto on pääasiallinen sovelluskohde. VAHTI-ohjeita kehitetään ja päivitetään nopeaan tahtiin. Varsinkin viime vuosina on luotu monia uusia dokumentteja ja ohjeita.

VAHTI-ohjeissa otetaan huomioon tietoturvan nollatasolta lähtevät organisaatiot. Tietoturvatyössä tarvittavaa osaamista voi hankkia kouluttautumalla ja oppimalla käytännön tilanteista. Tietoturva-alan jatkuva kehittyminen vaatii asiantuntijoiltaan kehityksen seuraamista ja lisäkoulutusta. Apuvälineinä on erilaisia aputyökaluja (toolbox) sekä ulkopuolisten ammattilaisten tarjoama apu. Tietoturvatyössä erilaisten tietolähteiden yhdistäminen on tarpeellista, sillä harvoin jokin yksittäinen standardi, hyvien käytäntöjen kokoelma tai ohjeisto on yksinään riittävä. Näiden eri lähteiden näkemyserot, menetelmät ja ominaisuudet antavat monia näkökulmia tietoturvaan. Lisäksi näiden erot, heikkoudet ja vahvuudet, soveltuvuus, ajankohtaisuus, laajuus ja ymmärrettävyys vaihtelevat. Viisas valitsee näistä parhaat osat.

ITILiin sisältyvien parhaiden käytäntöjen käyttöön ottaminen on tehokasta, sillä näin vältytään yleisimmiltä ongelmilta, kun aletaan kehittää omia menetelmiä. ITIListä saadaan parhaita käytäntöjä, joita voidaan suoraan muokata omaan käyttöön sopiviksi. Organisaation jo olemassa olevia omia hyviä käytäntöjä pitää vaalia ja dokumentoida, sillä niiden käyttö voi olla

esimerkiksi vain tiettyjen ihmisten taitotietoja, jolloin kyseisten henkilöiden lähtiessä organisaatiosta ne häviävät.

Tiivistettynä BS 7799 kertoo, mitä pitää tehdä, ITIL kertoo miten ja VAHTI-ohjeet tekevät molempia. BS 7799 ja VAHTI ovat mielestäni pääasiallisia työkaluja niille, jotka ovat vasta aloittamassa tietoturvallisuuden hallintaa. ITIL on puolestaan aputyökalu niille, joilla on jo jonkinlainen tietoturvallisuuden hallintajärjestelmä ja siihen halutaan parannuksia. Pikaisella tutkinnalla näkökulmat ja käytetyt termit voivat olla erilaiset, mutta tavoite on kaikissa sama. Nämä seikat ovat myös hyviä syitä yhdistää näitä kolmea. Eri näkökulmista tarkasteltuna tietoturva-asioita voidaan ymmärtää paremmin, eikä juututa ajatukseen, että asioille on vain yksi sopiva ratkaisutapa. Jonkin standardin epäselvästi selitetty asia selkenee, kun etsitään vastaava kohta jostain toisesta ohjeistuksesta. Näin voidaan paremmin varmistua siitä, että ymmärretään ohjeistuksia niin kuin ne on tarkoitettu.

Yhteistä näille BS 7799:lle, ITILille ja VAHTI-ohjeille on se, että niiden täysivaltaiseen toteuttamiseen vaaditaan tietoturvallisuuden hallintajärjestelmä, joka toimii suunnittele-toteuta-tarkasta-kehitä-menetelmällä (PDCA). Jos tietoturvakehityksessä halutaan kattavasti etsiä eri vaihtoehtoja kehitystyön ohjeiksi, suosittelen, että näitä kolmea mainittua vertaillaan ja otetaan käyttöön itselle sopivat osat. Jos standardeja ja ohjeita seurataan orjallisesti, saattaa tietoturvaan tulla mukaan osa-alueita, joita ei oikeasti tarvita. Liian raskaan järjestelmän ylläpitäminen ei toimi ja huomiota ei riitä oikeasti tärkeille asioille.

15.2 Huomioita tietoturvallisuudesta ja tutkimuksesta

Tutkimuksen aikana minulle selvisi lukuisia mielenkiintoisia asioita tietoturvallisuudesta. Käyn läpi seuraavaksi esille tulleita ajatuksia ja teorioita. Nykyään organisaatioilta vaaditaan erityistä panostusta tietoturvaan. Apuna tässä on tietoturvallisuuden hallintajärjestelmä, jonka avulla tiedetään, mistä ollaan tulossa, mitä juuri nyt tapahtuu, minne pitäisi olla menossa ja mitä pitää tehdä, jotta tavoitteeseen päästään. Kehämallin periaatteen mukaan hallintajärjestelmä paranee niin kauan kuin sitä ylläpidetään. Tietoturvaympäristö ei pysy staattisena, koska sisäiset ja ulkoiset muutokset takaavat, että ajan kuluessa myönteisiä ja kielteisiä muutoksia tapahtuu. Näihin muutoksiin on sopeuduttava.

Vastuun ottaminen ja kehitysprosessin läpivienti ovat tietoturvallisuudessa tärkeitä tekijöitä. Kontrolleilla ja parhailla käytännöillä varmistutaan, että jokaisella osa-alueella tai resurssilla on siitä vastaava henkilö.

Hyvä tietoturva vaatii koulutusta ja asennetta. Haluttu tietoturvataso ei toteudu, jos ei panosteta riittävästi sekä osaavaan työvoimaan että turvalliseen tekniikkaan. Yrityksen tai organisaation johto ja sen asettamat

tietoturvaperiaatteet ja toimintaohjeet määrittävät, miten yrityksessä periaatteessa pitäisi toimia. Käytännössä nämä vaatimukset harvoin toteutuvat kirjaimellisesti ohjeiden mukaan, ja tähän on syytä varautua. Käytän termiä asettaa, sillä johdolla on valta päättää, miten he suhtautuvat tietoturvaan. Jos vastuuta ei tunnisteta tai asia ei kiinnosta, tietoturva jää huomioimatta. Työilmapiiri vaikuttaa myös tietoturvaan. Tietoturvan on siksi oltava vakituinen ja luonnollinen osa työkulttuuria ja arkityötä. Yksittäisen ihmisen panos kertautuu positiivisesti, kun kaikki työntekijät pitävät huolta tietoturvasta.

Johdolle pitää pystyä perustelemaan tietoturvan merkitys. Tietotekniikkapalveluista tulee kiinteämpi osa organisaatiota, jos niiden rooli ymmärretään paremmin. Kontrollit ja parhaat käytännöt vaativat tietoteknisten resurssien ja -palveluiden luokittelua ja tarkastelua sekä yksinään että kokonaisuutena. Tuloksena on resurssien selkeytyminen, kun vuorovaikutussuhteet tunnetaan. Tietotekniikkapalveluita on tutkittava koko niiden elinkaaren ajan. Usein ei nykyisten palveluiden tilaa tiedetä, jolloin eletään uskomusten varassa. Tutkimalla ja testaamalla saadaan todellista tietoa ja voidaan toimia paljon luotettavammin ja tehdä parempia suunnitelmia, kun yllätyksiä ei tapahdu niin helposti. Tietoturvan kehitysprosessin tukena on hyvä olla koulutettuja ihmisiä, konsultteja ja alan kirjallisuutta. Tietotekniikkahallinnan kustannustehokkuus paranee, kun tietojenkäsittelyn prosessit hallitaan ja tunnetaan paremmin. Kun tiedetään, mitä tarvitaan ja kenelle, ei synny ali – tai ylikapasiteettia. Prosessien läpikohtainen tunteminen antaa mahdollisuuden perustella, miksi tietoturvallisuuteen on panostettava varoja.

Organisaatioiden tietoturvan budjetti ei ikinä riitä täydellisiin ja kaikki osa-alueet kattaviin suojauksiin. Riskien hallinnalla ja kustannusten selvittämisellä saadaan tärkeää tietoa varojen osoittamiseen oikeisiin kohteisiin. Riskien todennäköisyyttä pienentämällä ja seurausten minimoimisella voidaan välttyä suurilta kustannuksilta, jos ja kun jokin uhka toteutuu.

Yhteisien kontrollien ja yhtenevien termien käytöllä helpotetaan huomattavasti organisaatioiden sisäistä ja -välistä kommunikaatiota tietotekniikka-asioista. Sekaannuksia tai väärinymmärryksiä tapahtuu näin vähemmän.

Tietoturvan kehityksen aloitus on vaativa tehtävä organisaatiolle. Tietoturvakehityksen ensimmäiseltä kehitystasolta on pyrittävä tarmokkaasti seuraavalle. Tavoitteena on aina toiminnan parantaminen, nopeuttaminen ja muut. Ensimmäisellä tasolla tietoturva on muutamien yksittäisten ihmisten vastuulla, samoin korkeammilla tasoilla muutamat ihmiset tekevät tärkeimmät ohjauspäätökset. Aloittavalla tietoturvaorganisaatiolla on kehitettävää joka osa-

alueella. On osattava priorisoida, mitä tehdään ja mitkä kohteet vaativat eniten kehitystä ja suojaa. Tärkein yksittäinen osa-alue on tietoturvan hallintajärjestelmä, joka pitää sisällään kaikki kehityksessä tarvittavat osat aina suunnitelmista käytännön menetelmiin. Erona AD Hoc toimintaan on muiden ihmisten ja järjestelmien tuki päätösprosessissa. Miten siis vakuutetaan organisaation johto tietoturvan tärkeydestä, ja miten saadaan tietoturvatyöhön resursseja? Vaaditaanko toteutuneita riskejä ennen kuin todella ymmärretään suojausten tärkeys?

Tietoturvakehityksen aloittamisessa organisaatiolla täytyy olla vastuuhenkilöt, myönteinen tietoturvakulttuuri, jokin toimiva hallintorakenne, jokin standardi tai ohjeisto, jonka mukaan toimia ja riittävä määrä budjetoituja resursseja. Kun tietoturvatyö on saatu alulle, sitä ei saa lopettaa. Saavutetut edut voidaan menettää, jos tietoturvaa ei mitata, seurata, ylläpidetä ja kehitetä. Eikä ole syytä unohtaa tietoturvan kaikkien tärkeintä osaa eli ihmistä. Ihminen tekee virheitä kuten myös parantaa tietoturvaa. Organisaation on panostettava tietoturvakoulutukseen, jos halutaan, että tietoturvakäytännöt ovat todella käytössä eivätkä vain hienoja suunnitelmia.

Organisaatiosta riippuen suurin ongelma tietoturvan parantamiselle ei ole välttämättä rahan riittäminen vaan muutosvastarinta ja toimintatapojen muuttamisen pelko työntekijöissä. Tietoturvan sosiaalinen puoli ei saa missään vaiheessa unohtua. Valittaessa tietoturvan kehitykseen standardeja ja ohjeita pitää huomioida, miten niissä otetaan huomioon sitä käyttävien ja sitä toteuttavien ihmisten tarpeet ja osaaminen. Jos onnistutaan saamaan työntekijät työskentelemään tietoturvan hyväksi pakottamatta ja omasta tahdosta, tietoturvan toteutumisen suurin este on voitettu.

Riskianalyysien teon aikana ymmärsin, että jo tiedostettuihin riskeihin ja uhkiin varautuminen ei pelkästään riitä. Ajan tasalla pysyminen ja muutosten hallinta antavat mahdollisuuden ennustaa ja arvioida mahdollisia uusia uhkia ja niiden mahdollistamia riskejä. Oman työympäristön tunteminen on vahvuus riskien hallinnassa, sillä valmiita riskianalyysiohjeita ainoastaan seuraamalla voi jäädä huomaamatta uniikkeja, juuri omaan työympäristöön liittyviä erityispiirteitä. Itse riskianalyysien suorittamista ja analyysimenetelmiä kannattaa myös kehittää ja parantaa, sillä tietoturvan hallintajärjestelmän parantaminen vaatii parempia työkaluja.

Tutkimuksessa tuli vastaan paljon minulle ja Kivelälle uusia asioita tietoturvasta. Pitkäkestoisen tutkimuksen vaatimukset ja yhteistyö muiden osapuolten kanssa antoivat paljon kokemusta. Tutkimukseni teoriat on koottu BS 7799:stä, ITIListä ja VAHTI-ohjeista. Niiden perusteita soveltumista käytäntöön on tutkittu huolellisesti ennen niiden julkaisua, joten pidin niitä luotettavina lähteinä. Myös lähdekirjojen kirjoittajat ovat maininneet

teorioidensa pohjautuvat omiin käytännön kokemuksiin. Riskianalyyseissa käytin VAHTI-ohjeiden mallia, joten analyysini toteuttavat VAHTI-ohjeiden vaatimuksia. Lähdemateriaalin kritiikkinä haluan erotella yksittäisten kirjoittajien ja standardien tyylieroja ja tapoja tuoda asioita esille. VAHTI, BS 7799 tai ITIL eivät juuri sisällä mielenkiintoisia huomautuksia tai uusia ideoita. Kirjojen kirjoittajilla oli mukana omia, omiin ajatusmalleihin ja kokemuksiin perustuvia näkemyksiä asioista. Mielestäni nämä kaksi näkökulmaa, persoonallinen ja persoonaton antoivat mahdollisuuden arvioida kummankin tyyppisiä kirjoituksia ja niiden tarkoitusperiä. Persoonaton teksti on tarkoitettu välittymään lukijalle sellaisenaan. Tarkoituksena ei ole välttämättä herättää erityisiä ajatuksia tai kyseenalaistaa sanomaa. Toisin on yksityisten kirjailijoiden teksteissä. He ilmoittavat, että tämä on heidän tapansa ilmaista asiat ja lukijalla on oikeus muodostaa ja arvostella lukemaansa ja siihen suorastaan kehotetaan.

Tutkimuksen edetessä kävi selväksi, että aihealueen laajuudesta johtuen ei olisi mahdollista tehdä täysin kaikenkattavaa tutkimusta, sillä liian pitkään kestävän tutkimuksen tulokset eivät valmistuessaan enää välttämättä olisi todellisuutta vastaavia. Tutkimuksen tarkoituksena oli toimia alkusysäyksenä tietoturvan parantamiselle HAMKissa ja vanhentuneet tiedot eivät olisi paljoa auttaneet. Myös tietoturvastandardeissa tapahtui kehitystä tutkimuksen aikana: BS 7799:stä kehitettiin ISO 17799 ja tämä kehitys jatkuu edelleen.

15.3 Tulokset HAMKille

HAMKille käytännön hyödyt tutkimuksesta ovat parannusehdotukset ja perustelut tietoturvallisuuden parantamiselle. Nämä ohjeet on koottu jokaisen luvun loppuun, josta ne on helppo poimia. Katson, että tämän tutkimuksen selvitys tietoturvallisuudesta ja siihen liittyvistä tekijöistä antaa riittävästi tietoa, jotta asiaan perehtymätön ymmärtää, miten laaja alue tietoturvallisuus on. Tämä toivottavasti selkeyttää sitä näkemystä, että tietoturvallisuus ei ole pelkästään tekninen asia, joka ei juuri kosketa tavallista työntekijää.

Luvun 5 riskienanalyysien lukemisella saa mielestäni hyvän tilannekatsauksen, sillä riskit on jaoteltu aihealueittain. Tätä listaa voi käyttää tarkistuslistana, kun riskitekijöihin aletaan puuttua.

Yksi tärkeimmistä huomioista HAMKin tapauksessa on se, että yhden henkilön täytyy aluksi ottaa vastuu tietoturvan kehityksestä. Tämän henkilön täytyy vakuuttaa HAMKin johto tarvittavista toimenpiteistä ja siitä että kehitystyötä viedään eteenpäin. Kun työ on kerran aloitettu, sitä on helpompi viedä eteenpäin, kun avuksi saadaan hallintajärjestelmä ja vastuuryhmä. Osaava henkilöstö on myös suureksi avuksi, sillä he osaavat toimia turvallisesti ja myös omatoimisesti. Tässä tutkimuksessa esitettyjen asioiden tulisi vakuuttaa

HAMKin johto siitä, että tietoturvallisuuteen on panostettava. Toivon, että tietoturva-asioihin panostaminen aloitetaan mahdollisimman pian. Hyvin suunniteltu on kuitenkin vasta puoliksi tehty. Alla olen tiivistänyt parannusehdotukset listaksi.

Tutkimukseni perusteella HAMKissa täytyy tietoturvan parantamiseksi tehdä seuraavat asiat:

- Koota asiantunteva tietoturvaryhmä
- Määrätä tietoturvallisuuteen liittyvät vastuut paremmin
- Luoda ja ylläpitää tietoturvan hallintajärjestelmä, joka noudattaa PDCA -mallia
- Luotava ja hyväksytettävä virallisiksi tietoturvapolitiikka ja muu tietoturvadokumentaatio ja – ohjeistukset
- Korjata riskianalyyseissä löydetyt tietoturvariskit tärkeysjärjestyksessä
- Parantaa henkilökunnan tietoturvatietoisuutta ja kouluttaa heitä
- Henkilökunnan tulisi lukea ja allekirjoittaa tietotekniikkapalveluiden käyttösäännöt

Yllä olevat asiat eivät ole varsinaisessa tärkeysjärjestyksessä, mutta suosittelen aloitettavaksi ylhäältä alas käytännön syistä. Tietoturvaryhmän luomisella saadaan paras aloitus tietoturvan kehittämiselle. Tämän jälkeen korjausten eteneminen tapahtuu luonnollisessa järjestyksessä, sillä työt täytyy ensin jakaa ja vastuuttaa, jotta ne tulevat tehdyiksi.

Kivelä halusi tutkimuksen antavan pohjan tietoturvan kehitykselle kokonaisuutena. Tämä tutkimus on tarkoitus esitellä HAMKin sisällä siitä kiinnostuneille henkilöille. Kaikkia tutkimuksen teossa tarvittavia henkilöitä HAMKista ei valitettavasti saatu kiinni tutkimuksen teon aikana ja heiltä olisin tarvinnut tietoja. Tämä ei kuitenkaan estänyt tutkimuksen tekemistä.

Toivon, että riskianalyysejä tehdään ja kehitetään myös jatkossa. Ajan tasalla on hyvä pysyä, siksi tietoturvallisuutta on syytä auditoida riittävän usein ja erityisesti suurten olomuutoksien jälkeen. Omat hyvät tietoturvakäytännöt kannattaa huomioida ja taltioida.

Tutkimukseni aikana HAMKissa tapahtui muutoksia, joilla oli vaikutuksia tietoturvallisuuteen. Hajanaisista verkkopalveluista siirryttiin yhtenäiseen portaaliin. Tietohallintojohtajan paikka annettiin hakuun ja täytettiin. Nämä kaikki vaikuttavat positiivisesti HAMKin tietoturvaan, sillä lisäresurssit ja toimintojen yhtenäistäminen tekevät hallinnasta tehokkaampaa. Tämän tutkimuksen tarkoitus on jatkaa tätä positiivista suuntaa.

VIITELUETTELO

[ACM] Association for Computing Machinery, ACM Code of Etchics and professional Conduct, http://www.acm.org/constitution/code.html (tarkistettu 11.02.2007).

[BS 7799-1:fi, 2000] Suomen Standardoimisliitto SFS, BS 7799-1:fi. ”*Tietoturvallisuuden hallinta. Osa 1. Tietoturvallisuuden hallintaa koskeva menettelyohje*”. 2000. 2. painos.

[BS 7799-2:fi, 2003] Suomen Standardoimisliitto SFS, BS 7799-2:fi. ”*Tietoturvallisuuden hallintajärjestelmät. Vaatimukset ja soveltamisohjeet*”. 2003. 3. painos.

[BSI-global] BSI British Standards homepage http://www.bsi-global.com/ (tarkistettu 18.12.2005).

[Burd et al., 2005] Information Security in Academic Institutions Emerging Issues and Remediation Strategies, *Journal of Security Education*, Volume 1, Numbers **2-3**, 3 March 2005, pp. 55-68(14).

[Bynum, 2001] Terrell Bynum, "*Computer Ethics: Basic Concepts and Historical Overview*", *The Stanford Encyclopedia of Philosophy (Winter 2001 Edition)*, Edward N. Zalta (ed.), saatavana myös http://plato.stanford.edu/archives/win2001/entries/ethics-computer/ (tarkistettu 11.02.2007).

[BSI-global] BSI British Standards homepage http://www.bsi-global.com/ (tarkistettu 11.02.2007).

[EFQM] European Foundation for Quality Management, http://www.efqm.org/ (tarkistettu 11.02.2007).

[Ficora] Viestintäministeriö, http://www.ficora.fi/suomi/index.html (tarkistettu 11.02.2007).

[Finlex, 2006] Finlex, Valtion säädöstietopankki, http://www.finlex.fi (tarkistettu 11.02.2007).

[Funet] Funetin ja tutkimusyhteisön muiden verkkojen käytön etiikasta, http://www.csc.fi/suomi/funet/etiikka.html.fi (tarkistettu 23.3.2006).

[Gehringer, 2005] Dr. Edward F. Gehringer, Department of Computer Science, North Carolina State University, http://ethics.csc.ncsu.edu/ (tarkistettu 11.02.2007).

[Helenius, 2005] Marko Helenius, *Tietoturvallisuuden tutkimus ja opetus, Nykytilanne ja kehittämismahdollisuudet, Selvitys, Tietoyhteiskuntainstituutin raportteja 2/2005*, Tietojenkäsittelytieteiden laitos, Tampereen yliopisto, Tampereen yliopistopaino Oy saatavana myös http://www.uta.fi/laitokset/ISI/dokumenttiarkisto/ISI-raportti2005_2.pdf (tarkistettu 11.02.2007).

[HAMKin verkkosivut, 2007] Hämeen ammattikorkeakoulun portaali, http://portal.hamk.fi/.

[IEEE] Institute of Electrical and Electronics Engineers Code of Conduct, http://www.ieee.com/portal/pages/about/whatis/code.html (tarkistettu 18.12.2005).

[ISO/IEC 17799:2005(E)] *ISO/IEC 17799 Information Technology - Security techniques- Code of Practice for information security management Second edition*, 2005.

[ITIL, 2004] IT Information Libarary, *Security Management*, 2004.

[Järvinen ja Järvinen, 2000] Pertti Järvinen ja Annikki Järvinen, *Tutkimustyön metodeista*. Opinpajan kirja, Tampere, 2000.

[Järvinen, 2003] Pertti Järvinen, *Atk-toiminnan johtaminen*, 2003.

[Järvinen, 2002] Petteri Järvinen, *Tietoturva & yksityisyys*, 2002.

[Kyrölä, 2001]Tuija Kyrölä, *Esimies ja tietoriskien hallinta*, 2001.

[Miettinen, 1999] Juha E. Miettinen, *Tietoturvallisuuden johtaminen - näin suojaat yrityksesi toiminnan*, 1999.

[Opetusministeriö, 2005] Tietoyhteiskunnan rakenteet oppilaitoksissa. Vuoden 2004 kartoitusten tulokset ja vuosien 2000 - 2004 yhteenveto, Opetusministeriön työryhmämuistioita ja selvityksiä 2005:31., 2005, saatavana myös http://www.minedu.fi/OPM/Julkaisut/2005/tietoyhteiskunnan_rakenteet_oppilaitoksissa_vuoden_2004_kartoit?lang=fi

[Paavilainen, 1998] Juhani Paavilainen, *Tietoturva*, Espoo, Suomen Atk-kustannus, 1998.

[Tammisalo, 2005] Tero Tammisalo, *Sosiaali- ja terveydenhuollon tietojärjestelmien tietoturvan ja tietosuojan hallinnan periaatteet ja hyvät käytännöt, Ohje sosiaali- ja terveydenhuollon organisaatioille ja toimintayksiköille tietojärjestelmien tietoturvan ja tietosuojan kehittämiseksi*, Stakesin monistamo, Helsinki, 2005.

[Tietosuojavaltuutettu] Tietosuojavaltuutetun toimisto, http://www.tietosuoja.fi (tarkistettu 11.02.2007).

[Tietoturvaopas] Tietoturvaopas, http://www.tietoturvaopas.fi/ (tarkistettu 11.02.2007).

[VAHTI] Valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI), http://www.vm.fi/vm/fi/13_hallinnon_kehittaminen/09_Tietoturvallisuus/01_tietoturvaryhma_VAHTI/index.jsp (tarkistettu 11.02.2007).

[VAHTI, 2006] Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) ohjeet määräykset vuosilta 1999-2006, saatavana myös http://www.vm.fi/vm/fi/13_hallinnon_kehittaminen/09_Tietoturvallisuus/02_tietoturvaohjeet_ja_maaraykset/index.jsp (tarkistettu 11.07.2006).

[VAHTI, 6/2006] Valtionhallinnon Tietoturvatavoitteiden asettaminen ja mittaaminen, VAHTI 6/2006, http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20060720Tietot/Vahti_6_06.pdf (tarkistettu 11.02.2007).

[VAHTI 3/2005] *Tietoturvapoikkeamien hallinta*, VAHTI 3/2005, saatavana myös http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20050101Tietot/95673.pdf (tarkistettu 11.02.2007)

[VAHTI 2/2005] *Valtionhallinnon sähköpostien käsittelyohje*, VAHTI 2/2005 saatavana myös http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/94935_fi.pdf (tarkistettu 11.02.2007).

[VAHTI 3/2004] *Haittaohjelmilta suojautumisen yleisohje*, VAHTI 3/2004, saatavana myös http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/88078_fi.pdf (tarkistettu 11.02.2007).

[VAHTI 2/2004] *Tietoturvallisuus ja tulosohjaus*, VAHTI 2/2004, saatavana myös http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20040420Tietot/86049.pdf (tarkistettu 11.02.2007).

[VAHTI 1/2004] *Valtionhallinnon tietoturvallisuuden kehitysohjelma 2004-2006*, VAHTI 1/2004, saatavana myös http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/70508_fi.pdf (tarkistettu 11.02.2007).

[VAHTI 7/2003] *Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa*, VAHTI 7/2003, saatavana myös http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/53828/53827_fi.pdf (tarkistettu 11.02.2007).

[VAHTI 6/2003] *Opas julkishallinnon tietoturvakoulutuksen järjestämisestä*, VAHTI 6/2003, http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/53763/53760_fi.pdf (tarkistettu 11.02.2007).

[VAHTI 5/2003] *Käyttäjän tietoturvaohje*, VAHTI 5/2003, saatavana myöshttp://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/51027/51024_fi.pdf (tarkistettu 11.02.2007).

[VAHTI 4/2003] *Valtionhallinnon tietoturvakäsitteistö*, VAHTI 4/2003, saatavana myös

http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/50903/50902_fi.pdf (tarkistettu 11.02.2007).

[VAHTI 3/2003] *Tietoturvallisuuden hallintajärjestelmän arviointisuositus*, VAHTI 3/2003, saatavana myöshttp://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/53808/53805_fi.pdf (tarkistettu 11.02.2007).

[VAHTI 1/2003] *Valtion tietohallinnon Internet-tietoturvallisuusohje*, VAHTI 1/2003, saatavana myös http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/39680/39681_fi.pdf (tarkistettu 11.02.2007).

[VAHTI 3/2002] *Valtionhallinnon etätyön tietoturvallisuusohje*, VAHTI 3/2002, saatavana myös http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20060411Valtio/etatyon_ohje.pdf (tarkistettu 11.02.2007).

[VAHTI 1/2002] *Tietoteknisten laitetilojen turvallisuussuositus*, VAHTI 1/2002, saatavana myös http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20020101Tietot12158/turvallisuussuositus.pdf (tarkistettu 11.02.2007).

[VAHTI 6/2001] *Valtion tietotekniikkahankintojen tietoturvallisuuden tarkistuslista*, Vahti 6/2001, saatavana myöshttp://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/6193/6194_fi.pdf (tarkistettu 11.02.2007).

[VAHTI 4/2001] *Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje*, Vahti 2001, saatavana myöshttp://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/3371/3372_fi.pdf (tarkistettu 11.02.2007).

[VAHTI 2/2001] *Valtionhallinnon lähiverkkojen tietoturvallisuussuositus*, VAHTI 2/2001, saatavana myöshttp://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/3375/3378_fi.pdf (tarkistettu 11.02.2007).

[VAHTI 3/2000] *Valtionhallinnon tietojärjestelmäkehityksen tietoturvallisuussuositus*, VAHTI 3/2000, saatavana myös http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valt

ionhallinnon_tietoturvallisuus/3389/3391_fi.pdftarkistettu (tarkistettu 11.02.2007).
[VM] Valtiovarainministeriö, http://www.vm.fi/ (tarkistettu 11.02.2007).
[Yliopistojen tietoturvasivut] Yliopistojen tietoturvasivut, http://www.yliopistojentt.fi/ (tarkistettu 11.02.2007).
[Yliopistojenit] Yliopistojen tietotekniset palvelusivut, http://www.yliopistojenit.fi (tarkistettu 11.02.2007).
[Yliopistojen U-CIRT, 2005] Tietoturvapolitiikka, Yliopistojen U-CIRT -työryhmä 17.1.2005, http://www.yliopistojentt.fi/yhteiset/tietoturvapolitiikka2005.pdf (tarkistettu 11.02.2007).
[Vahti cd 2004] VAHTI tietoturva cd 2004 cd, http://www.yliopistojentt.uta.fi/VAHTI-CD/ (tarkistettu 11.02.2007).
[Yliopistojen U-CIRT, 2005] Seuraamusasteikot (henkilökunta, opiskelija, muut), Yliopistojen U-CIRT -työryhmä 17.1.2005, http://www.yliopistojentt.fi/yhteiset/sanktioasteikko.pdf (tarkistettu 11.02.2007).
[Yliopistojen U-CIRT, 2005] Tietotekniikkarikkomusten seuraamiskäytäntö, Yliopistojen U-CIRT -työryhmä 17.1.2005, http://www.yliopistojentt.fi/yhteiset/seuraamukset2005.pdf (tarkistettu 11.02.2007).
[Yliopistojen U-CIRT, 2005] Tiedottaminen poikkeamatilanteissa, Yliopistojen U-CIRT -työryhmä 17.1.2005, http://www.yliopistojentt.fi/yhteiset/tiedottaminen_poikkeamatilanteissa2005.pdf (tarkistettu 11.02.2007).
[Yliopistojen U-CIRT, 2005] Tietoturvapoikkeamiin reagoiminen, Yliopistojen U-CIRT -työryhmä 17.1.2005, http://www.yliopistojentt.fi/yhteiset/reagointiohje2005.pdf (tarkistettu 11.02.2007).
[Yliopistojen U-CIRT, 2005] Tietojärjestelmien ylläpitosäännöt, Yliopistojen U-CIRT -työryhmä 17.1.2005, http://www.yliopistojentt.fi/yhteiset/yllapito2005.pdf (tarkistettu 11.02.2007).
[Yliopistojen U-CIRT, 2005] Ohjeet tietoaineistojen käsittelystä tietojärjestelmien käyttöoikeuden haltijan kuoltua, Yliopistojen U-CIRT -työryhmä 17.1.2005, http://www.yliopistojentt.fi/yhteiset/kuolemantapaus2005.pdf (tarkistettu 11.02.2007).
[Yliopistojen U-CIRT, 2005] Toimenpiteet tietojärjestelmien käyttöoikeuden loputtua, Yliopistojen U-CIRT -työryhmä 17.1.2005,

http://www.yliopistojentt.fi/yhteiset/muu_poistuminen2005.pdf (tarkistettu 11.02.2007).

[Yliopistojen U-CIRT, 2005] Sähköpostin suodatusohje, Yliopistojen U-CIRT -työryhmä 17.1.2005, http://www.yliopistojentt.fi/yhteiset/suodatusohje2005.pdf (tarkistettu 11.02.2007).

[Yliopistojen U-CIRT, 2005] Sovellusohje sääntöön Sähköpostin käsittelysäännöt, Yliopistojen U-CIRT -työryhmä 17.1.2005, http://www.yliopistojentt.fi/yhteiset/sahkopostin_sovellusohje2005.pdf (tarkistettu 11.02.2007).

[Yliopistojen U-CIRT, 2005] Sähköpostin käsittelysäännöt, Yliopistojen U-CIRT -työryhmä 17.1.2005, http://www.yliopistojentt.fi/yhteiset/sahkopostisaanto2005.pdf (tarkistettu 11.02.2007).

[Yliopistojen U-CIRT, 2005] Tietojärjestelmien käyttösäännöt, Yliopistojen U-CIRT -työryhmä 17.1.2005, http://www.yliopistojentt.fi/yhteiset/kayttosaannot2005.pdf (tarkistettu 11.02.2007).

LIITE 1. HAMKIN RISKIEN ARVIOINTILOMAKE

		Kohde: HAMK ja Kehittämisyksikkö Laatijat: Lauri Hämäläinen ja Jari Kivelä			**Analyysit suoritettu 2006-2007**
Vaaraa/uhkaa aiheuttava tilanne	**Arvio: Kyllä, Ei, Ei koske meitä**	**Seuraukset**	**Riski**	**Nykyinen varautuminen**	**Toimenpide-ehdotukset/ lisäkysymyksiä**
1. Tietoriskien hallinnan johtaminen ja organisointi					
1.1 Hallinnollinen tietoturvallisuus					
1.1.1 Johdon tietoisuus riskeistä					
Onko organisaation johto tietoinen tietoriskien vaikutuksista liiketoimintaan?	Kyllä	Johto ei ymmärrä tietoriskien ja tietoturvallisuuden merkitystä	0	Johto on tietoinen tietoriskeistä	Ei vaadi toimenpiteitä
Onko tunnistettu organisaation toiminnalle elintärkeät tiedot?	Kyllä	Jos elintärkeitä tietoja ei tunnisteta, niitä ei osata ja voida suojata	0	Elintärkeät tiedot on tunnistettu	Ei vaadi toimenpiteitä
1.1.2 Oireita tietoriskeistä					
Onki toimitilojen rikosturvallisuudesta on huolehdittu?	Kyllä	Rikosturvallisuuden laiminlyönti altistaa murroille, ilkivallalle, varkauksille ja omaisuusvahingoille	0	Rikosturvallisuudesta on huolehdittu	Ei vaadi toimenpiteitä
Ovatko työntekijät ovat sitoutuneet työhönsä ja työnantajaansa eivätkä ole esim. siirtymässä kilpailijalle?	Kyllä	Työntekijän menettäminen	0	Työntekijät eivät ole siirtymässä muualle	Ei vaadi toimenpiteitä
Voiko luottaa siihen, että organisaation palveluksesta lähteneet tai irtisanotut eivät levitä tietoja organisaatiosta?	Kyllä	Organisaation luottamuksellisia tietoja levitetään ulkopuolelle	0	Työntekijöihin luotetaan	Ei vaadi toimenpiteitä
Onko laitteiston ja toimitilojen paloturvallisuudesta on huolehdittu?	Kyllä	Laitteisto ja toimitilat ovat alttiita tulipaloille	0	Turvallisuudesta on huolehdittu	Ei vaadi toimenpiteitä

Toimiiko koko henkilöstö huolellisesti ja rehellisesti?	Kyllä	Epärehellinen tai huolimaton toiminta altistaa riskeille	0	Henkilöstö toimii huolellisesti ja rehellisesti	Ei vaadi toimenpiteitä
Seurataanko edellä mainittuja häiriötilanteita?	Ei	Ei tiedetä mitä on sattunut ja mitä vaikutuksia häiriöillä on ollut	3	Ei ole varsinaista seurantaa. Rikosturvallisuutta seurataan	Häiriötilanteita pitäisi seurata tarkemmin ja kirjata ylös
1.1.3 Tietoriskien hallinnan johtaminen					
Onko organisaation omaisuuden ja tietojen suojaamistahto vastuutettu nimetylle henkilölle organisaation johdossa?	Ei	Toiminnan turvallisuuden hallinnasta ei vastaa kukaan	0	Ei ole yleistä turvallisuuspäällikköä, vastuut on hajautettu.	Ei vaadi toimenpiteitä
Onko organisaation omaisuuden ja tietojen suojaamistahto konkretisoitu tietoturvapolitiikaksi ja käytännöiksi?	Ei	Tietoriskien johtaminen on vaikeaa ilmain yhtenäisiä periaatteita ja käytäntöjä	4	Tietoturvapolitiikka on keskeneräinen ja käytännöt hajanaisia.	On luotava virallinen tietoturvapolitiikka, josta käy ilmi parempi suojaamistahto
Arvioidaanko tietojen käsittelytapoja ja turvajärjestelyjä laatujärjestelmän audiointien yhteydessä?	Ei	Turvajärjestelyjen ja tietojen käsittelytapoja ei tunneta tarpeeksi hyvin	4	Käytössä ei ole auditointeja	Itseaudioinnin kehittäminen ja käyttöönottaminen tulevaisuudessa suunnitelmien mukaan. Yksiköt auditoivat toisiaan.
Onko johdolla valmiutta vakuuttaa sidosryhmille tietojen ja tietämyksen säilyvyys organisaatiossa?	Ei	Audiointien puuttuessa ei ole konkreettisia todisteita esittää pyydettäessä	2	Selvitykset viranomaisille, kuntayhtymälle ja yhteistyökumppaneille ovat kunnossa	Auditointien käyttöönotolla saadaan todisteet tietojen suojauksien toimivuudesta
Onko laadittu tietoturvasuunnitelmaa?	Ei	Tietoturvan hallintaprosessia ei voi aloittaa ilman suunnitelmia	4	Tietoturvasuunnitelma on keskeneräinen	Tietoturvasuunnitelma tehdään loppuun, hyväksytetään ja otetaan käyttöön
Raportoidaanko tietoturvasta suoraan ylimmälle johdolle?	Ei	Johto ei ole tietoinen organisaation tietoturvatilasta, ei osata resursoida riittävästi	2	Raportoidaan vain tapahtuneista asioista	On järjestettävä 6-12 kk välein katsauksia, joissa käydään läpi menneitä tapahtumia ja suunnitellaan jatkoa
1.1.4 Tietoriskien tunteminen					
Onko tunnistettu tilanteet, jotka saattavat lamauttaa toiminnan?	Ei	Tilanteisiin ei voida riittävästi varautua	3	Tunnetaan osittain, esim. tietoliikennekatko ja jäähdytysjärjestelmän häiriö.	On tunnistetta lisää lamauttavia tilanteita ja kirjattava ne ylös

Onko tunnistettu tilanteet, jotka häiritsevät ja haittaavat toiminnassa tarvittavien tietojen saantia?	Kyllä	On tunnistettu todennäköisimmät tilanteet	3	Yksittäinen tietojärjestelmä voi aiheuttaa häiriöitä	Kirjataan ylös kuvaukset tilanteet, jotka voivat vaikuttaa tietojen saantiin
Onko tunnistettu tilanteet, jotka voivat aiheuttaa tietojen häviämisen tai muuttumisen?	Ei	Tietojen muuttumisella voi olla vakavia seurauksia	3	Muuttumista on vaikea havaita , virheet ovat harvinaisia, mutta esim. päivitykset voivat niitä aiheuttaa	On selvitettävä miten tarkasti ja millä menetelmillä pidetään tiedot
Onko arvioitu em. tilanteiden menetyksiä tai vahinkoja?	Ei	Vakuuttaminen ja varautuminen tilanteisiin on tuntematonta	3	Mittausta ei voi tehdä tai se on vaikeaa	Arvioidaan vähintään karkeasti pahimpien riskien seurauksia
Onko turvakäytäntöjen kehittämiskustannukset suhteutettu toiminnan keskeytymisestä aiheutuviin menetyksiin?	Ei	Menetyksien sattuessa ei ole resursseja palautumiseen	3	Ei tiedossa	Turvakäytäntöjen kehityskustannusten suhde menetyksiin on arvioitava vähintään karkeasti
1.1.5 Tietoriskien hallintamenettelyt					
Onko turvaamisen tavoitteet määritelty?	Ei	Ilman tavoitteita ei tiedetä mitä pitää suojata	3	Turvaamisen tavoitteet keskeneräisinä suunnitelmissa	Turvaamisen tavoitteet täytyy määritellä
Onko turvatyön mittarit määritelty?	Ei	Tietoturvatyön onnistumista ei voi mitata	2	Mittareita ei ole käytössä	On otettava käyttöön selkeät laadulliset ja määrälliset mittarit
Onko organisaatiolla toiminnan turvaamisen strategia osana toimintastrategiaa?	Ei	Toiminnan turvaamista ei huomioida tarpeeksi	1	Toiminnan turvaamista ei erityisesti tuoda esiin. Perusasiat ovat kunnossa	Ei vaadi toimenpiteitä
Onko organisaatiolla käytettävissä laaja-alaista turva-asioiden osaamista	Ei	Tietoturvaa on vaikeaa hallita ilman pätevää osaamista	3	Puute tällä hetkellä	Tietohallintojohtajan virka on vasta täytetty.
Onko olemassa toimintamalli tietokonevirusten hallitsemiseksi?	Kyllä	Tietokonevirukset leviävät hallitsemattomasti ilman turvamallia	1	Malli on käytössä	Ei vaadi toimenpiteitä
Onko olemassa toipumissuunnitelma ja toimintaohjeet, jotka ohjaavat vastuuhenkilöitä ja muuta henkilöstöä varajärjestelyjen käyttöönotossa ja toiminnassa häiriötilanteissa?	Ei	Häiriöistä on vaikea toipua, palveluihin syntyy katkoksia	3	Ei tiedossa	Suunnitelmat ja ohjeet on luotava
Onko peruskäyttäjille laadittu ja tiedotettu tietoturvaohjeet?	Ei	Peruskäyttäjä ei osaa toimia oikein tietoturvan hyväksi ja ei ole olemassa ohjeita	2	Hajanaisia ohjeita, joissa paljon parannettavaa	On luotava tietoturvaohjeet ja tiedotettava ne tehokkaasti ja

					ymmärrettävästi käyttäjille
Seurataanko järjestelmien käyttöä esimerkiksi etäkäyttöä epämääräisinä kellonaikoina, tärkeiden tietojen kopiointia tai lähettämistä?	Ei	Järjestelmiä käytetään käyttötarkoitusten vastaisesti	1	Ei aktiivisesti seurata	?
Onko olemassa tiedottamismenettely, jolla kerrotaan organisaatiossa tapahtuneesta häiriötilanteesta tarvittaville osapuolille?	Ei	Häiriöistä ei kulje tietoa tai se vääristyy tai kulkee ulkopuolisille	2	Ei ole olemassa valmista menettelyä	On luotava tiedottamismenettely
Vastaako joku turvakäytäntöjen kehittämisestä?	Kyllä	Turvakäytäntöjä ei kehitetä ilman vastuuta		Kehittämisyksikkö vastaa	Ei vaadi toimenpiteitä
Onko organisaatiossa tietoturvaryhmä?	Ei	Tietoturvan parantamisessa tarvitaan monta osapuolta	1	Ei ole	Tietoturvaryhmän voisi koota taloushallinnosta, opiskelijahallinnosta ja teknisestä henkilöstöstä ja kokoontua 1-2 kertaa vuodessa
Onko poikkeusolojen tietojenkäsittelyn valmiussuunnitelma?	EKM	Poikkeusoloissa pitää toimia eri tavalla kuin tavallisesti	1	Poikkeusoloissa HAMKin ei tarvitse toimia.	Ei vaadi toimenpiteitä
Onko laadittu suunnitelmia häiriötilanteisiin ja tietoturvahyökkäysten/haittaohjelmien varalle?	Ei	Häiriöt ja hyökkäykset aiheuttavat vahinkoja	3	Ei ole	Tarvitaan suunnitelmia uhkan pienentämiseksi
2. Tietoriskit suhteissa asiakkaisiin ja sidosryhmiin					
2.1 Hallinnollinen tietoturvallisuus					
2.1.1 Asiakas ja sidosryhmäsuhteiden suunnittelu					
Onko yhteistyökumppanit luokiteltu toiminnan jatkuvuuden kannalta elintärkeisiin, tärkeisiin ja tarpeellisiin?	Ei	?	2	Kumppaneita ei ole paljoa, luokittelua ei tarvita	ATK-laite-, tietoliikenne- ja puhelutoimittajat ovat tärkeimmät

Onko eri osapuolten valinnassa otettu myös tietoriskit huomioon? (Tahojen luotettavuus, kyky hallita heille luovutettuja tietoja jne.)	Ei	Osapuoliksi saatetaan valita epäluotettavia kumppaneita	1	Tietoriskejä ei suoraan oteta huomioon, mutta toimittajan luotettavuus on tärkeä valintakriteeri.	Tietoriskien pitäisi olla yksi valintakriteereistä
Onko kaikilla osapuolilla sama käsitys yhteistyösuhteiden luonteesta?	Kyllä	Yhteistyö ei suju jos asioista ollaan eri mieltä	0	Yhteistyötä tehdään yhteisymmärryksessä	Ei vaadi toimenpiteitä
2.1.2 Toiminnan tietoriskien tunnistaminen					
Onko arvioitu kumppaneilla tapahtuvat tilanteet, jotka aiheuttavat haittaa organisaation toiminnalle?	Ei	Kumppaneille tapahtuvat ongelmat voivat yllättää	0	Kumppaneita ei arvioida	Kumppanit vastaavat itsestään
Onko kumppaneilla kirjallinen tietoturvapolitiikka ja toimintamallit tietojen käsittelyyn?	EKM	Kumppanien tietoturvaa ei voi todeta	0	?	Kumppanit vastaavat itsestään
Onko omassa organisaatiossa tietoturvapolitiikka dokumentoitu siten, että dokumentti voidaan luovuttaa kumppaneille ja kumppanit saavat sen perusteella kuvan toiminnan luotettavuudesta?	Ei	Kumppaneille ei voi luovuttaa mitään, luottamus voi kärsiä	1	Ajantasaista dokumentointia ei ole tehty. Vanha dokumentti ei ole enää kelvollinen.	Tietoturvapolitiikka dokumentoidaan sen valmistuttua
Onko kaikkien kumppanien tietoturvallisuustoiminta katselmoitu yhteistyössä?	EKM	Turvallisuustoiminnan laatua ei tunneta	0	Katselmointia ei tehdä	Kumppanit vastaavat itsestään
2.1.3 Verkosto- ja alihankintasuhteiden käynnistys					
Onko yhteistyöhön luotu yhteiset tietoturvaperiaatteet?	Ei	Yhteistyö toimii ilman tietoturvaperiaatteita	3	Ei ole luotu	Yhteistyöhön tarvitaan tietoturvaperiaatteet
Onko yhteistyökumppanien välisiin sopimuksiin liitetty organisaation tietoturvavaatimukset sekä tietojen siirron ja käsittelyn menettelyohjeet?	Ei	Sopimuksista ei ole apua jos tietoturvassa esiintyy ongelmia	3	Ei ole tehty	Sopimuksiin tulisi liittää tietoturvavaatimukset ja menettelyohjeet tietojen käsittelylle
Sovitaanko erilliskäytäntöjä luottamuksellisten, kuten tuotekehityksen, tietojen käytöstä, siirto- ja suojaustavoista?	Ei	Luottamuksellisia tietoja käytetään väärin	0	Erilliskäytännöistä sovitaan tarvittaessa	Ei vaadi toimenpiteitä

Onko kaikki osapuolet koulutettu yhteisiin tietojärjestelmiin?	EKM	Yhteisien tietojärjestelmien käyttö ei suju	0	Ei koske	Ei koske
Onko yhteistyössä edellytettävät tietoturvaperiaatteet, menettelytavat ja järjestelmät koulutettu alihankkijoille?	EKM	Alihankkijoiden kanssa toiminta on vaikeaa	0	Ei koske	Ei koske
Onko suunniteltu, miten hallitaan yhteistyösuhteen päättyminen?	Ei	Kumppanille saattaa jäädä tunnuksia tai muuta tietoa, joihin ei ole enää oikeutta	3	Suunnitelmia ei ole	On luotava suunnitelmat yhteistyön päättymiselle
2.2 Fyysinen turvallisuus					
2.2.1 Asiakkaiden ja yhteistyökumppaneiden käynnit toimitiloissa					
Syntyykö asiakaskäynneillä tai yhteistyökontakteissa kuva oman organisaation luotettavuudesta ja luottamuksellisuudesta?	Ei	Organisaation maine kärsii, jos asioita ei hoideta uskottavasti	0	Asia kunnossa	Ei vaadi toimenpiteitä
Pidetäänkö muiden asiakkaiden, yhteistyötahojen ja projektien tiedot suojassa? (Ei neuvotteluhuoneissa, ei asiakaspalvelutiloissa)	Ei	Tiedot voivat kadota tai niitä voidaan varastaa	0	Asia kunnossa	Ei vaadi toimenpiteitä
Onko neuvottelutilat ääni- ja näköeristetty?	EKM	Asiattomat voivat seurata ja salakuunnella neuvotteluja	0	Ei koske	Eristykselle ei ole tarvetta
Selvitetäänkö uusien vierailijoiden taustat riittävän huolellisesti? (Koskee sekä kotimaisia että ulkomaisia vierailijoita).	EKM	Epämääräsiten vieriaden päästäminen organisaation tiloihin luo riskejä	0	Ei koske	Ei ole tarvetta selvittää
2.3 Käyttöturvallisuus					
2.3.1 Tietoturvaratkaisut					
Onko olemassa käytäntö, jolla käsitellään kumppanin henkilöstön tarve päästä organisaation tietoliikenneverkkoon ja järjestelmiin?	Kyllä	Hallitsematon tietoverkkoihin ja järjestelmiin pääsy on vaarallista. Järjestelmissä ja verkoissa voi aiheuttaa vahinkoa helpommin kuin niiden ulkopuolella	0	On olemassa, sovitaan kumppanikohtaisesti	Ei vaadi toimenpiteitä
Onko sovittu osapuolten toimenpiteet eri häiriötilanteiden hoitamiseksi?	Ei	Häiriötilanteissa vastuut ja toiminta vaativat selvittämistä	2	Ei ole sovittu	On sovittava toimenpiteet ennen häiriöitä

Arvioidaanko kumppanien turvakäytäntöjä?	Ei	Kumppaninen turvakäytännöt voivat olla puutteellisia		Ei arvioida / Ei koske	Kumppanit vastaavat itsestään
3 Henkilöstön tietoisuus ja toimintatavat tietoriskien hallinnassa					
3.1 Henkilöstöturvallisuus					
3.1.1 Henkilöstön tietoisuus tietoriskeistä					
Onko henkilöstölle koulutettu toiminnan luottamuksellisuuteen ja tietosuojaan liittyviä yleispiirteitä?	Ei	Toiminnan luottamuksellisuus ja tietosuojan tunteminen eivät ole kaikilla tiedossa	3	Toiminnan luottamuksellisuus ja tietosuojan tunteminen eivät ole kaikilla tiedossa	On korostettava henkilöstölle toiminnan luottamuksellisuutta ja tietosuojaan liittyviä asioita koulutuksen avulla
Tunteeko henkilöstö organisaation vastuut tietojen luottamuksellisuuden ja muun tietoturvallisuuden suhteen?	Ei	Jos vastuita ei tunneta, tietoturvallisuus ja luottamuksellisuus kärsivät	3	Koko henkilöstö ei tiedä vastuitaan, mutta jotkut ryhmät tietävät.	On korostettava henkilöstölle tietoturvallisuuden ja siihen liittyvien vastuiden merkitystä esim. koulutuksen avulla
Onko kaikille selvää, millaiset tiedot ovat kaikkein tärkeimpiä ja joiden suojaaminen on erityisen tärkeää?	Ei	Tärkeimpien tietojen suojeleminen ei ole pääasia	3	Koko henkilöstö ei tiedä mitkä ovat tärkeimpiä tietoja	Korostetaan työtehtävästä riippuen mitkä ovat tärkeimmät suojeltavat tiedot
Onko kaikille selvää, mitä organisaation toiminnasta saa kertoa ulkopuolisille?	Ei	Organisaation luottamuksellisia tietoja levitetään ulkopuolelle	3	Kaikille ei ole selvää.	Määritetään ohjeet organisaation tietojen kertomiselle ulkopuolisille
Onko organisaatiolle määritelty tietoturvaperiaatteet ja laadittu niiden toteuttamiseksi ohjeet?	Ei	Tietoturvan hallinnalle ei ole toimintatapoja	4	Organisaation tietoturvaperiaatteet ja niiden toteuttamisohjeet ovat keskeneräisiä	On luotava tietoturvaperiaatteet ja toteuttamisohjeet niille
Kattavatko ohjeet sähköisten tietojärjestelmien lisäksi suullisen viestinnän ja paperidokumenttien käsittelyn ja jakelun?	Ei	Suullisessa viestinnässä ja paperidokumenttien käsittelyssä voi syntyä riskejä	4	Suulliselle viestinnälle ja paperidokumenttien käsittelylle ei ole ohjeita	On luotava ohjeet viestintään ja dokumenttien käsittelyyn
Onko henkilöstö koulutettu tunnistamaan tietoriskejä ja noudattamaan turvakäytäntöjä?	Ei	Riskejä toteutuu, kun niitä ei osata varoa. Turvakäytäntöjä ei ole ja niitä ei osattaisi käyttää.	4	Henkilöstöllä ei ole kattavaa tietoturvakoulutusta	Henkilöstöä on koulutettava mielekkäästi ja työtehtävien vaatimusten mukaan.

Onko olemassa menettely tietoturva-asioiden käsittelyä varten?	EKM	Tietoturva-asioita hoidetaan vaihtelevilla tavoilla, yhtenäisyyden puute aiheuttaa ongelmia	3	Ei ole erityisiä käytäntöjä käytössä	Käytännöt on luotava
Onko jokainen työntekijä allekirjoittanut tietojen käyttösäännöt?	Ei	Työntekijät voivat vedota väärinkäytöksissä siihen, että he eivät tunne tai ole hyväksyneet käyttösääntöjä	3	Kaikki työntekijät eivät ole allekirjoittaneet	Kaikkien työntekijöiden pitää kirjoittaa käyttösäännöt
Onko tietojen luokittelu ja ohjeet osa arkipäivän käytäntöä?	Ei	Tietoja ei luokitella	1	Tietojen luokittelua ei käytetä	Joitakin tietoja on tarpeen luokitella
Tietääkö henkilöstö, minne ilmoittaa havaitsemistaan tietoturvarikkeistä tai käytäntöjen puutteista?	Ei	Ongelmia ja puutteita ei selvitetä,	0	ATK-ylläpitohenkilöstölle ilmoitetaan tarvittaessa	Ei vaadi toimenpiteitä
3.1.2 Uudet työntekijät ja työsuhteen päättyminen					
Tarkistetaanko uusien työntekijöiden taustat ennen työsuhteen alkamista?	EKM	Rikosrekisteri tai muut epäselvyydet voivat tehdä työntekijästä sopimattoman työtehtävään	0	Taustoja ei tarkisteta	Taustoja ei ole tarpeen tarkistaa
Ovatko tietoturva-asiat mukana uusien työntekijöiden perehdyttämisessä?	Ei	Tietoturva ei ole mukana työntekijän työtavoissa ja asenteessa	4	Ei ole erityisesti korostettu koulutuksessa	Uusien työntekijöiden perehdyttämisessä kerrotaan tietoturvasta
Selvitetäänkö myös uusille ja väliaikaisille työntekijöille yrityksen tietoturvapolitiikan ja vaitiolositoumuksen merkitys?	Ei	Uudet ja väliaikaiset työntekijät eivät ole tietoisia tietoturvapolitiikan ja vaitiolositoumuksen merkityksestä	4	Työntekijöille ei ole kerrottu tietoturvapolitiikasta. Vaitiolovelvollisuus ymmärretään paremmin.	Työntekijöille pitää selvittää tietoturvapolitiikan ja vaitiolositoumuksen merkitys
Allekirjoittavatko työntekijät erillisen sitoumuksen tietojen ja järjestelmien käytöstä sekä tietojen palauttamisesta työsuhteen jälkeen?	Ei	Sopimukseen on vaikea vedota, jos sitä ei ole allekirjoitettu	4	Työntekijät eivät kattavasti allekirjoita sitoumusta	Kaikkien työntekijöiden tulisi lukea ja allekirjoittaa sopimus
3.1.3 Työsuhteen päättyminen					

Onko henkilön irtisanoutumistilanteessa esimiehellä tieto kaikista henkilön käyttäjätunnuksista ja käyttöoikeuksista, joiden voimassaolo tulee poistaa?	Ei	Henkilö saattaa päästä vanhoilla tunnuksilla organisaation järjestelmiin tietoihin käsiksi tarpeettomasti	0	Tunnuksien poisto on automatisoitu, esimiehen ei tarvitse hoitaa tunnusten poistoa	Ei vaadi Toimenpiteitä
Onko suunniteltu muut toimet tietoturvallisuuden varmistamiseksi työsuhteiden päättyessä?	Ei	Avaimia, laitteita tai vastaavia tavaroita saattaa jäädä henkilölle. Sähköposti ja puhelin pitää sulkea, jotta niitä ei voi käyttää omiin tarkoituksiin	1	Ei suunnitelmia, tapauskohtaista	On suunniteltava toimenpiteet työsuhteen päättymisen hoitamiseksi turvallisesti.
3.1.4 Henkilöstön toimintatavat					
Käsittelevätkö työntekijät luottamuksellisia tietoja vain työnsä kannalta tarkoituksenmukaisella tavalla?	Kyllä	Tietoja voidaan käyttää muuhun kuin työhön	0	Työntekijöihin luotetaan	Ei vaadi toimenpiteitä
Onko organisaation keskeiset tiedot suojattu mm. rajaamalla niiden saatavuus ja määrittelemällä niiden käyttöoikeudet?	Kyllä	Tietojen vapaa saatavuus kaikille altistaa tiedot väärinkäytöksille ja vahingoille	0	Käyttöoikeuksien hallinta on käytössä tietojen suojaamisessa	Ei vaadi toimenpiteitä
Onko minimoitu mahdollisuus myydä tai luovuttaa ulos organisaatiosta sille keskeisiä tietoja ja dokumentteja?	Ei	Tietojen ja dokumenttien leviäminen organisaation ulkopuolelle ei ole sallittua ja voi vahingoittaa organisaatiota	1	Organisaatiossa ei ole varsinaisia kaupallisesti hyödynnettäviä tai salaisia tietoja. Hankkeissa voi olla yhteistyöyritysten tietoja.	Ei vaadi toimenpiteitä
Ovatko organisaation sisäiset valvontajärjestelmät kunnossa (työn työnvalvonta, tilojen valvonta, tietojen käytön ja tietojärjestelmien valvonta)?	Ei	Väärinkäytöksiä ja muita ongelmia ei havaita ja tunnisteta	1	Organisaation sisäinen valvonta on löysä. Tärkeimmissä kohteissa kuten taloushallinto valvonta hoidetaan vaaditulla tavalla	Ei vaadi toimenpiteitä
Onko työntekijöiden omin töiden tekeminen työpaikalla hallittua (ajat, kulkuoikeudet, valvonta)?	Ei	Työntekijät käyttävät työaikaa muuhun kuin varsinaiseen työhönsä	1	Työntekijät eivät tee muita töitä työajallaan	Ei vaadi toimenpiteitä
Onko luottamuksellisten tietojen säilyttämiseen riittävästi lukollisia tiloja?	Kyllä	Lukottomien tilojen käyttö altistaa tiedot varkauksille ja väärinkäytölle	0	Lukollisia tiloja on tarpeeksi	Ei vaadi toimenpiteitä

Hoidetaanko jätepaperin keräys ja käsittely hallitusti?	Kyllä	Jätepaperin huolimattomassa käsittelyssä saattaa joukkoon jäädä luottamuksellista tietoa luotettavassa muodossa	0	Jätepaperin käsittelyn hoitaa ulkoinen yritys ja paperi säilytetään lukituissa astioissa	Ei vaadi toimenpiteitä
Ovatko puhelinkäyttäytymisen ohjeet olemassa?	Ei	Puhelimessa voidaan vahingossa kertoa suojeltavia tietoja, jos ei ole ohjeistettu toimintaa	1	Puhelimessa ei anneta esim. tarpeettomasti tietoja	Ei vaadi toimenpiteitä
Onko tulipalon varalle toiminta ohjeistettu ja harjoiteltu?	Ei	Tulipalot voivat aiheuttaa henkilö- ja omaisuusvahinkoja, jos niiltä suojautumista ei harjoitella	0	Toimintaa harjoitellaan vakituisesti	Ei vaadi toimenpiteitä
Onko tehtävien varahenkilöjärjestelyistä huolehdittu?	Ei	Pätevän varahenkilön puuttuminen tai huono saatavuus vaarantaa tarvittavan työtehtävän suorittamisen ajoissa	2	Varahenkilöjärjestelyjä ei ole hoidettu tarpeeksi hyvin	Varahenkilöjärjestelyt on luotava niin, että pätevä varahenkilö saadaan tarvittaessa käyttöön
3.1.5 Tietojärjestelmien ja tietokoneiden käyttö					
Onko henkilöstöllä riittävä perusosaaminen järjestelmien käyttöön	Kyllä	Riittämätön perusosaaminen altistaa riskeille, virheille yms.	0	Käyttäjillä on tarvittava perusosaaminen	Ei vaadi toimenpiteitä
Käyttääkö jokainen työntekijä työssään vain omaa käyttäjätunnustaan?	Kyllä	Muiden tunnusten käyttämisellä ei voi luotettavasti tunnistaa todellista käyttäjää	0	Työntekijät käyttävät vain omia tunnuksiaan	Ei vaadi toimenpiteitä
Onko ohjeistettu turvallisen salasanan muodostaminen?	Kyllä	Heikot salasanat on helppo ja nopea murtaa	0	Turvallisen salasanan luomiseen on olemassa ohjeet	Ei vaadi toimenpiteitä
Pystyvätkö muut työntekijät lukemaan tai muuttamaan käyttäjän tietoja käyttäjän huomaamatta?	Ei	Käyttäjän tietoihin pääsee käsiksi käyttäjän tietämättä, jolloin voidaan tuhota tai muuttaa tietoja	0	Vain ylläpito voi muuttaa käyttäjän tietoja	Ei vaadi toimenpiteitä
Onko varmuuskopioiden ottamiseen ja palauttamiseen olemassa	Ei	Varmuuskopioiden käsittely ei ole ennalta sovittua, voi tapahtua virheitä	3	Joitain ohjeita on olemassa. Kun tarvitaan palautusta, etsitään osaava henkilö tekemään se	On luotava ohjeet varmuuskopioiden ottamiseen ja palauttamiseen

Valvotaanko varmuuskopioiden ottamista?	Kyllä	Varmuuskopioinnissa voi sattua valvonnan puuttuessa virheitä tai sitä ei tehdä säännöllisesti	0	Varmuuskopioiden ottamista valvotaan ja käytetään lokitiedostoja	Ei vaadi toimenpiteitä
Onko Internetin käyttö ohjeistettu?	Ei	Internetin huolimaton käyttö altistaa organisaation monille eri uhkille, mm viruksille ja tietovarkauksille	2	Kaikki käyttö on sallittua	On luotava ohjeistus
Onko sähköpostin käyttö ohjeistettu?	Kyllä	Sähköpostin vapaa käyttö altistaa viruksille, roskapostille ja tietojen tarpeettomalle leviämiselle	0	Sähköposti käyttö on ohjeistettu	Ei vaadi toimenpiteitä
Onko virusten torjuntamenettelyt ohjeistettu niin työkoneiden kuin kotikoneiden osalta?	Ei	Virusten leviämisen estäminen ja vaikutusten lieventäminen eivät toimi, jos menettelyitä ei hallita	2	Torjuntamenettelyt on ohjeistettu työkoneiden osalta, kotikoneiden osalta ei	Kotikoneiden suojausta on parannettava
Onko virusohjelmien ja muiden vastaavien päivitykset automatisoitu?	Kyllä	Vanhentuneilla tunnisteilla ei löydetä uusia uhkia, manuaaliset päivitykset saattavat unohtua	0	Päivitykset on automatisoitu	Ei vaadi toimenpiteitä
Salakirjoitetaanko kannettavilla tietokoneilla olevat luottamukselliset tiedot?	Ei	Salaamattomat tiedot voi lukea kun tietokone on saatu haltuun	1	Salausta ei tehdä, ei ole salaisia tietoja	Ei vaadi toimenpiteitä
Onko käyttäjiä kielletty asentamasta organisaation verkkoon ulkopuolisia ohjelmistoja tai modeemeja?	Kyllä	Tuntemattomat ja vihamieliset ohjelmistot altistavat uhkille ja ulkopuoliset modeemit mahdollistavat luvatonta tietoliikennettä	0	Käyttäjiä on kielletty asentamasta ulkopuolisia ohjelmistoja ja modeemeja	Ei vaadi toimenpiteitä
4. Toimintaympäristön, työ- ja palvelutilojen tietoturvallisuus					
4.1 Fyysinen turvallisuus					
4.1.1 Kiinteistön turvallisuus					
Onko kiinteistö altis onnettomuuksille? Sijaitseeko se lähellä rautatietä tai isoa valtatietä?	Ei	Sijainti lähellä uhkatekijöitä, rakenteellisia ongelmia kuten kiinteistön kunto	2	Uhkiin on varauduttu	Ei vaadi toimenpiteitä
Onko sähkönsyötön häiriöihin varauduttu?	Kyllä	Sähkökatkot ja ylijännitteet aiheuttavat laitteistovahinkoja ja toiminnan keskeytymisen	0	Palvelinhuoneessa on ups-laitteisto.	Ei vaadi toimenpiteitä

Onko kiinteistöllä suojelupäällikkö ja turvasuunnitelma?	Kyllä	Suojaamista ei ole vastuutettu ja dokumentoitu, joten riskejä ei hallita	0	Toimitaan määräysten mukaisesti.	Ei vaadi toimenpiteitä
Onko kiinteistössä organisaatioita, joissa liikkuu paljon vieraita henkilöitä?	Kyllä	Kaikkia kiinteistössä liikkuvia ei tunneta	1	Tiloissamme liikkuu opiskelijoita, joita emme kaikkia tunne.	Ei vaadi toimenpiteitä
Onko rakenteellinen suojaus palon, murron, vesivahingon ja sabotaasin varalta hoidettu?	Kyllä	Tulipalot ja vesivahingot leviävät hallitsemattomasti ja murroille ja sabotaasille ei ole esteitä	0	Toimitaan määräysten mukaisesti.	Ei vaadi toimenpiteitä
Onko kiinteistössä kulunvalvonta?	Kyllä	Kiinteistössä voi liikkua vapaasti	0	Tärkeissä ovissa sähkölukot, joista pääsee kulkukortilla.	Ei vaadi toimenpiteitä
Onko kiinteistössä vartiointi?	Ei	Kiinteistön suojauksia ja omaisuutta ei valvota	0	Vartijoille menevät hälytykset ja he tarkastavat ulko-ovia.	Ei vaadi toimenpiteitä
Onko organisaation tiloihin pääsy suojattu kulunvalvonnalla?	EKM	Organisaation tiloihin pääsee asiattomia	1	Johinkin tiloihin (erit. palvelinhuone) on pääsy vain kulkukortilla (sähkölukko)	Ei vaadi toimenpiteitä
Onko kiinteistön yleisiin tiloihin, kuten puhelinkeskukseen, piha-alueelle, kellariin, katolle, asiaton pääsy estetty ja valvottu?	Ei	Asiattomat pääsevät aiheuttamaan vahinkoa yleisiin tiloihin	2	Oppilaitoskiinteistö on kuitenkin julkista tilaa, jonne on melko vapaa pääsy.	Ei vaadi toimenpiteitä
Onko toimitiloissa kulunvalvonta ja vartiointi?	Ei	Ulkopuoliset pääsevät toimitiloihin	1	Päiväaikaan ovet ovat auki. Iltaisin pääsy on kulkukortilla. Vartijoita ei paikalla.	Ei vaadi toimenpiteitä
Onko toimitiloissa hälytysjärjestelmää?	Kyllä	Tiloihin murtautumista ei huomata ajoissa	0		Ei vaadi toimenpiteitä
Ovatko takaovet ja -ikkunat lukittu?	Kyllä	Lukitsemattomista ovista ja ikkunoista voidaan tunkeutua kiinteistöön	0		Ei vaadi toimenpiteitä
Säilytetäänkö avaimia huolella?	Kyllä	Kadotetuilla avaimilla voidaan päästä kiinteistöön jälkiä jättämättä	0		Ei vaadi toimenpiteitä
4.1.2 Toimitilojen turvajärjestelyt					
Onko kulkuoikeuksien myöntäminen nimetty vastuuhenkilölle?	Kyllä	Kulkuoikeuksien myöntäminen on monimutkaista tai sattumanvaraisia	0	Kulkuoikeudet rajattuihin tiloihin (esim. palvelinhuone) vaatii vastuuhenkilön hyväksynnän.	Ei vaadi toimenpiteitä

Onko kulkeminen tiloissa rajattua ja valvottua?	Ei	Tiloissa voi kulkea ja aiheuttaa vahinkoa	1	Tilat ovat pääosin julkisia.	Ei vaadi toimenpiteitä
Onko muilla kuin työntekijöillä kulkuavaimet tiloihin?	Ei	Ulkopuoliset voivat kulkea tiloissa ja murtojälkiä ei ole	0	Siivoojilla(siivousyrityksen) on avaimet siivottaviin huoneisiin.	Ei vaadi toimenpiteitä
Onko työntekijöiden omein töiden tekeminen työpaikalla hallittua (ajat, kulkuoikeudet, valvonta)?	Ei	Työaikaa kuluu muuhun kuin varsinaiseen työhön, välineiden resursseja varataan omaan käyttöön	0	Opetushenkilökunta voi tehdä omia töitään melko vapaasti.	Ei vaadi toimenpiteitä
Onko vierailusäännöt ja -käytännöt olemassa?	Ei	Asiattoman vierailijan tai asiattoman toiminnan tunnistaminen on vaikeaa	1	Tilat ovat pääosin julkisia.	Ei vaadi toimenpiteitä
Onko tärkeät laitteet, kuten työasemat ja palvelimet, sijoiteltu valvottuihin tiloihin?	Kyllä	Tärkeitä laitteita ei voida seurata aktiivisesti	0	Vain rajatulla joukolla on pääsy palvelinten luo.	Ei vaadi toimenpiteitä
Onko tärkeät tilat sijoiteltu pois viemärien ja putkistojen lähistöltä?	Ei	Vesivahinkojen sattuessa tärketä tilat ja laitteet kärsivät vesivahinkoja	4	Palvelinhuoneessa on viemäri- ja vesiputkia.	Palvelimille täytyy järjestää turvalliset tilat
Ovatko laitetilat alttiita lämpötilan vaihteluille?	Kyllä	Lämpötilan vaihtelut vahingoittavat laitteita	4	Palvelinhuoneen jäähdytysjärjestelmä on vikaantunut muutaman kerran.	Laitetilojen turvallisuuteen kiinnitettävä enemmän huomiota
Onko alkusammutuskaluston käyttöä harjoiteltu?	Ei	Tulipalon sattuessa alkusammutusta ei osata tehdä	3	Ei tiedossa	On selvitettävä henkilöstön valmius käyttää sammutuskalustoa
Onko tulipalon varalle harjoiteltu tiloista poistumista?	Kyllä	Tulipalon sattuessa voi aiheutua henkilövahinkoja	0	Harjoituksia on ollut säännöllisesti.	Ei vaadi toimenpiteitä
4.2 Tietoaineistoturvallisuus					
4.2.1 Asiakaspalvelutilat					
Pidetäänkö luottamukselliset tiedot poissa asiakaspalvelutiloista?	Ei	Luottamukselliset tiedot voivat päätyä sivullisten käsiin	1	Työhuoneet ovat usein myös asiakaspalvelutiloja. Tiedot eivät yleensä ole salaisia.	Ei vaadi toimenpiteitä
Pidetäänkö tietokonepäätteet, kirjoittimet, faksit yms. poissa kulkuväyliltä?	Kyllä	Tietojärjestelmiin murtautuminen on helpompaa, laitteet altistuvat varkauksille	2	Henkilökunnan tietokoneet ovat työhuoneissa. Tietokoneluokat ovat usein auki.	Henkilökunnan on pidettävä työtilojaan lukittuina tarpeen vaatiessa
Onko asiakastilat sijoitettu siten, että asiakkaiden liikkumista voidaan valvoa?	Ei	Asiakastiloissa voi olla asiattomia	1	Asiakkaat (opiskelijat) voivat liikkua lähes kaikissa tiloissa.	Ei vaadi toimenpiteitä

Ovatko neuvottelutilat ääni- ja näköeristettyjä?	Ei	Sivulliset voivat seurata ja kuunnella neuvotteluhuoneiden tapahtumia	1	Neuvotteluhuoneet ovat ihan tavallisia huoneita. Luottamuksellisia tietoja ei ole usein käsittelyssä.	Ei vaadi toimenpiteitä
Huolehditaanko neuvottelutilojen siivouksesta siten, että vanhojen palaverien asiakirjat, fläpit ja piirtoheitinkalvot eivät jää tilaan?	Ei	Vanhat materiaalit saattavat joutua ulkopuolisten käsiin	0	Siivous ei tapahdu jokaisen päivän päätteeksi.	Ei vaadi toimenpiteitä
Onko asiakkaita varten suunniteltu esim. puhelin sellaiseen paikkaan, että sen käyttö ei aiheuta riskiä	EKM	Asiakkaat voivat päästä käyttämään puhelinta paikkoihin, joille heidän ei kuulu päästä	0	Ei tiedossa	Ei vaadi toimenpiteitä
4.3 Käyttöturvallisuus					
4.3.1 Tietojen ja järjestelmien käyttöperiaatteet					
Onko järjestelmien käyttöoikeuksien hallinta nimetty vastuuhenkilölle?	Kyllä	Kukaan ei ole suoraan vastuussa käyttöoikeuksien hallinnasta	0	Järjestelmillä on käyttöoikeuksia myöntävät vastuuhenkilöt.	Ei vaadi toimenpiteitä
Onko käyttöoikeuksien käsittely ja myöntäminen ohjeistettu?	Ei	Käyttöoikeuksien myöntäminen, ylläpito ja poisto ei ole järjestelmällistä	2	Joidenkin käyttöoikeuksien poistaminen kaipaa ohjeistusta ja menettelytapoja.	Käyttöoikeuksien hallinnalle on luotava kattava ohjeistus
Onko jokaisella käyttäjällä oma käyttäjätunnus ja henkilökohtainen salasana?	Kyllä	Yhdellä tunnuksella voi olla useita käyttäjiä, joten oikeata käyttäjää ei voi yksilöidä	0	Muutamia ryhmätunnuksia on käytössä, mutta käyttö on varsin rajattua.	Ei vaadi toimenpiteitä
Onko työntekijöille rajattu pääsy vain omiin työtehtävän edellyttämiin tietoihin?	Kyllä	Työntekijät voivat päästä käsiksi heille kuulumattomiin tietoihin	0	Vain tietohallinnon henkilöstöllä on laajat oikeudet, mutta he tietävät vastuunsa.	Ei vaadi toimenpiteitä
Onko luottamuksellisille asiakirjoille ja muille tietovälineille lukitut kaapit?	Kyllä	Sivulliset pääsevät käsiksi luottamukselliseen materiaaliin	0	Tärkeät paperit ja tietovälineet ovat joko holvissa, kassakaapissa tai lukitussa kaapissa.	Ei vaadi toimenpiteitä
Onko luottamuksellisten tietojen hävittämiseen silppurit tai lukitut paperisäiliöt?	Kyllä	Luottamuksellisia tietoja ei hävitetä asianmukaisesti ja niitä voidaan anastaa	0	Tietosuojasäiliöt ovat yleisesti käytössä.	Ei vaadi toimenpiteitä

Sallitaanko tietojen siirtely tietolevykkeillä (korput, kirjoittavat CD:t yms.)?	Kyllä	Tietojen luvaton kopiointi ja siirto on mahdollista. Haittaohjelmat voivat levitä saastuneilta tietovälineiltä.	1	Työntekijät ja opiskelijat saavat vapaasti käyttää mm. usb-tikkuja. Myös kannettavia tietokoneita siirrellään työpaikasta pois ja takaisin.	Ei vaadi toimenpiteitä
Ovatko laitteet, ohjelmistot ja tiedot kirjattu omaisuusrekisteriin?	Ei	Laitteiden, ohjelmistojen ja muiden tietojen kuten lisenssien olemassaoloa on vaikea seurata ja todentaa	2	Laitteiden ja varsinkin lisenssien kirjaukset ovat puutteelliset.	Laitteiden, ohjelmistojen ja lisenssien tiedot kirjattava rekisteriin ja tietoja on ylläpidettävä
Onko turvalliset etätyötavat ohjeistettu?	Ei	Ohjeistuksen puuttuessa altistutaan lukuisille tietoturvariskeille, kuten haittaohjelmille	3	Etätyöntekijöitä ei ole vielä kovin paljon, mutta riskit ovat todellisia.	Etätyöhön on luotava tai otettava käyttöön ohjeistus
5. Tietojärjestelmien suojaus					
5.1 Tietoliikenneturvallisuus					
Toimivatko modeemiyhteydet takaisinsoittoperiaatteella?	Ei	Takaisinsoitolla varmistetaan, että yhteydenottaja on oikeutettu yhteyteen	0	Modeemiyhteyksissä on käyttäjäntunnistus, joka estää asiattoman käytön.	Ei vaadi toimenpiteitä
Onko asiaton pääsy ja muu asiaton verkkoliikenne organisaation verkkoon estetty?	Kyllä	Ulkopuoliset voivat aiheuttaa vahinkoja ja häiriöitä verkkoon päästessään	3	Langatonta verkkoa ei ole ihan kokonaan suojattu kunnolla.	Langattoman verkon suojausta parannettava
Ovatko paikallisverkko, extranet- ja WWW-palvelimet eristetty toisistaan riittävästi?	Ei	Virukset nopeammin ja asiaton pääsy verkosta toiseen on helpompaa	3	Palveluiden ja lähiverkkojen pilkkominen on vasta meneillään.	Eristystyö on saatettava loppuun
Tarkistetaanko sähköpostiliitteiden asianmukaisuus ja virukset ennen pääsyä organisaation verkkoon?	Kyllä	Liitetiedostoissa kulkeutuu viruksia	2	Virustorjunnasta huolimatta läpi pääsee joskus uusia viruksia.	Virustorjunnan päivityksistä on pidettävä huolta paremmin
Tarkistetaanko lähtevät sähköpostiliitteet?	Kyllä	Virukset leviävät liitteiden mukana	2	Aina torjuntakaan ei heti auta, jos virukset ovat uusia.	Virustorjunnan päivityksistä on pidettävä huolta paremmin
Suojataanko kannettavat tietokoneet kattavasti? (niin että varkaat eivät pääse tietoihin käsiksi)	Ei	Varastettujen tietokoneiden tietoja voidaan käyttää hyväksi	2	Kannettavissa tietokoneissa olevat tiedot on synkronoitu kotihakemistosta (salattu). Tiedot eivät yleensä salaisia.	Ei vaadi toimenpiteitä
5.2 Ohjelmistoturvallisuus					
5.2.1 Ohjelmistot					

Hankitaanko ohjelmistot, laitteet ja muu tuki osaavilta toimittajilta?	Kyllä	Laitteiden ominaisuuksissa, kunnossa tai asennuksissa voi ilmetä vikoja ja virheitä	0	Toimittajan luotettavuus on tärkeä valintakriteeri.	Ei vaadi toimenpiteitä
Onko käytössä vain lisensoidut lailliset ohjelmistoversiot?	Kyllä	Kopiosuojattujen ohjelmien laiton käyttö on rangaistavaa ja laittomat ohjelmat sisältävät mahdollisesti haittaohjelmia	0	Periaate: Tietohallinto ei suostu asentamaan laittomia ohjelmia.	Ei vaadi toimenpiteitä
Onko laadittu järjestelmäkehityksen tietoturvasuunnitelma?	Ei	Järjestelmäkehityksessä ei oteta tietoturva-asioita huomioon riittävästi	2	Vain hajanaisia periaatteita on olemassa (ei paperilla).	Järjestelmäkehityksen tietoturvaperiaatteet on ohjeistettava
Otetaanko hankintojen yhteydessä huomioon ohjelmistojen turvallisuus ja luotettavuus? (Tietojen hankinta luotettavuudesta, oma testaus)	Ei	Kehitys ei ole järjestelmällistä ja riskejä ei hallita	2	Vain hajanaisia periaatteita on olemassa (ei paperilla).	Hankinnoissa on otettava huomioon ohjelmistojen turvallisuus ja luotettavuus
Ovatko tietojen varmistuskäytännöt vastuutettu ja suunniteltu?	Ei	Tietoja suojaaminen on puutteellista ja tietoja voi kadota, muuttua tai korruptoitua	1	Varmistusten ottoa ei ole dokumentoitu kunnolla, vaikka varmistuksia varmaan otetaan tarpeeksi.	Varmistusten ottaminen tulee dokumentoida
Onko harjoiteltu varmistusten palautusten onnistumista?	Kyllä	Varmistukset eivät toimi, niitä ei osata palauttaa tai toiminta ei ole riittävän nopeaa	2	Useimpien tietojen palautuksia on tehty, mutta ei varsinaisesti harjoiteltu. Joitakin palautuksia ei voida harjoitella.	Varmistusten palauttamista olisi hyvä harjoitella
Onko paloturvakaappi tietojen varmistuksille?	Kyllä	Varmistukset voivat tuhoutua tulipalossa tai vesivahingossa	0	Paloturvakaapissa on kaikkien keskeisten järjestelmien varmistusnauhat.	Ei vaadi toimenpiteitä
Onko kaikissa työasemissa virustorjunta?	Kyllä	Suojaamattomat työasemat altistuvat viruksille ja levittävät niitä edelleen	0	Kaikissa lähiverkkoon kytketyissä on virustorjunta, mutta eräissä labroissa ei.	Ei vaadi toimenpiteitä
Onko virustentorjuntaohjelmiston ajantasaisuudesta huolehtiminen vastuutettu?	Kyllä	Viruspäivityksiä ei asenneta riittävän usein tai ollenkaan, jolloin virusturva ei ole ajan tasalla	2	Vastuutus on hiukan joissakin paikoissa epäselvä.	Virustorjunpäivitysten vastuutus pitää olla selvä, epäselvät vastuut jäävät helposti hoitamatta
Tapahtuuko työasemien virustentorjuntaohjelmistojen ja vastaavien päivitys automaattisesti?	Kyllä	Viruspäivitykset täytyy asentaa manuaalisesti, jolloin päivitykset voivat unohtua taiu puuttua kokonaan	0	Kaikki päivitykset (virustorjunta, Windows) on automatisoitu.	Ei vaadi toimenpiteitä

5.3 Tietoaineistoturvallisuus					
5.3.1 Tietojen ja järjestelmien käyttöperiaatteet					
Onko järjestelmien käyttöoikeuksien hallinta nimetty vastuuhenkilölle?	Kyllä	Käyttöoikeuksia jaetaan hajanaisesti	0	Järjestelmillä on käyttöoikeuksia myöntävät vastuuhenkilöt.	Ei vaadi toimenpiteitä
Onko käyttöoikeuksien käsittely ja myöntäminen ohjeistettu?	Ei	Käyttöoikeuksien käsittely ja myöntäminen	2	Joidenkin käyttöoikeuksien poistaminen kaipaa ohjeistusta ja menettelytapoja.	Käyttöoikeuksien hallinnalle on luotava kattava ohjeistus
Onko jokaisella käyttäjällä oma käyttäjätunnus ja henkilökohtainen salasana?	Kyllä	Käyttäjää ei voida yksilöidä	0	Muutamia ryhmätunnuksia on käytössä, mutta käyttö on varsin rajattua.	Ei vaadi toimenpiteitä
Onko työntekijöille rajattu pääsy vain omiin työtehtävän edellyttämiin tietoihin?	Kyllä	Työntekijä pääsee hänelle kuulumattomiin tietoihin käsiksi	0	Vain tietohallinnon henkilöstöllä on laajat oikeudet, mutta he tietävät vastuunsa.	Ei vaadi toimenpiteitä
Onko luottamuksellisille asiakirjoille ja muille tietovälineille lukitut kaapit?	Kyllä	Luottamuksellinen materiaali on sivullisten saatavissa	0	Tärkeät paperit ja tietovälineet ovat joko holvissa, kassakaapissa tai lukitussa kaapissa.	Ei vaadi toimenpiteitä
Onko luottamuksellisten tietojen hävittämiseen silppurit tai lukitut paperisäiliöt?	Kyllä	Luottamuksellista tietoa ei tuhota asianmukaisesti	0	Tietosuojasäiliöt ovat yleisesti käytössä.	Ei vaadi toimenpiteitä
Sallitaanko tietojen siirtely tietolevykkeillä (korput, kirjoittavat CD:t yms.)?	Kyllä	Tietojen luvaton kopiointi ja siirto on mahdollista. Haittaohjelmat voivat levitä saastuneilta tietovälineiltä.	1	Työntekijät ja opiskelijat saavat vapaasti käyttää mm. usb-tikkuja. Myös kannettavia tietokoneita siirrellään työpaikasta pois ja takaisin.	Ei vaadi toimenpiteitä
Onko laitteet, ohjelmistot ja tiedot kirjattu omaisuusrekisteriin?	Ei	Laitteiden, ohjelmistojen ja muiden tietojen kuten lisenssien olemassaoloa on vaikea seurata, todentaa ja selvittää omistajaa	2	Laitteiden ja varsinkin lisenssien kirjaukset ovat puutteelliset.	Laitteiden, ohjelmistojen ja lisenssien tiedot kirjattava rekisteriin ja tietoja on ylläpidettävä
Onko turvalliset etätyötavat ohjeistettu?	Ei	Ohjeistuksen puuttuessa altistutaan lukuisille tietoturvariskeille, kuten haittaohjelmille	3	Etätyöntekijöitä ei ole vielä kovin paljon, mutta riskit ovat todellisia.	Etätyöhön on luotava tai otettava käyttöön ohjeistus
5.4 Käyttöturvallisuus					

5.4.1 Teknisen ympäristön hallinta ja valvonta					
OvatkoOnko tietotekniset turvatehtävät vastuutettu?	Kyllä	Turvatehtävien hoito ei ole riittävän	2	Vastuutuksissa on puutteita (erit. haittaohjelmien torjunta).	Vastuutukset on hoidettava kattavasti
Vastaavatko teknisen ympäristön ylläpidosta henkilöt, joilla on siihen riittävä tekninen osaaminen?	Kyllä	Epäpätevyys mahdollistaa virheiden tekemisen	0	Osaamattomuus ei ole aiheuttanut haittaa. Tekijöillä on yleensä riittävä ammattitaito.	Ei vaadi toimenpiteitä
Onko sähköpostipalvelimien asennus ohjeistettu?	Kyllä	Palvelimissa voi olla tietoturva-aukkojatai ne eivät toimi tehokkaasti	0	Sähköpostipalvelimet on keskitetty. Asennukset on dokumentoitu.	Ei vaadi toimenpiteitä
Onko järjestelmien ylläpidosta vastaavat koulutettu tietoriskien hallintaan ja järjestelmien suojaamiseen?	Ei	Riskejä ei tunnisteta ja ei osata torjua niitä	2	Järjestelmällistä koulutusta ei ole järjestetty. On luotettu henkilökunnan omaan tietämykseen ja ammattitaitoon.	Lisäkoulutusta voidaan järjestää tarpeen mukaan
Ovatko varahenkilöt tietoisia nykykäytännöistä?	Ei	Virheiden tekeminen on todennäköisempää	2	Varahenkilöjärjestelyjä ei ole hoidettu tarpeeksi hyvin	Varahenkilöjärjestelyt on hoidettava paremmin
Onko tietojärjestelmäsuunnittelijoilla valmius ennakoida järjestelmää uhkaavat tilanteet ja suunnitella ja arvioida tarpeellisia suojaustapoja?	Ei	Tietojärjestelmät sisältävät aukkoja ja virheitä, jotka mahdollistavat tietoriskien toteutumisen	1	Teemme itse hyvin vähän ja pieniä tietojärjestelmiä.	Ei vaadi toimenpiteitä
Seurataanko järjestelmän virheitä ja levytilojen täyttymistä?	Ei	Ongelmia ei voida riittävästi ennakoida seurannan puuttuessa	1	Jatkossa tiedot saadaan kirjattua helpdesk-järjestelmään.	Ei vaadi toimenpiteitä
Seurataanko järjestelmän käyttöä ja puututaanko siihen tarvittaessa?	Ei	Järjestelmiä voidaan väärinkäyttää haitallisiin tarkoituksiin tai resursseja varata turhaan	1	Vain tietoliikennettä seurataan ongelmien ilmaantuessa.	Ei vaadi toimenpiteitä
5.4.2 Teknisen järjestelmän hankinta, huolto, muutokset ja poisto käytöstä					
Otetaanko tietoturva-asiat huomioon laitehankinnoissa?	Kyllä	Hankitaan laitteita, joiden käytössä on riskejä	0	Tietoturva on tarpeen mukaan valintakriteerinä.	Ei vaadi toimenpiteitä
Onko varauduttu teknisten järjestelmien rikkoutumiseen (varaosien saatavuus, kahdennus, varajärjestelmät, korvaavat toimintatavat)?	Kyllä	Varajärjestelmien puuttuessa toiminta keskeytyy	2	Tärkeimpien järjestelmien osalta on varauduttu melko hyvin. Mutta kehitettävää löytyy vieläkin.	Varatoimenpiteitä pitää ulottaa myös muihin järjestelmiin

Käytetäänkö luotettavia huoltoyrityksiä, joiden kautta tiedot eivät ole vaarassa joutua kolmansille osapuolille?	Kyllä	Huoltoyritykset voivat jakaa eteenpäin organisaation tietoja	0	Käytetään yleensä laitteiden takuuhuoltoja hoitavia yrityksiä.	Ei vaadi toimenpiteitä
Onko tekninen ympäristö ja sen muutokset dokumentoitu?	Ei	Dokumentoinnilla kuvataan tarkasti teknistä ympäristöä, joten sen puuttuessa muutosten ja ongelmien selvittäminen on hankalaa.	3	Dokumentoinnissa on suuria puutteita. Vain muutaman järjestelmän ylläpito on dokumentoitu kunnolla. Helpdeskiin tulee CMDB, joka auttaa dokumentoinnissa.	Dokumentointi on otettava käyttöön ja ylläpidettävä sitä
Onko tietojen hävitysmenettely olemassa, jos laitteita myydään työntekijöille tai ulkopuolisille?	Ei	Hävitettävät laitteet voivat sisältää arkaluonteisia tietoja organisaatiosta	0	Tietokoneiden kovalevyt tyhjennetään erikoisohjelmistolla.	Ei vaadi toimenpiteitä
5.4.3 Tekniset suojaamiskeinot					
Onko suojaamiskeinojen kattavuus tarkistettu / auditoitu?	Ei	Suojaamiskäytännöt eivät ole riittävät, ajantasaiset tai niitä ei ole hyväksytty	1	Suojaamiskeinojen arviointi perustuu keinojen kuvauksien tutkimiseen. Käytännössä toimivuutta toki seurataan.	Ei vaadi toimenpiteitä
Onko järjestelmien käyttö ilman käyttäjän luotettavaa yksilöintiä estetty?	Kyllä	Ongelmatapauksissa käyttäjiä ei voida yksilöidä	0	Vain joissakin tapauksissa työasemaan kirjautuminen tapahtuu ryhmätunnuksella. Ilman tunnusta ei pääse mihinkään.	Ei vaadi toimenpiteitä
Ovatko tietojen varmistukset automaattiset ja aukottomat?	Ei	Tietoja ei varmisteta riittävän hyvin ja usein, jolloin, tietoa voi kadota ja korruptoitua	2	Varmistukset otetaan automaattisesti keskeisistä tiedoista. Toimintahäiriöitä sattuu liian usein.	Toimintahäiriöiden syyt on selvitettävä ja korjattava
Onko UPS-laitteita varasähkön varmistamiseksi?	Kyllä	Virransyöttöongelmatapauksissa laitteille ei ole saatavilla varasähköä ja toiminta keskeytyy	1	Palvelintietokoneet ovat upsin takana, mutta kaikki tietoliikennelaitteet eivät.	Tietoliikennelaitteille on hankittava varajärjestelmiä mahdollisuuksien mukaan
Salakirjoitetaanko työasemilla ja palvelimilla olevat tiedot ja sähköpostiliikenne?	Ei	Asiattomat voivat lukea ja kaapata tietoja	1	Tietokoneissa olevia tietoja ei salakirjoiteta (salaisimpia ovat henkilötiedot). S-postiliikenne ei salattua.	Ei vaadi toimenpiteitä

Vaatiiko käyttöä valvova ohjelmisto salasanalle tietyn määrä muotoisuuden ja salasanan ennalta ajoitetun vaihtamisen?	Kyllä	Salasanojen käyttöä ei valvota riittävästi ja niiden antama suoja ei ole riittävä	2	Salasanoille asetetaan ehtoja, mutta ei ihan kaikissa järjestelmissä.	Kaikissa järjestelmissä pitäisi olla käytössä turvalliset vaatimukset salasanoille
Tarkistetaanko työntekijöiden salasanojen muoto ja turvallisuus ajoittain?	Ei	Heikkoja salasanoja voidaan murtaa nopeasti, lisäksi pitkään voimassa ollut salasana voi vuotaa ulkopuolisille	0	Luotamme salasanoille asettaviin vaatimuksiin.	Ei vaadi toimenpiteitä
Jääkö järjestelmän lokitiedostoihin merkintä järjestelmän käyttäjistä?	Ei	Ongelmatilanteissa ei voida identifioida käyttäjää yksiselitteisesti	2	Joissakin järjestelmissä jää ja joissakin ei.	Mahdollisuuksien mukaan on käytettävä kaikissa järjestelmissä lokitiedostoja
Rajataanko ulkopuolisilta pääsy organisaation verkkoon?	Kyllä	Asiattomien pääsy verkkoon altistaa väärinkäytöksille	2	Rajauksia ei ole viety loppuun asti, työ on kesken.	Rajaus on tehtävä valmiiksi

Liite2. Tietoturvallisuuspolitiikan Malli

[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 keskeytyksettömästä 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. Politiikkaa tarkennetaan tietojen käsittelyn säännöissä ja ohjeissa.

Tiedon turvaaminen on oleellinen osa yliopiston toiminnan ja palveluiden laatua, kokonaisturvallisuutta ja yliopistossa tapahtuvaa päivittäistä tietojen käsittelyä. Tietoturvallisuuden hyvä hallinta edellyttää kaiken toiminnan jatkuvaa seurantaa, 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 käytettävyydestä[1]. Yliopiston tavoitteena on turvata riittävällä ja tarkoituksenmukaisella tasolla toiminnalleen tärkeiden tietojen, tietojärjestelmien, palveluiden ja tietoverkkojen toiminta, estää niiden valtuudeton 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 seurantaa. Sillä pyritään ennalta ehkäisemään sisäisistä ja ulkoisista tietoon kohdistuvista uhkista aiheutuvat vahingot tai rajoittamaan ne hyväksyttävälle tasolle sekä varautumaan poikkeamatilanteista toipumiseen. Normaaliajan 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 suosituksia[2].

2 Tietoturvan organisointi ja vastuut

Tässä luvussa kuvataan keskeisimmät tietoturvallisuuteen liittyvät toimijat yliopistossa sekä heidän vastuunsa ja velvollisuutensa. Tarkempi vastuiden erittely kerrotaan tietoturvapolitiikan 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 ohjeita[3].*
- *Tietoturvapolitiikasta 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 voimassaolevien 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 tulosohjausta.*

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.

käyttösäännöillä 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.

Tietoturvapolitiikan ja riskikartoituksien 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 tietoturvallisuusohjeet. Opiskelijoille tiedotetaan tietoturvallisuudesta ja heitä koskevista säännöistä ja suosituksista. Yleensäkin yliopistoyhteisön jäsenten tietoturvallisuustietoisuutta lisätään tiedottein ja kirjoituksin eri tiedotuskanavissa sekä järjestämällä koulutustilaisuuksia. [Yliopiston tietojenkäsittelyn ja tietojärjestelmien tietoturvallisuuden tasoa arvioidaan sisäisen tarkastuksen keinoin, tarvittaessa myös ulkoista tarkastusta käyttäen. Tietoturvallisuuden puutteet analysoidaan järjestelmien ylläpitäjien ja omistajien kanssa.]

4 Tiedottaminen

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

Yliopiston tietoturvallisuuteen liittyvästä tiedottamisesta yliopiston ulkopuolelle ja yliopiston sisällä yleisellä tasolla vastaa ja huolehtii yliopiston tietoturvapäällikkö tietoturvasuunnitelman mukaisesti. Yksiköiden sisäiseen tiedottamiseen osallistuvat myös yksiköille nimetyt vastuuhenkilöt.

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

5 Tietoturvallisuuden seuranta ja ongelmatilanteiden käsittely

Tietoturvallisuuden ylläpito edellyttää jatkuvaa seurantaa, johon kuuluvat tietoturvallisuuden valvonta sekä sen tason ja poikkeamien raportointi. Seurantaa toteutetaan sekä automaattisesti teknisin keinoin että henkilöiden toimesta mm. osana esimiesvastuuta. Teknisestä seurannasta on erilliset ohjeensa. [Tietoturvapäällikkö] koordinoi tietoturvallisuuden seurantaa ja raportoi tietoturvallisuudesta yliopiston johdolle.

[Tietoturvapäälliköllä ja tietoturvallisuuden 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 tietoturvallisuuden puutteista, tietoturvallisuuteen liittyvistä väärinkäytöksistä tai epäilemistään tietoturvarikkomuksista yksikkönsä [tietoturvayhdyshenkilölle tai] johtajalle sekä tietoturvapäällikölle, 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 kuririen ja tietoaineistoja sisältävien lähetysten turvallisuuden.

Hallinnollinen tietoturvallisuus (administrative and organizational information security)

Tietoturvallisuuteen 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, tietoturvallisuus, henkilöturvallisuus, toimitilaturvallisuus ja rikosturvallisuus.

Käytettävyys (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 tietoturvallisuuden parantamiseksi.

Laitteistoturvallisuus (computer security; facilities security)

tietojenkäsittely- ja tietoliikennelaitteiden ja tilojen käytettävyyteen, toimivuuteen, kokoonpanojen määrittelyyn ja pääsynvalvontaan sekä varaosien ja tarvikkeiden saatavuuteen liittyvät toimet tietoturvallisuuden 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-, eristämis-, pääsynvalvonta- ja varmistusmenettelyt, tarkkailu- ja paljastustoimet, lokimenettelyt ja laadunvarmistus sekä ohjelmistojen ylläpitoon ja päivitykseen liittyvät toimet tietoturvallisuuden parantamiseksi.

Perusturvallisuus (baseline security):
Vähimmäistoimenpiteet, 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 luokittelemisen 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 luetteloinnin ja luokitus sekä tietovälineiden ohjeistettu hallinta, käsittely, säilytys ja hävittäminen.

Tietoliikenneturvallisuus (telecommunications security)
1) tavoitetila, jossa tietoturvallisuus on toteutettu tietoliikenteen laitteiden, järjestelmien ja niissä kulkevien tietojen osalta
2) lainsäädäntö, normit ja toimet, joilla pyritään aikaansaamaan tietoliikenteen turvallisuus.
Tietoliikenneturvallisuuteen tähtääviä keinoja ovat mm. laitteistojen ja siirtoyhteyksien ylläpito ja niiden kokoonpanojen hallinta, verkonhallinta, pääsynvalvonta, tietoliikenteen käytön valvonta ja tarkkailu, ongelmatilanteiden kirjaaminen ja selvittäminen, viestinnän salaus ja varmistaminen sekä tietoliikenneohjelmien testaus ja hyväksyminen.

Tietotekniikan turvallisuus (IT security):
organisaation tietotekniikkaan kuten tietoliikenteeseen, laitteistoihin, ohjelmistoihin ja niiden käyttöön liittyvä tietoturvallisuus.

Tietoturvallisuus (information security):
1) tavoitetila, jossa tiedot, tietojärjestelmät ja palvelut saavat asianmukaista suojaa 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 tietoturvallisuus
(1) niin normaali- kuin poikkeusoloissa.
Tietoturvallisuuden toteuttamisessa on tapana erottaa kahdeksan toimenpidealuetta: hallinnollinen, henkilöstö-, fyysinen, tietoliikenne-, laitteisto-, ohjelmisto-, tietoaineisto- ja käyttöturvallisuus.

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 tietoturvallisuuden kehittämistoimintaa tai sitä suorittavia organisaatioita.

Tietoturvaohjeisto (information security manual):
Yliopiston yhteinen, yksiköiden sisäinen ja palvelu- tai järjestelmäkohtainen ohjeistus tietojenkäsittelyn turvaamiseksi.

Tietoturvapolitiikka (information security policy) :
Sama kuin tietoturvastrategia (information security strategy).
Tietoturvalinjaukset, tietoturvaperiaatteet.
Organisaation tasolla johdon hyväksymä näkemys tietoturvallisuuden päämääristä, periaatteista ja toteutuksesta.

Tietoturvasuunnitelma (information security plan):
perusturvallisuuden toteutusta ja ylläpitoa normaalioloissa koskeva suunnitelma.
Suunnitelmassa esitetään organisaation tietoturvallisuustoiminnan 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, perusturvallisuuden 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 säädeltyjä 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 tulosohjaus, 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 laitetilojen 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 asioinnin tietoturvallisuuden yleisohje, VAHTI 4/2001
- Salauskäytäntöjä koskeva valtionhallinnon tietoturvallisuussuositus, VAHTI 3/2001
- Valtionhallinnon lähiverkkojen tietoturvallisuussuositus, VAHTI 2/2001
- Valtion viranomaisen tietoturvallisuustyön yleisohje, VAHTI 1/2001
- Valtionhallinnon tietojärjestelmäkehityksen tietoturvallisuussuositus, VAHTI 3/2000
- Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohje, VAHTI 2/2000
- Tietojärjestelmäselosteen laadintasuositus, VM 17.2.2000
- Salassa pidettävien tietojen ja asiakirjojen turvaluokittelu- ja merkintäohje, VM 19.1.2000
- Valtion tietohallintotoimintojen ulkoistamisen tietoturvallisuussuositus, 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 tietoturvallisuuteen liittyvät säännöt ja ohjeet

- Tietoturvapolitiikka (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).

- Tietoturvapoikkeamiin reagoiminen (ohje)
- Tiedottaminen poikkeamatilanteissa (ohje)
- Todistusaineiston suojausohje.

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

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

Rehtorin kolmivuotiskausiksi asettama tietoturvallisuuden johtoryhmä valmistelee ja ohjaa yliopiston tietoturvallisuuden 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 valmistelee 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 tietoturvallisuusnäkemyksiä

- huolehtia henkilöstön turvallisuustietoisuuden lisäämisestä ja tietoturvallisuuskoulutuksen suunnittelusta
- huolehtia tietoturvallisuuden toteutumisesta ostetuissa atk-palveluissa ja
- raportoida ylimmälle johdolle tietoturvallisuudesta
- tehdä rehtorille, hallintokeskukselle ja tietokonekeskuksen johtokunnalle yliopiston tietoturvallisuutta koskevia ehdotuksia ja aloitteita sekä hallintokeskukselle tietoturvasuunnitelman edellyttämiä määrärahaesityksiä.

Tietoturvapäällikön tehtävänä on:

- valmistella tietoturvallisuuden kehittämishankkeita yhdessä tietoturvallisuuden johtoryhmän kanssa
- vastata tietoturvallisuuden kehittämishankkeiden toteutuksesta
- vastata tietoturvallisuuskoulutuksen järjestämisestä
- tiedottaa tietoturvallisuusasioista ja -ongelmista
- osallistua turvallisuusperiaatteiden määrittelyyn
- avustaa johtoa ja yksiköitä tietoturvallisuuden toimeenpanossa
- kehittää ehdotuksin tietoturvallisuutta
- järjestää tietoturvallisuutta koskeva seuranta
- raportoida ylimmälle johdolle tietoturvallisuudesta
- toimia tietoturvallisuuden johtoryhmän sihteerinä
- tehdä muut tietoturvallisuuden johtoryhmän hänelle antamat tehtävät.

Tietokonekeskuksen tehtävänä on:

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

Laitoksen / muun yksikön johtajan tehtävänä on:

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

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

- soveltaa ja toteuttaa yliopiston tietoturvallisuusperiaatteita omaa erikoisasiantuntemusta hyödyntäen
- vastata tietoturvallisuustoimenpiteistä omalla alueellaan
- noudattaa hyvää tietoturvallisuustapaa ja
- raportoida tietoturvallisuudesta ja siihen kohdistuvista häiriöistä.

Tietopalveluista ja asiakirjahallinnosta vastaavien tehtävänä on:

- toimeenpanna tietoturvallisuus tietopalveluissa ja asiakirjahallinnossa hyvän tiedonhallintatavan ja tietoturvallisuustavan 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 tietoturvallisuutta tietojärjestelmässä ja
- raportoida tietoturvallisuudesta 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 tietoturvallisuuden kannalta
- varautua poikkeaviin tapahtumiin ja niiden vaatimiin vastatoimenpiteisiin ja
- raportoida turvallisuutta vaarantavista tapahtumista ja häiriöistä.

Yksiköiden atk-yhdyshenkilöiden ja tietoturvavastaavien tehtävänä on:

- ylläpitää ja valvoa vastuullaan olevien järjestelmien tietoturvallisuutta yliopiston tietoturvallisuuden yleisohjeistuksen mukaisesti ja
- raportoida tietoturvallisuudesta ja siihen vaikuttavista tekijöistä

Loppukäyttäjien tehtävänä on:

- tuntea tietoturvallisuudesta annetut ohjeet ja noudattaa niitä
- osallistua heille suunnattuun tietoturvakoulutukseen sekä
- raportoida havaitsemistaan ongelmista, uhkista ja ohjeiden vastaisista menettelyistä.

Konsulttien ja palveluyritysten tehtävänä on:

- noudattaa hyvää tietojenkäsittely- ja tietoturvallisuustapaa
- ylläpitää ja valvoa yliopistoon liittyvässä toiminnassaan valtionhallinnon tietoturvallisuuden yleisohjeistuksen mukaista ja ohjeistettua tietoturvallisuutta sekä
- raportoida tietoturvallisuudesta ja siihen vaikuttavista tekijöistä.

Tietoturvallisuusvastuita on myös muilla keskeisillä henkilöryhmillä kuten

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

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

]

LIITE 2. TIETOTEKNIIKKARIKKOMUSTEN SEURAAMUSKÄYNTÄNTÖ

TIETOTEKNIIKKARIKKOMUSTEN SEURAAMUSKÄYTÄNTÖ

Sisällysluettelo:

1 Käyttöoikeuksien rajoittaminen selvitystyön ajaksi 1
2 Seuraamukset 1
2.1 Opiskelijat 2
2.2 Henkilökunta 2
3 Seuraamustaulukot 2
3.1. Käsitteitä 2

Tietotekniikkarikkomuksina pidetään yliopiston tietojärjestelmien käytöstä annettujen sääntöjen tai määräysten vastaista toimintaa tai tietojärjestelmien käyttöä Suomen lakien vastaisesti.

Tässä dokumentissa on kuvattu toimenpiteitä, joita henkilöön kohdistetaan, kun tietotekniikkarikkomus on havaittu tai sitä on perusteltua syytä epäillä. Toimenpiteet on jaettu käyttöoikeuksien rajoituksiin rikkomuksen *selvitystyön ajaksi* sekä mahdollisiin rikkomuksesta määrättyihin *seuraamuksiin*.

Dokumentti keskittyy ensisijaisesti yliopiston tutkinto-opiskelijoihin ja henkilökuntaan. Yliopiston järjestelmiin voi olla käyttäjätunnuksia myös mm.

- OPM-rahoituksella toimivilla tutkijoilla, emerituksilla ja ulkopuolisten palveluntarjoajien työntekijöillä, sekä
- täydennyskoulutuksen ja avoimen yliopiston opiskelijoilla.

Ryhmän heterogeenisuudesta johtuen sen osalta käytetään enemmän tapauskohtaista harkintaa.

Kaikki havaitut tietotekniikkarikkomukset ja niistä aiheutuneet toimenpiteet on ilmoitettava yliopiston tietoturvapäällikölle.

1 Käyttöoikeuksien rajoittaminen selvitystyön ajaksi

Käyttöoikeuksia voidaan rajoittaa joko sulkemalla kaikki tai osa käyttäjän käyttäjätunnuksista tai muutoin estämällä jonkin tietojärjestelmän käyttö (esim. poistamalla tiedon muutosoikeus)

Selvitystyön ajaksi

- *opiskelijalta* pääsääntöisesti suljetaan käyttäjätunnukset ja hänet kutsutaan keskustelemaan tietoturvapäällikön tai järjestelmästä vastaavan henkilön kanssa
- henkilökuntaan kuuluvan käyttöoikeuksia rajoitetaan tarvittavassa määrin. Rajoituksena verkkohäiriötilanteissa voi olla myös työaseman kytkeminen irti verkosta.

Käyttöoikeuksia on rajoitettava aina, kun on perusteltua syytä epäillä, että käyttäjä on syyllistynyt väärinkäytökseen, ja on mahdollista, että käyttöoikeudesta on haittaa rikkomuksen selvittämiselle tai vahinkojen minimoimiselle.

Käyttöoikeuksien rajoittamisesta selvitystyön ajaksi päättää tietojärjestelmän omistaja, yksikön johtaja tai muu tehtävään nimetty henkilö. Rajoittamisen toteuttaa ylläpitäjä. Kiireellisissä tapauksissa ylläpitäjä voi omalla päätöksellään rajoittaa käyttöoikeuksia enintään kolmeksi päiväksi, mistä tulee välittömästi ilmoittaa rajoituksista vastaavalle henkilölle.

2 Seuraamukset

Lievimmissä tapauksissa käyttäjälle huomautetaan asiattomasta toiminnasta.

Tietotekniikkarikkomuksen seurauksena käyttäjä on korvausvastuussa sekä väärinkäyttämistään resursseista (esim. koneaika) että väärinkäytön selvitystyöstä aiheutuneista kustannuksista.

2.1 Opiskelijat

Opiskelijalle kohdistettavia seuraamuksia voivat olla tietojärjestelmien käyttöoikeuksien rajoittaminen (käyttäjätunnusten sulkeminen) [1], yliopiston sisäiset hallinnolliset toimet (kirjallinen varoitus, määräaikainen erottaminen) [2] sekä rikosilmoituksen tekeminen (laissa rangaistaviksi määritellyt teot).

Käyttäjätunnusten sulkemisesta päättää yliopiston nimeämä henkilö. Käytön rajoitusaikaan ei lasketa mukaan tunnusten sulkemista selvitystyön ajaksi.

Kirjallisen varoituksen antamisesta opiskelijalle päättää yliopiston rehtori ja määräaikaisesta erottamisesta yliopiston hallitus. Käyttöoikeudet perutaan erottamisen ajaksi. Käyttöoikeuksien rajoittamisen kokonaiskesto on kuitenkin vähintään liitteenä olevassa taulukossa esitetyn mittainen..

2.2 Henkilökunta

Henkilökuntaa koskevia seuraamuksia voivat olla yliopiston työ- ja virkamiesoikeudelliset toimet (kirjallinen varoitus, irtisanominen, palvelussuhteen purku) [3] sekä rikosilmoituksen tekeminen (laissa rangaistaviksi määritellyt teot). Varoituksen antaa yksikön johtaja tai hallintojohtaja. Käyttöoikeudet yksittäisiin järjestelmiin voidaan väärinkäytöksestä johtuvan luottamuspulan synnyttyä evätä määräajaksi tai pysyvästi.

3 Seuraamustaulukot

Liitteen taulukoissa annetaan suositukset tietotekniikkarikkomusten seuraamuksista yliopiston tutkinto-opiskelijoille, henkilökunnalle ja muille.

Taulukoissa on esimerkkejä tyypillisistä tietojärjestelmien käytön yhteydessä esiintyvistä rikkomuksista luokiteltuina rikkomuksen vakavuusasteen mukaan. Seuraamuksiin vaikuttaa rikkomuksen vakavuuden lisäksi teon tahallisuuden aste.

Taulukon seuraamusruuduissa ylin rivi on varattu mahdolliselle rikosilmoitukselle, seuraavalla rivillä ovat hallinnolliset toimet ja alimmalla tietohallinnon / atk-yksikön toteuttamat toimet.

Jos käyttäjä on sekä opiskelija että henkilökuntaa, sovelletaan häneen henkilökunnan taulukkoa.

3.1. Käsitteitä

Rikoslain alaisen materiaalin oikeudeton käsittely

- *rikoslain alaista materiaalia* ovat esimerkiksi lapsiporno, eläimiin sekaantuminen, raaka väkivalta, rasistinen aineisto ja kansankiihottamismateriaali
- *käsittelyä* ovat mm. materiaalin levittäminen ja hallussapito

Tekijänoikeuslain alaista materiaalia on esimerkiksi musiikki, videot, sarjakuvat, elokuvat, pelit ja ohjelmistot.

Palvelu on toiminto, jota voidaan käyttää koneen ulkopuolelta. Esimerkiksi

- sähköpostipalvelu (smtp, imaps, …)

---

[1] Viittaus paikallisiin käyttösääntöihin

[2] Yliopistolaki 19§ ja Yliopistoasetus 20§

[3] Virkamieslaki 24§, 33-34§, 40§ ja Työsopimuslaki 7 luku,2§ 8luku,1§

- tiedostonsiirtopalvelu (ftp, http, scp, ...)
- vertaisverkko- palvelu (Kazaa, eDonkey,...)

Tunnuksen luovuttamista on esim. salasanan kertominen toiselle käyttäjälle tai istunnon auki jättäminen niin, että joku toinen pääsee valvomattomasti käyttämään toisen tunnusta.

Tiedon luottamuksellisuuden vaarantamista ovat esim.

ei-julkiseksi luokitellun tiedon luovuttaminen henkilölle, jolla ei ole oikeutta saada sitä, esim. palvelinten käyttäjätietojen luovutus

- ei-julkiseksi luokitellun tiedon tietoturvan laiminlyönti, esim. puutteelliset suojaukset järjestelmässä, jossa tietoa käsitellään
- salassapitorikokset
- henkilötietolain rikkominen

Henkilökohtaisen tietoturvan laiminlyöntiä on esimerkiksi salasanan jättäminen näkyviin.

LIITE 3. TIETOJÄRJESTELMIEN KÄYTTÖSÄÄNNÖT

TIETOJÄRJESTELMIEN KÄYTTÖSÄÄNNÖT

Sisällysluettelo:

1 Sääntöjen tarkoitus 1
2 Käytön periaatteet 1
3 Käyttöoikeus ja käyttäjätunnukset 2
4 Käyttöoikeuden voimassaolo 2
5 Tietojärjestelmien ylläpito 2

1 Sääntöjen tarkoitus

Yliopisto on sekä tiede- ja tutkimusyhteisö, opetusta antava laitos että valtion viranomainen. Sen tulee turvata kaikkien käyttäjäryhmiensä tietojen luottamuksellisuus, eheys ja käytettävyys sekä tarjota luotettava ja turvallinen ympäristö tietojen käsittelyyn. Nämä ja muut säännöt on laadittu auttamaan eri ryhmiin kuuluvia käyttäjiä tunnistamaan käyttöoikeuksiinsa liittyvät oikeudet, vastuut ja velvollisuudet. Käyttöoikeuksiin liittyvien velvollisuuksien tahatonkin laiminlyöminen saattaa vaarantaa muidenkin käyttäjien omistamien tietojen eheyden, luottamuksellisuuden ja käytettävyyden.

Näitä sääntöjä sovelletaan kaikkiin yliopiston hallinnassa tai muutoin yliopiston vastuulla oleviin tietojärjestelmiin ja niiden käyttöön sekä käyttäjien osalta myös muihin sellaisiin palveluihin, joiden käyttömahdollisuus tai käyttöoikeus on saatu yliopiston välityksellä. Säännöt koskevat myös yliopistolla yleisessä käytössä olevia työasemia ja kaikkia yliopiston verkkoon liitettyjä laitteita.

Kaikkien yliopiston tietotekniikan käyttäjien tulee noudattaa näiden sääntöjen lisäksi myös muita yliopiston tietojärjestelmistä antamia sääntöjä ja ohjeita, hyviä tapoja sekä Suomen lakia. Näiden tai muiden tietojärjestelmän käyttöä koskevien sääntöjen vastainen käyttö käsitellään [seuraamusohjeen] mukaisesti.

Sääntöjen kulloinkin voimassa oleva versio löytyy [MISTÄ].

2 Käytön periaatteet

Kaikkea käyttöä ja käyttösääntöjen tulkintaa ohjaavia keskeisiä yleisperiaatteita ovat:

- Kaikilla käyttöön oikeutetuilla on mahdollisuus kohtuulliseen ja asialliseen käyttöön.
- Muille käyttäjille tai tietoliikenneverkossa oleville organisaatioille tai tietojärjestelmille ei saa aiheuttaa haittaa tai vahinkoa.
- Yksityisyyden suojaa tulee kunnioittaa.
- Yliopiston myöntämä käyttöoikeus on henkilökohtainen.
- Käyttäjä vastaa kaikesta tunnuksensa käytöstä.

Yliopiston tietojärjestelmät on tarkoitettu työvälineeksi tehtäviin, jotka liittyvät opiskeluun, tutkimukseen, opetukseen tai hallintoon [yliopistossa]. Muu käyttö edellyttää erillistä sopimusta.

Yksityinen käyttö on sallittu vähäisessä määrin ja vain siltä osin kuin se ei haittaa muuta järjestelmän käyttöä eikä ole ristiriidassa kyseistä järjestelmää koskevien tai yleisten käytöstä annettujen sääntöjen kanssa. Yksityinen aineisto tulee yksityisyyden suojan varmistamiseksi pitää selkeästi erillään työhön liittyvästä aineistosta.

Kaupallinen käyttö muun kuin yliopiston lukuun on sallittu vain nimenomaisella luvalla.

Käyttö poliittiseen toimintaan (kuten vaalimainontaan) on kielletty. Poikkeuksena ovat yli-

opistovaalit, ylioppilaskunnan [toimintaan liittyvien poliittisten opiskelijajärjestöjen / alayhdistysten] sekä henkilökunnan ammattiyhdistysten yms. toiminta.

Kaikkien käyttäjien tulee omalta osaltaan huolehtia yhteiseen tietoturvallisuuteen liittyvistä asioista. Vaikka käyttäjällä itsellään ei olisikaan erityistä suojattavaa, muilla käyttäjillä saattaa olla. Kaikilla käyttäjillä on omalta osaltaan vastuu tietojärjestelmän kokonaisturvallisuudesta. Havaituista tai epäillyistä tietoturvallisuuden puutteista ja väärinkäytöksistä tulee ilmoittaa [tietoturvapäällikölle].

Yliopisto pyrkii suojaamaan kaikkia käyttäjiä haittaohjelmilta, roskapostilta ja yrityksiltä tunkeutua järjestelmiin tai yksittäisiin työasemiin. Käyttäjien on myös huolehdittava tässä toiminnassa omasta osuudestaan annettujen ohjeiden mukaisesti.

Käyttäjä vastaa itse tiedostojensa suojauksesta sekä viime kädessä niiden varmuuskopioinnista. Yliopisto varmuuskopioi keskitettyjen tietojärjestelmien tiedostot, mutta ei vastaa tiedostojen mahdollisen tuhoutumisen aiheuttamista vahingoista.

Käyttäjällä on vaitiolovelvollisuus järjestelmien tietosisällöstä, käyttötavoista, turvatasosta ja ominaisuuksista silloin, kun tietojärjestelmien käyttötarkoitus, niiden käytöstä annetut määräykset tai lainsäädäntö sitä vaativat.

Yliopiston verkkoon saa kytkeä vain verkon ylläpitäjän hyväksymiä ja rekisteröimiä laitteita. Liittämisessä tulee noudattaa annettuja ohjeita. [Yleiseen käyttöön tai käyttäjien omille laitteille varatut verkon osat on merkitty näkyvästi erikseen.]

3 Käyttöoikeus ja käyttäjätunnukset

Käyttäjälle myönnetään käyttöoikeus nimettyihin tietojärjestelmiin. Käyttöoikeus perustuu käyttäjän asemaan yliopistossa tai se voidaan erityisestä syystä myöntää yliopistoon kuulumattomalle.

Käyttöoikeuden aktivoinnin edellytyksenä on, että käyttäjä sitoutuu noudattamaan näitä sääntöjä sekä muita käyttöön liittyviä ohjeita ja määräyksiä. Käyttäjän on etukäteen tutustuttava järjestelmää koskeviin käyttöohjeisiin ja sääntöihin.

Käyttöoikeutta ei saa luovuttaa edelleen. Jos on syytä epäillä salasanan tai muun tunnisteen joutuneen jonkun muun tietoon/haltuun, salasana on vaihdettava tai tunnisteen käyttö on estettävä välittömästi. Salasana on vaihdettava määräajoin ja sen tulee olla [vaikeasti arvattava/murrettava / yliopiston salasanapolitiikan mukainen].

4 Käyttöoikeuden voimassaolo

Käyttöoikeus päättyy automaattisesti,

- kun käyttäjä ei enää kuulu yliopistoon,
- kun määräaikaisesti myönnetty käyttöoikeus vanhenee tai
- kun käyttäjän asema muuttuu siten, ettei kyseisen tietojärjestelmän käyttöoikeudelle enää ole perustetta.

Käyttäjän on ennen tätä itse huolehdittava käyttäjätunnuksensa omistuksessa olevien tietojen asianmukaisesta siirtämisestä tai poistamisesta. Käyttäjän tiedostot ja postilaatikko poistetaan [ajan] kuluttua tunnuksen käytön / käyttöoikeuden loppumisesta.

5 Tietojärjestelmien ylläpito

Kullakin yliopiston tietojärjestelmällä on oltava nimetty vastuutaho (omistaja), joka on vastuussa järjestelmän käyttötarkoituksesta, toiminnasta ja sisällöstä sekä sen käytöstä. Tietojärjestelmän omistaja laatii käyttöohjeet ja huolehtii siitä, että tietojärjestelmän palvelut ja sen käyttö ovat näiden sääntöjen mukaisia. Yliopiston yhteisten tietojärjestelmien ylläpidosta vastaa [atk-keskus]. Yliopiston yksiköiden hallinnoimista tietojärjestelmistä vastaa yksikön johtaja tai tämän kirjallisesti nimeämä henkilö. Kunkin yksikön järjestelmien vastuuhenkilöistä

ja ylläpitohenkilökunnasta pidetään erillistä luetteloa.

Tietojärjestelmien ylläpidosta, ylläpitäjän vastuista ja oikeuksista tietojärjestelmän toiminnan ja käytön hallintaan sekä sen tietoturvasta huolehtimiseen määrätään tarkemmin erillisessä ylläpitosäännössä.

Tietojärjestelmien toiminnasta ja käytöstä tallentuu lokia seuraavia tarkoituksia varten:

- palvelun toteuttamiseksi, kehittämiseksi ja sen tietoturvasta huolehtimiseksi
- järjestelmien sisältämien tietojen tietosuojasta huolehtimiseksi
- mahdollisten ongelmien ja teknisten vikojen havaitsemiseksi ja korjaamiseksi
- palveluun kohdistuvien väärinkäytösten havaitsemiseksi, estämiseksi, selvittämiseksi ja esitutkintaan saattamiseksi.

[Lokien käsittelystä määrätään tarkemmin erillisissä lokitietojen käsittelysäännöissä].

LIITE 4. SÄHKÖPOSTIN KÄSITTELYSÄÄNNÖT

SÄHKÖPOSTIN KÄSITTELYSÄÄNNÖT

Sisällysluettelo:

1 Yleistä ... 1
2 Sähköpostiviestien ja -osoitteiden määritelmät sekä käsittely ... 2
2.1 Määritelmät ja käyttötarkoitukset ... 2
2.2 Sähköpostiosoitteiden julkaiseminen ... 2
2.3 Organisaation sähköpostiviestien käsittely ... 3
2.4 Virkasähköpostiviestien käsittely ... 3
2.5 Henkilökohtaisten sähköpostiviestien käsittely ... 3
2.6 Muiden sähköpostiviestien käsittely ... 4
3 Erityistoimenpiteitä edellyttävät viestit ... 4
3.1 Sähköpostiviestien ja niiden liitetiedostojen rajoittaminen ... 4
3.2 Roskapostiviestien käsittely ... 4
3.3 Perille menemättömän sähköpostiviestin käsittely ... 5
3.4 Väärään osoitteeseen saapunut sähköpostiviesti ... 5
4 Sähköpostin käsittely erityistilanteissa ... 5
4.1 Automaattiset vastaukset viesteihin ... 5
4.2 Palvelussuhteen tai opiskeluoikeuden päättyminen ... 5
4.3 Menettelysäännöt työntekijän ollessa väliaikaisesti poissa ... 5
4.4 Sähköpostijärjestelmää haittaavat tai vaarantavat viestit ja postilaatikot ... 6
5 Sähköpostiviestin salaus ja todentaminen ... 6
6 Sähköpostin käytön valvonta sekä lokitietojen kerääminen ja säilyttäminen ... 6
7 Näiden sääntöjen valvonta ... 6

1 Yleistä

Sähköisten asiakirjojen käsittelyssä sovelletaan yliopistossa kirjesalaisuuden, yksityisyyden suojan ja hyvän hallintomenettelyn periaatteita samalla tavalla kuin muussakin virallisten asioiden hoidossa. Viestinnän osapuolten oikeudet on turvattava. Käyttäjiä koskevat vaitiolovelvollisuudet ja hyväksikäyttökiellot on kuvattu myöhemmin tässä dokumentissa sekä Tietojärjestelmien käytön säännöissä ja Tietojärjestelmien ylläpitosäännöissä.

Sähköpostiviestin perillemenosta varmistuminen on lähettäjän vastuulla. Sähköisessä asioinnissa lähettäjä voi varmistua viestin perille saapumisesta viranomaisen lähettämästä kuittauksesta viestin vastaanottamisesta.[1]

Yliopistolla on oikeus määrätä, mihin sähköpostia ja tietoverkkoa käytetään, ja käyttöoikeuksia voidaan rajoittaa puhelinsoiton estojen tapaan.

Sähköpostijärjestelmää ei ole tarkoitettu tiedostojen massajakeluun eikä suurten tiedostojen välittämiseen.

[1] Sähköisellä asioinnilla tarkoitetaan hallintoasiain sähköistä vireillepanoa ja sen täydentämistä, käsittelyä (ml. ratkaisu) ja päätöksen tiedoksiantoa tai oikeudenkäyntiasiakirjan lähettämistä sähköisenä viestinä yleiselle tuomioistuimelle tai sen määräämälle henkilölle.

Ohjeet ja suositukset sähköpostin käsittelyssä huomioitavista asioista perustuvat voimassaolevaan lainsäädäntöön ja valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI, http://www.vm.fi/vahti) ohjeisiin sähköpostin käsittelystä.

Tämä sääntö ja muita ohjeita yliopiston tietojärjestelmien käytöstä on saatavilla yliopiston www-palvelimelta [URL] sekä [MISTÄ PAPERILLA].

2 Sähköpostiviestien ja -osoitteiden määritelmät sekä käsittely

2.1 Määritelmät ja käyttötarkoitukset

Sähköpostiviestit on tässä säännössä jaettu neljään eri luokkaan sen mukaisesti, millaiseen osoitteeseen ne liittyvät. Säännössä sekä lähetetyt että vastaanotetut viestit määritellään seuraavasti:

- organisaation sähköpostiviesti on yliopiston tai yksikön organisaatio-osoitteeseen (esim. kirjaamo@DOMAIN.fi,valinta@DOMAIN.fi) liittyvä viesti.
- virkasähköpostiviesti liittyy sekä yliopiston työntekijälle työkäyttöön antamaan henkilökohtaiseen virkasähköpostiosoitteeseen (esim. vili.virta@DOMAIN.fi) että työntekijän työtehtäviin. Opiskelijan esim. yliopiston hallintoelimien tai tutkimustyöryhmien osana toimimiseen liittyvä sähköpostiviesti rinnastetaan virkasähköpostiviestiin.
- henkilökohtainen sähköpostiviesti on yliopiston antamaan sähköpostiosoitteeseen (yleensä sama kuin virkasähköpostiosoite tai opiskelijan sähköpostiosoite) liittyvä henkilökohtainen viesti.
- muu sähköpostiviesti on käyttäjän yliopiston ulkopuoliseen sähköpostiosoitteeseen esim. vili.virta@omakaytto.fi tai vili.virta@muuorganisaatio.fi) liittyvä viesti.

[Virka- ja henkilökohtaiset sähköpostiosoitteet muodostuvat käyttäjän nimestä. Muotoon etunimi.sukunimi@DOMAIN.fi tekevät poikkeuksen samannimiset henkilöt, joiden kaikkien osoitteisiin lisätään erotteleva osa. Myös sähköpostiviestin lähetysosoitteen tulee olla joko organisaatio-osoite tai nimimuotoinen virkasähköpostiosoite].

Luonnollisen henkilön sähköpostiosoite on henkilötietolain (523/1999) mukaan henkilötieto. Henkilötiedot on rekisteröity yliopiston henkilötietorekistereihin, joista on laadittu rekisteriselosteet. Henkilötietoja käsitellään yliopistossa rekisteriselosteiden mukaisella tavalla ja tarkoituksessa.

Yliopistolla ja sen yksiköillä tulee virallisten asioiden hoitoa ja palveluiden tarjoamista varten olla organisaatio-osoitteet (esim. kirjaamo@DOMAIN.fi tai humanistinen.tiedekunta@DOMAIN.fi). Yliopiston palveluita tulee lähestyä ensisijaisesti organisaatio-osoitteiden, eikä yksittäisten työntekijöiden virkasähköpostiosoitteiden kautta.

2.2 Sähköpostiosoitteiden julkaiseminen

Julkaisemisella tarkoitetaan sähköpostiosoitteen ilmaisemista muun muassa yliopiston puhelinluettelossa tai muussa julkaisussa, yliopiston julkisilla www-sivuilla, käyntikortissa ja hakemistopalvelussa.

Yliopisto julkaisee organisaatio-osoitteet sekä työntekijöidensä virkasähköpostiosoitteet, niiltä osin kuin se on tarpeen palveluiden käytön ja tehtävien hoidon kannalta. Pääsääntöisesti opiskelijan sähköpostiosoitteen julkaiseminen edellyttää opiskelijan suostumuksen. Yliopisto ei julkaise yliopiston ulkopuolisia sähköpostiosoitteita.

[Sähköpostiosoitteena tulee käyttää aina nimimuotoista osoitetta niin sähköpostiohjelmien asetuksissa kuin muutoinkin osoitetta julkaistessa].

2.3 Organisaation sähköpostiviestien käsittely

Jokaiselle organisaatio-osoitteelle tulee nimetä vähintään yksi vastuuhenkilö. Organisaation tulee huolehtia osoitteeseen saapuvien viestien säännöllisestä käsittelystä.

Organisaatiosähköpostin välittäminen tai automaattinen ohjaaminen yliopiston ulkopuoliseen sähköpostiosoitteeseen on kiellettyä tietosuojan ja tiedonhallinnan vuoksi.

Jos saapuneessa viestissä on kuittauspyyntö, lähetetään kuittausviesti ilman tarpeetonta viivettä. Sähköisessä asioinnissa viranomaisen on viipymättä ilmoitettava sähköisen asiakirjan vastaanottamisesta lähettäjälle kuittausviestillä. Automaattikuittauksia ei tule käyttää muissa kuin erityisesti sitä varten suunnitelluissa asiointijärjestelmissä.

Työntekijän lähettämästä yliopiston vastauksesta tulee ilmetä, että se on lähetetty vastauksena organisaatio-osoitteeseen tulleeseen viestiin. Vastauksessa on myös korostettava tai asetettava paluuosoite siten, että yhteydenotot jatkossakin tapahtuvat organisaatio-osoitteeseen.

Tarvittaessa sähköpostiviestiin voidaan lisätä luottamuksellisuutta osoittava lopputeksti.

Organisaation sähköpostiviestejä käsitellään lain viranomaisten toiminnan julkisuudesta (julkisuuslain, 621/1999) edellyttämällä tavalla. Julkisuuslaissa säädetään muun muassa, mikä on viranomaisen asiakirja, mitkä ovat salassa pidettävät tiedot ja milloin on oikeus saada tieto asiakirjasta. Lisätietoja julkisen hallinnon sähköpostisuosituksesta JHS 132 (http://www.intermin.fi/juhta).

Organisaation sähköpostiviestejä käsitellään ja ne arkistoidaan tarvittaessa arkistonmuodostussuunnitelmassa ilmenevällä tavalla.

2.4 Virkasähköpostiviestien käsittely

Virkasähköpostin välittäminen tai automaattinen ohjaaminen yliopiston ulkopuoliseen sähköpostiosoitteeseen on kielletty tietosuojan ja tiedonhallinnan vuoksi.

Yliopisto kohtelee virkasähköpostiosoitteella toimitettua viestiä pääsääntöisesti vastaanottajalle osoitettuna henkilökohtaisena viestinä, koska vastaanottaja ei voi estää henkilökohtaisten viestien saapumista.

Työnantajan oikeudesta hakea esille tai avata työntekijälle lähetettyjä tai tämän lähettämiä sähköpostiviestejä (TETSL, 759/2004) säädetään tarkemmin luvussa 4.3

Jos saapuneessa viestissä on kuittauspyyntö, lähetetään kuittausviesti ilman tarpeetonta viivettä. Sähköisessä asioinnissa viranomaisen on viipymättä ilmoitettava kuittausviestillä lähettäjälle sähköisen asiakirjan vastaanottamisesta. Kuittausviestin lähettää asiaa käsittelevä henkilö, automaattikuittauksia ei tule käyttää. (Automaattikuittauksista säädetään tarkemmin luvussa 4.1).

Työntekijän lähettämästä virkasähköpostiviestistä tulee ilmetä, että sen lähettäjä on viranomainen, ei yksittäinen työntekijä, esim. liittämällä allekirjoitukseen asema ja yksikön nimi. Mikäli kysymyksessä on hakemus tms. viranomaistoimenpiteitä edellyttävä toimenpide, tulee paluuosoite asettaa siten tai muistuttaa asiakasta siitä, että jatkoyhteydet hoidetaan organisaatio-osoitteen kautta.

Tarvittaessa sähköpostiviestiin voidaan lisätä luottamuksellisuutta osoittava lopputeksti.

Virkasähköpostiviestejä käsitellään lain viranomaisten toiminnan julkisuudesta (julkisuuslain, 621/1999) edellyttämällä tavalla. Julkisuuslaissa säädetään muun muassa mikä on viranomaisen asiakirja, mitkä ovat salassa pidettävät tiedot ja milloin on oikeus saada tieto asiakirjasta.

Virkasähköpostiviestejä käsitellään ja ne arkistoidaan tarvittaessa arkistonmuodostamissuunnitelmassa ilmenevällä tavalla.

2.5 Henkilökohtaisten sähköpostiviestien käsittely

Työntekijän henkilökohtaiset viestit tulee erottaa selvästi yliopistolle kuuluvista viesteistä. Työntekijän tulee siirtää virkasähköpostiosoitteeseensa tulevat henkilökohtaiset viestit välit-

tömästi omiin kansioihinsa, joiden nimestä yksityisyys on nähtävissä (private, yksityisasiat tms.). Tämä koskee sekä saapuvia että lähteviä viestejä.

Yliopiston sähköpostiosoitteen käyttö työntekijän tai opiskelijan henkilökohtaisiin tarkoituksiin on luvallista vähäisessä määrin ja siten, että se ei haittaa yliopiston toimintoja. Kuitenkin käyttö kaupalliseen tai poliittiseen tarkoitukseen, kuten yksityiseen yritystoimintaan tai yliopiston ulkopuolisten vaalien ehdokasmainontaan, on ehdottomasti kiellettyä lukuunottamatta yliopistovaaleja sekä opiskelijajärjestöjen ja henkilökunnan ammattiyhdistysten toimintaa.

Ketjukirjeitä tai massapostituksia ei saa lähettää yliopiston sähköpostipalvelimilla. Yliopiston tarve laajaan tiedotukseen yliopistoyhteisön jäsenille harkitaan tapauskohtaisesti.

2.6 Muiden sähköpostiviestien käsittely

Yliopiston ulkopuolinen sähköpostiosoite (eli muu osoite kuin @DOMAIN.fi) on yksityisasia, jota ei tässä tarkemmin ohjata. Työntekijä ei saa käyttää yliopiston ulkopuolista sähköpostiosoitetta yliopistoon liittyviin työtehtäviin.

Opiskelijan opiskeluun ja muuhun yliopistoyhteisön osana toimimiseen ei pidä käyttää yliopiston ulkopuolista sähköpostiosoitetta. Yliopisto voi edellyttää yliopiston sähköpostiosoitteen käyttöä sähköpostin avulla tapahtuvassa asioinnissa. Muiden kuin tutkinto-opiskelijoiden osalta (ei aina yliopiston antamaa sähköpostiosoitetta) ohjeistetaan erikseen.

Yliopiston ulkopuoliseen sähköpostiosoitteeseen liittyvillä käyttäjätunnuksilla ei saa käyttää samoja salasanoja kuin yliopiston tarjoamilla käyttäjätunnuksilla.

Yliopiston ulkopuolisen sähköpostiosoitteen ja –palvelun käyttöä yliopiston työasemilta käsin ei suositella.

3 Erityistoimenpiteitä edellyttävät viestit

3.1 Sähköpostiviestien ja niiden liitetiedostojen rajoittaminen

Yliopistolla on oikeus ohjelmallisesti tarkistaa sähköpostiviestit ja niiden liitetiedostot mahdollisten virusten ja muiden haittaohjelmien osalta sekä rajoittaa mahdollisesti haitallisten tai liian suurien/monilukuisten liitetiedostojen vastaanottamista ja lähettämistä. Yliopistolla on oikeus myös poistaa viruksia ja muita haittaohjelmia sisältävät viestit ja liitetiedostot. Yliopiston ei tarvitse tiedottaa yksittäisen viestin suodattamisesta tai tuhoamisesta viestin lähettäjälle. Suodatus tapahtuu sähköpostijärjestelmässä automaattisesti. Käyttäjille tiedotetaan näistä rajoituksista Sähköpostin suodatusohjeessa.

3.2 Roskapostiviestien käsittely

Yliopisto suojaa sähköpostipalveluaan ja vähentää roskapostiongelmaa suodattamalla viestit, jotka saapuvat tunnetuista roskapostia välittävistä palvelimista tai jotka luokitellaan roskapostiksi otsikkotietojensa tai automaattisen sisältöanalyysin perusteella. Esto toteutetaan teknisin menetelmin sähköpostipalvelussa. Yliopisto voi myös tuhota suodatetut viestit käyttäjän puolesta.

Yliopiston ei tarvitse tiedottaa yksittäisen roskapostiviestin suodattamisesta tai tuhoamisesta viestinnän osapuolille tai palauttaa tuhottua viestiä lähettäjälle. Suodatuksessa käytetyistä metodeista yliopisto tiedottaa Sähköpostin suodatusohjeessa.

Roskapostiin ei pidä vastata, koska näin vain lisätään roskapostin saapumista. Vastaamalla osoittaa sähköpostiosoitteensa toimivaksi, ja se lisätään roskapostittajien osoitelistoille.

Käyttäjä voi ilmoittaa häiritsevästä roskapostista ylläpitohenkilöstölle tai atk-tukihenkilölle. Käytännössä ylläpito voi pyrkiä puuttumaan vain Suomesta lähetettyihin viesteihin.

3.3 Perille menemättömän sähköpostiviestin käsittely

Sähköpostiviestin lähettäjällä on vastuu viestin luettavuudesta, viestin perillemenosta, mahdollisen määräajan ylittymisestä ja muista näihin verrattavista seikoista, kunnes hän on saanut tiedon viestin onnistuneesta perillemenosta.

Mikäli saapuvan viestin osoite ei ole sähköpostijärjestelmän tiedossa, lähetetään viestin lähettäjälle automaattisesti virheilmoitus. Ilmoitus lähetetään lähettäjälle myös, jos vastaanottajan sähköpostin tilakiintiö on täynnä. Käyttäjät vastaavat itse tilakiintiöstään.

Lähetys- ja palautusvelvollisuudet eivät koske haittaohjelmaviestejä eivätkä roskapostia.

3.4 Väärään osoitteeseen saapunut sähköpostiviesti

Mikäli käyttäjä saa toiselle henkilölle tarkoitetun sähköpostiviestin, käyttäjällä on vaitiolovelvollisuus ja hyväksikäyttökielto niin viestin sisällöstä kuin olemassaolostakin.

Toiselle henkilölle (esimerkiksi kaimalle) tarkoitettu sähköpostiviesti on ohjattava edelleen oikeaan osoitteeseen, jos osoite on tiedossa. Mikäli osoitetta ei ole tiedossa, on viestin vastaanottajan lähetettävä alkuperäiselle lähettäjälle tieto epäonnistuneesta toimituksesta ja hävitettävä saapunut viesti.

Yliopiston tai virkamiehen toimivaltaan kuulumaton, ilmeisestä erehdyksestä tai tietämättömyydestä lähetetty sähköpostiviesti on siirrettävä hallintolain (434/2003) 21 §:n mukaisesti toimivaltaiseksi katsotulle viranomaiselle, jos se on tiedossa; siirrosta on ilmoitettava viestin lähettäjälle. Ellei siirto ole mahdollinen, viesti palautetaan ja hävitetään yliopiston palvelimilta.

Lähetys- ja palautusvelvollisuudet eivät koske haittaohjelmaviestejä eivätkä roskapostia.

4 Sähköpostin käsittely erityistilanteissa

4.1 Automaattiset vastaukset viesteihin

Automaattisten vastausten käyttöä ei suositella. Jos automaattivastaus kuitenkin katsotaan välttämättömäksi (esimerkiksi työntekijöiden pitkät lomat tai virkavapaudet tai palvelussuhteen päättyminen), tulee siinä kehottaa lähettäjää ottamaan yhteyttä ensisijaisesti sopivaan organisaatio-osoitteeseen.

4.2 Palvelussuhteen tai opiskeluoikeuden päättyminen

Henkilön käyttöoikeus yliopiston antamaan sähköpostiosoitteeseen päättyy palvelussuhteen tai opiskeluoikeuden päättyessä. Yliopiston ulkopuolisten henkilöiden käyttöoikeuksien voimassaolosta vastaa käyttöoikeutta puoltaneen yksikön esimies. Käyttöoikeuden päättymisen jälkeen yliopisto ei ota vastaan henkilölle lähetettyjä viestejä vaan ilmoittaa automaattisesti lähettäjälle osoitteen toimimattomuudesta.

Ennen palvelussuhteen päättymistä työntekijän tulee ilmoittaa viestintäkumppaneilleen sähköpostiosoitteensa poistumisesta ja poistaa henkilökohtaiset viestinsä. Muut viestit jäävät yliopiston haltuun. Jos työntekijä lakkaa hoitamasta tehtäviään jo ennen työsuhteen päättymistä, tulee sähköpostin vastaanotto estää jo siinä vaiheessa. (Automaattisista vastauksista katso luku 4.1.)

Ennen käyttöoikeuden päättymistä on opiskelijan vastuulla ilmoittaa viestintäkumppaneilleen sähköpostiosoitteensa poistumisesta ja poistaa viestinsä.

Tarkemmat ohjeet löytyvät [erillisistä ohjeista].

4.3 Menettelysäännöt työntekijän ollessa väliaikaisesti poissa

Kun kyse on ennakoidusta poissaolosta, työntekijän ja esimiehen on huolehdittava työntekijän sähköpostin asianmukaisesta hoidosta. Suositeltavin tapa on postilaatikon lukuoikeuden anta-

minen tehtäviä poissaolon aikana hoitavalle henkilölle pääsyoikeuslistojen avulla. (Automaattisista vastauksista katso luku 4.1.)

Yliopistolla on oikeus lain yksityisyyden suojasta työelämässä (759/2004, 18-20§) asettamissa rajoissa saada käyttöönsä yliopistolle kuuluvat, sen toiminnan jatkumisen kannalta välttämättömät viestit työntekijän ollessa estyneenä. Työntekijälle virkasähköpostiosoitteella lähetettyjen tai tämän lähettämien viestien sekä selville saaminen että niiden avaaminen perustuu ensisijaisesti työntekijän suostumukseen sekä siihen että työntekijän luottamukselliset henkilökohtaiset viestit ovat erotettavissa yliopistolle selvästi kuuluvista viesteistä. (viestien erottelusta ks. luku 2.5).

Mikäli työntekijä ei ole antanut toiselle työnantajan hyväksymälle henkilölle suostumusta, että tämä saa etsiä ja avata työntekijän poissa ollessa tämän sähköpostiviesteistä työnantajalle kuuluvat viestit, tai vakavan sairauden takia häneltä ei voida suostumusta saada, voi hallintojohtaja määrätä henkilön esimiehen postipalvelimen pääkäyttäjän avulla selvittämään ja avaamaan työntekijän poissa ollessa yllä määritellyt virkasähköpostiviestit. Viestien etsinnän ja avaamisen syy, siihen osalliset ja ajankohta sekä kenelle avatusta viestistä on annettu tieto, on kirjattava ja ilmoitettava ilman aiheetonta viivytystä työntekijälle.

4.4 Sähköpostijärjestelmää haittaavat tai vaarantavat viestit ja postilaatikot

Sähköpostijärjestelmän ylläpidon oikeudesta puuttua sähköpostin kulkuun sähköpostijärjestelmän palvelutason tai turvallisuuden takaamiseksi säädellään tarkemmin Tietojärjestelmien ylläpitosäännöissä.

5 Sähköpostiviestin salaus ja todentaminen

Käyttäjällä on oikeus salata sähköpostiviestinsä salausmenetelmää käyttäen.

Erittäin salaisiksi tai salaisiksi turvaluokiteltuja asiakirjoja ei saa lähettää sähköpostilla.

Muita kuin julkisia tietoja ja julkisia henkilötietoja sisältäviä asiakirjoja ei tule siirtää sähköpostina tai muuna tietoverkon yli tapahtuvana tiedonsiirtona ilman salausta.

Salassa pidettäviä henkilö- ja muita tietoja voidaan kuitenkin siirtää sähköisesti, mikäli tiedon salaukseen käytetään riittävän vahvoja salausalgoritmeja tai koko tiedonsiirtoväylää voida pitää riittävän turvallisena.

Käytettävien salausohjelmien tulee organisaatio- ja virkasähköpostiviestien osalta olla yliopiston hyväksymiä ja käyttöönottamia.

Sähköpostilla vastaanotetun asiakirjan oikeellisuus ja aitous on tarvittaessa varmistettava.

Jos virkasähköposti on salattu siten, että vain vastaanottaja voi avata sen, se on avattava välittömästi siirron jälkeen. Tarvittaessa se voidaan salata uudestaan siten, että se on muidenkin asian käsittelijöiden avattavissa. Velvollisuus ei koske haittaohjelmia sisältäviä viestejä eikä roskapostia.

6 Sähköpostin käytön valvonta sekä lokitietojen kerääminen ja säilyttäminen

Sähköpostin käytön valvonta sekä lokitietojen kerääminen ja säilyttäminen on ohjeistettu Tietojärjestelmien ylläpitosäännöissä [ja Lokien käsittelysäännöissä].

7 Näiden sääntöjen valvonta

Näiden sääntöjen valvonnasta vastaavat yliopiston [atk-keskus, muiden mahdollisten yliopiston yksiköiden sähköpostipalvelinten omistajat] sekä työnjohdollisesti esimiehet. Sääntörikkomusten käsittely tapahtuu [Tietotekniikkarikkomusten seuraamuskäytännön] mukaisesti.

Sääntöjä päivitetään tarvittaessa tai yliopistojen yhteisen sääntösuosituksen muuttuessa. Päivitystarvetta seuraa [tietoturvapäällikkö].

Liite 5. TIETOJÄRJESTELMIEN YLLÄPITOSÄÄNNÖT

TIETOJÄRJESTELMIEN YLLÄPITOSÄÄNNÖT

Sisällysluettelo:

1 Johdanto 1
1.1 Määritelmät 1
1.2 Ylläpitäjän valtuudet 2
2 Vastuut 2
3 Toimintaperiaatteet 3
3.1 Hyvä ylläpitotapa 3
3.2 Yksityisyyden suojan kunnioittaminen 3
3.3 Vaitiolovelvollisuus 3
4 Toimintakäytännöt 3
4.1 Identiteetit, salasanat 3
4.2 Käyttöoikeuksien rajoittaminen selvitysmenettelyn ajaksi 3
4.3 Sähköpostin käsittely 4
4.4 Muiden tiedostojen käsittely 4
4.5 Hakemistojen ja tiedostolistausten seuranta 5
4.6 Ohjelmien ja prosessien seuranta 5
4.7 Tietoliikenneverkon seuranta 6
4.8 Lokitietojen käsittely 6
4.9 Tietojen säilytys 6
5 Näiden sääntöjen valvonta 7
Liite 1: Ohjaava lainsäädäntö 7
Liite 2: Salassapitositoumus 8

1 Johdanto

1.1 Määritelmät

Ylläpidolla tarkoitetaan näissä säännöissä

- tietojärjestelmien pitämistä toimintakuntoisina ja tietoturvallisina
- tarpeelliseksi havaittujen muutosten tai korjausten tekemistä tietojärjestelmiin,
- käyttäjätunnusten sekä käyttö- ja pääsyoikeuksien hallinnointia tietojärjestelmissä sekä
- tietojärjestelmien toiminnan ja käytön seurantaa ja tilastointia.

Tietojärjestelmällä tai järjestelmällä tarkoitetaan näissä säännöissä

- yksittäistä atk-laitetta tai -laitteistoa tai niiden muodostamaa kokonaisuutta,
- yliopiston tietoliikenneverkkoa,
- yllä olevissa toimivia ohjelmistoja ja palveluita sekä
- niissä olevaa tietosisältöä.

Ylläpitäjällä tarkoitetaan kaikkia yliopiston tietojärjestelmien atk-teknisestä ylläpidosta vastaavia henkilöitä sekä muita yliopiston atk-tukihenkilöitä, jotka näiden kanssa vastaavat järjestelmien ylläpitoon liittyvistä toimista sekä käyttäjien tuesta ja ohjauksesta. Laajasti ymmärrettynä ylläpitäjällä tarkoitetaan jokaista henkilöä, jolla on pääkäyttäjän oikeuksia järjestelmään.

Yliopiston yksiköllä tarkoitetaan yliopiston laitosta, osastoa tai muuta toiminnallista vastuualuetta.

Yliopiston tietojärjestelmän vastuullinen omistaja on se yliopiston yksikkö, jonka toimintaa ja tietojenkäsittelyä varten järjestelmä on hankittu ja joka määrittelee järjestelmän käyttöön oi-

keutetut. Ohjelmien, www-sivujen yms. aineiston omistajana voi olla myös aineiston tekijä eli käyttäjä, tekijänoikeuslain mukaisesti.

Yliopiston tietojärjestelmän hallinnoijan tehtävänä on teknisesti huolehtia tietojärjestelmästä. Tietojärjestelmän omistaja on myös sen hallinnoija, ellei hallinnointivastuuta ole sopimuksella siirretty yliopiston toiselle yksikölle tai ulkopuoliselle palveluntarjoajalle.

1.2 Ylläpitäjän valtuudet

Ylläpitäjällä on tietojärjestelmien toiminnallisuuden takaamiseksi kattavat oikeudet tutkia järjestelmien tilaa sekä tarvittaessa myös puuttua järjestelmien toimintaan, yksittäisen käyttäjän tietojärjestelmien käyttöön sekä hänen tietojärjestelmissä oleviin aineistoihinsa.

Tietoturvaloukkausten torjumiseksi ja tietoturvaan kohdistuvien häiriöiden poistamiseksi ylläpitäjällä on oikeus ryhtyä välttämättömiin toimiin tietoturvan varmistamiseksi.

Jotta ylläpitäjän erioikeudet eivät olisi ristiriidassa järjestelmän käyttäjien oikeusturvan kanssa, ylläpitäjän erioikeuksien käyttöä säädellään ohjeilla ja määräyksillä, jotka perustuvat ensisijaisesti Suomen lainsäädäntöön[1] ja lisäksi yliopiston tietojärjestelmien käytön sääntöihin ja yliopiston tietoturvaperiaatteisiin. Ylläpitäjää koskevat tietoturvaperiaatteet on kirjattu yliopiston Tietoturvapolitiikassa, Sähköpostin käsittelysäännöissä, Tietotekniikkarikkomusten seuraamuskäytännössä, näissä Ylläpitosäännöissä sekä Lokitietojen käsittelysäännöissä.

Nämä säännöt sitovat yliopiston kaikkia ylläpitäjiä, myös opiskelijaa, jos hän ylläpitää yliopiston verkkoon kytkettyä tietojärjestelmää.

Nämä säännöt ja muita ohjeita yliopiston tietojärjestelmien käytöstä ovat saatavilla yliopiston www-palvelimelta [http://www.*yliopisto*.fi/… sekä tietohallinnon/atk-osaston/atk-keskuksen/tietokonekeskuksen käyttäjäinfosta.]

2 Vastuut

Yksikön on dokumentoitava omistamansa tietojärjestelmät tai järjestelmäkokonaisuudet, tärkeysluokiteltava ne sekä nimettävä niiden hallinnoijat ja ylläpitäjät. Omistaja vastaa mahdollisten tietojärjestelmäselosteiden olemassaolosta ja saatavuudesta. 2.

Tietojärjestelmän omistaja ja viime kädessä yksikön esimies vastaa siitä, että järjestelmässä noudatetaan lakia, hyvää ylläpitotapaa sekä yliopiston voimassaolevia sääntöjä ja politiikkoja. Omistajalla on aina lopullinen vastuu järjestelmän ylläpidosta. Tietojärjestelmän hallinnoija vastaa järjestelmien hyvän ylläpitotavan mukaisesta teknisestä ylläpidosta. Jokaisella järjestelmällä on oltava nimetyt ylläpitäjät. Ylläpitotehtävät jaetaan mahdollisuuksien mukaan usealle henkilölle, joilla on eri käyttövaltuudet. Myös ylläpitäjien toimenpiteistä kerätään tarvittavaa lokitietoa.

Tietojärjestelmän omistaja tai hallinnoija ei ole vastuussa käyttäjän henkilökohtaisten aineistojen sisällöstä, vaan käyttäjä itse vastaa aineistojensa laillisuudesta ja suojaa ne yliopiston antamien ohjeiden mukaisesti. Järjestelmän hallinnoijalla on kuitenkin laissa säädetty oikeus ja velvollisuus puuttua käyttäjän aineistoihin, jos on perusteltua syytä epäillä, että niissä on tietoturvauhkia tai lainvastaisuuksia (ks. Tietotekniikkarikkomusten seuraamuskäytäntö).

Jos ylläpitäjän epäillään tai havaitaan väärinkäyttäneen erioikeuksiaan, otetaan yhteyttä yksikön esimieheen, joka tekee päätöksen[tietoturvapäällikön / tietohallintojohtajan / tietoturvavastaavan] kanssa jatko- ja suojatoimenpiteistä Tietotekniikkarikkomusten seuraamuskäytännönmukaisesti.

---

[1] Keskeisimmät lait Liittessä 1

[2] Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta, JulkA 1030/1999 8§ VM 7/01/2000, Julkisuuslain mukaisen tietojärjestelmäselosteen laadintasuositus, VAHTI-ohjeissa http://www.vm.vahti/

3 Toimintaperiaatteet

3.1 Hyvä ylläpitotapa

Tietojärjestelmiä on ylläpidettävä hyvän ylläpitotavan mukaisesti. Tietojärjestelmien hyvä ylläpitotapa tarkoittaa suunnitelmallista, vastuuntuntoista ja ammattitaitoista ylläpitoa, jossa otetaan huomioon julkisuuslaissa ja -asetuksessa säädetty hyvä tiedonhallintatapa[3].

3.2 Yksityisyyden suojan kunnioittaminen

Yliopiston tietojärjestelmien hallinnoinnissa otetaan huomioon käyttäjien ja heidän viestintäkumppaniensa oikeus yksityisyyteen ja viestintäsalaisuuteen. Yliopistolla on kuitenkin nämä perusoikeudet huomioon ottaen oikeus määrätä itse omistamiensa tietojärjestelmien tietosisällöstä ja käyttötarkoituksesta. Tämä koskee myös yliopiston omistaman tietoliikenneverkon liikennettä. Käyttötarkoituksesta on säädelty tarkemmin yliopiston Tietojärjestelmien käytön säännöissä tai järjestelmäkohtaisissa säännöissä.

Käyttäjän pyytäessä ylläpitäjää käsittelemään sähköpostiaan tai muita tiedostojaan ylläpitäjän tulee varmistua käyttäjän henkilöllisyydestä asianmukaisella tavalla, esim. kelvollisen henkilöllisyystodistuksen kautta, ellei hän tunne käyttäjää.

Kun ylläpitäjällä on tarve ottaa yhteyttä käyttäjään, voidaan se tehdä joko hallinnon tietojärjestelmistä löytyvään puhelinnumeroon tai sähköpostilla. Jos on kuitenkin syytä epäillä käyttäjätunnuksen olevan väärissä käsissä, ei sähköpostia tule käyttää.

3.3 Vaitiolovelvollisuus

Ylläpitäjällä on vaitiolovelvollisuus ja hyväksikäyttökielto työtehtäviä hoitaessaan tietoonsa saamistaan työtehtäviin liittymättömistä asioista sekä niiden olemassaolosta. Työtehtäviin liittyvistä ei-julkisista asioista saa keskustella vain sellaisten henkilöiden tai viranomaisten kanssa, joita sitoo sama vaitiolovelvollisuus, ja joiden työtehtäviin käsiteltävä asia liittyy.

Ylläpitäjää sitoo erityisesti rikoslain 40 luvun 5 §. Sen mukaan ylläpitäjä ei saa oikeudettomasti paljastaa tai hyödyntää palvelusuhteensa aikana tai sen päätyttyä tehtävänsä tai asemansa vuoksi tietoonsa saamiaan salassa pidettäviä tai muita sellaisia asioita, joita ei saa lain mukaan paljastaa kuten käyttäjien yksityisasioita.

Ylläpitäjä tekee salassapitositoumuksen (Liite 2).

4 Toimintakäytännöt

4.1 Identiteetit, salasanat

Ylläpitäjä ei tehtäviensä hoitamiseksi tarvitse käyttäjän salasanaa eikä hänen tule sitä käyttäjältä tiedustella.

Mikäli ongelman selvitys edellyttää käyttäjän identiteetin hetkellistä käyttöä, tulee joko käyttäjän olla itse paikalla antamassa salasana autentikointipalvelulle tai ylläpitäjän on otettava käyttäjän identiteetti käyttöönsä ylläpitäjän erioikeuksien avulla. Jälkimmäisestä on ilmoitettava käyttäjälle niin pian kuin se on mahdollista. Identiteettiä ei saa käyttää kauemmin kuin ongelman ratkaisemiseksi on välttämätöntä.

Ylläpitäjän on näissä tilanteissa varmistauduttava käyttäjän henkilöllisyydestä asianmukaisella tavalla.

Pääkäyttäjän oikeuksia käytetään vain, kun niitä tarvitaan ylläpitotehtäviin.

4.2 Käyttöoikeuksien rajoittaminen selvitysmenettelyn ajaksi

Mikäli epäillään yliopiston tietoturvallisuuden vaarantuneen tai käyttäjän syyllistyneen käyttöohjeiden vastaiseen menettelyyn, on ylläpitäjällä oikeus rajoittaa käyttöoikeudet selvittelymenettelyn ajaksi.

---

[3] Laki julkisuudesta viranomaisen toiminnassa, JulkL 621/1999, 18§ sekä JulkA 1-4§

Todetun väärinkäytön seuraamukset käsitellään Tietotekniikkarikkomusten seuraamuskäytännön mukaisesti.

4.3 Sähköpostin käsittely

Henkilökohtaisen kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on Suomen perustuslain mukaan loukkaamaton, ellei laissa toisin säädetä. Sähköposti on rinnastettavissa kirjeeseen. Sähköposti on luottamuksellinen, ellei sitä ole tarkoitettu yleisesti vastaanotettavaksi.

Sähköpostin normaalit käsittelyperiaatteet säädellään Sähköpostin käsittelysäännöissä. Näissä Tietojärjestelmien ylläpitosäännöissä säädellään erikoistilanteista, joissa ylläpitäjän on puututtava postin kulkuun järjestelmän palvelutason tai turvallisuuden takaamiseksi.

Ylläpitäjä voi joutua avaamaan käyttäjien sähköpostia sisältäviä tiedostoja seuraavissa tilanteissa:

- Käyttäjän pyytäessä sitä ylläpitäjältä. Pyyntö voidaan esittää esim. tilanteessa, jossa sähköpostilaatikko ei aukea käyttäjän käytettävissä olevilla ohjelmilla. Lupa koskee vain yhtä nimenomaista kertaa. Mikäli käyttäjä pyytää tietoa postilaatikon sisällöstä, ylläpitäjän on ehdottomasti varmistuttava pyytäjän henkilöllisyydestä (ks luku 3.2).
- Käyttäjän postilaatikon aiheuttaessa häiriötilanteita esimerkiksi suuren koon tai vaurioituneen rakenteen vuoksi.
  - Suuren kokonsa takia postinkulkua haittaava postilaatikko tulee ensisijaisesti siirtää avaamattomana muualle. Käyttäjälle on ilmoitettava, missä postilaatikko sijaitsee, mikäli postijärjestelmä ei automaattisesti löydä sitä uudesta sijaintipaikasta. Jos postilaatikkoa ei voida suuren kokonsa takia sijoittaa käyttäjän tavoitettavissa olevaan paikkaan, on käyttäjän kanssa sovittava toimenpiteistä viestien luovuttamiseksi käyttäjälle. Siirretyn postilaatikon saa pakata vähemmän tilaa vievään muotoon, mikäli käyttäjälle annetaan tarkat ohjeet kuinka postiviesteihin pääsee jälleen käsiksi. Suuri postilaatikko voidaan erityisessä poikkeustilanteessa myös tuhota, ellei sille kohtuudella voida tehdä muuta. Päätöksen tekee järjestelmää hallinnoivan yksikön [ylläpitoryhmän esimies].
  - Ylläpitäjä saa korjata rakenteellisesti rikkinäisen postilaatikon kysymättä käyttäjältä erikseen lupaa. Ylläpitäjällä ei ole kuitenkaan lupaa lukea vain vastaanottajalle tarkoitettua tekstisisältöä. Tässä, kuten kaikissa muissakin tilanteissa, ylläpitäjää sitoo vaitiolovelvollisuus.
  - Postilaatikkoon kohdistuvista ei-automaattisista toimenpiteistä ilmoitetaan käyttäjälle viipymättä.
- Kun postijärjestelmä ei kykene toimittamaan sitä eteenpäin puutteellisen tai vaurioituneen rakenteen vuoksi. Tällöin ylläpitäjällä on lupa tutkia ja korjata viestin teknisiä ohjaustietoja, mutta ylläpitäjän tulee mahdollisuuksien mukaan olla tutustumatta viestin vastaanottajalle tarkoitettuun tekstisisältöön.

Ylläpitäjällä on myös oikeus poistaa välitettävänä olevan sähköpostin jonosta postijärjestelmän toiminnan vaarantavat sekä ilmeisen tarpeettomat teknisestä virheestä aiheutuneet viestit.

4.4 Muiden tiedostojen käsittely

Ylläpitäjällä ei ole yleistä oikeutta lukea tai muuten käsitellä käyttäjien omistuksessa olevien tiedostojen sisältöä.

Ylläpitäjällä on kuitenkin oikeus käsitellä tiedostoja esimerkiksi seuraavissa tilanteissa:

- Kun käyttäjä on antanut siihen luvan ongelmatilanteen selvittämiseksi.
- Erityisestä kirjallisesta pyynnöstä (esim. mikäli yliopiston tehtävien hoito on vaarassa vaikeutua poissaolon vuoksi, voidaan poissaolevan työntekijän/opiskelijan omistuksessa olevia, muilta suojattuja tiedostoja joutua käsittelemään. Yksikön esimies, tai vastaava, voi määrätä ylläpitäjän antamaan nimetylle henkilölle käyttöoikeuden tarvittaviin tiedostoihin).

- Jos käyttäjätunnuksen hallussa on ohjelmia tai alustustiedostoja, jotka aiheuttavat häiriöitä järjestelmän toiminnalle, turvallisuudelle tai muiden käyttäjien tietosuojalle. Tällöin ylläpitäjä voi tarkistaa ohjelmatiedostojen sisällön ja tarvittaessa estää niiden toiminnan.
- Jos on perusteltu syy epäillä, että käyttäjätunnus on joutunut vääriin käsiin ja että sen omistuksessa on tiedostoja tai ohjelmia, jotka aiheuttavat vaaraa tai uhkaa yliopiston toimintakyvylle tai turvallisuudelle.
  - Mikäli ylläpitäjä epäilee tunnuksen olevan väärissä käsissä, on ylläpitäjällä oikeus tilapäisesti sulkea tunnus, ja muutoin toimitaan Tietoturvapoikkeamiin reagoimisen]sekä Tietotekniikkarikkomusten seuraamuskäytännön mukaisesti. Yleisperiaatteena on, että käyttäjään pyritään saamaan yhteys ennen toimenpiteitä, mutta suojaus- ja korjaustoimenpiteet voidaan joutua tekemään välittömästi ennen yhteydenottoa.
- Jos on perusteltu syy epäillä, että käyttäjätunnuksen haltija on itse syyllistynyt väärinkäytökseen ja voidaan olettaa, että tietyissä käyttäjän omistamissa tiedostoissa on todisteita väärinkäytöksestä.
  - Ylläpitäjällä on oikeus tilapäisesti sulkea tunnus väärinkäyttötapauksessa. Käyttäjän väärinkäytös käsitellään yliopiston Tietojärjestelmien käytön sääntöjen, Tietotekniikkarikkomusten seuraamuskäytännön sekä Tietoturvapoikkeamiin reagoimisen mukaisesti.
- Ylläpidolla on oikeus estää sellaisten www-sivujen näkyminen, jotka ovat lain, yliopiston [www-politiikan] tai Tietojärjestelmien käytön sääntöjen vastaisia.
- Kun tiedostojen suojaus sen muutenkin sallii.

Edellä mainitun lisäksi ylläpitäjällä on aina oikeus:

- lukea ja muuttaa käyttäjien kotihakemistoissa sijaitsevia alustustiedostoja, postinohjaus- tai lajittelutiedostoja sekä muita järjestelmän toimintaan vaikuttavia tiedostoja, mikäli niiden havaitaan uhkaavan järjestelmän toimintaa, turvallisuutta tai käyttäjien tietosuojaa. Jos mahdollista muutosta ei pystytä tekemään ilman, että käyttäjän itse tekemät muutokset häviävät, käyttäjän tekemä vanha versio siirretään toiselle nimelle, ja käyttäjälle ilmoitetaan muutoksesta.
- tutkia, ettei yhteisillä levyalueilla ole laittomia tai järjestelmän toimintaa, turvallisuutta tai käyttäjien tietosuojaa uhkaavia tiedostoja. Tällaisia ovat esimerkiksi haittaohjelmat, tekijänoikeuksia loukkaavat tallenteet tai rikoslaissa lainvastaisiksi nimetyt aineistot.
- tuhota väliaikaistallennukseen tarkoitetuilta levyalueilta käsin tai automaattisesti tiedostoja ennalta määriteltyjen periaatteiden mukaisesti. Poistamisperiaatteet tulee olla käyttäjien nähtävissä, mutta periaatteiden mukaisista poistoista ei tarvitse ilmoittaa käyttäjälle.

4.5 Hakemistojen ja tiedostolistausten seuranta

Ylläpitäjä ei voi normaalissa ylläpidossa kokonaan välttää käyttäjien omistamien hakemistojen tiedostolistausten ottamista ja näkemistä. Hakemistorakenteiden, tiedostojen nimien, muutospäivämäärien, koon ja suojaustason sekä muiden tiedostoa koskevien tietojen käsittely on osa normaalia ylläpitoa, joka tehdään hyvää ylläpitotapaa noudattaen.

Mikäli havaitaan, että jonkin tiedoston tai hakemiston suojaukset ovat sen luonteeseen nähden liian heikot, ylläpitäjällä on oikeus muuttaa suojaus tarpeelliselle tasolle.

Ylläpitäjää koske vaitiolovelvollisuus. Ylläpitotehtävien hoidossa pyritään siihen, ettei tiedostojen yms. nimiä näytetä tarpeettomasti. Esimerkiksi kun tarvitaan tiedostolistauksia ongelmatapausten käsittelyssä, tulostetaan "private" käyttäjien niiden tiedostonimien kohdalle, jotka eivät liity käsittelyssä olevaan asiaan.

4.6 Ohjelmien ja prosessien seuranta

Ylläpitäjä määrittelee järjestelmän hallinnoijan kanssa, mitkä ohjelmistot ovat järjestelmässä käytettävissä. Ohjelmia voidaan kieltää tai poistaa käytöstä, mikäli niiden käyttö ei ole yliopiston toiminnan kannalta tarpeellista ja ne ovat uhka palvelutasolle tai turvallisuudelle. Päätöksen tekee järjestelmää hallinnoivan yksikön [ylläpitoryhmän esimies].

Ylläpitäjä seuraa tietojärjestelmissä ajettavia ohjelmia osana normaalia ylläpitoa.

Ylläpitäjä saa muuttaa suorituksessa olevan prosessin suorituksprioriteettia, mikäli se kuluttaa järjestelmän resursseja kohtuuttomasti.

Ylläpitäjä saa päättää prosessin suorituksen, mikäli

- prosessin toiminta on selvästi häiriintynyt,
- prosessi haittaa muun järjestelmän toimintaa ylimääräisellä kuormituksella, eikä ole yliopiston toiminnan kannalta perusteltu, tai
- prosessi liittyy ohjelmistoon, jonka käyttö on ylläpitäjän antamien ohjeiden ja määräysten vastainen. Tällöin käyttäjälle ilmoitetaan prosessin päättämisestä ja ko. määräyksistä.

4.7 Tietoliikenneverkon seuranta

Yliopiston tietoliikenneverkon ylläpitäjä seuraa mm. verkonkuunteluohjelmilla ja lokitietojen perusteella yliopistoverkon ja ulkoyhteyksien liikennettä voidakseen taata kohtuullisen palvelutason ja turvallisuuden sekä huolehtia ulkoyhteyden kustannustehokkaasta käytöstä.

Liikennettä seurattaessa ei tarkkailla siirrettävän tiedon sisältöä, vaan liikenteen määrää ja liikennöintitapoja. Kohde- ja lähdekoneiden seuranta on tilastollista eikä kohdistu yksittäiseen käyttäjään. Liikennettä voidaan kuitenkin seurata tarkemmin myös yksittäisen järjestelmän osalta, kun selvitetään liikennöintiin liittyviä poikkeamia, esimerkiksi erityisen suuren kuormituksen aiheuttamista.

Tietoliikenneverkon ylläpitäjä voi ottaa yhteyttä suuren liikennemäärän tai muun poikkeaman aiheuttaneen koneen vastuuhenkilöön mahdollisen häiriö- tai väärinkäytöstilanteen selvittämiseksi.

Tietoliikenneverkon ylläpitäjällä on lupa estää tietoliikenneyhteydet tai tietyn palvelun käyttö koneeseen tai verkon osaan,

- joka aiheuttaa verkkoliikenteen palvelutasoa tai turvallisuutta uhkaavaa liikennettä,
- jos on perusteltua syytä epäillä, että kone tai koneita on väärissä käsissä tai haittaohjelman saastuttama,
- jossa rikotaan Tietojärjestelmien käytön sääntöjä tai
- joka ei ole erityisesti tietoturvallisuuden suhteen asianmukaisesti ylläpidetty.

Kaikissa tapauksissa koneen tai verkon osan vastuulliseen ylläpitäjään on otettava viipymättä yhteyttä liikenteen estämisen jälkeen.

4.8 Lokitietojen käsittely

Yliopiston tietojärjestelmät tallentavat lokitietoja järjestelmän toiminnan dokumentoimiseksi, mahdollisten häiriö- tai väärinkäyttötilanteiden selvittämiseksi sekä laskutustiedon keräämiseksi. Yliopistossa lokitietoja käytetään normaalisti vain vaitiolovelvollisten ylläpitäjien teknisluontoisiin tehtäviin ja laskutuksen mahdollistamiseksi. Lokitietojen käsittelyn periaatteet säännellään tarkemmin Lokitietojen käsittelysäännöissä. Lokitiedot voivat muodostaa henkilörekisterin, josta säädetään henkilötietolaissa (HetiL 523/1999), tai sisältää tunnistamistietoja, joista säädetään sähköisen viestinnän tietosuojalaissa (SVTSL 516/2004).

4.9 Tietojen säilytys

Tietojärjestelmäpalvelujen tarjoajan tulee osana ylläpitoa huolehtia järjestelmiensä varmuuskopioinnista. Varmuuskopioita tulee ottaa levyrikkojen varalta tarpeeksi usein. Kopioita tulisi ottaa ainakin muuttuneista tiedostoista päivittäin.

Varmuuskopiot tulee säilyttää asianmukaisesti ja ylläpitäjän on huolehdittava varmuuskopioiden lukukelpoisuudesta. Varmuuskopioilla olevia tietoja tulee käsitellä samoilla periaatteilla kuin vastaavia tietojärjestelmissä olevia tietoja. Varmuuskopioiden tuhoamisen tulee tapahtua siten, että niiden sisältämien tietojen luottamuksellisuus ei vaarannu.

5 Näiden sääntöjen valvonta

Näiden sääntöjen valvonnasta vastaavat yliopiston [atk-keskus]sekä muiden mahdollisten yliopiston yksiköiden tietojärjestelmien omistaja. Sääntörikkomusten käsittely tapahtuu Tietotekniikkarikkomusten seuraamuskäytännön mukaisesti. Sääntöjä päivitetään tarvittaessa tai yliopistojen yhteisen sääntösuosituksen muuttuessa. Päivitystarvetta seuraa [tietoturvapäällikkö.]

Liite 1: Ohjaava lainsäädäntö

Kaikessa ylläpidossa noudatetaan Suomen lakia. Ylläpitoa ohjaavia lakeja ovat:

- Perustuslaki (731/1999), yksityiselämän suojaa sekä sananvapautta ja julkisuutta koskevat säädökset,
- Henkilötietolaki (523/1999),
- Laki viranomaisen toiminnan julkisuudesta (621/1999),
- Asetus julkisuudesta viranomaistoiminnassa ja hyvästä tiedonhallintatavasta (1030/1999),
- Sähköisen viestinnän tietosuojalaki (516/2004),
- Laki yksityisyyden suojasta työelämässä (759/2004),
- Laki yhteistoiminnasta valtion virastoissa ja laitoksissa annetun lain (651/1988) muuttamisesta (479/2001),
- Laki tietoyhteiskuntapalveluiden tarjoamisesta (458/2002),
- Rikoslaki (39/1889),
- Pakkokeinolaki (450/1987) sekä

edellisten perusteella annetut asetukset, muut säädökset ja määräykset.

Liite 2: Salassapitositoumus

[YLIOPISTO]

SALASSAPITOSITOUMUS

Sitoudun siihen, että en [yliopiston] palveluksessa ollessani tai muuten yliopistossa tai sen toimeksiannosta toimiessani, paljasta sivulliselle asiakirjojen salassa pidettävää sisältöä enkä muutakaan tietoon saamaani seikkaa, josta lailla tai asetuksella on säädetty vaitiolo- tai salassapitovelvollisuus.

Sitoudun siihen, että en käytä väärin tehtävieni vuoksi saamiani ei-julkisia ja salassa pidettäviä tietoja ja enkä jätä niitä sivullisten nähtäville tai muuten helposti saataville.

Vaitiolo- ja salassapitovelvollisuus on voimassa myös palvelus- tai toimeksiantosuhteen päätyttyä.

Salassapidon piiriin kuuluvia tietoja ovat esimerkiksi useat henkilötiedot ja turvallisuusjärjestelyihin liittyvät tiedot sekä yhteistyökumppaneiden liike- ja ammattisalaisuudet. Sivullisia ovat myös ne [yliopistossa] tai sen yhteistyökumppaneilla työskentelevät henkilöt, jotka eivät heille määrättyjen tai sovittujen tehtävien perusteella tarvitse asiaa tietoonsa.

Palvelus- tai toimeksiantosuhteen päättyessä luovutan hallussani olevat [yliopistoa] tai sen yhteistyötahoja koskevat ei-julkista tai salassa pidettävää tietoa sisältävät asiakirjat ja tietovälineet sekä niiden mahdolliset kopiot [yliopistolle].

Olen perehtynyt minulle esitettyihin, voimassaoleviin laissa säädettyihin vaitiolovelvollisuus- ja hyväksikäyttökieltosäännöksiin, yliopiston Tietoturvapolitiikkaan ja Tietojärjestelmien ylläpitosääntöihin sekä Lokitietojen käsittelysääntöihin. Sitoudun noudattamaan kulloinkin voimassa olevia ohjeita tai määräyksiä [, jotka löytyvät MISTÄ]. Niiden rikkominen saattaa eräissä tapauksissa muodostaa rikokseksi katsottavan teon.

Päiväys

Allekirjoitus ja nimen selvennys

Jakelu kirjaamo, henkilö

LIITE 6 TIETOTURVAPOIKKEAMIIN REAGOIMINEN

TIETOTURVAPOIKKEAMIIN REAGOIMINEN

Sisällysluettelo:

1 Johdanto 1
1.1 Tietoturvapoikkeamien reagointisuunnitelman tarkoitus ja soveltamisala 1
1.2 Tietoturvapoikkeamien käsittely 2
2 Organisaatio 2
3 Reagoiminen tietoturvapoikkeamiin 3
3.1 Tietoturvapoikkeamien vakavuuden arviointi ja reagointiryhmän laajentaminen 3
3.2 Vastatoimien laajentamisessa huomioitava 5
3.3 Toimintavastuu 5
3.4 Viranomaisilmoitukset 6
3.5 Poikkeaman jälkeinen toiminta 6
3.6 Poikkeamista tiedottaminen 6
4 Ohjeen päivittäminen 6
5 Liitteet 7

Suunnittele – Kouluta – Harjoittele

1 Johdanto

1.1 Tietoturvapoikkeamien reagointisuunnitelman tarkoitus ja soveltamisala

Reagointisuunnitelman tavoitteena on, että tietoturvapoikkeamiin reagoiminen on ennakolta suunniteltua, harjoiteltua, poikkeaman vaikutukset minimoivaa ja niistä tehokkaasti palautuvaa. Tämä tapahtuu varmistamalla, että tietoturvapoikkeamat tunnistetaan yliopistossa nopeasti, niihin reagoiminen aloitetaan viipymättä ja se tehdään ennalta sovitun menettelytavan (tämä ohje) mukaisesti.

Tietoturvapoikkeama on tahallinen tai tahaton tapahtuma tai olotila, jonka seurauksena yliopiston vastuulla olevien tietojen ja palvelujen käytettävyys[1] ei ole suunnitellulla tasolla tai tietojen eheys [2] tai luottamuksellisuus [3] on vaarantunut.

---

[1] Käytettävyyttä uhkaavia tilanteita: sähkö-, LVI-, laite- ym. häiriöistä aiheutuva palvelutason lasku sovitusta tasosta kaikille käyttäjille tai palvelutasoa vaarantavat palvelunestohyökkäykset ja muut haittaohjelmistojen toiminnot.

[2] Eheyttä uhkaavia tilanteita: laitteistojen ja/tai ohjelmistojen virheellinen toiminta, haittaohjelmien toiminnan vaikutuksesta uhkaava tietojen muuttuminen tai tuhoutuminen.

[3] Luottamuksellisuutta uhkaavia tilanteita: ohjelmien ja laitteiden virhetoiminnot, ihmisten tarkoituksellinen tai vahingossa tapahtuva luvaton toiminta (hakkerointi), erilaisten haittaohjelmien toiminta ja niiden käyttäminen (esimerkiksi virus, joka lähettää koneeseen talletettuja tiedostoja tai niiden osia).

Reagointisuunnitelmaa on noudatettava kaikkien tietojärjestelmien, myös yksittäisten työasemien hallinnoinnissa.

Jokaisen yksikön tulee laatia palvelinjärjestelmäkohtaiset reagointisuunnitelmat (malli liitteessä 1), vahvistaa ne ja toimittaa tietoturvapäällikölle tiedoksi. Tämä koskee yksiköitä, joilla on omia itsenäisiä palvelinjärjestelmiä.

Jokaisen yksikön tulee myös ylläpitää luetteloa yksikkönsä työasemien ja niissä mahdollisesti käytettävien erityisohjelmistojen pääkäyttäjistä, ylläpitäjistä ja tukihenkilöistä. Nämä henkilöt toimivat työasemien tietoturvapoikkeamia seuraavina henkilöinä yksikkötasolla ja avustavat käyttäjiä työasemien seurannassa.

1.2 Tietoturvapoikkeamien käsittely

Tietoturvapoikkeamien käsittely jaetaan kolmeen vaiheeseen:

1. havainnointi
2. reagointi
3. palautuminen

1. Havainnointi: käsittää normaalin käytettävyysvalvonnan sekä tietoturvallisuusvalvonnan.

2. Reagointi: tähän toimintaan ryhdytään, jos näyttää ilmeiseltä, että sovitussa käytettävyystasossa ei pysytä tai kun on ilmeistä tai mahdollista, että tietojen eheys tai luottamuksellisuus on uhattuna. Reagoinnilla pyritään estämään tai minimoimaan poikkeaman vaikutuksia.

3. Palautuminen: seuraa reagointia ja on sen välitön jatkotoimenpide. Palautumisessa korjataan tietoturvapoikkeaman vaikutukset ja siirrytään toiminnan normaalitilaan.

2 Organisaatio

Tietoturvapoikkeaman vakavuuden ja vaikutuksien arvioinnin mukaisesti määritetään vastatoimien laajuus ja tarvittavat henkilöt kytketään toimintaan mukaan.

Reagointiryhmän kokoonpano määräytyy poikkeaman perusteella aina tapauskohtaisesti, ja sen muodostuminen on kuvattu kohdassa 3.1. Sen tehtävänä on varmistaa, että poikkeamiin reagoidaan suunnitelmien mukaan, ja että kaikissa tilanteissa on mukana riittävästi asiantuntemusta ja asianmukaiset vastuuhenkilöt.

Vähäiseksi todetussa poikkeamatilanteessa ei välttämättä tarvita koko reagointiryhmän toimintaa, vaan järjestelmän vastuuhenkilö voi reagoida poikkeamaan itse, kunhan tiedottaa poikkeamasta tietoturvapäällikölle ja reagointiryhmän jäsenille. Merkittävissä ja vakavissa tietoturvapoikkeamissa toimintaan kytketään mukaan perusryhmä sekä tapauskohtaiset tahot.

Perusryhmään kuuluvat:

- [Tietohallintopäällikkö/-johtaja] (ryhmän johtaja)
- Tietoturvapäällikkö (sihteeri, koollekutsuja, toimeenpanija, [esittelijä])
- [Tietohallinnon/atk-keskuksen turvaryhmä/CSIRT-ryhmä]
- Tapauskohtaiset ryhmän lisäjäsenet (Liite 5).

Perusryhmällä on valmiudet ja valtuudet päättää voimakkaista suojatoimista vakavissa ja yllättävissä tilanteissa. Perusryhmä on elin, jonka jäsenet saavat tiedon poikkeamista, tarjoavat tapauskohtaista asiantuntemusta ja ovat parhaiten perillä tietoturvallisuuden kokonaiskuvasta yliopistossa. Yleisimmissä käytännön tilanteissa perusryhmä arvioi suositeltavimmat vastatoimet saamiensa tietojen perusteella ja antaa ohjeet henkilölle, joka suorittaa varsinaiset toimenpiteet.

3 Reagoiminen tietoturvapoikkeamiin

3.1 Tietoturvapoikkeamien vakavuuden arviointi ja reagointiryhmän laajentaminen

Kun tietoturvapoikkeama havaitaan, tavanomaisen toiminnan tai järjestelmien vastuuhenkilöiden tulee arvioida poikkeaman ja sen suorien tai potentiaalisten vaikutusten laajuus ja välittömien reagointitoimenpiteiden lisäksi laajentaa tarvittaessa toiminta seuraavalle tasolle. Toiminnan tason laajentuessa reagointiin osallistuvien henkilöiden määrä kasvaa ja merkittävissä tilanteissa myös vastuuhenkilö vaihtuu. Mikäli poikkeama koskettaa koko yliopiston tietoturvallisuutta, lopullisen toimintavastuun täytyy myös olla keskitettyä.

On huomattava, että tiedon luottamuksellisuuden todellinen vaarantuminen on luokiteltava aina vakavaksi poikkeamaksi (esim. tietyt virustartunnat).

Huom: taulukossa tarkoitettu kriittisyys määritellään keskitetysti koko yliopiston kannalta. Yksiköiden ylläpitämien sovelluksien, ohjelmistojen, palvelimien ja palveluiden kriittisyysluokitus riippuu yksikön toiminnoista.

Normaalitila	Henkilöt	Kuvaus
Työasemat	Järjestelmien vastuuhenkilöt Käyttäjät [Lähituki] [Helpdesk]	Käyttäjät seuraavat työasemiensa toimintaa. Vastuuhenkilöt seuraavat työasemaverkon toimintaa ja varoituksia eri lähteistä.
Palvelimet, järjestelmät, palvelut	Järjestelmän vastuuhenkilö Järjestelmän pääkäyttäjä(t) [Lähituki] [Helpdesk] [Tietoturvallisuusasiantuntija]	Vastuuhenkilöt ja pääkäyttäjät seuraavat järjestelmien toimintaa ja varoituksia eri lähteistä. Käyttäjät havainnoivat järjestelmän toimintaa.

Laajentamisvastuu: järjestelmän vastuuhenkilö tai erikseen määritellyissä tilanteissa [lähituki tai helpdesk] arvioi, onko kyseessä normaalitilanne vai poikkeama, ja toimii sen mukaan. Jos kyseessä on poikkeama, toimitaan seuraavasti:

Poikkeaman laajuus ja vakavuus	Reagointiryhmän kokoonpano	Kuvaus ja toimenpiteet

Vähäinen	Järjestelmän vastuuhenkilö Järjestelmän pääkäyttäjä(t) [Lähituki] [Helpdesk] [Yksikkökohtainen tietoturva-asiantuntija] Käyttäjä (jos tarpeen)	Poikkeama, jonka vaikutus arvioidaan vähäiseksi. Esimerkiksi eristetty virustartunta, yksittäisen sovelluksen tilapäinen käyttökatkos, lyhytaikainen tietoliikennekatkos, virustorjunnan ja tietoturvapäivitysten laiminlyönti, resurssien tuhlaus jne. Kootaan reagointiryhmä. Määriteltävä vaikutukset ja vastatoimenpiteet. Informoitava tarvittaessa henkilöstöä toimenpiteistä. Informoidaan tietoturvapäällikköä, [ja/tai kirjataan tapahtuma keskitettyyn CERT-järjestelmään].

Laajentamisvastuu: järjestelmän vastuuhenkilö (sekä oman harkintansa mukaan myös [tietoturvapäällikkö]) arvioi poikkeaman vakavuuden ja tarvittaessa siirtää reagoinnin perusryhmän vastuulle. Tämä tapahtuu [kirjaamalla hälytys/poikkeamaraportti keskitettyyn CSIRT-järjestelmään toimenpiteitä varten. Hätätilanteessa voi myös soittaa tietoturvapäällikölle].

Merkittävä	Perusryhmä Järjestelmän vastuuhenkilö Järjestelmän pääkäyttäjä [Lähituki] [Helpdesk]	Poikkeama, joka vaikutus arvioidaan merkittäväksi. Esimerkiksi sovelluksen toimintahäiriö, joka ylittää tai jonka arvioidaan ylittävän sovitun sallitun käyttökatkoajan. Tällaisia ovat esim. kaikki merkittävät tietoliikennekatkot, sähköpostikatkot, kriittisten sovellusten katkot, joiden kestoaika voidaan arvioida, ja haittaohjelmien toiminta, joka häiritsee useampien työasemien/henkilöiden toimintaa tai estää sen kokonaan. Merkittävää voi olla myös, jos käyttäjän hallusta löytyy luvattomia ohjelmia tai materiaalia. Määriteltävä toimenpiteet haitan rajoittamiseksi ja poistamiseksi. Informoitava tarvittaessa henkilöstöä toimenpiteistä.

Laajentamisvastuu: perusryhmän johtaja (tietohallintopäällikkö) arvioi, onko kyseessä merkittävä vai vakava poikkeama. Äkillisissä tilanteissa myös tietoturvapäällikkö voi suoraan todeta poikkeaman vakavaksi.

Vakava	Perusryhmä Tapauskohtaiset ryhmän jäsenet Järjestelmän vastuuhenkilö [Lähituki] [Helpdesk]	Poikkeama, jonka vaikutus arvioidaan vakavaksi. Esimerkiksi kaikki kriittisten sovellusten häiriöt, jotka ylittävät tai joiden arvioidaan ylittävän sallitun käyttökatkoajan, ja joiden kestoaikaa ei ole arvioitavissa. Haittaohjelmat, jotka tuhoavat tietoja, häiritsevät suuren joukon työasemien/henkilöiden toimintaa tai estävät sen kokonaan. Kaikki tilanteet, joissa tietojen luottamuksellisuus tai eheys on uhattuna, varsinkin onnistuneet tietomurrot tai murron yritykset yliopiston sisältä. Määriteltävä toimenpiteet haitan rajoittamiseksi ja poistamiseksi. Informoitava henkilöstöä. Valmistaudutaan mahdolliseen rikostutkintaan ja muihin seurauksiin.

3.2 Vastatoimien laajentamisessa huomioitava

Tietoturvapoikkeamiin reagoitaessa on huomioitava useita vaikuttavia tekijöitä, kun harkitaan toiminnan laajentamista. Tällaisia tekijöitä ovat:

- Miten laaja poikkeama on?
- Mikä sen vaikutus toimintaan on?
- Kuinka vaikeaa on rajoittaa poikkeamaa?
- Miten nopeasti poikkeama laajenee?
- Mikä on sen arvioitu rahallinen vaikutus?
- Mikä on sen arvioitu vaikutus julkisuuskuvaan?

3.3 Toimintavastuu

Vastuu toiminnasta on kohdan 3.1. mukaisesti määritellyllä henkilöllä; normaalitilanteissa ja vähäisissä poikkeamissa järjestelmän vastuuhenkilöllä, merkittävissä ja vakavissa poikkeamissa kohdassa 2 kuvatulla perusryhmän johtajalla. Hänen tehtävänään on johtaa ja ohjata torjuntatoimia tässä ja muissa yliopiston ohjeissa määriteltyjen menettelytapojen mukaan. Toimintaa laajennettaessa vastuu siirtyy vasta silloin, kun seuraava vastuuhenkilö on ilmoittanut ottaneensa vastuun, ei vielä ilmoitushetkellä.

Reagointiin osallistuvat henkilöt ovat omalta osaltaan vastuussa siitä, että päävastuussa olevan ohjeita noudatetaan.

Kaikesta tietoturvapoikkeamaan liittyvästä toiminnasta pidetään tapahtumapäiväkirjaa, johon kirjataan toimenpiteet, ajankohdat, päätökset jne. Vastuu tapahtumapäiväkirjan pidosta on vastuuhenkilöllä, mutta jokaisen ryhmän jäsenen tulee kirjata päiväkirjaan omat toimenpiteensä.

Reagointiryhmä päättää, kuka poikkeamasta tiedottaa. Reagointiryhmän kokoonpanon muuttuessa (laajentamisen yhteydessä) myös tiedotusvastuu siirtyy vastaavasti. Tiedotus ohjeistetaan tarkemmin ohjeessa Tiedottaminen poikkeamatilanteissa.

Todistusaineisto on suojattava poikkeamissa, joista voi olla odotettavissa jälkiseurauksia.

3.4 Viranomaisilmoitukset

FUNET-CERT:lle ja CERT-FI:n organisaatioon (Viestintävirastossa) ilmoitetaan kaikista merkittävistä ja vakavista poikkeamista. Myös yliopistojen SEC-ryhmälle on hyvä lähettää ilmoitus, jos siitä voidaan arvella olevan hyötyä muille yliopistoille.

Ilmoituksen lähettää aina tietoturvapäällikkö.

Tietotekniikkarikoksen tunnusmerkistö täyttyy, kun tietojenkäsittelyrauhaa loukataan. Tietotekniikkarikokset määräytyvät rikoslain mukaisesti. Kyseessä voi olla esim. tietomurto (Rikoslaki 38:8§), tietokoneen luvaton käyttö (RL 28:7§),

vahingontekorikos (RL 35:1§) tai törkeän viestintäsalaisuuden loukkaaminen (RL 38:4§).

Jos on aihetta epäillä jotain edellä mainituista rikoksista, [tietohallinto / -johtaja / tietoturvapäällikkö] harkitsee otetaanko yhteys poliisiin. Mahdollisen varsinaisen tutkintapyynnön laatii [tietohallinto/-johtaja/tietoturvapäällikkö] ja/tai yliopiston lakimies [rehtorin/hallintojohtajan] hyväksyttäväksi.

3.5 Poikkeaman jälkeinen toiminta

Toiminnasta kohdan 3.3. mukaisesti vastuussa oleva henkilö pitää huolen, että välittömästi poikkeaman jälkeen

- Kerätään ja analysoidaan tapahtumapäiväkirjat ja muut kriisin aikana tehdyt muistiinpanot sekä tarvittaessa haastatellaan asianosaisia
- Analysoidaan tapahtumalokit niiltä osin kuin sitä ei ole tehty jo poikkeaman selvittelyn aikana
- Kirjataan keskeiset poikkeaman aikana esiintyneet vaikeudet, ongelmat, resurssipuutteet, jne.
- Tehdään yhteenveto toiminnasta, johon sisältyy arvio lopputuloksen kannalta hyvin ja huonosti sujuneista toimista. Lisäksi yhteenvetoon tulee aina kirjata ehdotukset toiminnan kehittämiseksi
- Päätetään muun kertyneen aineiston käsittelystä
- Yhteenveto toimitetaan [tietoturvapäällikölle ja kirjataan keskitettyyn CSIRT-järjestelmään].

3.6 Poikkeamista tiedottaminen

Tiedottamisen tulee olla informoivaa, ohjaavaa, ohjeistavaa ja rauhoittavaa ja sen perustarkoituksena on ylläpitää tietoisuutta tosiasioista ja toimenpiteistä. Sen tulee ehtiä väärien tietojen edelle. Kaikista toimista informoidaan ainakin niitä henkilöitä, joiden toimintaan ne vaikuttavat.

Vahinkotilanteissa tiedottamisen nopeusvaatimus korostuu. Vahinkojen ollessa laajalle ulottuvia tarvitaan tavanomaisten toimenpiteiden lisäksi valmiuksia myös syntyneen tilanteen hoitamiseksi organisaation ulkopuolella tehokkaasti ja mahdollisimman vähin vaurioin.

Poikkeamatilanteiden tiedotusta käsitellään tarkemmin ohjeessa Tiedottaminen poikkeamatilanteissa.

4 Ohjeen päivittäminen

Reagointiohjetta päivitetään tarvittaessa sekä yliopistojen yhteisen suosituksen muuttuessa. Päivitystarvetta seuraa [tietoturvapäällikkö].

5 Liitteet

[HUOM: liitteet ovat vain esimerkkejä erilaisista reagointiohjeen aihepiiriin liittyvistä asiakirjoista, ne eivät ole valmiita pohjia.]

Liite 1: Järjestelmäkohtainen suunnitelma – palvelimet/palvelut

Liite 2: Ilmoitus tietoturvallisuuteen liittyvästä havainnosta

Liite 3: Suojakeinot

Liite 4: Tapahtumapäiväkirja

Liite 5: Perusryhmän yhteystietoja

Liite 1:

Asiakirjan turvaluokitus (kun täytetty)

Turvaluokiteltu (TLL III)
LUOTTAMUKSELLINEN
JulkL (621/1999) 24.1 §:n 7 ja 8 k

JÄRJESTELMÄKOHTAINEN SUUNNITELMA

PALVELIMET/PALVELUT

YKSIKKÖ	Yksikkö	Tiedekunta	Vastuualue
Palvelimen vastuuhenkilö (omistaja)	Nimi		
	Asema		
	Toimipaikan osoite		
	Puhelin	Matkapuhelin	Sähköposti
	HUOM: Palvelimen vastuuhenkilöksi katsotaan yleensä yksikön/vastuualueen johtaja ellei toisin ole määrätty tässä tai muussa asiakirjassa.		
Palvelimen käyttö-tarkoitus			
	Seurattavat ominaisuudet, normaalitilan määritelmä		
Järjestelmän kuvaus	Palvelintyyppi Julkinen palvelin	Extranet (rajattu pääsy)	Intranet (sisäinen käyttö)
	Tarkka sijainti kulunvalvonta	Murtohälyttimet	Olosuhdevalvonta
	Laitteistokuvaus (merkki, malli, lisälaitteet)		
	Käyttöjärjestelmä ja versio		
	Ohjelmistosovellukset (versiotietoineen)		

	Alihankkijat, ulkoistetut ylläpitäjät ja/tai yhteistyökumppanit, huoltosopimukset, varalaitesopimukset			
Ylläpitoryhmä	(Luettelo on ymmärrettävä myös kiinniottolistaksi ao. järjestyksessä. Luettelossa olevat henkilöt sekä [atk-keskuksen edustaja] muodostavat järjestelmäkohtaisen reagointiryhmän.) Onko palvelimen omistaja myös pääkäyttäjä? kyllä			
Pääkäyttäjät	Nimi	Puhelin	Matkapuhelin	Sähköposti
	Nimi	Puhelin	Matkapuhelin	Sähköposti
	Nimi	Puhelin	Matkapuhelin	Sähköposti
	Nimi	Puhelin	Matkapuhelin	Sähköposti
Tiedotuksesta vastaavat	Nimi	Puhelin	Matkapuhelin	Sähköposti
	Nimi	Puhelin	Matkapuhelin	Sähköposti
	Mahdollinen tarkentava tehtäväjako			
	Onko palvelimelle/palvelulle laadittu tietojärjestelmä- tai henkilörekisteriseloste? kyllä, kopio liitteenä ei			
	Onko palvelimelle/palvelulle laadittu riskianalyysi, tärkeysluokitus ja/tai jatkuvuussuunnitelma? kyllä, kopio liitteenä ei			
	Onko palvelimella viranomaispalveluita ja/tai toiminnallisia sopimusvelvoitteita opetus- ja perustutkimustoiminnan lisäksi? kyllä, selvitys liitteenä ei			
Lisätietoja				

Käytä tarvittaessa liitteitä.

Allekirjoitus	Paikka ja päiväys Allekirjoitus

Liite 2:

ILMOITUS TIETOTURVALLISUUTEEN LIITTYVÄSTÄ POIKKEAMASTA

Millaisesta tietoturvapoikkeamasta on kyse (lyhyt kuvaus):

Mihin tietoon tai järjestelmään uhka tai vahinko kohdistuu:

Milloin ja missä vahinko on tapahtunut:

Mitä vahinkoja on aiheutunut/aiheutuu:

Esimerkiksi tietojen tai palvelujen saatavuus, tietojen luottamuksellisuus, tietojen oikeellisuus, taloudelliset vahingot tai vahinkouhkat, vakavammat vahingot.

Muu vaara, millainen:

Kuka on vastuussa tästä tiedosta tai järjestelmästä:

Keneltä saa lisätietoja yllä esitetystä havainnosta (yhteystiedot):

Muuta:

Ilmoittajan nimi:

Ilmoittamisen ajankohta:

Kenelle/keille ilmoitus toimitettiin:

Liite 3:

SUOJAKEINO (esitetään jälkeenpäin, kun tietoturvapoikkeama on korjattu ja tilanteesta on palattu normaalitilaan)

Kuinka edellä kuvattu uhka tai vahinko voidaan jatkossa estää tapahtumasta:

Suojakeinon mahdolliset kustannukset, toteuttamisen aikataulu ja tarpeelliset yhteistyökumppanit:

Millaisilla muilla keinoilla uhkaan voidaan varautua tai on jo varauduttu:

Keneltä saa lisätietoja yllä esitettyihin suojakeinoihin liittyen:

Muuta:

Liite 4:

TAPAHTUMAPÄIVÄKIRJA

Päiväys, kellonaika:	Tapahtumakuvaus siitä kuka teki ja mitä tehtiin:

Mitä opittiin tapahtumasta?

Ennakoivat ja korjaavat toimenpiteet vastaavan tilanteen välttämiseksi ja normaalitilanteen palauttamiseksi:

Jakelu:

Liite 5:

PERUSRYHMÄN YHTEYSTIETOJA

Organisaatio ja yhteystiedot:

Turvaluokiteltu (TLL IV)
VIRANOMAISKÄYTTÖ
JulkL (621/1999) 24.1 §:n 7 ja 8 k

Perusryhmä

Tietohallintopäällikkö
puh.
Tietoturvapäällikkö
puh.
Atk-keskuksen sec-ryhmä

(Huom: tietohallintopäällikön ja tietoturvapäällikön varahenkilöt on määrättävä poikkeustilanteiden varalta. Varahenkilöluettelo on salainen (TL II).)

Tapauskohtaiset ryhmän jäsenet

[Tämä luettelo voi olla hankala laatia koko yliopistoa palvelevaksi]

Lakimies
Tiedotusyksikön edustaja
Järjestelmäasiantuntija
Tietoliikenneasiantuntija
Järjestelmän kehittäjä
Tietokanta-asiantuntija
Järjestelmän omistaja
Turvallisuuspäällikkö
Valmiuspäällikkö/-ryhmä
Järjestelmäasiantuntija

Teleliikenne, viranomaisverkko
Tietoliikenne, palomuurit, yhdysliikenne
Sähköposti-, virus- ja nimipalvelut
Työasema-palvelinverkko
Järjestelmän kehittäjä
    Tilanteen mukaan
Tietokanta-asiantuntija
    Tilanteen mukaan
Järjestelmän omistaja
    Tilanteen mukaan

LIITE 7. TIEDOTTAMINEN POIKKEAMATILANTEISSA

TIEDOTTAMINEN POIKKEAMATILANTEISSA
Ohje toiminnan suunnittelemiseksi

Sisällysluettelo:

1 Tarkoitus ja soveltamisala
2 Poikkeamasta tiedottaminen
3 Viestintäkanavat
4 Toimenpiteet poikkeamatilanteen jatkuessa
5 Esimerkkejä tiedotteiden sisällön perusrungosta
6 Ohjeen päivittäminen

Tiedottamisen tulee olla informoivaa, ohjaavaa, ohjeistavaa ja rauhoittavaa ja sen perustarkoituksena on ylläpitää tietoisuutta tosiasioista ja toimenpiteistä. Sen tulee ehtiä väärien tietojen edelle. Vastuun tiedottamisesta tulee pysyä yksissä käsissä.

Kaikista toimista informoidaan ainakin niitä henkilöitä, joiden toimintaan ne vaikuttavat.

Tietoturvapoikkeama on

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

1 Tarkoitus ja soveltamisala

Tietoturvapoikkeamasta tiedottavalta taholta edellytetään nopeaa reagointia ja tavanomaista tehostetumpaa viestintää. Poikkeamatilanteet ja muu niihin reagoiminen on määritelty ohjeessa Tietoturvapoikkeamiin reagoiminen.

Poikkeamatilanteissa korostuu jatkuvasti saatavilla olevan, luotettavan ja ajantasaisen tiedon tarve. Tilanteissa käytetään niihin kulloinkin parhaiten soveltuvia viestintäkanavia.

Työnjaon ja vastuiden on oltava selkeitä, ja vastuuhenkilöiden on hallittava tilanteen kokonaisuus. Tilanteiden onnistunut hoito vaatii atk-henkilöstön ja tiedotushenkilöstön yhteistä harjoittelua ja varautumista.

Tiedottaminen poikkeamatilanteissa –ohjeen tarkoitus on määritellä viestintä- ja tiedotusvastuut ja muut viestinnässä huomioitavat asiat, esimerkiksi viestinnästä vastaavan tahon käytännön toimet poikkeamatilanteissa. Ohjeeseen tulee liittää konkreettiset, yliopistokohtaiset toimintaohjeet.

2 Poikkeamasta tiedottaminen

Poikkeamatiedottamisessa nopeusvaatimus korostuu. Poikkeaman vaikutusten ollessa vakavia ja laajalle ulottuvia tarvitaan tavanomaisten toimenpiteiden lisäksi valmiuksia myös tiedottamiseen organisaation ulkopuolelle tehokkaasti.

Ohjeessa Tietoturvapoikkeamiin reagoiminen määritellään, kuka tai millainen ryhmä poikkeamaa käsittelee ja kuka siitä tiedottaa. Tiedottava taho ilmoittaa poikkeaman laajuuden mukaisesti vaikutuksen kohteena oleville henkilöille ja yksiköille toimenpiteistä, vaikutuksista ja palautumisen tilanteesta, sekä mahdollisista jatkotoimenpiteistä. Kaikista merkittävistä tai vakavista poikkeamista informoidaan [viestintäyksikköä]. [Viestintäyksikköä] informoidaan myös aina niissä tapauksissa, joissa poikkeama näkyy toiminnassa organisaatiosta ulospäin.

Tiedotusvastuuta voidaan tarvittaessa jakaa, mutta vastuut on määriteltävä selkeästi ryhmän sisällä. Reagointiryhmä määrittelee tarvittavan työnjaon. Ainoastaan [tietoturvapäällikköllä] tai [tietohallintojohtajalla] on oikeus poikkeamatilanteissa tiedottaa [yliopiston] ulkopuolelle (tiedotteet, tiedotusvälineitten haastattelupyynnöt, yms.). Yliopiston johdolle raportoi aina Tietoturvapoikkeamiin reagoiminen –ohjeessa määritellyn perusryhmän johtaja, [tietoturvapäällikkö]tai [tietohallintojohtaja].

Poikkeamatiedotus hoidetaan käytettävissä olevia tiedotuskanavia pitkin, mutta erityisesti poikkeamasta toipumisen ajan on tiedottamisen sisällön oltava harkittua. Tiedotteiden sisällön perusrungon, sekä käytössä olevien viestintäkanavien tulee olla mahdollisimman hyvin etukäteen selvillä, jotta vältytään turhalta ja aikaa vievältä työltä poikkeamatilanteessa. Informaation yksityiskohtaisuus riippuu kunkin kohderyhmän tarpeista.

Informoitavia sisäisiä kohderyhmiä ovat mm. yliopiston johto, tietohallinto tai atk-yksikkö, ylläpitohenkilöstö, neuvonta tai helpdesk, mikrotuki, käyttäjät ja viestintäyksikkö.

Ulkoisia kohderyhmiä ovat mm. muut yliopistot, yleisö, tiedotusvälineet, alihankkijat, toiset virastot ja operaattorit. Julkisuusperiaatteen mukaisesti ei poikkeamatilanteista ole syytä jättää tiedottamatta ellei tiedottaminen vaaranna tietoturvallisuutta.

Viestinnän tulee poikkeamatilanteissa olla kaksisuuntaista; reagointiryhmä tiedottaa poikkeaman vaikutuksista kontaktihenkilön kautta yllämainituille tahoille ja saa informaatiota (virheilmoituksia jne.) käyttäjien kanssa suorassa vuorovaikutuksessa olevilta tahoilta (mm. neuvonta, helpdesk) kontaktihenkilön kautta. Kontaktihenkilönä vuorovaikutteisessa viestinnässä toimii [tietoturvapäällikkö] tai tämän nimeämä muu henkilö. Kaikkien reagointiryhmään tulevien yhteydenottojen tulee kulkea kontaktihenkilön kautta, jotta reagointiryhmälle taataan työrauha.

3 Viestintäkanavat

Yliopiston reagointiryhmälle ja [tietoturvapäällikölle] on ensiarvoisen tärkeää olla selvillä kaikista yliopistolla käytössä olevista viestintäkanavista. Selvitystyö tulee tehdä tiedotussuunnitelman käyttöönoton yhteydessä erillisenä liitteenä, jota ylläpitää [tietoturvapäällikkö] tai viestintäyksikkö. Liitteen tulee sisältää myös tärkeät puhelinnumerot ja muut yhteystiedot. Liitteen tulee olla saatavilla myös ei-sähköisessä muodossa. Mikäli selvityksessä havaitaan puutteita viestintäkanavissa, tulee tiedotusyksikön ryhtyä toimenpiteisiin uusien kanavien luomiseksi. Viestintäkanavat tulee eritellä sähköisiin ja perinteisiin kanaviin. Alla muutama esimerkki:

Perinteiset viestintäkanavat

- puhelin (neuvonta, vikapäivystys, helpdesk, soittoringit)
- puheposti / vastausautomaatti
- kirjalliset tiedotteet (viikkotiedote, yliopiston oma lehti)
- faksi
- campuksen ilmoitustaulut
- suullinen informaatio (laitosten mikrotuet, ym.)

Sähköiset viestintäkanavat

- sähköposti / sähköpostilistat
- tekstiviestit (SMS yhdyskäytävä)
- sähköiset ilmoitustaulut (esim. Intranetissä)
- sisäänkirjautumisviestit
- www-sivut (ajankohtaista, tapahtumakalenterit, jne.)
- pikaviestit (netSend, wall)
- uutisryhmät
- info-TV

Käytettävät kanavat määräytyvät poikkeaman laajuuden, sen aiheuttamien vaikutusten, sähköisten palveluiden sen hetkisen käytettävyyden sekä kohderyhmän perusteella. Tiedottamisen sisällöstä päättää aina reagointiryhmä!

4 Toimenpiteet poikkeamatilanteen jatkuessa

Poikkeaman vaikutusten ollessa selkeästi pitkäkestoisia, tulee niiden kohteena oleville henkilöille ja yksiköille antaa välittömästi vaikutusten kiertämistä tai lieventämistä koskevia ohjeita. Ohjeiden olemassaolosta tiedottamiseen käytetään samoja tiedotuskanavia kuin poikkeamatiedottamiseen.

Käyttäjien kanssa suorassa vuorovaikutuksessa toimivan tahon (helpdesk, vikapäivystys, neuvonta) tulee olla koko ajan tilanteen tasalla.

Muutoksista poikkeamatilanteessa tai tilanteeseen liittyvistä uusista tiedoista tai ohjeista tulee myös tiedottaa käyttäjille.

5 Esimerkkejä tiedotteiden sisällön perusrungosta

Mitä reagointiryhmä kertoo vikapäivystykselle, neuvonnalle tai helpdeskille

- Millaisesta poikkeamasta on kyse
- Miten poikkeama vaikuttaa; laitteistot, palvelut
- Keitä vaikutukset koskettavat
- Kuinka pitkä on poikkeamasta aiheutuvan häiriön arvioitu kestoaika
- Kuka on yhteyshenkilö / vastuuhenkilö tapauksessa
- Miten poikkeamasta aiheutuneita haittoja voidaan vähentää tai kiertää
- Mitkä ovat neuvonnalta / päivystykseltä vaaditut toimenpiteet
- Mitkä ovat loppukäyttäjiltä vaadittavat toimenpiteet

Mitä vikapäivystyksestä, neuvonnasta, helpdeskistä kerrotaan reagointiryhmän kontaktihenkilölle

- Missä järjestelmissä tai palveluissa poikkeama ilmenee
- Missä ja milloin poikkeama ilmeni ensimmäisen kerran
- Mitä tapahtui ennen poikkeaman ilmaantumista
- Miten poikkeama ilmenee
  - Tarkka virheilmoitus
  - Miten toistettavissa
  - Koskeeko kaikkia järjestelmän käyttäjiä
  - Mitä on tehty tai kokeiltu poikkeamasta aiheutuneen vian poistamiseksi
- Poikkeaman laatu, jos tunnistettavissa
- Kenelle ilmoitetaan
- Kenelle ilmoitettu
- Kuka ilmoittaa, ilmoittajan yhteystiedot

Mitä vikapäivystyksestä, neuvonnasta, helpdeskistä kerrotaan käyttäjille

- Mikä on vialla
- Miten häiriö vaikuttaa loppukäyttäjän käyttämiin palveluihin
- Keihin poikkeama vaikuttaa
- Kuinka pitkä on poikkeamasta aiheutuneen häiriön arvioitu kestoaika
- Mistä saa lisätietoja poikkeamasta aiheutuneen vian korjauksen edistymisestä
- Miten poikkeaman haittoja voidaan vähentää tai kiertää
- Mitkä ovat mahdolliset loppukäyttäjältä vaadittavat toimenpiteet

Vikapäivystyksestä, neuvonnasta tai helpdeskistä käyttäjille jaetun informaation tulee olla reagointiryhmän kontaktihenkilöltä saatua informaatiota. Ainoastaan vikapäivystys, neuvonta tai helpdesk saa tiedottaa poikkeamasta yliopiston sisällä, ellei tiedottamisesta ole annettu erillisohjetta [tietoturvapäällikön] tai [tietohallintojohtajan] toimesta. Kaikki käyttäjiltä tulevat kyselyt tulee ohjata vikapäivystykseen, neuvontaan tai helpdeskiin.

ÄLÄ ARVAILE, JOS ET TIEDÄ!

6 Ohjeen päivittäminen

Tiedottaminen poikkeamatilanteissa -ohjetta päivitetään tarvittaessa sekä yliopistojen yhteisen suosituksen muuttuessa. Päivitystarvetta seuraa [tietoturvapäällikkö] yhteistyössä [viestintäyksikön] kanssa.

LIITE 8. HÄMEEN AMMATILLISEN KORKEAKOULUTUKSEN KUNTAYHTYMÄN TIETOTURVAPOLITIIKKA

[Laadittu: 29.8.2003]

Päämäärä ja tavoitteet

Tietoturvapolitiikka määrittelee Hämeen ammatillisen korkeakoulutuksen kuntayhtymän (myöhemmin kuntayhtymä) tietoturvallisuuden tavoitteet, vastuut ja toteutuskeinot. Tietoturvallisuus on osa kuntayhtymän laatujärjestelmää.

Kuntayhtymän tietoturvallisuustyön päämäärä on turvata kuntayhtymän toiminnalle tärkeiden tietojärjestelmien ja tietoverkkojen keskeytymätön toiminta, estää tietojen ja tietojärjestelmien valtuudeton käyttö, tahaton tai tahallinen tiedon tuhoutuminen tai vääristyminen sekä minimoida aiheutuvat vahingot. Normaaliajan toiminnan tietojenkäsittelyn turvaamisen lisäksi varaudutaan toiminnan keskeyttäviin uhkatilanteisiin ja niistä toipumiseen.

Hallinnollisten, teknisten ja muiden toimenpiteiden avulla kuntayhtymän tiedot, tietojenkäsittelyjärjestelmät ja -palvelut pidetään asianmukaisesti suojattuina sekä normaali- että poikkeusoloissa.

Kuntayhtymän tavoitteena on, että tietoturvajärjestelyt ovat hyvää kansallista ja kansainvälistä tasoa. Lisäksi tavoitteena on, että tietoturvallisuuden perustaso kattaa kuntayhtymän kaiken tietojenkäsittelyn ottaen huomioon yksikköjen perusluonteen ja mahdollisen tarpeen tietoturvallisuuden tehostamiseen.

Tietoturvallisuus

Tietoturvallisuus tarkoittaa tietojenkäsittelyn turvaamista. Tietoturvallisuus rakentuu tiedon luottamuksellisuudesta, eheydestä ja käytettävyydestä sekä soveltuvilta osin pääsynvalvonnasta ja kiistämättömyydestä:

- Luottamuksellisuus tarkoittaa, että tiedot ovat sovituilla tavoilla ja sovittuun aikaan vain niiden käyttöön oikeutettujen saatavissa ja ettei tietoja paljasteta tai muutoin saateta sivullisten tietoon.
- Eheys tarkoittaa, että tiedot ja tietojärjestelmät ovat luotettavia, oikeellisia ja ajantasaisia eivätkä ole muuttuneet tai vahingoittuneet laitteisto- tai ohjelmistovikojen, luonnontapahtumien tai oikeudettoman inhimillisen toiminnan seurauksena.
- Käytettävyys tarkoittaa, että tiedot ja tietojenkäsittelyjärjestelmät ovat toiminnan kannalta hyväksyttävän ajan kuluessa käytettävissä ja käyttökelpoisia valtuutetuille käyttäjille.
- Pääsynvalvonta tarkoittaa, että tietoa tai tietojärjestelmää ei voi käyttää ilman lupaa.
- Kiistämättömyys tarkoittaa todisteiden luomista sen varmistamiseksi, ettei yksikään tietojen käsittelyn tai siirron osapuoli voi jälkikäteen kiistää osuuttaan siihen.

Tietoturvallisuustyö on tietoturvallisuuden saavuttamiseksi tehtävien toimenpiteiden suunnittelua ja toteuttamista. Toimintaan kuuluvat tietojen turvaamisen menetelmät, välineet ja toimenpiteet, työhön osoitetut resurssit sekä välineistön tietoturvaominaisuudet.

Tietoturvallisuus kattaa kaikenlaiset kuntayhtymän tietojenkäsittelytehtävät sisältäen myös toimistotyöt ja arkistoinnin. Tietoturvallisuustoimet koskevat sähköisessä, audiovisuaalisessa, suullisessa ja kirjallisessa muodossa olevan tiedon käsittelyä, siirtoa ja säilyttämistä.

Tietoturvallisuustyö on tietoturvallisuuden saavuttamiseksi tehtävien toimenpiteiden suunnittelua ja toteuttamista. Toimintaan kuuluvat tietojen turvaamisen menetelmät, välineet ja toimenpiteet, työhön osoitetut resurssit sekä välineistön tietoturvaominaisuudet. Toimenpiteiden perusteella tietoturvallisuuden osa-alueita ovat:

- Hallinnollinen turvallisuus muodostuu johdon hyväksymistä periaatteista, vastuun jaosta, tarkoitukseen varatuista resursseista ja riskien arvioinnista. Varsinaiset toimenpiteet perustuvat hallinnollisiin ohjeisiin, mutta periaatteet muodostavat pohjan kaikelle turvallisuustyölle.
- Henkilöstöturvallisuuden avulla vältetään erilaisia riskejä henkilöstön oikealla valinnalla ja koulutuksella sekä irtisanomisten yhteydessä noudatettavilla menettelytavoilla. Näitä periaatteita sovelletaan kaikkiin henkilöstöryhmiin koskien myös sijaisia ja tilapäisiä työntekijöitä.
- Fyysinen turvallisuus tarkoittaa niitä toimenpiteitä, joilla tietojenkäsittelyyn liittyviä kohteita suojellaan fyysisiltä vahingoilta ja vahingoittamisyrityksiltä. Laitteet ja tietovarastot suojataan asiaankuulumattomilta henkilöiltä ja erilaisilta palo-, vesi- ja kiinteistövahingoilta.
- Tietoliikenneturvallisuudella tarkoitetaan toimenpiteitä, joilla varmistetaan tietojen turvallisuus siirrettäessä niitä järjestelmästä toiseen joko kuntayhtymän sisällä tai kuntayhtymän ja jonkun muun organisaation välillä.
- Laitteisto- ja ohjelmistoturvallisuudella tarkoitetaan järjestelmissä olevia turvallisuusominaisuuksia, jotka on toteutettu joko tietokonelaitteistoa tai ohjelmistoa hyväksikäyttäen.
- Käyttöturvallisuudella tarkoitetaan toimenpiteitä, joilla luodaan ja ylläpidetään tietotekniikan turvallisen käytön vaatimat toimintaolosuhteet huolehtimalla tekniikan toimivuuden valvonnasta, käytön valvonnasta, ohjelmistotuesta ja varmistuksista.
- Tietoaineistoturvallisuudella tarkoitetaan tietojen ja niitä sisältävien järjestelmien tunnistusta, luokittelua ja valvontaa käsittelyn eri vaiheissa.

Kuntayhtymän tietoturvallisuuden varmentaminen tapahtuu kansallisten ja kansainvälisten tietoturvallisuutta koskevien säädösten ja suositusten pohjalta sekä valtionhallinnon tietoturvallisuudesta annettuja ohjeita ja suosituksia noudattaen.

Vastuut

Ylin vastuu tietoturvallisuudesta on kuntayhtymän hallituksella ja rehtorilla. Kuntayhtymän johtajat vastaavat tietoturvasta tulosvastuualueidensa osalta.

Tietojärjestelmäpäällikkö vastaa tietoturvallisuuden kehittämisestä kokonaisuutena, toteutuksen valvonnasta ja tietoturvatietouden edistämisestä kuntayhtymässä saamiensa resurssien ja toimintavaltuuksien puitteissa.

Tietoturvallisuuden toteuttamista kuntayhtymän yksiköissä ja niiden tietojenkäsittelyjärjestelmissä ohjaa ja valvoo kullekin yksikölle nimettävä tietoturvavastaava.

Kuntayhtymässä nimetään tietokonejärjestelmien ylläpitäjät (ylläpidon vastuuhenkilöt). Jokaiselle tietojärjestelmälle ja tarvittaessa sen osalle nimetään vastuuhenkilö.

Jokainen kuntayhtymän tietojärjestelmien tai tietoverkkojen ylläpitäjä ja käyttäjä on vastuussa tietoturvallisuuden toteuttamisesta omalta osaltaan. Kukin kuntayhtymän tietojärjestelmien ja niiden sisältämien tietojen ylläpitäjä tai omistaja vastaa tietojensa ja tietojärjestelmiensä suojaamisesta.

Kuntayhtymän tulosvastuullisten yksikköjen tulee omissa toimintasuunnitelmissaan varautua oman ympäristönsä tietoturvallisuuden toteuttamisen kustannuksiin.

Tietoturvallisuuden seuranta ja ongelmatilanteiden käsittely

Tietoturvasta vastaamaan nimetyillä henkilöillä on asianmukainen valtuutus ja velvollisuus tehdä kuntayhtymän tietojärjestelmien tietoturvallisuuden kartoituksia ja ryhtyä toimenpiteisiin havaittujen tietoturvallisuuden heikkouksien parantamiseksi.

Jokainen kuntayhtymän tietojenkäsittelyjärjestelmien käyttäjä on velvollinen noudattamaan kuntayhtymän johdon hyväksymiä käyttösääntöjä ja tietoturvaohjeita.

Käyttäjien ja ylläpitäjien tulee ilmoittaa havaitsemistaan tietoturvallisuuden puutteista, tietoturvallisuuteen liittyvistä väärinkäytöksistä tai epäilemistään tietoturvarikkomuksista yksikkönsä tietoturvavastaavalle tai tietojärjestelmäpäällikölle. Nämä reagoivat niihin erikseen määriteltävällä tavalla.

Vakavien rikkomusten varalle kuntayhtymässä nimetään erityinen ryhmä, joka päättää rikkomuksen takia vaadittavista, välittömistä toimenpiteistä.

Vakaviin tietoturvarikkomuksiin liittyvä sisäinen ja julkinen tiedottaminen hoidetaan tapauskohtaisesti Hämeen ammattikorkeakoulun kehittämisyksikön tietotekniikkayksikön kautta, joko rehtorin tai tietojärjestelmäpäällikön taikka heidän valtuuttamansa henkilön toimesta.

Tietoturvallisuuden toteuttaminen käytännössä

Tietoturvallisuuden tavoitteiden saavuttaminen on jatkuva prosessi, joka sisältää hallinnollisia, fyysisiä ja teknisiä ratkaisuja. Tietoturvapolitiikan pohjalta laaditaan kuntayhtymän tietoturvaa koskevat suunnitelmat ja käyttösäännöstö. Myös kuntayhtymän toimintayksiköissä ja eri tietojärjestelmiä koskien laaditaan tarkempia tietoturvallisuuden kehityssuunnitelmia ja menettelytapaohjeita.

Kuntayhtymän tietoturvallisuuden kehittämistarpeiden ja -tavoitteiden määrittelemiseksi kuntayhtymän tietoturvallisuusriskit kartoitetaan. Myös kartoitus on jatkuva prosessi. Kartoituksen tavoitteena on tunnistaa toimintaa vaarantavat uhat, kartoittaa tietojenkäsittelyn haavoittuvat kohdat ja arvioida menetykset uhan toteutuessa sekä arvioida tietoturvallisuuden rakentamisen kustannukset riskien vähentämiseksi. Tietoturvallisuusriskit kartoitetaan kuntayhtymän opetuksen, hallinnon sekä muiden järjestelmien ja käyttöympäristöjen tasolla. Lisäksi kartoitetaan kuntayhtymän yksiköiden erityiset tietoturvallisuusriskit.

Tietoturvallisuustason määrittämiseksi kuntayhtymän tietoaineistot ja tietojärjestelmät luokitellaan: tietoaineistot luottamuksellisuuden mukaan ja tietojärjestelmät tärkeyden mukaan. Kullekin turvallisuusluokalle määritellään tietoturvallisuustaso ja sen mukaiset tietoturvatoimenpiteet.

Järjestelmien suunnittelussa, toteuttamisessa, ylläpidossa ja käytössä noudatettavat tietoturvallisuusohjeet laaditaan kunkin järjestelmän tai käyttöympäristön tietoturvallisuuden kehittämissuunnitelmaksi ja toimitetaan ao. ryhmille. Erilaisille tietojärjestelmätyypeille ja tietoliikenneyhteyksille luodaan tietoturvallisuusstandardit, jotka määrittävät vaadittavat turvaamistoimenpiteet. Jokaisella tietojärjestelmälle tai sen osalle nimetään yksikäsitteinen vastuuhenkilö.

Henkilökunnan saatavissa on sekä www-palvelun kautta, että kirjallisessa muodossa heidän toimissaan tarvitsemansa tietoturvallisuusohjeet. Opiskelijoille tiedotetaan tietoturvallisuudesta ja heitä koskevista säännöistä ja suosituksista. Yleensäkin kuntayhtymän jäsenten tietoturvallisuustietoisuutta lisätään eri tavoin tiedottamalla ja koulutustilaisuuksia järjestämällä. Kuntayhtymän tietojenkäsittelyn ja tietojärjestelmien tietoturvallisuuden tasoa arvioidaan sisäisen tarkastuksen keinoin, tarvittaessa myös ulkoista tarkastusta käyttäen. Tietoturvallisuuden puutteet analysoidaan järjestelmien ylläpitäjien ja omistajien kanssa.

LIITE 9. HÄMEEN AMMATILLISEN KORKEAKOULUTUKSEN KUNTAYHTYMÄN TIETOTEKNIIKKAPALVELUIDEN KÄYTTÖSÄÄNNÖT

1. Yleistä

Hämeen ammatillisen korkeakoulutuksen kuntayhtymän tietohallinto pitää yllä opiskelua, opetusta, tutkimusta ja hallintoa palvelevia tietojärjestelmiä ja tietoverkkoja. Kuntayhtymän tavoitteena on tarjota asiakkailleen hyvät mahdollisuudet tietojärjestelmien ja tietoverkkojen käyttöön. Hyvien työskentelyolojen takaamiseksi jokaisen tulee noudattaa käytölle asetettuja sääntöjä.

Näitä sääntöjä sovelletaan kaikkiin Hämeen ammatillisen korkeakoulutuksen kuntayhtymän hallinnassa tai omistuksessa oleviin tietojärjestelmiin ja tietoverkkoihin. Käyttäjien osalta sääntöjä sovelletaan myös muihin järjestelmiin, joiden käyttömahdollisuus tai käyttölupa on saatu kuntayhtymältä. Näihin kuuluvat ainakin ammattikorkeakoulun internet-liittymä (Funet-liittymä), toimipisteet yhdistävä alueverkko ja sen etäyhteydet (esim. ADSL-yhteydet), toimipisteiden sisäiset tietoliikenneverkot, palvelintietokoneet, työasemat, mikrotietokoneet, päätelaitteet sekä tietoliikennelaitteet.

Käyttösäännöt löytyvät kuntayhtymän www-sivuilta (http://www.hamk.fi/tietotekniikka).
Näiden sääntöjen lisäksi voidaan antaa täydentäviä, erillisten laitteiden, ohjelmistojen ja tietoliikenneverkkojen käyttöön liittyviä ohjeita.
Näitä käyttösääntöjä vastaavia käyttösääntöjä on voimassa muissa yhteisöissä (esim. Funet-tietoverkossa), joiden osaksi kuntayhtymän tietojärjestelmät voidaan tulkita tai joihin niistä on yhteyksiä. Kyseisiä käyttösääntöjä noudatetaan myös kuntayhtymässä.

2. Käyttölupa

Tietotekniikkapalveluiden käyttö edellyttää voimassaolevaa käyttölupaa. Myönnetyt luvat ja käyttäjätunnukset ovat henkilökohtaisia eikä niitä voida siirtää edelleen toiselle henkilölle. Käyttäjä on vastuussa kaikesta oman käyttölupansa puitteissa tapahtuvasta käytöstä.

Jokaiselle henkilökuntaan kuuluvalle myönnetään käyttölupa. Kaikille niille opiskelijoille, joiden opinnot sitä edellyttävät, myönnetään käyttölupa, ellei hakijan lupaehtojen vastainen menettely tai jokin muu syy ole luvan myöntämisen esteenä. Muille lupa voidaan myöntää perustelluista syistä määräajaksi.
Käyttölupa on opiskelijoilla voimassa opintojen edellyttämän ajan ja henkilökunnalla vähintään työsuhteen keston ajan. Käyttölupa mitätöidään sen voimassaolon edellytysten päätyttyä ja samalla poistetaan kaikkia asiakkaan tunnukset, tiedostot ja sähköpostit. Työntekijä sopii esimiehensä kanssa tiedostojensa ja sähköpostiensa käsittelystä työsuhteen päättyessä.
Käyttölupa oikeuttaa käyttämään laitteita ja tietoliikenneverkkoja ainoastaan välittömästi opetukseen, opiskeluun, tutkimukseen ja

hallintoon liittyviin toimiin. Käyttö muuhun toimintaan (esim. liike- tai ansiotoimintaan) on sallittua vain kuntayhtymän myöntämällä kirjallisella luvalla.

3. Sääntöjen yleisperiaatteet

Tietotekniikkapalveluiden käyttösäännöt perustuvat seuraaviin yleisperiaatteisiin:

1.	Tietotekniikkapalvelut on tarkoitettu ainoastaan opetus-, opiskelu-, tutkimus- ja hallintokäyttöön.
2.	Tietotekniikkapalveluiden käyttö edellyttää voimassa olevaa käyttölupaa.
3.	Kaikilla käyttöluvan haltijoilla on oltava mahdollisuus asialliseen käyttöön.
4.	Tietotekniikkapalveluiden käyttäjille ei saa aiheuttaa haittaa.
5.	Käyttäjien yksityisyyden suojaa pitää kunnioittaa.
6.	Käytön on oltava lakien ja hyvien tapojen mukaista.
7.	Kuntayhtymä ei vastaa tietotekniikkapalveluiden käyttäjille mahdollisesti aiheutuneista vahingoista tai menetyksistä

Käyttösääntöjen vastaisen toiminnan johdosta tietojärjestelmien käyttölupa voidaan välittömästi poistaa vakavissa rikkomuksissa pysyvästi tai lievissä rikkomuksissa määräajaksi.

Kuntayhtymällä on oikeus muuttaa näitä sääntöjä ja muutokset astuvat voimaan välittömästi. Näihin käyttösääntöihin tehdään tarvittaessa muutoksia ja täydennyksiä.

4. Ylläpitäjien osuus

Kuntayhtymä ylläpitää tietojärjestelmiä ja huolehtii hyvien työskentelyolosuhteiden takaamisesta. Ylläpitoon nimetään toimipaikkoihin ja yhteisiin tietojärjestelmiin vastuuhenkilöt.

Ylläpitohenkilökunnalla on seuraavat oikeudet ja velvollisuudet:

1.	Antaa järjestelmien käyttöön liittyviä ohjeita.
2.	Tiedottaa järjestelmien muutoksista ja niiden vaikutuksista.
3.	Rajoittaa ja säädellä järjestelmien käyttöä hyvän palvelutason takaamiseksi.
4.	äännöllisesti varmuuskopiot kaikista käyttäjien omista tiedostoista rkeiden tietojärjestelmien tiedoista.
5.	Salassapitovelvollisuus: Mitään järjestelmän käytön seurannan tai ylläpidon yhteydessä saatuja tietoja ei saa käyttää väärin tai luovuttaa edelleen ilman tietojen omistajan lupaa.
6.	Tutkia käyttäjien tiedostoja ja sähköpostia, mikäli järjestelmän tilan selvittäminen joko häiriötilanteessa tai mahdollisten väärinkäytösten yhteydessä sitä edellyttää. Tutkiminen suoritetaan vain lain sallimissa rajoissa yksityisyyttä loukkaamatta.

Ylläpitohenkilökunnan toimintaa ohjaa tietojärjestelmien ylläpitopolitiikka.

5. Käyttäjien osuus

Kuntayhtymän tietotekniikkapalveluiden käyttäjien on noudatettava käyttösääntöjä, jotta palvelut toimivat hyvin ja palveluiden ylläpito sujuu suunnitellulla tavalla. Näitä sääntöjä sovelletaan myös tuleviin tietotekniikkapalveluihin.

Sähköpostin käyttöä ohjaa lisäksi kuntayhtymän sähköpostin käyttöpolitiikka.

Käyttäjän pitää noudattaa seuraavia ohjeita:

1.	Käyttää aina omaa henkilökohtaista käyttäjätunnustaan.
2.	Vaihtaa salasanansa riittävän usein ja säilyttää sen niin, ettei se joudu muiden tietoon. Salasana ei saa olla helposti arvattavissa. Jokainen on vastuussa omalla käyttäjätunnuksella tapahtuvasta tietotekniikkapalveluiden käytöstä.
3.	Ottaa huomioon muut tietotekniikkapalveluiden käyttäjät.
4.	Ilmoittaa kuntayhtymän tietotekniikkahenkilöstölle havaitsemistaan tai aiheuttamistaan laitteistojen tai ohjelmistojen virhetoiminnoista ja turvallisuusaukoista.
5.	Seurata ja noudattaa tietotekniikkapalveluiden käytöstä annettuja ohjeita. Ohjeita julkaistaan kuntayhtymän www-sivuilla ja ilmoitustauluilla.

6. Käytön rajoitukset

Kuntayhtymän tietotekniikkapalveluiden käyttösääntöjen tarkoituksena on taata, että palvelut toimivat hyvin ja palveluiden ylläpito sujuu suunnitellulla tavalla. Säännöt sisältävät seuraavia rajoituksia ja kieltoja:

1.	Ilman voimassaolevaa henkilökohtaista käyttölupaa ei saa käyttää eikä yrittää käyttää kuntayhtymän tietotekniikkapalveluita.
2.	Tietotekniikkapalveluiden käyttäminen toisen henkilön käyttöluvan avulla on kielletty.
3.	Oman käyttöluvan valtuuksien ylittäminen ja ylittämisen yrittäminen on kielletty.
4.	Muiden käyttäjien häiritseminen sekä heidän tietojensa luvaton tutkiminen on kielletty.
5.	Tietotekniikkapalveluiden ja tietoverkkoyhteyksien myynti kolmansille osapuolille on kielletty ilman tietojärjestelmäpäällikön lupaa.
6.	Laitteistoja tai systeemiohjelmistoja ei saa asentaa, poistaa tai muuttaa. Vain tietotekniikkahenkilöstö saa asentaa, kopioida tai poistaa ohjelmia.
7.	Laitteistoja ja tietoverkkoa ei saa käyttää muihin järjestelmiin murtautumiseksi.
8.	Turvallisuusaukkojen etsiminen ja käyttö ovat kielletty.
9.	Sähköpostia ei saa käyttää asiattomien kiertokirjeiden ja

	massapostitusten välittämiseen.
10.	Tekijänoikeudella suojatun materiaalin levittäminen (esim. kotisivujen, sähköpostin tai jako-ohjelmien avulla) ilman tekijänoikeuden haltijan lupaa on kielletty.
11.	Tietotekniikkapalveluiden käyttö liike-, ansio- tai muuhun kaupalliseen tai poliittiseen toimintaan on kielletty ilman kuntayhtymän myöntämää lupaa.
12.	Tietotekniikkapalveluita ei saa käyttää laittomaan tai hyvien tapojen vastaiseen toimintaan.

7. Laitteiden liittäminen verkkoon

Tietoverkkoon liitettävät laitteet eivät saa vaarantaa tietoturvaa tai häiritä muita tietotekniikkapalveluiden käyttäjiä. Tämän vuoksi julkisten palvelinten, langattomiin yhteyksiin liittyvien laitteiden ja etäyhteydellä tietoverkkoon kytkeytyvien laitteiden liittämiseksi kuntayhtymän alueverkkoon tarvitaan lupa. Luvan myöntää laitteesta riippuen joko toimipaikan tietoturvavastaava tai tietojärjestelmäpäällikkö.

Ainakin seuraavien laitteiden liittäminen alueverkkoon vaati luvan:

	julkisessa verkossa näkyvät palvelintietokoneet,
	kotikoneiden liittäminen etäyhteydellä (esim. adsl-liittymä) alueverkkoon,
	langattoman verkon tukiasemat ja
	muut kuin kuntayhtymän hallinnoimat tietokoneet ja langattomat laitteet.

Yllä mainittujen laitteiden tietoturvallisuudesta vastaa joko laitteen ylläpitäjä tai omistaja. Jokaisella tällaisella laitteella on oltava nimettynä tietoturvasta vastaava henkilö.

Tietoturvallisuuteen kuuluvat ainakin tietojen ja pääsyn suojaaminen sekä virustorjunnan järjestäminen. Näiden laitteiden liittäminen verkkoon ei saa avata ulkopuolisille pääsyä alueverkkoon. Laitteiden käyttöönotosta ja ylläpidosta täytyy olla olemassa asianmukainen dokumentointi, jonka perusteella voidaan varmistua tietoturvallisuudesta.

8. Www-sivut ja www-sivustot

Kuntayhtymän henkilökunta ja opiskelijat voivat laatia ja julkaista omia www-sivujaan heidän käyttöönsä osoitetuissa www-palvelintietokoneissa. Henkilökohtaiset www-sivut talletetaan yleensä omaan kotihakemistoon erillisessä ohjeessa kuvatulla tavalla.
Jokainen henkilö on itse vastuussa julkaisemastaan materiaalista ja kuntayhtymällä on oikeus poistaa www-sivuilta laiton tai muuten näiden käyttösääntöjen vastainen materiaali. Julkaistavat www-sivut

- eivät saa olla sisällöltään lain vastaisia,
- eivät saa sisältää tekijänoikeuksien vastaista materiaalia,

- eivät saa sisältää yritystoimintaa tai poliittista toimintaa edistävää materiaalia ja
- eivät saa sisältää muita henkilöitä tai yhteisöjä loukkaavaa materiaalia.

Henkilökohtaiset www-sivut poistetaan palvelimelta samalla kun henkilön käyttäjätunnus poistetaan käyttöoikeuden päättyessä.

Kuntayhtymässä toimivat yhteisöt, kuten opiskelija- ja työntekijäjärjestöt, voivat julkaista kuntayhtymän www-palvelimissa omaan toimintaansa liittyviä www-sivustoja. Heille osoitetaan jokin www-palvelin, jossa he voivat ylläpitää www-sivujaan. Palvelimessa on tarjolla tietotekniikkahenkilöstön toimiviksi ja turvallisiksi toteamat ohjelmistot.

9. Väärinkäytökset ja niiden seuraamukset

Tietotekniikkapalveluiden väärinkäytöllä tarkoitetaan näiden käyttösääntöjen kirjaimen tai hengen vastaista toimintaa. Tietotekniikkahenkilöstö valvoo näiden sääntöjen noudattamista ja tarvittaessa tulkitsee niitä. Kiistatapauksissa sääntöjen tulkitsija voi olla tietojärjestelmäpäällikkö, hänen esimiehensä tai viime kädessä rehtori. Viranhaltijan tekemästä päätöksestä voi hakea oikaisua yhtymähallitukselta.

Väärinkäytöksen seuraamuksena

- Tietotekniikkahenkilöstöllä on oikeus välittömästi estää tai rajoittaa tietotekniikkapalveluiden käyttöä.
- Käyttölupa voidaan poistaa määräajaksi (1 – 4 kk) tai ääritapauksissa pysyvästi.
- Käyttäjä voidaan velvoittaa suorittamaan vahingonkorvausta hänen väärinkäytöksellään aiheuttamistaan vahingoista.
- Teon vakavuudesta riippuen tekijälle voidaan antaa kirjallinen varoitus, opiskelija voidaan erottaa määräajaksi ja työntekijän työsuhde tai viranhaltijan virkasuhde voidaan päättää.

Mikäli väärinkäytös on lain vastainen, voidaan se antaa poliisiviranomaisen tutkittavaksi. Tällöin saattaa olla kyse tekijänoikeuslain, henkilötietolain tai rikoslain vastaisesta toiminnasta.

LIITE 10. HAMKIN TYÖNTEKIJÖIDEN KÄYTTÄJÄTUNNUSHALLINTO

1. Johdanto

Kuntayhtymän tietotekniikkapalveluiden käytössä tarvittavien käyttäjätunnusten ja eräiden ryhmien hallinta on automatisoitu. Työntekijöiden, opiskelijoiden ja kumppaneiden käyttäjätunnusten syntyminen ja poistaminen perustuu ns. auktoritäärisiin rekistereihin. Näille käyttäjäryhmille ei enää luoda manuaalisesti käyttäjätunnuksia.

Työntekijöiden käyttäjätunnushallinta perustuu henkilöstöhallintojärjestelmä Primaan, josta työsuhteiden tiedot siirretään HASI-järjestelmään, jossa niitä edelleen täydennetään.

Opiskelijoiden käyttäjätunnushallinta perustuu Winha Pro-järjestelmän tietoihin

Kumppaneiden käyttäjätunnushallinta perustuu sidosryhmärekisteriin

Jos työntekijä on myös opiskelija, niin hänellä on näitä kumpaakin roolia varten oma käyttäjätunnus.
Tässä dokumentissa esitetään työntekijöiden käyttäjätunnushallinnon pääperiaatteet sekä eri toimijoiden vastuut.

2. Työntekijöiden käyttäjätunnusten käsittely

2.1 Työntekijätunnuksen synty

Uuden työntekijän käyttäjätunnus syntyy seuraavasti:

1. Prima, henkilöstöhallinnon järjestelmä
    - Uuden työntekijän palkkaava esimies toimittaa työsuhteen tiedot henkilöstöhallintoon ***hyvissä ajoin*** ennen työsuhteen alkamista. Käytännössä tiedot tulee toimittaa henkilöstöhallintoon viimeistään kaksi viikkoa ennen työsuhteen alkamista. Myös tiedot määräaikaisen työsuhteen jatkumisesta täytyy toimittaa ajoissa henkilöstöhallintoon.
    - Henkilöstöhallinto kirjaa uuden työsuhteen tiedot Prima-järjestelmään.

2. HASI, henkilörekisteri
    - Uuden työntekijän ja työsuhteen tiedot siirtyvät HASI:iin joka yö.
    - Henkilön esimies täydentää uuden työntekijän tietoihin HASI:ssa ***ensisijaisen toimipaikan***. Työntekijän yhteystietojen päivittäminen on myös suositeltavaa.

3. Käyttäjähakemisto
    - Työntekijän käyttäjätunnus luodaan automaattisesti tarpeellisiin käyttäjähakemistoihin ja järjestelmiin (kuten sähköpostijärjestelmä) sen jälkeen, kun ***työntekijälle on HASIssa täydennetty ensisijainen toimipaikka***.
    - Atk-tukihenkilö luovuttaa tunnuksen uudelle työntekijälle varmentaen samalla hänen henkilöllisyytensä.

Huomautuksia:
1. Alkavan työsuhteen ja uuden työntekijän tiedot siirtyvät nyt HASI:in vasta, kun työsuhde alkaa. Myöhemmin HASI:in siirtyvät myös kaikki Primaan syötetyt tulevaisuudessa alkavat työsuhteet.

2. Uusille työntekijöille ei enää tehdä manuaalisesti käyttäjätunnuksia. vaan tunnusten luonti perustuu Priman ja HASI:n tietoihin. Poikkeuksena ovat työntekijöihin rinnastettavat henkilöt, joilla ei ole työsuhdetta kuntayhtymään (ks. luku 3).

2.2. Työntekijätunnuksen poisto

Työntekijän käyttäjätunnus poistetaan seuraavasti:

1. Prima, henkilöstöhallinnon järjestelmä
    - Henkilön esimies toimittaa ***välittömästi*** tiedon työsuhteen päättymisestä henkilöstöhallintoon, jos henkilö irtisanoutuu työsuhteesta. Myös määräaikaisen työsuhteen päättymisestä on hyvä ilmoittaa.
    - Henkilöstöhallinto kirjaa päättyvän työsuhteen tiedot Prima-järjestelmään.
    -
2. HASI, henkilörekisteri
    - Päättyneen työsuhteen tiedot EIVÄT enää siirry HASI:iin, joten työntekijän tiedot poistuvat HASI:sta, mutta vasta kun työsuhde päättyy.

3. Käyttäjähakemisto
    - Työntekijän käyttäjätunnus tehdään toimimattomaksi heti sen jälkeen, kun työntekijät tiedot ovat poistuneet HASI:sta, mutta sitä EI heti poisteta.
    - Poistuneen henkilön esimies ilmoittaa käyttäjätunnushallinnolle (atk-tukihenkilölle tai helpdesk-palveluun), että poistuneen henkilön kotihakemiston tiedostot ja sähköpostit on käsitelty asianmukaisesti.
    - Käyttäjätunnushallinto poistaa työntekijän käyttäjätunnuksen, kotihakemiston sekä sähköpostit.

Huomautuksia:

*1. Esimiehen on toimitettava ajoissa henkilöstöosastolle **määräaikaisen työsuhteen** jatkamiseen liittyvät tiedot, jotta kyseisen työntekijän käyttäjätunnus ei lakkaa toimimasta.*

*2. Poistuvan **työntekijän on esimiehensä määräyksestä** siirrettävä kotihakemistostaan (P-levy) tarpeelliset tiedostot/dokumentit niitä tarvitseville työntekijöille tai esimiehelle. Samoin hänen on poistettava sähköpostistaan kaikki henkilökohtaiset viestit ja sovittava työtovereidensa kanssa mitä hänen sähköpostissa jakamissaan kansioissa oleville viesteille ja dokumenteille tehdään.*

*3. Poistuneen työntekijän sähköpostilaatikon poistaminen hävittää myös kaikki hänen sähköpostissa jakamansa kansiot ja niiden sisällöt. Tämän vuoksi **jaettujen kansioiden tarkastaminen** on tehtävä ennen tunnuksen poistoa.*

*4. Poistuneen työntekijän **sähköpostit voidaan arkistoida** ennen tunnuksen poistoa, jos sähköpostit pitää säilyttää jonkin määräajan (esim. EU-hankkeen tiedot). Työntekijän esimies sopii arkistoinnista käyttäjätunnushallinnon kanssa (atk-tukihenkilö tai helpdesk-palvelu). Arkistoidut postit voidaan myöhemmin palauttaa, jos se on tarpeen.*

2.3. Työntekijän poissaolojen vaikutus käyttäjätunnukseen

Työntekijän käyttäjätunnus pysyy toimintakunnossa niin kauan kun hänellä on voimassaoleva työsuhde kuntayhtymään. Virkavapaudet, vanhempainlomat tai varusmiespalvelus eivät aiheuta käyttäjätunnuksen poistamista.

Jos työntekijän pääsyä tietotekniikkapalveluihin halutaan rajoittaa poissaolon aikana, niin esimiehen täyty sopia siitä käyttäjähallinnon kanssa (atk-tukihenkilö tai helpdesk-palvelu).

3. Työntekijään rinnastuvien henkilöiden käyttäjätunnukset

Käyttäjätunnushallinta luo työntekijöille käyttäjätunnukset vain, jos heidän tietonsa viedään henkilöstöhallinnon järjestelmään Primaan. Työpaikalla toimii kuitenkin henkilöitä, joita pitää käyttäjätunnushallinnan näkökulmasta käsitellä työntekijöinä. Tällaisia ovat mm. henkilövuokrauksen kautta tulleet työntekijät, joille kuntayhtymä ei maksa palkkaa.

Tällaisen henkilön ***esimies toimittaa käyttäjätunnuspyynnön*** käyttäjätunnushallintoon (atk-tukihenkilölle tai helpdesk-palveluun). Tunnus on aina määräaikainen ja yleensä henkilökohtainen. Esimies ilmoittaa myös mitä tietotekniikkapalveluita henkilö tarvitsee (esim. kotihakemisto, portaali ja sähköposti).

4. Kumppaneiden käyttäjätunnushallinnasta

Kuntayhtymän organisaatioyksiköillä voi olla kumppaneita, jotka tarvitsevat käyttäjätunnistusta vaativia tietotekniikkapalveluita (esim. työasemaan kirjautuminen, kotihakemisto ja portaali). Kumppani saa käyttäjätunnuksen, jos ***hänen tietonsa sidosryhmärekisterissä ovat kunnossa*** (esim. henkilötunnus ja tieto tarvittavista tietotekniikkapalveluista).

LIITE 11. MALLI TIETOSUOJAPOLITIIKAKSI

Seuraavassa on esitettynä malli tietosuojapolitiikaksi, joka on käytettävissä sellaisenaan. Organisaatio voi lisätä malliin tarpeen mukaan omia tietojaan. Dokumentin nimeäminen tietosuojapolitiikaksi ei välttämättä kuvaa dokumentin sisältöä riittävän hyvin kohderyhmälle. Siksi sille voidaan antaa nimeksi myös esimerkiksi '*kuvaus henkilötietojen käsittelystä*', '*yksityisyyden suojaaminen tietojenkäsittelyssä*' tai '*tietosuojaseloste*'.

Termi "tietosuoja" on juridinen, joten asiakirja keskittyy tietojenkäsittelyn lainmukaisuuteen. Sen ei tarvitse sisältää yksityiskohtaista tietoa. Tarpeen mukaan voidaan viitata myös tietoturvapolitiikkaan, joka voidaan jakaa lisätietoja haluaville. Asiakirja on julkinen.

Johdanto

<Organisaation nimi, esimerkiksi 'Keskussairaala Abc'> noudattaa potilaidensa ja asiakkaidensa henkilötietojen ja muiden luottamuksellisten tietojen käsittelyssä voimassa olevaa lainsäädäntöä ja hyvää, turvallista ja standardien mukaista tietojenkäsittelytapaa. Lähtökohtaisesti kaikki viranomaisen toiminta on julkista. Toisaalta laki myös edellyttää, että henkilön yksityisyydensuoja on turvattava. Tämän yksityisyydensuojan takaamiseksi kaikki <organisaation nimi> hallussa olevat henkilöä koskevat tiedot on suojattu. Niitä voidaan käsitellä ainoastaan valtuutettujen henkilöiden toimesta, luovuttaa ainoastaan henkilön itsensä suostumuksella ja niitä säilytetään ja käsitellään siten, että ulkopuolisilla ei ole mahdollisuutta päästä tietoihin käsiksi.

Tietojenkäsittelyn turvallisuus on `<organisaation nimi>` toiminnan ja palveluiden laadun kannalta erittäin tärkeää. Tietoturvallisuutta toteutetaan käyttämällä ennalta määrättyä, turvallista tietojenkäsittelytapaa a turvallisia menetelmiä ja teknologioita. Koko henkilöstö on tietoinen tietoturvallisuudesta ja sen merkityksestä, koulutettu ja ammattitaitoinen toimimaan turvallisella tavalla. Jokainen noudattaa yössään kaikkia turvallisuuteen liittyviä ohjeita ja määräyksiä. Kaikista tietojärjestelmistä on olemassa käyttöohjeet, joista käyttäjä saa tarvitsemansa tiedon järjestelmien ja niissä olevien tietojen oikeanlaisesta käytöstä. Kaikille käyttäjille järjestetään riittävä määrä tietojärjestelmien käyttökoulutusta ja turvakoulutusta. Turvallisuuteen liittyen käytössä on useita määräyksiä ja ohjeita. Yleiset tietoturvaperiaatteet on julkaistu dokumentissa *tietoturvapolitiikka*. Tietoturvallisuustyöstä ja sen lainmukaisuudesta vastaa `<toimintaa johtava elin, esimerkiksi 'keskussairaalan johtaja'>`, joka johtaa ja valvoo koko organisaation turvallisuustoimintaa ja vastaa potilasasiakirjoihin liittyvistä ohjeista, tietojenkäsittely- ja menettelytavoista toimintayksikössä. Tietoturvallisuudesta, arkaluonteisten tietojen käsittelystä ja erityisesti

potilastiedoista on säädetty useassa eri laissa, joista tässä yhteydessä oleellisimmiksi voidaan katsoa laki viranomaisen toiminnan julkisuudesta (621/1999), henkilötietolaki (523/1999), laki potilaan asemasta ja oikeuksista (785/1992) ja Sosiaali- ja terveysministeriön asetus potilasasiakirjojen laatimisesta sekä niiden ja muun hoitoon liittyvän materiaalin säilyttämisestä (99/2001).

Tietoturvatoiminnan tavoitteet ja periaatteet

Tietoturvalla ja tietoturvallisuudella tarkoitetaan tietojen, tietojärjestelmien, tiedonvälityksen ja niitä käyttävien palveluiden turvaamista ja suojaamista siten, että tietojen olemassaolo, oikeellisuus, käytettävyys, luottamuksellisuus ja palveluiden jatkuvuus eivät vaarannu. Suojaaminen sisältää erilaisia hallinnollisia ja teknisiä päätöksiä, periaatteita, menettelytapoja ja toimenpiteitä, joilla varaudutaan tietoihin kohdistuviin uhkiin ja estetään riskien toteutuminen tai vähennetään niiden vaikutuksia. Suojaamistoimet koskevat kaikkien sähköisessä, kirjallisessa tai muussa muodossa olevien tietojen käsittelyä, siirtoa ja säilytystä riippumatta siitä, onko tietoihin kohdistuva uhka tahallinen tai tahaton, esimerkiksi järjestelmän vikaantuminen, tapaturma tai luonnonkatastrofi.

Stakes, Raportteja 5/2005 Tietoturvallisuustyö on tietoturvallisuuden saavuttamiseksi tehtävien toimenpiteiden suunnittelua ja toteuttamista, jonka päämääränä on turvata <organisaation nimi> toiminnalle tärkeiden tietojärjestelmien ja tietoverkkojen oikeanlainen ja keskeytymätön toiminta, estää tietojen ja tietojärjestelmien joutuminen ulkopuolisille, estää niiden valtuudeton käyttö, tahaton tai tahallinen tietojen tuhoutuminen tai vääristyminen sekä vähentää tietoturvariskejä ja minimoida niistä aiheutuvat vahingot.

Tietosuoja on oleellinen osa tietoturvallisuutta. Sillä tarkoitetaan henkilötietojen ja muiden henkilön luottamuksellisten tai arkaluonteisten tietojen suojaamista. Lainsäädäntö suojaa henkilötietoja usein tarkemmin kuin organisaation käytössä olevia muita luottamuksellisia tietoja. Tietosuojalainsäädäntö edellyttää, että henkilötietojen käsittely on turvattava ja henkilötiedot on suojattava asiattomalta käsittelyltä.

Henkilötietojen oikeellisuus on varmistettava, ne on pidettävä salassa ulkopuolisilta, niitä ei saa tuhota tai käsitellä asiattomasti ja niiden on oltava tarpeen mukaan käytettävissä. Tietosuojalainsäädännössä säädetään lisäksi monista oikeuksista, joita henkilöllä on omiin tietoihinsa liittyen. Terveydenhuollon ammattihenkilökunnan toimintaa ohjaavat lain- ja määräysten mukaiset velvollisuudet ja oikeudet sekä näiden lisäksi

ammattietiikka, johon sisältyy vastuu hyvästä toimintatavasta ja velvollisuus tietojen salassapidosta ja vaitiolosta.

Tietojen säilytyksen ja luovutuksen periaatteet

<Organisaation nimi> voi saada haltuunsa potilasta koskevia tietoja useista lähteistä: hoitosuhteen aikana tietoja sekä saadaan potilaalta itseltään että niitä syntyy hoitotapahtuman yhteydessä. Säilytyksessä voi olla tietoja potilaan edellisistä hoitosuhteista. Niitä voi olla vastaanotettu muilta hoitoyksiköiltä tai muilta viranomaisilta. Jos tietojen suojaamiseksi näitä tietoja tarvitsee ryhmitellä erillisiksi kokonaisuuksiksi esimerkiksi säilytystä tai luovutusta varten, näin voidaan tarpeen mukaan tehdä.

Tietojen säilytyksestä on säädetty laissa, ja siitä on erikseen annettu ministeriön ohjeita. Erilaisia potilastietoja koskevat erilaiset säilytysvaatimukset. On myös erikseen säädetty, milloin vanhat tiedot täytyy poistaa. Väärien, vanhentuneiden ja virheellisten tietojen käsittely on kielletty, ja näiden oikaiseminen on tehtävä tarpeen mukaan. Tietoja voidaan luovuttaa ainoastaan potilaan nimenomaisella suostumuksella. Edellä mainitusta huolimatta voi olla olemassa tilanteita, joissa hoitohenkilökunnalla saattaa olla tietty oikeus käsitellä potilaan tietoja ilman hänen lupaansa. Näitä tilanteita voivat olla esimerkiksi potilaan tajuttomuustila vaikeassa loukkaantumisessa, potilaan vajaakykyisyys päättää itse asiasta tai oikeusviranomaisen määräämä pakkokeino. Säilytykseen ja luovutukseen liittyvien määräysten osalta voi tarkemmin tutustua edellä mainittuihin lakeihin ja asetuksiin sekä Sosiaali- ja terveysministeriön oppaaseen terveydenhuollon henkilöstölle, oppaita 2001:3: *Potilasasiakirjojen laatiminen sekä niiden ja muun hoitoon liittyvän materiaalin säilyttäminen*.

Tietojen käsittelyn ja tietojärjestelmien turvallisuus

Tietoihin ja tietojärjestelmiin pääsy on tarkoin määritelty. Henkilöillä on tietojen saantioikeus vain silloin, kun siihen on olemassa peruste. Tällainen peruste voi olla esimerkiksi hoitosuhteen olemassaolo, jolloin hoitavalla lääkärillä voi olla pääsy henkilön tietoihin, kuitenkin vain niihin, joita hoitosuhteen aikana potilaan hoidossa tarvitaan. Tietoja saa käsitellä vain siinä käyttötarkoituksessa ja laajuudessa kuin on välttämätöntä. Tämän lisäksi myönnettävät pääsyoikeudet riippuvat potilasta hoitavan henkilön roolista: esimerkiksi sairaanhoitajalla on eritasoinen pääsy tietoihin kuin lääkärillä. Potilaan mahdollinen tietojen käyttö muualla, esimerkiksi toisessa sairaalassa, on potilaan itse päätettävissä: kaikkiin tietojen luovutuksiin tarvitaan potilaan lupa.

Tietojärjestelmiä käyttävät henkilöt tunnistetaan ja todennetaan siten, että henkilön esiintyminen toisena ei ole mahdollista. Käytössä on tarvittavat käyttäjätunnus-, salasana-, toimikortti- ja PINkoodimenettelyt. Tietojärjestelmiä käytettäessä tietoihin pääsy voidaan estää siten, että henkilöllä ei ole edes mahdollisuutta nähdä tietoja, joihin hän ei ole oikeutettu. Tämä ei usein ole mahdollista esimerkiksi paperimuodossa olevien asiakirjojen osalta. Stakes, Raportteja 5/2005 Käytössä olevat tietoliikenneyhteydet ovat turvallisia, ja tietoliikenne on salattua eikä salakuuntelu ole mahdollista. Käytettävät tietojärjestelmät ja ohjelmistot ovat turvallisia, ja niiltä edellytettävät turvaominaisuudet on testattu ennen käyttöönottoa. Toimitilat, joissa tietojärjestelmiä säilytetään, on fyysisesti suojattu sekä valtuudetonta pääsyä ja murtautumista että erilaisia vikatilanteita, sähkökatkoja ja tulipaloja vastaan. Kaikkia normaalista poikkeavia tapahtumia ja tilanteita valvotaan ja seurataan, ja korjaushenkilökunta hälytetään tarvittaessa ongelmanselvitystyöhön. Kaikista väärinkäytöksistä rangaistaan.

Henkilön oikeus omiin tietoihinsa

Henkilötietolain mukaan rekisterinpitäjän on laadittava henkilörekisteristä rekisteriseloste, josta ilmenee esimerkiksi rekisterinpitäjän yhteystiedot ja rekisterin suojaus, henkilötietojen käsittelyn tarkoitus, kuvaus rekisteröityihin liittyvistä tiedoista ja se, mihin tietoja säännönmukaisesti luovutetaan. Rekisteriselosteen on oltava saatavilla. Sen saa pyydettäessä `<paikka, esimerkiksi 'vastaanotosta tai lääkäriltä'>.`

Henkilötietolain mukaan jokaisella on oikeus saada tietää, mitä häntä koskevia tietoja henkilörekisteriin on talletettu tai, ettei rekisterissä ole häntä koskevia tietoja. Tiedot voi haluttaessa tarkastaa ottamalla yhteyden `<yhteydenottopiste, esimerkiksi 'vastaanottoon tai lääkäriin'>`, jossa voi täyttää tarkastuslomakkeen, jonka perusteella rekisteröidyn tiedot tarkastetaan ja annetaan tutustuttaviksi. Jos rekisterissä oleva henkilötieto on virheellinen, tarpeeton, puutteellinen tai vanhentunut, rekisterinpitäjän on oikaistava, poistettava tai täydennettävä tieto oma-aloitteisesti tai henkilön vaatimuksesta.

`<Organisaation nimi>` johto on sitoutunut tietoturvalliseen toimintaan ja suhtautuu vakavasti kaikkeen saamaansa palautteeseen. Kaikki palaute havaituista epäkohdista voidaan antaa vastaanottoon, jossa palautteen antamista varten on erillinen lomake. Myös verkkosivut `<verkkosivun osoite, esimerkiksi 'http://www.abc.fi/palaute'>` ovat käytettävissä. Jos henkilö havaitsee epäkohtia rekisteriselosteessa tai sen saatavuudessa, tietojensa tarkastamisessa, oikeellisuudessa tai mahdollisuudessa niiden korjaamiseen, tai jos hän havaitsee tai epäilee mahdollisia tietosuojaloukkauksia, hän voi saattaa asian myös tietosuojavaltuutetun käsiteltäväksi.

LIITE 12. TIETOTURVALLIUUSPOLITIIKAN MALLI

[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 keskeytyksettömästä 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. Politiikkaa tarkennetaan tietojen käsittelyn säännöissä ja ohjeissa.

Tiedon turvaaminen on oleellinen osa yliopiston toiminnan ja palveluiden laatua, kokonaisturvallisuutta ja yliopistossa tapahtuvaa päivittäistä tietojen käsittelyä. Tietoturvallisuuden hyvä hallinta edellyttää kaiken toiminnan jatkuvaa seurantaa, 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 käytettävyydestä[1]. Yliopiston tavoitteena on turvata riittävällä ja tarkoituksenmukaisella tasolla toiminnalleen tärkeiden tietojen, tietojärjestelmien, palveluiden ja tietoverkkojen toiminta, estää niiden valtuudeton 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 seurantaa. Sillä pyritään ennalta ehkäisemään sisäisistä ja ulkoisista tietoon kohdistuvista uhkista aiheutuvat vahingot tai rajoittamaan ne hyväksyttävälle tasolle sekä varautumaan poikkeamatilanteista toipumiseen. Normaaliajan 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 suosituksia[2].

2 Tietoturvan organisointi ja vastuut

Tässä luvussa kuvataan keskeisimmät tietoturvallisuuteen liittyvät toimijat yliopistossa sekä heidän vastuunsa ja velvollisuutensa. Tarkempi vastuiden erittely kerrotaan tietoturvapolitiikan 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 ohjeita[3].*
- *Tietoturvapolitiikasta 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 voimassaolevien 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 tulosohjausta.*

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.

käyttösäännöillä 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.

Tietoturvapolitiikan ja riskikartoituksien 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 tietoturvallisuusohjeet. Opiskelijoille tiedotetaan tietoturvallisuudesta ja heitä koskevista säännöistä ja suosituksista. Yleensäkin yliopistoyhteisön jäsenten tietoturvallisuustietoisuutta lisätään tiedottein ja kirjoituksin eri tiedotuskanavissa sekä järjestämällä koulutustilaisuuksia. [Yliopiston tietojenkäsittelyn ja tietojärjestelmien tietoturvallisuuden tasoa arvioidaan sisäisen tarkastuksen keinoin, tarvittaessa myös ulkoista tarkastusta käyttäen. Tietoturvallisuuden puutteet analysoidaan järjestelmien ylläpitäjien ja omistajien kanssa.]

4 Tiedottaminen

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

Yliopiston tietoturvallisuuteen liittyvästä tiedottamisesta yliopiston ulkopuolelle ja yliopiston sisällä yleisellä tasolla vastaa ja huolehtii yliopiston tietoturvapäällikkö tietoturvasuunnitelman mukaisesti. Yksiköiden sisäiseen tiedottamiseen osallistuvat myös yksiköille nimetyt vastuuhenkilöt.

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

5 Tietoturvallisuuden seuranta ja ongelmatilanteiden käsittely

Tietoturvallisuuden ylläpito edellyttää jatkuvaa seurantaa, johon kuuluvat tietoturvallisuuden valvonta sekä sen tason ja poikkeamien raportointi. Seurantaa toteutetaan sekä automaattisesti teknisin keinoin että henkilöiden toimesta mm. osana esimiesvastuuta. Teknisestä seurannasta on erilliset ohjeensa. [Tietoturvapäällikkö] koordinoi tietoturvallisuuden seurantaa ja raportoi tietoturvallisuudesta yliopiston johdolle.

[Tietoturvapäälliköllä ja tietoturvallisuuden 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 tietoturvallisuuden puutteista, tietoturvallisuuteen liittyvistä väärinkäytöksistä tai epäilemistään tietoturvarikkomuksista yksikkönsä [tietoturvayhdyshenkilölle tai] johtajalle sekä tietoturvapäällikölle, 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 kuririen ja tietoaineistoja sisältävien lähetysten turvallisuuden.

Hallinnollinen tietoturvallisuus (administrative and organizational information security)

Tietoturvallisuuteen 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, tietoturvallisuus, henkilöturvallisuus, toimitilaturvallisuus ja rikosturvallisuus.

Käytettävyys (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 tietoturvallisuuden parantamiseksi.

Laitteistoturvallisuus (computer security; facilities security)

tietojenkäsittely- ja tietoliikennelaitteiden ja tilojen käytettävyyteen, toimivuuteen, kokoonpanojen määrittelyyn ja pääsynvalvontaan sekä varaosien ja tarvikkeiden saatavuuteen liittyvät toimet tietoturvallisuuden 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-, eristämis-, pääsynvalvonta- ja varmistusmenettelyt, tarkkailu- ja paljastustoimet, lokimenettelyt ja laadunvarmistus sekä ohjelmistojen ylläpitoon ja päivitykseen liittyvät toimet tietoturvallisuuden parantamiseksi.

Perusturvallisuus (baseline security):
Vähimmäistoimenpiteet, 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 luokittelemisen 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) tavoitetila, jossa tietoturvallisuus on toteutettu tietoliikenteen laitteiden, järjestelmien ja niissä kulkevien tietojen osalta
2) lainsäädäntö, normit ja toimet, joilla pyritään aikaansaamaan tietoliikenteen turvallisuus.
Tietoliikenneturvallisuuteen tähtääviä keinoja ovat mm. laitteistojen ja siirtoyhteyksien ylläpito ja niiden kokoonpanojen hallinta, verkonhallinta, pääsynvalvonta, tietoliikenteen käytön valvonta ja tarkkailu, ongelmatilanteiden kirjaaminen ja selvittäminen, viestinnän salaus ja varmistaminen sekä tietoliikenneohjelmien testaus ja hyväksyminen.

Tietotekniikan turvallisuus (IT security):
organisaation tietotekniikkaan kuten tietoliikenteeseen, laitteistoihin, ohjelmistoihin ja niiden käyttöön liittyvä tietoturvallisuus.

Tietoturvallisuus (information security):
1) tavoitetila, jossa tiedot, tietojärjestelmät ja palvelut saavat asianmukaista suojaa 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 tietoturvallisuus
(1) niin normaali- kuin poikkeusoloissa.
Tietoturvallisuuden toteuttamisessa on tapana erottaa kahdeksan toimenpidealuetta: hallinnollinen, henkilöstö-, fyysinen, tietoliikenne-, laitteisto-, ohjelmisto-, tietoaineisto- ja käyttöturvallisuus.

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 tietoturvallisuuden kehittämistoimintaa tai sitä suorittavia organisaatioita.

Tietoturvaohjeisto (information security manual):
Yliopiston yhteinen, yksiköiden sisäinen ja palvelu- tai järjestelmäkohtainen ohjeistus tietojenkäsittelyn turvaamiseksi.

Tietoturvapolitiikka (information security policy) :
Sama kuin tietoturvastrategia (information security strategy).
Tietoturvalinjaukset, tietoturvaperiaatteet.
Organisaation tasolla johdon hyväksymä näkemys tietoturvallisuuden päämääristä, periaatteista ja toteutuksesta.

Tietoturvasuunnitelma (information security plan):
perusturvallisuuden toteutusta ja ylläpitoa normaalioloissa koskeva suunnitelma.
Suunnitelmassa esitetään organisaation tietoturvallisuustoiminnan 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, perusturvallisuuden 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 säädeltyjä 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 tulosohjaus, 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 laitetilojen 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 asioinnin tietoturvallisuuden yleisohje, VAHTI 4/2001
- Salauskäytäntöjä koskeva valtionhallinnon tietoturvallisuussuositus, VAHTI 3/2001
- Valtionhallinnon lähiverkkojen tietoturvallisuussuositus, VAHTI 2/2001
- Valtion viranomaisen tietoturvallisuustyön yleisohje, VAHTI 1/2001
- Valtionhallinnon tietojärjestelmäkehityksen tietoturvallisuussuositus, VAHTI 3/2000
- Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohje, VAHTI 2/2000
- Tietojärjestelmäselosteen laadintasuositus, VM 17.2.2000
- Salassa pidettävien tietojen ja asiakirjojen turvaluokittelu- ja merkintäohje, VM 19.1.2000
- Valtion tietohallintotoimintojen ulkoistamisen tietoturvallisuussuositus, 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 tietoturvallisuuteen liittyvät säännöt ja ohjeet

- Tietoturvapolitiikka (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).

- Tietoturvapoikkeamiin reagoiminen (ohje)
- Tiedottaminen poikkeamatilanteissa (ohje)
- Todistusaineiston suojausohje.

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

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

Rehtorin kolmivuotiskausiksi asettama tietoturvallisuuden johtoryhmä valmistelee ja ohjaa yliopiston tietoturvallisuuden 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 valmistelee 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 tietoturvallisuusnäkemyksiä

- huolehtia henkilöstön turvallisuustietoisuuden lisäämisestä ja tietoturvallisuuskoulutuksen suunnittelusta
- huolehtia tietoturvallisuuden toteutumisesta ostetuissa atk-palveluissa ja
- raportoida ylimmälle johdolle tietoturvallisuudesta
- tehdä rehtorille, hallintokeskukselle ja tietokonekeskuksen johtokunnalle yliopiston tietoturvallisuutta koskevia ehdotuksia ja aloitteita sekä hallintokeskukselle tietoturvasuunnitelman edellyttämiä määrärahaesityksiä.

Tietoturvapäällikön tehtävänä on:

- valmistella tietoturvallisuuden kehittämishankkeita yhdessä tietoturvallisuuden johtoryhmän kanssa
- vastata tietoturvallisuuden kehittämishankkeiden toteutuksesta
- vastata tietoturvallisuuskoulutuksen järjestämisestä
- tiedottaa tietoturvallisuusasioista ja -ongelmista
- osallistua turvallisuusperiaatteiden määrittelyyn
- avustaa johtoa ja yksiköitä tietoturvallisuuden toimeenpanossa
- kehittää ehdotuksin tietoturvallisuutta
- järjestää tietoturvallisuutta koskeva seuranta
- raportoida ylimmälle johdolle tietoturvallisuudesta
- toimia tietoturvallisuuden johtoryhmän sihteerinä
- tehdä muut tietoturvallisuuden johtoryhmän hänelle antamat tehtävät.

Tietokonekeskuksen tehtävänä on:

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

Laitoksen / muun yksikön johtajan tehtävänä on:

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

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

- soveltaa ja toteuttaa yliopiston tietoturvallisuusperiaatteita omaa erikoisasiantuntemusta hyödyntäen
- vastata tietoturvallisuustoimenpiteistä omalla alueellaan
- noudattaa hyvää tietoturvallisuustapaa ja
- raportoida tietoturvallisuudesta ja siihen kohdistuvista häiriöistä.

Tietopalveluista ja asiakirjahallinnosta vastaavien tehtävänä on:

- toimeenpanna tietoturvallisuus tietopalveluissa ja asiakirjahallinnossa hyvän tiedonhallintatavan ja tietoturvallisuustavan 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 tietoturvallisuutta tietojärjestelmässä ja
- raportoida tietoturvallisuudesta 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 tietoturvallisuuden kannalta
- varautua poikkeaviin tapahtumiin ja niiden vaatimiin vastatoimenpiteisiin ja
- raportoida turvallisuutta vaarantavista tapahtumista ja häiriöistä.

Yksiköiden atk-yhdyshenkilöiden ja tietoturvavastaavien tehtävänä on:

- ylläpitää ja valvoa vastuullaan olevien järjestelmien tietoturvallisuutta yliopiston tietoturvallisuuden yleisohjeistuksen mukaisesti ja
- raportoida tietoturvallisuudesta ja siihen vaikuttavista tekijöistä

Loppukäyttäjien tehtävänä on:

- tuntea tietoturvallisuudesta annetut ohjeet ja noudattaa niitä
- osallistua heille suunnattuun tietoturvakoulutukseen sekä
- raportoida havaitsemistaan ongelmista, uhkista ja ohjeiden vastaisista menettelyistä.

Konsulttien ja palveluyritysten tehtävänä on:

- noudattaa hyvää tietojenkäsittely- ja tietoturvallisuustapaa
- ylläpitää ja valvoa yliopistoon liittyvässä toiminnassaan valtionhallinnon tietoturvallisuuden yleisohjeistuksen mukaista ja ohjeistettua tietoturvallisuutta sekä
- raportoida tietoturvallisuudesta ja siihen vaikuttavista tekijöistä.

Tietoturvallisuusvastuita on myös muilla keskeisillä henkilöryhmillä kuten

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

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

]