TURUN AMMATTIKORKEAKOULU
ÅBO YRKESHÖGSKOLA

Veli Nietula

Yrityksen tietoturvakartoitus

Opinnäytetyö

Tietoliikenteen koulutusohjelma

Lokakuu 2011

TURUN AMMATTIKORKEAKOULU

TIIVISTELMÄ

Bioalat ja liiketalous	
Koulutusohjelma Tietojenkäsittelyn koulutusohjelma	
Tekijä(t) Veli Nietula	
Työn nimi Yrityksen tietoturvakartoitus	
Suuntautumisvaihtoehto Tietoliikenne	Ohjaaja Esko Vainikka
Aika Lokakuu 2011	Sivumäärä 43

Opinnäytetyössä tutkitaan tietoturvakartoituksen tekemistä yritykselle. Tietoturvakartoituksen tarkoituksena on selvittää yrityksen tämän hetkinen tietoturvan taso, havaita siinä mahdollisesti olevat puutteet sekä tehdä korjausehdotukset saatujen tietojen pohjalta.

Työn teoriaosuudessa on selvitetty ja esitelty tietoturvan osa-alueet sekä periaatteet. Myös yksityisyyden suojaa on käsitelty lakien osalta. Teoriaosuus on pyritty tekemään niin, että se mahdollisimman selkeästi tuo esiin asiat, jotka kuuluvat tietoturvaan.

Tietoturvakartoituksen pohjana on käytetty kansainvälisesti tunnettua kyselyä, joka on muokattu opinnäytetyötä varten sopivaksi. Muokattu kysely on annettu eteenpäin yrityksen tietoturvasta vastaavalle henkilölle täytettäväksi. Vastausten perusteella on tehty supistettu tietoturvakartoitus yritykselle.

Työn tavoitteena on tehdä yritykselle raportti, josta selviää yrityksen tietoturvan tämän hetken tilanne. Lisäksi tarkoituksena on parantaa yrityksen tietoturvan tasoa.

Luottamuksellinen: osittain
Hakusanat: tietoturva, tietoturvakartoitus, tietoturvan osa-alueet
Säilytys: Turun ammattikorkeakoulun kirjasto, Lemminkäisenkatu

TURKU UNIVERSITY OF APPLIED SCIENCES

ABSTRACT

Life Sciences and Business	
Degree programme Business Information Technology	
Author(s) Veli Nietula	
Title Information Security Survey for a Business	
Specialization line Data Communications	Instructor Esko Vainikka
Date October 2011	Total number of pages 43

This thesis examines creating an information security survey for a business. The main purpose of the survey was to examine the organizations current information security level, find out the possible weaknesses and to make correction proposals based on the results of survey.

In the theory section of the thesis, the reader is introduced to information security basics and sections. All of the eight different sections are explained and opened to the reader. Privacy policy concerning Finnish laws is also presented.

The survey is based on an internationally known inquiry which was modified to fit this thesis. The modified inquiry was filled in by the organization's information security person. An information security report was generated based on the answers.

The results of the information security survey reveal, that the organization's information security is on a good level. There are some minor points where the organization can still improve their information security.

Confidentiality status: partly

Keywords: information security, information security survey, information security sectors

Deposit at: Turku University of Applied Sciences Library, Lemminkäisenkatu

SISÄLTÖ

1 JOHDANTO

Tänä päivänä tieturvasta huolehtiminen on jokaisen yrityksen toiminnan edellytys. Toimiva tietoturva takaa yrityksen luotettavan toiminnan ja se on edellytys liiketoiminnan jatkumiselle. Tämän tutkimuksen aiheena on tietoturvakartoituksen tekeminen yritykselle. Tutkimuksen toimeksiannon sain Jimm's PC-Store Oy:ltä, jossa olen työskennellyt vuodesta 2007. Osa opinnäytetyöstä tulee olemaan salattu, koska opinnäytetyö sisältää yrityksen liiketoiminnan kannalta luottamuksellista informaatiota.

Tutkimuksen tavoitteena on ensisijaisesti saada lopputuloksena yritykselle kattava tietoturvaraportti, josta selviää yrityksen tämän hetkinen tietoturvan taso. Koska aihe on valtavan laaja, raportissa käydään läpi yleisesti kaikki tietoturvan osa-alueet lisättynä muutamilla tarkentavilla kohdilla. Muina tavoitteina tutkimuksessa pidän oman henkilökohtaisen tietoturvaosaamisen kasvattamista sekä ammattitaidon lisääntymistä alalla.

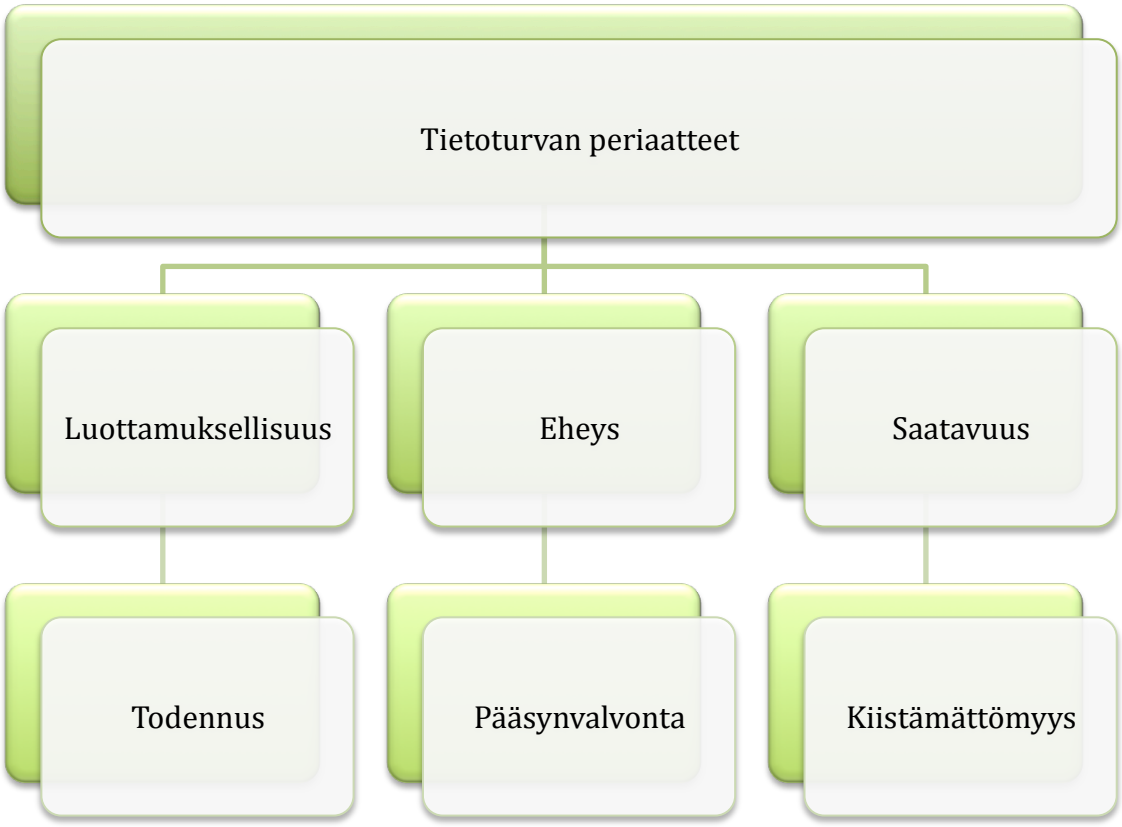
Tietoturvakartoituksella pyritään ennalta havaitsemaan yrityksessä olevia tietoturvariskejä. Tietoturvakartoituksen tarkoituksena on havaita yrityksen tietoturvassa olevat haavoittuvuudet ja esittää niihin parannuksia kartoituksen pohjalta. Santa Fe Groupin Standardized Information Gatherin (SIG) version 5.0 kyselyn **(**Shared Assessments 2011 [viitattu 25.8.2011]**)** (liite 1) pohjalta tein Jimm's PC-Store Oy:lle kyselyn liittyen yrityksen tietoturvaan. Kyselyn vastausten pohjalta on kirjoitettu yritykselle supistettu tietoturvakartoitus (liite 4), joka on salattu.

Opinnäytetyön teoriaosuudessa selvitetään asiat, joista tietoturva koostuu sekä sen periaatteet. Tutkimuksen aihe on ajankohtainen toimeksiantajalle sekä muussa työelämässä. Aiheen laajuus tuo haasteen tutkimuksen tekemiselle, koska tietoturva käsitteenä on valtavan laaja. Tutkimuksessa aiheen rajaaminen opinnäytetyötä varten on jo suuri tehtävä. Lähteinä käytetään sähköisiä materiaaleja, suomalaista kirjallisuutta sekä sertifikaatteja. Tietoturvakartoituksessa käytettävä kysely on käytännöllinen ja monipuolinen sekä se on helposti muokattavissa erilaiseen käyttöön. Kyselyä päivitetään säännöllisesti vastaamaan nykypäivän tarpeita. Kyselyn monipuolisuus ja muokattavuus tekee siitä käyttökelpoisen jokaisen yrityksen käyttöön.

Opinnäytetyö tehdään Jimm’s PC-Store Oy:lle, joka on toiminut tietotekniikan alalla vuodesta 2001. Yritys on asiantunteva tietotekniikan, komponenttien ja viihde-elektroniikan verkkokauppa, jolla on uutuudet ensimmäisenä. Yrityksen toimipiste sijaitsee Turussa ja sen palveluksessa on tällä hetkellä noin 40 henkilöä. Yrityksellä on myös verkkokaupan lisäksi noutopalvelumyymälä Turussa. Opinnäytetyöstä on ajankohtaista hyötyä yritykselle, koska se saa näin tilannekartoituksen tämänhetkisestä tietoturvan tilastaan.

2 TIETOTURVAN PERIAATTEET

Tietoturvan periaatteet jaetaan perinteisesti kolmeen osa-alueeseen, joihin toiminnalla pyritään: tiedon luottamuksellisuus (confidentiality), eheys (integrity) ja saatavuus (availability). Näiden lisäksi tietoturva edellyttää kolmen muun periaatteen toteutumista, jotka ovat todentaminen (authentication), pääsynvalvonta (access control) ja kiistämättömyys (non-repudiation). (Järvinen 2002, 22-28.) Tietoturvan tavoitteena on osa-alueiden ja niiden periaatteiden turvaaminen esimerkiksi laitteisto- ja ohjelmistovikojen aiheuttamilta uhilta ja vahingoilta.



Kuvio 1. Tietoturvan periaatteet.

2.1 Luottamuksellisuus ja todennus

Luottamuksellisuudella tarkoitetaan, että henkilöille jaetaan tietyt oikeudet järjestelmään. Tietoja pääsevät lukemaan ja muokkaamaan vain henkilöt, joilla on ennalta

annettu oikeudet niihin. (Järvinen 2002, 22.) Tiedon luottamuksellisuus voidaan yrityksen sisällä jakaa neljään luokkaan, jotka ovat julkinen, sisäinen, luottamuksellinen ja salainen. Liitteessä 2 oleva taulukko havainnollistaa esimerkkiä tietojen luokittelusta. (Laaksonen, Nevasalo & Tomula 2006, 157.)

Luottamuksellisuus vaarantuu välittömästi mikäli tietoja pääsee käsittelemään henkilö, jolla ei siihen ole oikeuksia. Tiedot saattavat joutua myös vääriin käsiin mikäli tietoverkkoon päästään sisälle murtautumalla. Tämän takia tietoverkot on suojattava asianmukaisesti. Luottamuksellisuus korostuu erityisesti käsiteltäessä arkaluontoista tietoa, esimerkiksi henkilörekisteriä tai yrityksen taloudellisia asioita. (Miettinen 1999, 25.)

Jotta tietoihin pääsevät käsiksi vain ne henkilöt, joilla siihen on oikeus, pitää heidät ensin todentaa. Tiedon muilta suojaamista varten tarvitaan salausta (encryption). Tiedon todentamista tapahtuu koko ajan. Esimerkiksi, kun vastaamme tulee tuttu henkilö todennamme hänet ulkonäön perusteella. Tietojärjestelmässä todennusmenetelmänä on käyttäjän todentaminen. Käyttäjällä on salasana, jonka avulla hän todentaa olevansa oikeutettu käyttämään tietoa.

Todentamista varten on kolme mahdollisuutta, jotka ovat

- Yksilölliset ominaisuudet
- Esine
- Tieto.

Yksilöllisen ominaisuuden perusteella voidaan tunnistaa vain elävät henkilöt. Yksilöllisiä ominaisuuksia ovat esimerkiksi käsiala, ääni tai ulkonäkö. Ihmisen ominaisuuksia kuten sormenjälkeä tai verkkokalvon tunnistusta voidaan myös käyttää teknisesti todentamiseen. Tällöin kyseessä on biometrinen tunnistus.

Pelkästään esineen käyttäminen todentamisessa on heikko tapa. Esineitä pystytään helposti väärentämään. Käytettäessä esinettä todennuksessa sitä kannattaa tehostaa käyttämällä vielä muuta tietoa.

Tiedolla todennuksessa tarkoitetaan tietoa, joka pitäisi olla ainoastaan käyttäjällä tiedossa. Tällaisia asioita ovat esimerkiksi salasana ja pankkikortin PIN-koodi. (Järvinen 2002, 24-27.)

2.2 Eheys ja pääsynvalvonta

Tiedon eheydellä tarkoitetaan, että tietoja ei pääse luvatta muokkaamaan tai että niitä ei synny tai häviä itsestään. Tietojärjestelmään murtautumalla pystytään aiheuttamaan eheyden menetys. Lisäksi virukset rikkovat tiedostojen eheyden tarttuessaan niihin. Tiedon eheys saatetaan menettää myös tahattomasti esimerkiksi kiintolevylle tulleen vian vuoksi.

Tiedon eheyden kannalta on tärkeää ottaa varmuuskopioita tiedoista, jotka ovat yritykselle tärkeitä. Tiedostossa oleva eheytysvika saattaa olla todella hankala, koska jos vikaa ei huomata tarpeeksi ajoissa saattaa automaattisen varmuuskopioinnin yhteydessä vioittunut tiedosto siirtyä itse varmuuskopioksi. Tällaisessa tapauksessa tiedon saa palautettua vain mikäli on tallessa tarpeeksi vanha tiedosto, joka on vielä ehjä. (Järvinen 2002, 22-23.)

Pääsynvalvonta pitää huolta siitä, että sisälle järjestelmään pääsevät ainoastaan henkilöt, jotka ovat todennettuja. Siihen liittyvät myös käytön seuranta ja lokitiedostot. Lokitiedostoihin tallentuu tieto käyttäjistä, jotka ovat avanneet ja muokanneet tiedostoa. Lokitiedostoista on suurta hyötyä tutkittaessa tahallisesti tai tahattomasti tapahtunutta tietoturvarikkomusta. (Järvinen 2002, 27.)

Pääsynvalvonnalla pyritään estämään luvatonta käyttöä, joka saattaa altistaa tietojärjestelmän haittaohjelmien leviämiseen. Tämä taas johtaa eheyden ja luottamuksellisuuden menetykseen. Erityisesti langattomien verkkojen pääsynvalvontaan on syytä kiinnittää enemmän huomiota. (Hakala, Vainio & Vuorinen 2006, 6.)

2.3 Saatavuus ja kiistämättömyys

Tietojärjestelmien toimivuus liittyy olennaisesti tiedon saatavuuteen. Mikäli verkkoyhteydet tai tietokoneet eivät toimi, kun tietoa tarvitsee käsitellä, on tiedon saatavuus menetetty. Tiedon saatavuuden turvaamiseksi käytettäviä tekniikoita ovat esimerkiksi UPS -laitteet sähkökatkoksien varalta sekä varmuuskopiointi. (Järvinen 2002, 24.)

Tiedon saatavuus voidaan menettää kahdella tavalla; joko tahallisen toiminnan vuoksi tai tahattomasti. Saatavuutta voidaan tahallisesti häiritä esimerkiksi tukkimalla yrityksen tietoverkko ylimääräisellä liikenteellä. (Miettinen 1999, 28.) Tällaista tekoa kutsutaan palvelunestohyökkäykseksi. Verkon kaatuminen tai jonkin aktiivilaitteen hetkellinen vikaantuminen aiheuttaa hetkellisesti saatavuuden menetyksen.

Kiistämättömyydellä tarkoitetaan, että esimerkiksi kaupankäynnissä voidaan myöhemmin sitovasti todistaa ostotapahtumaan kuuluvat vaiheet. Tyypilliset vaiheet ostotapahtumassa ovat tilauksen tekeminen, tilauksen vastaanotto ja tuotteen toimittaminen. (Järvinen 2002, 28.) Verkkokaupan myötä kiistämättömyyden tarve tulee vastaan erityisesti. Myyjän tulee pystyä todistamaan, että asiakas on tehnyt tilauksen ja se on käsitelty ja toimitettu asiakkaalle.

3 TIETOTURVA

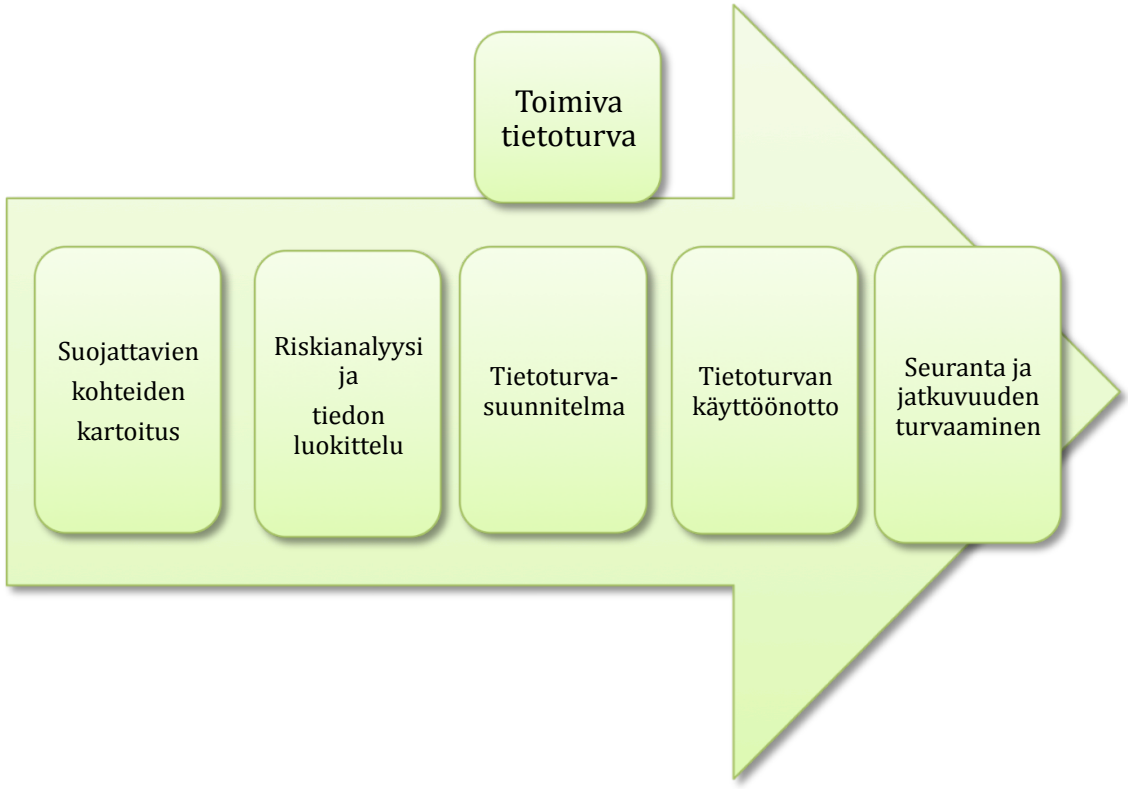
Yleisesti

Tietoturvasta puhuttaessa se yleensä mielletään tietokoneen virustentorjunnaksi ja palomuuriksi. Nämä molemmat liittyvät tietoturvaan, mutta ovat vain sen pieniä osia. Käytännössä tietoturva kattaa kaiken sen, mikä liittyy tietojen saatavuuden, oikeellisuuden ja luottamuksellisuuden säilyttämiseen. (Järvinen 2002.)

Tietoturvallisuudella tarkoitetaan tietojen ja niitä tukevien järjestelmien sekä tietoliikenteen suojaamista. Lisäksi tietoturvallisuuden tarkoituksena on varmistaa kyseisiin

asioihin kohdistuvien riskien hallintaa teknisillä ja muilla toimenpiteillä. (Valtionvarainministeriö 2007 [viitattu 25.8.2011]).

Toimiva tietoturva tiivistettynä tarkoittaa riskien ennakointia, joidenkin tietojen suojaamista lain edellyttämällä tavalla ja sitä, että tietoturvan ylläpito on suunnitelmallista ja jatkuvaa toimintaa. Toimiva tietoturva rakentuu useasta portaasta, jota havainnollistaa kuvio 2.



Kuvio 2. Toimivan tietoturvan portaat (Yrityksen tietoturvaopas 2010 [viitattu 25.8.2011]).

Tietoturva voidaan jakaa esimerkiksi seuraaviin osa-alueisiin:

- Hallinnollinen tietoturvallisuus
- Henkilöstöturvallisuus
- Fyysinen turvallisuus eli toimitilaturvallisuus
- Tietoliikenteen turvallisuus
- Laitteistoturvallisuus
- Ohjelmistoturvallisuus

- Käyttöturvallisuus
- Tietoaineistoturvallisuus.(Viestintävirasto 2009 [viitattu 25.8.2011]).

3.1 Hallinnollinen turvallisuus

Hallinnollisella turvallisuudella tarkoitetaan tietojärjestelmän tietoturvan eri osa-alueiden johtamista. (Ruohonen 2002, 4.) Siinä tarkastellaan mm. tietoturvallisuuden toimintapolitiikkaa, johtamista, resursointia ja tietoturvallisuusasioiden hoitoon liittyviä vastuita. Hallinnollisella turvallisuudella yrityksen johto luo edellytykset tietoturvallisuusasioiden ylläpidolle sekä kehittämiselle. (Miettinen 1999, 18.)

Kuviossa 3 on esitetty eri yrityksen rooleissa työskentelevien henkilöiden vastuut.

Kuvio 3. Roolit ja vastuut (Krutz & Vines 2003, 15).

Määrätietoinen ja organisoitu toiminta on perusta tietoturvallisuuden johtamiseen. Tietoturvallisuuden johtamiseen on useita eri malleja ja standardeja, joiden tarkoituksena on tuoda määrämuotoisuutta sen hallintaan liittyvissä käytännöissä. Tietoturvallisuuden liittäminen tiiviisti yrityksen varsinaiseen liiketoimintaan on perusta toimivalle tietoturvallisuudelle. Tietoturva olisi otettava huomioon yrityksen kaikissa yksiköissä osana päivittäistä johtamista ja saatava osaksi jokaisen työntekijän päivittäisiä toimia. (Laaksonen, Nevasalo & Tomula 2006, 115-116.)

3.2 **Henkilöstöturvallisuus**

Henkilöstöturvallisuudella tarkoitetaan työntekijöiden ohjeistusta ja koulutusta. Henkilöstöturvallisuudella pyritään vähentämään työntekijöiden tahattomia vahinkoja. Henkilöstöturvallisuuteen kuuluu myös henkilön taustojen tarkistus rekrytoinnin yhteydessä, perehdytyskoulutus sekä salassapito- ja kilpailukieltosopimukset. Perustana hyvälle henkilöstöturvallisuudelle on osaava ja sitoutunut henkilöstö.

Uutta henkilöstöä palkatessa on suositeltavaa varmistua vastapuolen taustoista. Taustatietojen tarkistuksella yritys voi vähentää uuden henkilön palkkaamiseen ja valintaan liittyviä riskejä. Taustatietojen tarkistukseen on useita eri vaihtoehtoja. Kriittisiin tehtäviin hakevista henkilöistä voi myös teettää suojelupoliisilla turvallisuusselvityksen. Kohteena olevan henkilön suostumus tarvitaan ennen kuin turvallisuusselvitys voidaan tehdä. (Leppänen 2006, 205.)

3.2.1 Salassapitosopimukset

”Salassapitosopimukset koskevat tietoja, jotka on saatu työsuhteessa työnantajasta, työhön liittyvistä salassa pidettävistä asioista, muista työntekijöistä tai kolmansista osapuolista.” (Leppänen 2006, 216.) Salassa pidettävä tieto on pidettävä salassa myös työsuhteen päättymisen jälkeen. Salassapitovelvoitteen rikkominen on rangaistava teko rikoslain mukaan. On kaksi tapaa, jolla salassapitorikos voi tapahtua. Salassa pidettävä seikka paljastetaan tai salaisuutta käytetään omaksi tai toisen hyväksi. Salassapitorikokseen voi syyllistyä vain sellainen henkilö, jolla on asiasta salassapitovel-

vollisuus. Teon pitää lisäksi olla tahallinen eli tekijän on tiedettävä asian olevan salassa pidettävä.

Salassapitosopimus voidaan tehdä normaalin työsopimuslain vaatimusten lisäksi. Ainakin seuraavat asiat on mainittava sopimuksessa: sopijaosapuolet, sopimuksen kesto, sopimuksen kohde riittävällä tarkkuudella sekä sopimuksen rikkomisen seuraamukset. Salassapitosopimuksen rikkominen on peruste irtisanomiselle. Työntekijä on velvollinen korvaamaan mahdollisesta vahingosta aiheutuneet kulut, jotka ovat tapahtuman johdosta aiheutuneet. (Leppänen 2006, 217.)

3.2.2 Asiakkaiden ja vierailijoiden turvallisuus

Asiakkaiden ja vierailijoiden turvallisuus kuuluu myös osana henkilöturvallisuuteen. Asiakkuuksien kannalta turvallisuusjärjestelyn toimivuus sekä asiallinen järjestäminen vaikuttavat siihen millaisen mielikuvan vierailija saa toiminnasta. Tällä saattaa olla suuri vaikutus lopulliseen asiakkuuden saamiseen. Liialliset tai liian vähäiset turvajärjestelyt saattavat antaa vierailijalle huonon kuvan organisaatiosta ja sen toiminnasta. Tästä syystä turvallisuusjärjestelyt tulisi tehdä jämäkästi ja asiallisesti. Turvallisuusjärjestelyihin voi kuulua esimerkiksi sisäänkirjautumis- ja vaitiolovelvollisuussitoumus sekä selkeät kyltit ja opasteet. (Leppänen 2006, 204.)

3.2.3 Avainhenkilöt ja sijaisjärjestely

Yleensä avainhenkilöitä ovat henkilöt, joilla on erityistä osaamista tai asiantuntemusta. He muodostavat sellaisen henkilöstöryhmän, joiden olemassaolo ja osaaminen ovat kriittisiä organisaation toiminnan kannalta. Avainhenkilöiden asiantuntemus liittyy yleisesti joko johtamiseen, tekniseen osaamiseen tai asiakassuhteisiin. On tyypillistä, että avainhenkilön todellinen arvo yritykselle huomataan vasta kun hänet menetetään. (Leppänen 2006, 206.)

Henkilöturvallisuuteen kuuluu myös sijaisjärjestely. Sen tarkoituksena on turvata, että yrityksen toiminta on häiriötöntä mikäli tapahtuu jotain odottamatonta. Odottamatto-

mia tapahtumia ovat esimerkiksi onnettomuudet tai sairastumiset. Vähintään kahden henkilön olisi hyvä osata tehdä samoja työtehtäviä. Sijaisjärjestelyillä sekä muun henkilökunnan osaamisen lisäämisellä on mahdollista vaikuttaa avainhenkilöriskien parempaan hallintaan. (Leppänen 2006, 208.)

3.3 Tietoliikenteen turvallisuus

Tietoliikenteen turvallisuudella tarkoitetaan yrityksen tietojärjestelmän sekä sisäisessä että ulkopuolisissa verkoissa kulkevien viestien suojaamista. Sen tavoitteena on turvata tietoliikenteen jatkuva ja häiriötön toiminta. Sillä pyritään siihen, että verkoissa siirrettävät tiedot eivät päädy ulkopuolisille ilman lupaa. (Miettinen 1999, 20.)

Yrityksen sisäverkon pitäisi olla yhtä hyvin suojattu kuin yrityksen ulkoverkon. Mikäli sisäverkossa ei ole suojausta, pääsee yrityksen luottamuksellisiin tietoihin helposti käsiksi mikäli ulkoverkosta löytyy heikko kohta. Sisäverkko tulee suojata niin, että käyttäjät pääsevät vain niihin tietoihin käsiksi, joihin heillä on oikeus.

Palomuurit sekä virustentorjuntaohjelmat ovat tärkeitä työkaluja tietoliikenneturvallisuuden kannalta. Viruksia voi tulla sähköpostien mukana, mutta niiden leviäminen vaatii käyttäjän toimenpiteitä. Mikäli virus aktivoidaan se pyrkii leviämään koko verkkoon ja saattaa aiheuttaa suurta vahinkoa. (Leppänen 2006, 296-297.)

3.4 Laitteistoturvallisuus

Laitteistoturvallisuudella tarkoitetaan verkon aktiivilaitteiden ja tietokoneiden toiminnan suojaamista. Laitteistoturvallisuudella turvataan laitteiston koko elinkaarta sen asennuksesta turvalliseen poistoon asti. Laitteistoturvallisuudella on selvä yhteys toimitilaturvallisuuteen. Yrityksen laitteisto on suunniteltava niin, että se vastaa yrityksen tarpeita ja vaatimuksia. Laitteiston hankinnassa yhteneväisten laitteiden hankinta helpottaa laitteiden mahdollista huoltoa sekä tulevaa päivitystarvetta.

Laitteiston dokumentoinnilla pystytään tarkastelemaan tietoja laitteistoista ja sen päivitystarpeesta. Lisäksi dokumentoinnin avulla pystytään helposti tarkastelemaan tämänhetkisen laitteiston huolto- ja lisenssisopimusten ajantasaisuutta.

Laitteistoturvallisuuteen kuuluu ehdottomasti myös poistettavien laitteiden asianmukainen tyhjentäminen. Kiintolevyt pitää tuhota, tyhjentää tai päällekirjoittaa niin, ettei vanhoja tiedostoja pysty enää palauttamaan. (Leppänen 2006, 300-301.)

3.5 Ohjelmistoturvallisuus

Ohjelmistoturvallisuudella tarkoitetaan käytössä olevien ohjelmien suojaamista, lisenssien hallintaa ja ohjelmien rekisteröintiä. Ohjelmistoturvallisuudella pyritään estämään laitonta kopiointia ja käyttöä. Ohjelmistojen päivityksillä pyritään parantamaan ohjelmistojen suojausta tietoturvan takia. Lisenssien ylläpito on tärkeää koska jokin ohjelma saattaa lopettaa kokonaan toimintansa, kun lisenssi vanhenee. (Miettinen 1999, 21-22.)

Laittomat kopiot ohjelmista saattavat sisältää piilossa olevia viruksia tai vakoiluohjelmia. Tällaisten avulla pyritään saamaan selville yrityksen toimintaa. Lisäksi laittomasti kopioitujen ohjelmien tietoturvassa saattaa olla aukkoja. Näiden aukkojen kautta pyritään pääsemään sisälle yrityksen verkkoon esimerkiksi vakoilutarkoituksissa.

Ohjelmistoturvallisuuteen vaikuttavat mm. käyttöjärjestelmän ja apuohjelmien asetukset sekä käyttäjien saama koulutus ja ohjeistus. Ohjelmistoturvallisuuteen voidaan myös vaikuttaa käyttämällä muita teknisiä turvakeinoja, kuten eriyttämällä tietoverkot toisistaan. (Valtionvarainministeriö 2007 [viitattu 25.8.2011].)

3.6 Käyttöturvallisuus

Käyttöturvallisuutta toteutetaan huolehtimalla esimerkiksi käyttöoikeuksien hallinnasta, lokien valvonnasta, ohjelmistotuesta ja ylläpito- sekä huoltotoimintoihin liittyvistä

turvallisuustoimenpiteistä. Se perustuu yrityksen tietojärjestelmissä olevien tietojen luokitteluun. (Valtionvarainministeriö 2007 [viitattu 25.8.2011].)

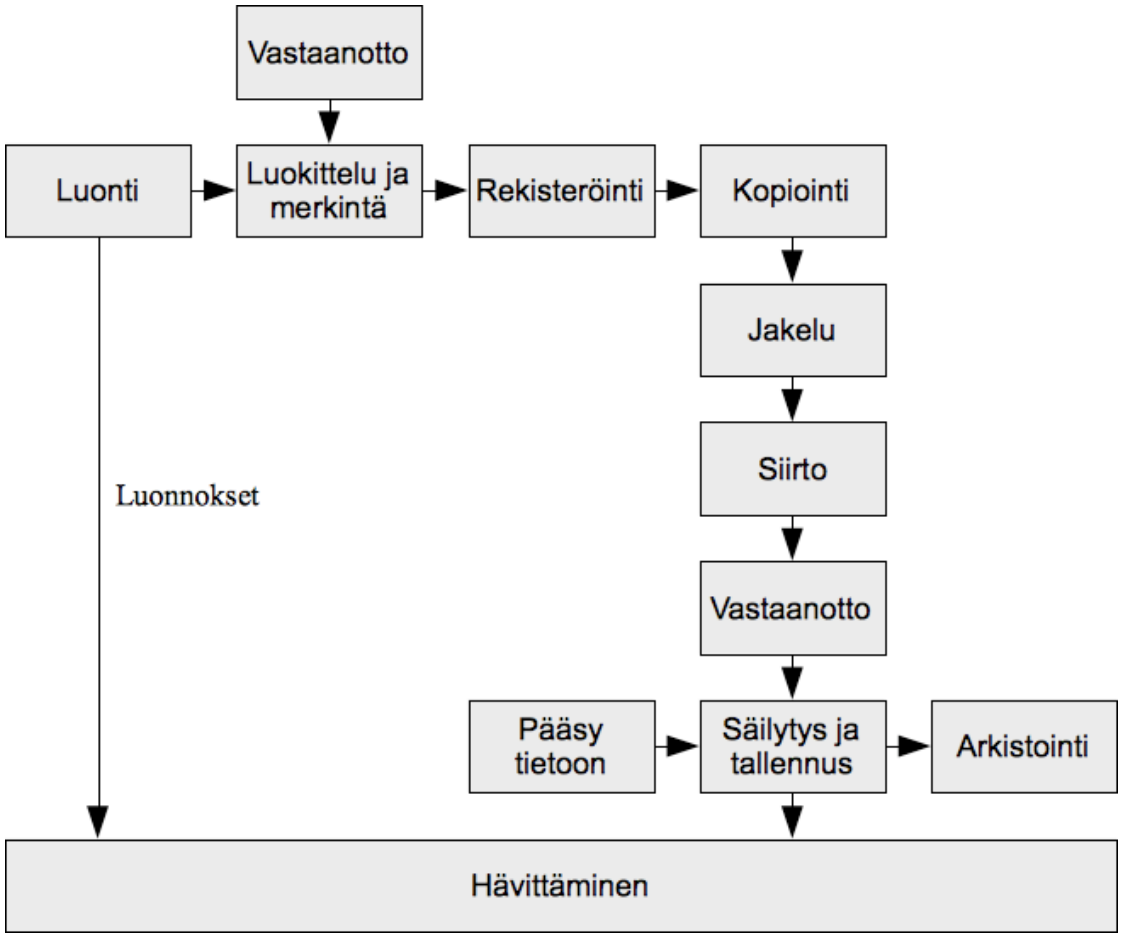
Käyttöturvallisuudella tulee varmistaa, että koko henkilökunta tietää ja hallitsee riittävät tietoturvaan kuuluvat toimenpiteet. Sen tavoitteena on tietojen käytöstä aiheutuvien riskien toteutumisen minimointi. Käyttöturvallisuuteen kuuluu mm. työasemien lukitseminen poistuttaessa työpisteeltä. Tällä varmistetaan, etteivät henkilöt, joilla ei ole asiaa tietokoneelle, pääse tutkimaan sen sisältöä. Lisäksi työpisteiden koneiden sisäosiin ei pitäisi päästä helposti käsiksi ettei tiedostoja sisältävää kiintolevyä pystyttäisi helposti varastamaan. Kannettavissa tietokoneissa on usein paljon tärkeitä tiedostoja, jotka eivät saisi päästä vääriin käsiin. Kannettava tietokone on helppo varastaa mikäli se jää ilman valvontaa.

Laitteiden huolimaton käyttö myös aiheuttaa arkaluontoisen tiedon välittymistä vääriin käsiin. Esimerkiksi junavaunussa salaisten tietojen käsittely saattaa helposti näkyä vieressä tai takana istuvalle. Myöskin puheluiden kuunteluun on helppo tapa vain seistä lähellä puhelimessa olevaa henkilöä. (Leppänen 2006, 303-305.)

3.7 Tietoaineistoturvallisuus

Tietoaineistoturvallisuus tarkoittaa tietojärjestelmän tietojen suojaamista eri tallennusmuodoissa. Sillä halutaan varmistaa, että tiedot pysyvät niillä henkilöillä, jotka tarvitsevat niitä päivittäisten työtehtäviensä suorittamiseen. Tietoaineistoturvallisuuden toteutukselle antaa perustan tietojen turvaluokitusjärjestelmä. (Miettinen 1999, 22-23.)

Tietoaineistoturvallisuus koskee paperiasiakirjoja, optisia ja USB –muistivälineitä, äänitteitä sekä muita tallennusvälineitä. Tietoaineistoturvallisuus koskee koko tietoaineiston elinkaarta ja siitä vastaa koko yrityksen henkilöstö. Kuvio 4 havainnollistaa tietoaineiston elinkaarta.



Kuvio 4: Tietoaineiston elinkaari (Valtionvarainministeriö 2007 [viitattu 25.8.2011].)

4 TOIMITILATURVALLISUUS

Toimitilaturvallisuudella tarkoitetaan toimitilojen fyysistä suojaamista ja sen tarkoituksena on turvata yrityksen häiriötön toiminta. Toimitilaturvallisuuden pääasialliset kohteet ovat toimitilat ja sekä niissä sijaitsevat suojattavat kohteet. Toimitilaturvallisuuteen kuuluvat kulunvalvonta, murtosuojaus ja lukitukset. Näillä asioilla pyritään välttämään vesi- sekä palovahinkoja, laitteistojen varastamista, salaa tapahtuvaa televalvontaa sekä asiattomien henkilöiden pääsyä yrityksen tiloihin.

Toimitilaturvallisuuteen vaikuttavat useat asiat, kuten esimerkiksi sijainti, aidat ja portit, valaistus, rakennuksen fyysiset rakenteet, lukitus ja avainten hallinta. Teknisiä

ratkaisuja, jotka liittyvät toimitilaturvallisuuteen, ovat rikos- ja paloilmoitinjärjestelmät, video-, ja kulunvalvontajärjestelmät sekä sammutus- ja savunpoistojärjestelmät.

Yrityksen kaikki tilat eivät ole fyysisen turvallisuuden kannalta samanarvoisia. Yleensä korkeaa suojausta vaativia kohteita ovat yrityksen vahvuusalueisiin liittyvät tilat. Hyvä apuväline suojaustarpeita suunnitellessa on toimitilojen tärkeysluokitus. Tilojen merkitys tietoturvan kannalta saadaan näin hyvin selvitettyä. Mikäli luokitusta ei suoriteta, saattavat vaarana olla virhearvioinnit ja resurssien hukkaaminen. (Laaksonen, Nevasalo & Tomula 2006, 125.)

4.1 Tärkeysluokitus

Yrityksen toimitilat voidaan esimerkiksi jaotella kolmeen osaan: ei-tärkeisiin, tärkeisiin ja erittäin tärkeisiin tiloihin. Yrityksen piha-alue sekä aula- ja odotustilat ovat tavallisesti ei-tärkeitä tiloja. Työhuoneet, avokonttorit ja valtaosa tuotantotiloista ovat tavallisesti tärkeitä tiloja. Laite- ja tuotekehitystilat sekä johdon kokous- ja neuvottelutilat ovat tavallisesti erittäin tärkeitä tiloja. Liitteessä 3 oleva taulukko havainnollistaa perussuojausvaatimuksia eri tärkeysluokkien tiloille. (Miettinen 1999, 178-179.)

4.2 Toimitilaturvallisuuden tasot

Toimitilaturvallisuuden määrittelemiseksi voidaan ottaa avuksi turvallisuustasot, joiden avulla kiinteistöturvallisuutta voidaan hallita. Turvallisuustasoja ovat seuraavat:

- Taso 1: Perussuojaus
  Perusturvallisuustasolla olevissa kohteissa ei ole yrityksen kannalta merkittävää toimintaa. Kohteeseen ei kohdistu erityisiä riskejä eivätkä ne toteutuessaan aiheuttaisi yritykselle merkittäviä vahinkoja. Turvallisuutta ylläpidetään aidoilla sekä lukituksilla. Turvallisuustason kohteita ovat mm. avoimet parkkihallit ja ulkovarastot. (Leppänen 2006, 343.)

- Taso 2: Tehostettu perussuojaus

  Tehostetun perussuojauksen alaisissa kohteissa on sellaista materiaalia, joka tulee varmistaa joko kulunvalvonnalla tai teknisillä ratkaisuilla. Yleisimpiä teknisiä ratkaisuja ovat rikosilmoitinjärjestelmät sekä kulunvalvonta. Turvallisuustason kohteita ovat mm. perustoimistotilat, asuinrakennukset ja yrityksen sisääntulot. (Leppänen 2006, 344.)

- Taso 3: Erityissuojaus

  Kohteet, jotka kuuluvat erityissuojauksen alaisuuteen, sisältävät yritykselle tärkeää materiaalia. Kohteen riskit ovat todennäköisiä ja voivat toteutuessaan aiheuttaa yritykselle merkittäviä vahinkoja. Erityissuojauksen toteuttamiseen on erilaisia toimenpiteitä, kuten esimerkiksi turvallisuussuunnitelman laatiminen, hälytykset, 24h kulunvalvonta, kameravalvonta, sähkönsyötön varmennus, aidat ja portit. Turvallisuustason kohteita ovat mm. Myymälät ja tavaravarastot. (Leppänen 2006, 344.)

- Taso 4: Täyssuojaus

  Täyssuojattujen tilojen kaikki osa-alueet ovat täysin valvottuja kaikilta osin. Tilat on suojattu siten, että kaikkien riskien vaikutukset on minimoitu. Tiloihin kohdistuu merkittäviä riskejä ja niiden vaikutukset yrityksen toimintaan ovat vakavia. Turvallisuustason toteuttamisessa käytettyjä asioita erityissuojauksen lisäksi ovat esimerkiksi seuraavat: erityiskorkeat aidat, tilojen rakenteiden vahvistettu suojaus, sähkönsyötön laaja varmennus, piiri-, tai paikallisvarmennus, tunkeutumisen hidastaminen erilaisilla toimenpiteillä, arvo-omaisuuden suojaaminen kassakaapeilla sekä kaikki tekniset turvajärjestelmät. Turvallisuustason kohteita ovat mm. rahan säilytystilat, salaisen tiedon ja materiaalin säilytystilat sekä atk-tilat. (Leppänen 2006, 345.)

4.3 Video- ja kulunvalvonta sekä kulunhallinta

Yksittäinen, ehkä tärkein tekijä toimitilaturvallisuudessa, on kiinteistön kulunhallinta. Sen tunnetuin osa-alue on kulunvalvonta, joka muodostuu niistä teknisistä menetelmistä, joilla valvotaan ja rajoitetaan ihmisten liikkumista yrityksessä. Kulunvalvontaa toteutetaan erilaisilla lukituksilla, joita ovat tavallisesti mekaaninen ja sähköinen lukitus. Mekaaninen lukitus tarkoittaa sitä, että yrityksen toimitilojen ovissa on lukot, jotka toimivat mekaanisilla avaimilla, kuten esimerkiksi Abloy-lukot. Sähköisillä lukituksilla vastaavasti työntekijöillä on avainkortti, johon voidaan ohjelmoida henkilön kulkuoikeudet. Sähköisen lukituksen etuja ovat joustava kulkuoikeuksien määrittely sekä katoamistapauksessa avain voidaan helposti poistaa ohjelmallisesti kulunvalvontajärjestelmästä. (Miettinen 1999, 180.)

Videovalvonnalla seurataan asennettujen videokameroiden avulla tapahtumia joissakin kohteissa. Valvonnan kohteessa videovalvonta on yleisesti käytössä 24 tuntia vuorokaudessa. Paras tulos videovalvonnasta saadaan kun valvonta nauhoitetaan ja säilytetään riittävän pitkäksi aikaa. Videovalvonnan toteutuksessa on otettava huomioon voimassa oleva lainsäädäntö. Esimerkkinä lainsäädännöstä on, että videovalvonnasta on löydyttävä selkeät merkinnät sen käytöstä yrityksen tiloissa. (Miettinen 1999, 181-182.)

4.4 Palo- ja murtosuojaus

Palosuojauksen avulla pyritään suojaamaan käytössä olevat tilat palovahinkoja vastaan. Paloturvallisuudesta huolehditaan Suomessa pääsääntöisesti hyvin johtuen kiinteistöjen teknillisistä rakennemääräyksistä. Lisäksi vakuutusyhtiöt ovat asettaneet omat tiukat vaatimuksensa paloturvallisuudelle.

Kuten taulukossa 1 (liite 3) suositellaan, on tärkeät sekä erittäin tärkeät tilat suojattava automaattisella paloilmoitinjärjestelmällä. Siihen kuuluu ilmaisimia, jotka tarkkailevat tilaa, sekä keskusyksikkö, joka tekee tarvittaessa palohälytyksen palolaitokselle tai

vartiointiliikkeeseen. Lisäksi erittäin tärkeät tilat on suojattava automaattisella sammutusjärjestelmällä. Automaattinen sammutusjärjestelmä on alkaneen tulipalon sammutusjärjestelmä, joka suihkuttaa korkealla paineella vesijohtovettä. (Miettinen 1999, 182-184.) Luonnollisesti laitetiloissa vedenkäyttö ei ole järkevää, jolloin sammutusaineena voidaan käyttää esimerkiksi tukahduttavia kaasuja.

4.5 Jimm's PC-Store Oy (salattu)

5 YKSITYISYYDEN SUOJA

Yksityisyyden suojaan kuuluu yrityksen työtekijöiden sekä sen toimintaan liittyvien henkilöiden tietojen suojaaminen. Yksityisyyden suojan tarkoituksena on, että tietoja käytetään vain asianmukaisiin tarkoituksiin. Asiakkaiden tiedot kerätään rekisteriin, joka on suojattu niin, etteivät tiedot pääse vääriin käsiin.

Yksityisyyden suojan tarkoituksena työelämässä on toteuttaa yksityiselämän suojaa sekä muita yksityisyyden suojaa turvaavia perusoikeuksia työelämässä. Lakia yksityisyyden suojasta työelämässä sovelletaan esimerkiksi työtekijälle tehtävissä testeissä ja tarkastuksissa sekä työntekijän sähköpostien hakemisessa ja avaamisessa. (Finlex lainsäädäntö 2004 [viitattu 25.8.2011].)

Kesäkuussa 2009 tuli voimaan sähköisen viestinnän tietosuojalaki, jonka tarkoituksena on turvata sähköisen viestinnän luottamuksellisuuden ja yksityisyyden toteutumista. Lisäksi sen on tarkoitus edistää sähköisen viestinnän tietoturvaa ja monipuolisten sähköisen viestinnän palvelujen tasapainoista kehittymistä. (Finlex lainsäädäntö 2004 [viitattu 25.8.2011].)

Sähköisen viestinnän tietosuojalaki tunnetaan paremmin nimellä Lex Nokia. Lex Nokia antaa yritykselle oikeuden selvittää verkkonsa käyttäjien tunnistamistietoja tiettyjen ehtojen täyttyessä. Tällaisia ehtoja ovat seuraavat:

- Tietoturvan täytyy olla kunnossa.

- Käyttäjiä tulee ohjeistaa kirjallisesti siitä, miten sen viestintäverkkoa saa käyttää.
- Ylläpidosta, tietoturvasta tai turvallisuudesta vastaavat henkilöt, jotka saavat käsitellä tietoja, pitää nimetä.
- Tietosuojavaltuutetulle pitää ilmoittaa tunnistamistietojen käsittelyn aloituksesta.

Lisäksi käyttäjälle on annettava selvitys perusteluista selvitykselle, syy miksi käsittelyyn on ryhdytty, käsittelijät, sekä käsittelystä päättänyt henkilö. Käsittelyyn osallistuneiden on allekirjoitettava selvitys. (Wikipedia 2011, Lex Nokia.)

5.1 Henkilötietolaki

Tärkeä laki tietoturvan kannalta on henkilötietolaki (523/1999), koska sitä on noudatettava henkilötietojen käsittelyssä. Sen tarkoituksena on toteuttaa yksityiselämän sekä yksityisyyden suojaa turvaavia perusoikeuksia. Henkilötietolaki tulee käytännössä sovellettavaksi lähes jokaisessa yrityksessä, jossa käsitellään yksittäisen henkilön henkilötietoja. (Laaksonen, Nevasalo & Tomula 2006, 31.)

Henkilötietolaki asettaa yritykselle useita vaatimuksia kun käsitellään henkilöiden tietoja.

- Yritys saa kerätä vain sellaisia tietoja, jotka ovat tarpeellisia. Rekisterinpitäjän on myös huolehdittava, että tieto on ajantasaista.
- Arkaluontoisia tietoja (esim. rotu, poliittinen ja uskonnollinen vakaumus, rikokset) ei saa käsitellä muussa kuin mm. viranomaiskäytössä.

5.2 Henkilötietolain tietoturvaperiaatteet

Henkilötietolaissa määritellään, että henkilörekisteri on suojattava niin, että laittomat yritykset päästä muokkaamaan siellä olevia tietoja, aiheuttavat viiveettä hälytyksen rekisterinpitäjälle. Käsiteltävien tietojen tasosta riippuu rekisteriltä vaadittava tietoturvan taso. Esimerkiksi pelkän nimen sekä osoitteen sisältävän rekisterin suojauksen ei

tarvitse olla samanlainen kuin arkaluontoisia tietoja, kuten henkilötunnus, sisältävän rekisterin tason.

Rekisterinpitäjän tulee kiinnittää huomiota käyttövaltuuksien määrittelyssä. Käyttöoikeudet on luonnollista määritellä kunkin työntekijän työtehtävien mukaisesti. (Laaksonen, Nevasalo & Tomula 2006, 42.)

6 TIETOTURVAKARTOITUS

Tietoturva koostuu useasta eri asiasta ja tietoturvallisuuden tutkimiseen on kehitetty useita eri välineitä ja tapoja. Maailmassa on useita eri yrityksiä, jotka tekevät tietoturvakartoituksia. Yleensä jokaisella yrityksellä on oma kyselynsä, joiden avulla kartoitus tehdään. Tietoturvakartoituksen teettäminen ulkoisella taholla tuottaa yritykselle lisäkustannuksia sekä luo vaaratekijän tietoturvallisuudelle. (Shared Assessments 2011 [viitattu 25.8.2011]).

6.1 Shared Assessments Program

Johtavat Yhdysvaltain talousinstituutiot yhdessä suurten kirjapitotoimistojen sekä palveluntarjoajien kanssa halusivat luoda standardoidun, johdonmukaisen ja kustannustehokkaan työkalun prosessia varten. Sen tarkoituksena on vähentää redundanssia ja luoda tehokkuutta sekä antaa kaikille osapuolille selkeän käsityksen tietoturvallisuuden tasosta.

Taustatyö saatiin valmiiksi vuonna 2005 ja Standardized Information Gathering (SIG) -kyselyn versio 1 julkaistiin helmikuussa 2006. The Santa Fe Group on omistautunut kehittämään valmistunutta työkalua. Heidän vastuullaan on päivittää sekä ylläpitää työkalua, jotta se on aina ajan tasalla. (Shared Assessments 2011 [viitattu 25.8.2011].)

6.2 SIG –kysely

The Santa Fe Groupin tekemä SIG –kysely on laajasti käytetty tietoturvakartoitukseen tarkoitettu kysely. Se on organisoitu ISO27001:2005 standardin mukaiseksi. Esimerkkejä tunnetuista yrityksistä, jotka käyttävät työkalua ovat IBM, AT&T, Bank of America ja Deutsche Bank. Kysely on ensisijaisesti suunnattu Yhdysvaltoihin, mutta sen muunneltavuus antaa mahdollisuuden jokaiselle yritykselle ottaa se käyttöönsä. Kartoituksen helppous antaa sen käyttäjälle mahdollisuuden sisällyttää se yrityksen tietoturvapolitiikkaan.

Kysely on yksinkertainen täyttää ja se sisältää hyvin yksityiskohtaisesti tietoturvan aihealueet. Kyselyn avulla pyritään selvittämään yrityksen tämän hetkinen tietoturvallisuuden taso. Kyselyn vastausten perusteella pystytään yritykselle tekemään tietoturvakartoitus.Kyselyssä mahdollisesti esiin tulleet haavoittuvuudet saadaan selville ja niihin pystytään ehdottamaan tarvittavat korjaustoimenpiteet.

7 PÄÄTELMÄT

Tutkimuksen tarkoituksena oli tietoturvakartoituksen tekeminen pk–yritykselle. Opinnäytetyö tuli toimeksiantona Jimm’s PC-Store Oy:ltä, jolle ei tietoturvakartoitusta ollut tehty lähiaikoina. Tutkimuksen tekemisen alkuvaiheessa huomasin jo, että tietoturvakartoitus alueena on valtavan laaja. Yrityksen toiveena oli, että kartoitus tehtäisiin jokaisesta tietoturvan osa-alueesta. Kuitenkin täydellisen, laajan tietoturvakartoituksen tekeminen olisi opinnäytetyöksi liian laaja toimeksianto. Tästä syystä sovimme yrityksen kanssa, että teen supistetun tietoturvakartoituksen yritykselle. Tämä käytännössä tarkoitti sitä, että kartoituksessa käytiin yleisesti lävitse jokainen tietoturvan osa-alue muutamalla tarkentavalla kohdalla.

Tietoturvakartoitusta varten sain The Santa Fe Groupin Standardized Information Gathering (SIG) kyselyn. Kaikki suuret ja johtavat yritykset Yhdysvalloissa käyttävät kyselyä omien tietoturvakartoituksien pohjana. Kyselyyn tutustuessani huomasin sen oleva äärettömän laaja ja tutkimukseni käyttöön tarvitsisin siitä vain pienen osan.

Muokkasin kyselystä omaan käyttööni soveltuvan version, jonka annoin yritykselle täytettäväksi. Kyselyssä käyttämäni versio 5.0 on vuoden 2009 lokakuulta. Kyselyä voidaan käyttää minkä tahansa yrityksen tietoturvan kartoituksessa sen monipuolisuuden vuoksi. Kyselyssä on paljon kysymyksiä, jotka ovat turhia johtuen esimerkiksi osittain Suomen maantieteellisestä sijainnista. Tästä syystä kyselyä tehtäessä olisi tutkijan hyvä perehtyä itse ensin kyselyyn ja poistaa siitä kysymykset, joilla ei ole merkitystä.

Kyselyyn saamieni vastausten perusteella tein supistetun tietoturvakartoituksen, joka on opinnäytetyöni liitteenä 4. Raportista selviää tarkemmin kyselyn tulokset. Raportti on salattu, koska se sisältää yrityksen tietoturvan kannalta oleellisia asioita.

Tekemästäni kartoituksesta on ollut minulle valtavasti hyötyä tulevaisuuden työtehtäviä ajatellessa. Työtä tehdessä olen saanut tutustua tietoturvan monipuolisuuteen ja tätä kautta yleistä tietoa aiheesta on tullut valtavasti lisää. Lisäksi olen joutunut tutustumaan aiheeseen paljon pintaa syvemmälle samalla kun olen opinnäytetyötä tehnyt. Tekemäni supistettu tietoturvakartoitus antaa hyvän pohjan sille, että yritykselle voidaan myöhemmin tehdä laajempi tietoturvakartoitus.

LÄHTEET

Finlex lainsäädäntö 2004. *Laki yksityisyyden suojasta työelämästä 13.8.2004/759* [online, viitattu 25.8.2011]. Saatavilla www-muodossa:
<URL: http://www.finlex.fi/fi/laki/ajantasa/2004/20040759>.

Finlex lainsäädäntö 2004. *Sähköisen viestinnän tietosuojalaki 16.6.2004/516* [online, viitattu 25.8.2011]. Saatavilla www-muodossa:
<URL:http://www.finlex.fi/fi/laki/ajantasa/2004/20040516>.

Hakala, Mika & Vainio, Mika & Vuorinen, Olli 2006, *Tietoturvallisuuden käsikirja.* Jyväskylä: Docendo Finland Oy.

Järvinen, Petteri 2002. *Tietoturva & yksityisyys.* Porvoo: Docendo Finland Oy.

Krutz, Ronald L. & Vines, Russel Dean 2003. *Tietoturvasertifikaatti – CISSP*. Helsinki: Edita Publishing Oy.

Laaksonen, Mika & Nevasalo, Terho & Tomula, Karri 2006. *Yrityksen tietoturvakäsikirja.* Helsinki: Edita Publishing Oy

Leppänen, Juha 2006. *Yritysturvallisuus käytännössä.* Helsinki: Talentum.

Miettinen, Juha 1999. *Tietoturvallisuuden johtaminen. Näin suojaat yrityksesi toiminnan.* Helsinki: Kauppakaari Oyj.

Ruohonen, Mika 2002. *Tietoturva.* Porvoo: Docendo Finland Oy.

Shared Assesments 2011. The *Shared Assessments Program - Standardized Information Gathering (SIG) Questionnaire.* [online, viitattu 25.8.2011]. Ladattavissa www-sivulta: <URL:http://sharedassessments.org/>.

Valtionvarainministeriö 2007. *Tietoturvallisuudella tuloksia, Yleisohje tietoturvallisuuden johtamiseen ja hallintaan.* [online, viitattu 25.8.2011]. Saatavilla www-muodossa:
<URL:http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20071128Tietot/vahti3_07_netti.pdf>.

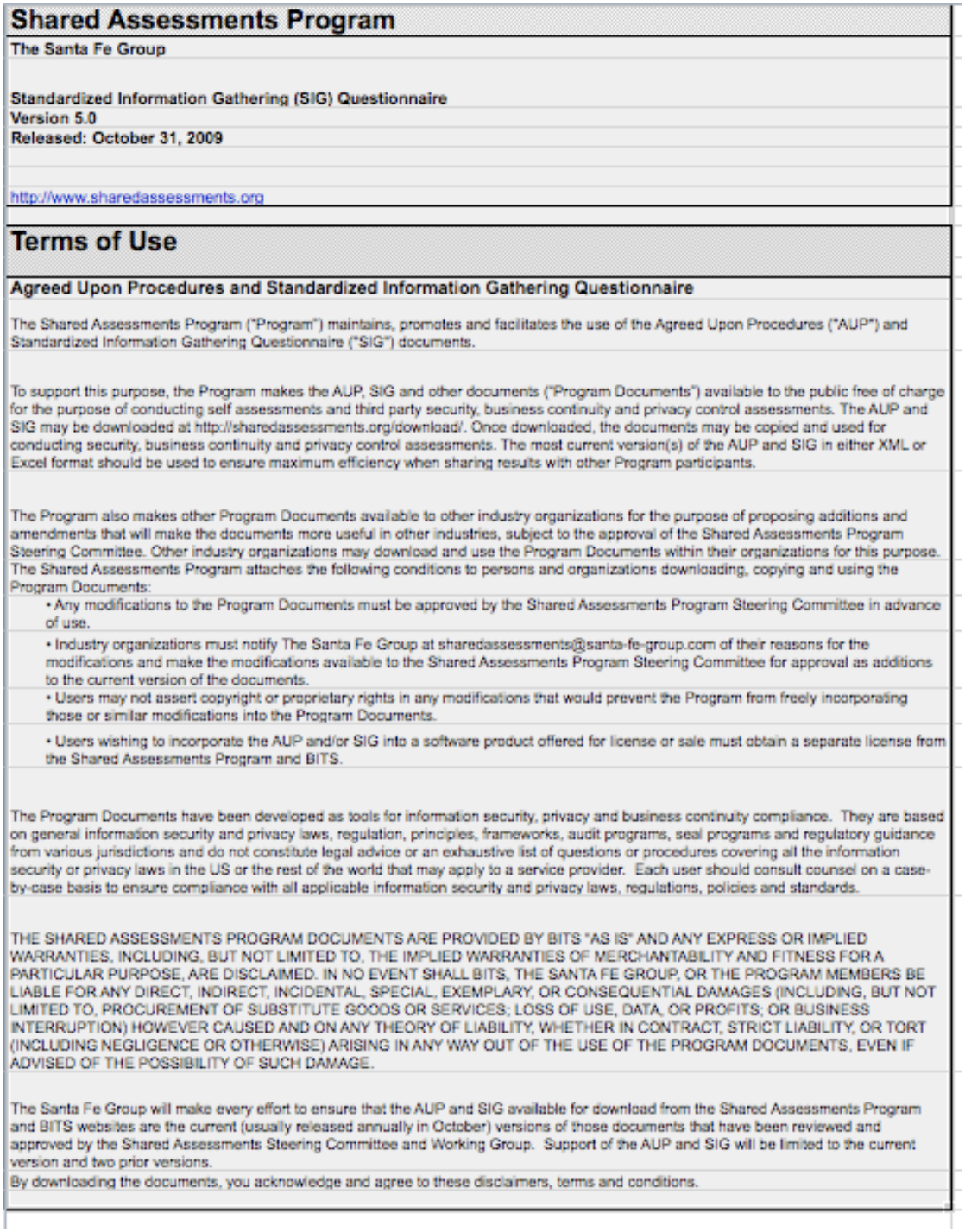
Yrityksen tietoturvaopas 2010. *Toimiva tietoturva – portaittain eteenpäin.* [online, viitattu 25.8.2011]. Saatavilla www-muodossa:
<http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/portaittain_eteenpain.html>.

Viestintävirasto 2009. *Tietoturvalliseen yhteiskuntaan.* [online, viitattu 25.8.2011]. Saatavilla www-muodossa:
<http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva.html#>.

Wikipedia 2011. *Lex Nokia.* [online, viitattu 25.8.2011]. Saatavilla www-muodossa: <URL:http://fi.wikipedia.org/wiki/Lex_Nokia>.

LIITTEET

Liite 1. Santa Fe Group Standardized Information Gathering (SIG) versio 5.0



Shared Assessments Program

The Santa Fe Group

Standardized Information Gathering (SIG) Questionnaire
Version 5.0
Released: October 31, 2009

http://www.sharedassessments.org

Terms of Use

Agreed Upon Procedures and Standardized Information Gathering Questionnaire

The Shared Assessments Program ("Program") maintains, promotes and facilitates the use of the Agreed Upon Procedures ("AUP") and Standardized Information Gathering Questionnaire ("SIG") documents.

To support this purpose, the Program makes the AUP, SIG and other documents ("Program Documents") available to the public free of charge for the purpose of conducting self assessments and third party security, business continuity and privacy control assessments. The AUP and SIG may be downloaded at http://sharedassessments.org/download/. Once downloaded, the documents may be copied and used for conducting security, business continuity and privacy control assessments. The most current version(s) of the AUP and SIG in either XML or Excel format should be used to ensure maximum efficiency when sharing results with other Program participants.

The Program also makes other Program Documents available to other industry organizations for the purpose of proposing additions and amendments that will make the documents more useful in other industries, subject to the approval of the Shared Assessments Program Steering Committee. Other industry organizations may download and use the Program Documents within their organizations for this purpose. The Shared Assessments Program attaches the following conditions to persons and organizations downloading, copying and using the Program Documents:

- Any modifications to the Program Documents must be approved by the Shared Assessments Program Steering Committee in advance of use.
- Industry organizations must notify The Santa Fe Group at sharedassessments@santa-fe-group.com of their reasons for the modifications and make the modifications available to the Shared Assessments Program Steering Committee for approval as additions to the current version of the documents.
- Users may not assert copyright or proprietary rights in any modifications that would prevent the Program from freely incorporating those or similar modifications into the Program Documents.
- Users wishing to incorporate the AUP and/or SIG into a software product offered for license or sale must obtain a separate license from the Shared Assessments Program and BITS.

The Program Documents have been developed as tools for information security, privacy and business continuity compliance. They are based on general information security and privacy laws, regulation, principles, frameworks, audit programs, seal programs and regulatory guidance from various jurisdictions and do not constitute legal advice or an exhaustive list of questions or procedures covering all the information security or privacy laws in the US or the rest of the world that may apply to a service provider. Each user should consult counsel on a case-by-case basis to ensure compliance with all applicable information security and privacy laws, regulations, policies and standards.

THE SHARED ASSESSMENTS PROGRAM DOCUMENTS ARE PROVIDED BY BITS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED. IN NO EVENT SHALL BITS, THE SANTA FE GROUP, OR THE PROGRAM MEMBERS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THE PROGRAM DOCUMENTS, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The Santa Fe Group will make every effort to ensure that the AUP and SIG available for download from the Shared Assessments Program and BITS websites are the current (usually released annually in October) versions of those documents that have been reviewed and approved by the Shared Assessments Steering Committee and Working Group. Support of the AUP and SIG will be limited to the current version and two prior versions.

By downloading the documents, you acknowledge and agree to these disclaimers, terms and conditions.

Business Information	
Question/Request	**Response**
Responder Name:	
Responder Job Title:	
Responder Contact Information:	
Date of Response:	
Company Profile	
What is the name of the holding or parent company?	
What is the company/business name?	
How long has the company been in business?	
Computer Equipment Details	
What is the production site physical address?	
What is the backup site physical address?	
Are there any additional location(s) where target data is stored?	
If so, provide locations (address, city, state, country).	
Please provide details in the following areas:	
- Operating system(s)	
- Workstations # of devices	
- Servers # of devices	

A	B	C
Level One Questions		
For each question choose either Yes, No or N/A. If N/A is chosen, an explanation is mandatory.		
Question/Request	Response	Additional Information
Risk Assessment and Treatment		
Is there a risk assessment program?		
Security Policy		
Is there an information security policy?		
Is there an Acceptable Use Policy?		
Organizational Security		
Is there an information security function responsible for security initiatives within the organization?		
Does management require the use of confidentiality or non-disclosure agreements?		
Asset Management		
Is there an asset management program?		
Is there insurance coverage for business interruptions or general services interruption?		
Human Resource Security		
Are background screenings of applicants performed to include criminal, credit, professional / academic, references and drug screening?		
Are new hires required to sign any agreements that pertain to non/disclosure, confidentiality, acceptable use or code of ethics upon hire?		
Physical and Environmental Security		
Is there a physical security program?		
Do the target systems reside in a data center?		
Communications and Operations Management		
Are operating procedures utilized?		
Are anti-virus products used?		
Are system backups of Target Data performed?		
Question/Request	Response	Additional Information
Are there external network connections (Internet, Intranet, Extranet, etc.)?		
Is wireless networking technology used?		
Access Control		
Are unique user IDs used for access?		
Are passwords required to access systems holding, processing, or transporting Target Data?		
Is remote access permitted into the environment?		
Incident Event and Communications Management		
Is there an Incident Management program?		
Is there an Incident Response Plan (formal or informal)?		
Business Continuity and Disaster Recovery		
Is there a Business Continuity/Disaster Recovery (BC/DR) program?		

Risk Assessment and Treatment

For each question choose either Yes, No or N/A. If N/A is chosen, an explanation is mandatory.

Question/Request	Response	Additional Information
Is there a risk assessment program?		
Is there an owner to maintain and review the Risk Management program?		
Do the assets include the following:		
People?		
Process?		
Information (physical and electronic)?		
Technology (applications, middleware, servers, storage, network)?		
Physical (buildings, energy)?		
IT system management software (BSM, CMDB, Firewalls, IDS/IPS, etc.)?		
Servers?		
Storage?		
Communications?		
Physical facilities?		
Is there a formal strategy for each identified risk?		
Does the strategy include:		
Risk acceptance?		
Risk avoidance?		
Risk transfer?		
Insurance?		
Is there a process to monitor all identified risks on an ongoing basis?		
Has the process been executed in the last 12 months?		
Has the process been updated in the last 12 months?		
Are controls identified for each risk discovered?		
Are controls classified as:		
Preventive?		
Detective?		
Corrective?		
Predictive?		

Security Policy

For each question choose either Yes, No or N/A. If N/A is chosen, an explanation is mandatory.

Question/Request	Response	Additional Information
Is there an information security policy?		
Which of the following leadership levels approve the information security policy:		
Board of directors?		
CEO?		
C-level executive?		
Senior leader?		
Other (Please explain in the "Additional Information" column)?		
Has the security policy been published?		
Is there an owner to maintain and review the policy?		
Do information security policies contain the following:		
Definition of information security?		
Objectives?		
Scope?		
Importance of security as an enabling mechanism?		
Statement of Management Intent?		
Risk assessment?		
Risk management?		
Legislative, regulatory, and contractual compliance requirements?		
Security awareness training/education?		
Business continuity?		
Penalties for non-compliance with corporate policies?		
Responsibilities for information security management?		
References to documentation to support policies?		
Have the policies been reviewed in the last 12 months?		

Organizational Security

For each question choose either Yes, No or N/A. If N/A is chosen, an explanation is mandatory.

Question/Request	Response	Additional Information
Is there an information security function responsible for security initiatives within the organization?		
Is there an individual or group responsible for security within the organization?		
Does this individual or group have the following responsibilities:		
Identify information security goals that meet organizational requirements?		
Integrate information security controls into relevant processes?		
Formulate, review and approve information security policies?		
Approve major initiatives to enhance information security?		
Provide needed information security resources?		
Approve assignment of specific roles and responsibilities for information security?		
Initiate plans and programs to maintain information security awareness?		
Develop and maintain an overall security plan?		
Review advice external information security specialists?		
Coordination of information security from different parts of the organization?		
Review and monitor information security / privacy incidents or events?		
Are information security responsibilities allocated to an individual or group?		
Does management require the use of confidentiality or non-disclosure agreements?		
Does the confidentiality or non-disclosure agreement contain the following:		
Definition of the information to be protected?		
Expected duration of an agreement?		
Required actions when an agreement is terminated?		
Responsibilities and actions of signatories to avoid unauthorized information disclosure?		
Ownership of information, trade secrets and intellectual property?		
The permitted use of confidential information, and rights of the signatory to use information?		
The right to audit and monitor activities that involve confidential information?		
Process for notification and reporting of unauthorized disclosure or confidential information breaches?		
Terms for information to be returned or destroyed when the agreement has expired?		
Expected actions to be taken in case of a breach of this agreement?		

Asset Management

For each question choose either Yes, No or N/A. If N/A is chosen, an explanation is mandatory.

Question/Request	Response	Additional Information
Is there an asset management program?		
Is there an asset management policy?		
Has it been approved by management?		
Is there an owner to maintain and review the policy?		
Is there an inventory of hardware/software assets?		
Does the inventory record the following attributes:		
Operating system?		
Physical location?		
Serial number?		
System owner?		
Environment (dev, test, etc.)?		
Host name?		
IP address?		
Is there a detailed description of software licenses, (e.g., number of seats, concurrent users, etc.) ?		
Are information assets classified?		
Is there an information asset classification policy?		
Has it been approved by management?		
Has the policy been published?		
Is there a procedure for handling of information assets?		
Does the procedure address the handling of information assets in accordance with the following classifications:		
Data access controls?		
Data in transit?		
Data labeling?		
Data on removable media?		
Data ownership?		
Data reclassification?		
Data retention?		
Data destruction?		

Question/Request	Response	Additional Information
Data disposal?		
Data encryption?		
Data in storage?		
Are there procedures for the disposal and/or destruction of physical media (e.g., paper documents, CDs, DVDs, tapes, disk drives, etc.)?		
Are there procedures for the reuse of physical media (e.g., tapes, disk drives, etc.)?		
Is there insurance coverage for business interruptions or general services interruption?		

Human Resource security

For each question choose either Yes, No or N/A. If N/A is chosen, an explanation is mandatory.

Question/Request	Response	Additional Information
Are security roles and responsibilities of constituents defined and documented in accordance with the organization's information security policy?		
Are security roles and responsibilities of dependent service providers defined and documented in accordance with the organization's information security policy?		
Are background screenings of applicants performed to include criminal, credit, professional / academic, references and drug screening?		
Is there a pre-screening policy?		
Is there an owner to maintain and review the policy?		
Is there an external background screening agency?		
Are the following background checks performed on:		
Criminal:		
Full time employees?		
Part time employees?		
Contractors?		
Temporary workers?		
Credit:		
Full time employees?		
Part time employees?		
Contractors?		
Temporary workers?		
Academic:		
Full time employees?		
Part time employees?		
Contractors?		
Temporary workers?		

Question/Request	Response	Additional Information
Reference:		
Full time employees?		
Part time employees?		
Contractors?		
Temporary workers?		
Resume or curriculum vitae:		
Full time employees?		
Part time employees?		
Contractors?		
Temporary workers?		
Drug Screening:		
Full time employees?		
Part time employees?		
Contractors?		
Temporary workers?		
Are new hires required to sign any agreements that pertain to non/disclosure, confidentiality, acceptable use or code of ethics upon hire?		
Are any agreements required to be re-read and re-accepted at least every 12 months?		
Is there a security awareness training program?		
Does the security awareness training include security policies, procedures and processes?		

Physical and Environmental

For each question choose either Yes, No or N/A. If N/A is chosen, an explanation is mandatory.

Enter Address of the site this tab refers to:		
Question/Request	**Response**	**Additional Information**
Is there a physical security program?		
Is there a documented physical security policy?		
Has it been approved by management?		
Has the policy been published?		
Is there an owner to maintain and review the policy?		
For the building or primary facility that stores Target Data (address noted in row 3 above), Is it located within 20 miles of:		
Chemical plant, hazardous manufacturing or processing facility?		
Natural gas, petroleum, or other pipeline?		
Airport?		
Railroad?		
Active fault line?		
Government building?		
Military base or facility?		
Gas / Oil refinery?		
Coast, harbor, port?		
Flood prone area?		
Emergency response services (e.g., fire, police, etc.)?		
Urban center or major city?		
Does the perimeter of the building have:		
A physical barrier (e.g., fence or wall)?		
Is the physical barrier monitored (e.g., guards, technology, etc)?		
Can vehicles come in close proximity to the building?		
Does the building that contains the Target Data:		
Have a single point of entry?		
Have exterior windows?		
Have windows have contact alarms that will trigger if opened?		
Have glass break detection?		
Have external lighting?		

Question/Request	**Response**	**Additional Information**
Have concealed windows?		
Have glass walls or doors?		
Use CCTV?		
Monitored 24x7x365?		
Pointed at entry points?		
Digitally recorded?		
Stored for at least 90 days?		
Have all entry and exits alarmed? If so, are they:		
Monitored 24x7x365?		
Have and use prop alarms on all doors?		
Is there a loading dock at the facility?		
Does the loading dock area contain the following:		
Smoke detector?		
Fire alarm?		
Wet fire suppression?		
Fire extinguishers?		
Is there a call center operated or maintained?		
Are calls randomly monitored?		
Are paper or electronic files used?		
Is there a clean desk policy?		
Are "secret caller" penetration tests conducted? If so, how often:		
Daily?		
Weekly?		
Monthly?		
Semi-annually?		
Annually?		
Is there a preventive maintenance process or current maintenance contracts in place for the following:		
UPS system?		
Security system?		
Fire alarm?		
Are the following tested:		
UPS system - annually?		

Question/Request	**Response**	**Additional Information**
Security alarm system - annually?		
Fire alarms - annually?		

Communications and Operations Management

For each question choose either Yes, No or N/A. If N/A is chosen, an explanation is mandatory.

Question/Request	Response	Additional Information
Are operating procedures utilized?		
Are operating procedures documented, maintained, and made available to all users who need them?		
Has the policy been published?		
Is there an owner to maintain and review the policy?		
Do procedures include the following:		
Processing and handling of information?		
Scheduling requirements, including interdependencies with other systems, earliest job start and latest job completion times?		
Support contacts in the event of unexpected operational or technical difficulties?		
System restart and recovery procedures for use in the event of system failure?		
Are system resources reviewed to ensure adequate capacity is maintained?		
Are anti-virus products used?		
Is there an anti-virus / malware policy or process?		
Has anti-virus software been installed on the following:		
Workstations?		
Mobile devices (e.g., PDA, blackberry, palm pilot, etc.)?		
Windows servers?		
UNIX and UNIX-based systems (e.g., Linux, Sun Solaris, HP-UX, etc.)?		
Email servers?		
Are workstation scans scheduled daily?		
Are servers scans scheduled daily?		
Can a non-administrative user disable anti-virus software?		
Are system backups of Target Data performed?		
Is backup of Target Data performed:		
Real-time?		
Daily?		
Weekly?		
Question/Request	**Response**	**Additional Information**
Monthly?		
Never?		
Are there external network connections (Internet, Intranet, Extranet, etc.)?		
Are network devices regularly reviewed and/or monitored for continued compliance to security requirements?		
Is every connection to an external network terminated at a firewall?		
Are network devices configured to prevent communications from unapproved networks?		
Are network traffic events logged to support historical or incident research?		
Are network system audit log sizes monitored to ensure availability of disk space?		
Are firewall rule sets and network access control lists reviewed:		
Every three months or less?		
Between three months and one year?		
Never?		
Is there a Network Intrusion Detection/Prevention System?		
Is there a network Intrusion Detection system?		
Is there a Network Intrusion Prevention System?		
Is wireless networking technology used?		
Is there wireless networking policy?		
Has the policy been published?		
Are wireless connections authenticated?		
Are logins via wireless connections logged?		
Are wireless connections encrypted?		
If so, what encryption methodology is used:		
WEP?		
WPA?		
WPA2?		
Is data sent or received (physical or electronic)?		
Is Target Data transmitted electronically?		
Is all Target Data encrypted while in transit?		
Question/Request	**Response**	**Additional Information**
Is there a policy or procedure to protect data for the following transmissions:		
Electronic file transfer?		
Transporting on removable electronic media?		
Email?		
Paper documents?		
Instant Messaging?		
File sharing?		
Is e-mail used?		
Is there a policy to protect Target Data when transmitted through email?		
Is automatic forwarding of email messages prohibited?		
Is Target Data transmitted through email encrypted?		

Access Control

For each question choose either Yes, No or N/A. If N/A is chosen, an explanation is mandatory.

Question/Request	Response	Additional Information
Are unique user IDs used for access?		
Are inactive userID(s) deleted or disabled after:		
Every three months or less?		
Three months to four months?		
Greater than four months?		
Never?		
Is there a process to review; access is only granted to those with a business need to know?		
Are reviews of privileged systems conducted to ensure unauthorized privileges have not been obtained?		
Do all users have a unique userID when accessing applications?		
Is the use of system utilities restricted to authorized users only?		
Are passwords required to access systems holding, processing, or transporting Target Data?		
Is there password policy for systems holding, processing, or transporting Target Data?		
Are password files and application system data stored in different file systems?		
Are users forced to change the password upon first logon?		
Are temporary passwords unique to an individual?		
Do temporary passwords expire after:		
10 days or less?		
10 days to 30 days?		
Greater than 30 days?		
Never?		
Is password reset authority restricted to authorized persons and/or an automated password reset tool?		
Are users required to:		
Change passwords when there is an indication of possible system or password compromise?		

Question/Request	Response	Additional Information
Change passwords at regular intervals?		
Not include passwords in automated logon processes? (e.g., stored in a macro or function key)?		
Logoff terminals, PC or servers when the session is finished?		
Lock (using key lock or equivalent control) when systems are unattended?		
Is remote access permitted into the environment?		
Is there a remote access policy?		
What type of hardware can users use for remote access into the network:		
Laptop?		
Desktop?		
PDA?		

Incident Event and Communications Management

For each question choose either Yes, No or N/A. If N/A is chosen, an explanation is mandatory.

Question/Request	Response	Additional Information
Is there an Incident Management program?		
Is there a documented incident management policy?		
Is there an Incident Response Plan (formal or informal)?		
Does the Incident Response Plan / Program include:		
A formal reporting procedure for any information security event(s)?		
An escalation procedure?		
A feedback processes to ensure that those reporting information security events are notified of results after the issue has been dealt with and closed?		
Event reporting forms to support the reporting action, and to list all necessary actions in case of an information security event?		
Security weaknesses reporting?		
Are there procedures to address the following:		
Unauthorized physical access?		
Information system failure or loss of service?		
Malware activity (anti-virus, worms, Trojans)?		
Breach or loss of confidentiality?		
Unauthorized logical access?		
Unauthorized use of system resources?		
Repair?		
Recovery?		

Business Continuity and Disaster Recovery

For each question choose either Yes, No or N/A. If N/A is chosen, an explanation is mandatory.

Question/Request	Response	Additional Information
Is there a Business Continuity/Disaster Recovery (BC/DR) program?		
Is there a documented policy for business continuity and disaster recovery?		
Is there a Business Continuity plan?		
Is there a Disaster Recovery plan?		
Has an internal group evaluated the BC/DR Program within the past 12 months?		
Has an independent external third party evaluated the BC/DR Program within the past 12 months?		
Is a Business Impact Analysis conducted at least annually?		
Does the Business Impact Analysis address the following:		
Business Process Criticality (high, medium, low or numerical rating) that distinguishes the relative importance of each process?		
Recovery Time Objective?		
Recovery Point Objective?		
Maximum allowable downtime?		
Costs associated with downtime?		
Impact to clients?		

Liite 2. Tietojen tärkeysluokitus

Taulukko 1. Tietojen luokittelun esimerkki (Laaksonen, Nevasalo & Tomula 2006, 157.)

Tiedon tärkeysluokka/ käsittelysääntö	**Julkinen**	**Sisäinen**	**Luottamuksellinen**	**Salainen**
Merkintä	Merkintä julkinen vähintään dokumentin etusivulla	Merkintä sisäinen vähintään dokumentin etusivulla	Merkintä luottamuksellinen vähintään dokumentin etusivulla	Merkintä salainen dokumentin jokaisella sivulla
Tiedonjakelu	Kaikille halukkaille	Kaikille yrityksen työntekijöille	Rajoitetulle määrälle yrityksen työntekijöitä	Erittäin rajoitetulle määrälle yrityksen työntekijöitä
Tiedon salaus	Ei pakollista	Ei pakollista	Pakollista, jos kuljetetaan tai lähetetään yrityksen ulkopuolelle	Aina pakollista
Lähetys sähköpostilla	Sallittu	Sallittu	Sallittu salattuna	Sallittu salattuna
Tietojen tallennus	Ei rajoituksia	Yrityksen keskitetyissä tietojärjestelmissä	Yrityksen keskitetyissä tietojärjestelmissä, asianmukaiset käyttöoikeudet	Yrityksen keskitetyissä tietojärjestelmissä, asianmukaiset käyttöoikeudet ja tiedon salaus
Tietojen tallennus siirrettäville muistivälineille	Sallittua	Sallittu, salaus suositeltava	Sallittua salattuna	Sallittu salattuna

Liite 3. Toimitilojen tärkeysluokitus

Taulukko 1. Eri tärkeysluokkiin kuuluvien tilojen perussuojausvaatimukset (Miettinen 1999, 179.)

Tärkeysluokka/ Suojausvaatimus	**Ei tärkeä tila**	**Tärkeä tila**	**Erittäin tärkeä tila**
Pääsyoikeus tilaan	Kaikilla henkilöillä	Niillä, jotka tarvitsevat pääsyoikeutta tilaan työtehtävien suorittamiseksi	Niillä, jotka tarvitsevat pääsyoikeutta tilaan työtehtävien suorittamiseksi
Henkilön identiteetin tunnistaminen	Henkilö, jolla on oltava kuvallinen henkilökortti, joka näytetään pyydettäessä	Henkilöllä on oltava kuvallinen henkilökortti, joka pidetään näkyvissä	Henkilöllä on oltava kuvallinen henkilökortti, joka pidetään näkyvissä
Kulunvalvonta	Tilassa mekaaninen lukitus, ei turvalukkoa	Tilassa mekaaninen lukitus sekä erillinen mekaaninen turvalukko	Tilassa kaikki käynnit rekisteröivä sähköinen kulunvalvonta
Murtosuojaus	Tilassa ei erillistä murtosuojausta	Tilassa automaattinen rikosilmoitinjärjestelmä	Tila vartioitu ja tilassa automaattinen rikosilmoitinjärjestelmä
Palosuojelu	Tilassa käsisammutin	Tilassa automaattinen paloilmoitinjärjestelmä sekä käsisammutin. Tila osittain palo-osastoitu	Tilassa automaattinen paloilmoitin- sekä sammutinjärjestelmä. Tila jaettu kattavasti palo-osastoihin

Liite 4. Supistettu tietoturvakartoitus (salattu)