Tietoturvapolitiikan kehittäminen Sulavalle

Janne Jalava

2021 Laurea

Laurea-ammattikorkeakoulu

Tietoturvapolitiikan kehittäminen Sulavalle

Janne Jalava
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Toukokuu, 2021

Laurea-ammattikorkeakoulu **Tiivistelmä**

Turvallisuusalan koulutusohjelma

Tradenomi (AMK)

Janne Jalava

Tietoturvapolitiikan kehittäminen Sulavalle

Vuosi 2021 Sivumäärä 47

Tämän opinnäytetyön tavoitteena oli kehittää ja toteuttaa Sulavalle julkinen tietoturvapolitiikka. Opinnäytetyö toteutettiin toiminnallisena opinnäytetyönä käyttäen kvalitatiivisia tutkimusmenetelmiä tukemaan toiminnallista osuutta. Yrityksellä oli olemassa olevia valmiita dokumentteja liittyen tietoturvaan ja sen valvontaan, mutta niistä ei oltu koostettu yhtenäistä tietoturvapolitiikkaa. Sulavan toiveena oli saada tietoturvapolitiikasta julkinen versio, jota voidaan käyttää esimerkiksi yrityksen internetsivuilla. Opinnäytetyön tarkoituksena oli tuoda myös esille tietoturvapolitiikan kehittämiseen ja toteuttamiseen vaadittavia asioita sekä tukemaan tietoturvan kehittämisen prosesseja.

Vaikka opinnäytetyön lopullinen tuotos oli rajattu julkiseen tietoturvapolitiikkaan, oli tietoa etsittävä myös koko tietoturvan kehittämiseen. Tietoperustana opinnäytetyössä käytettiin alan kirjallisuutta, standardeja ja tietoturvapolitiikkamalleja. Tietoturvaprosessien toteuttamiseen esitettiin muutamia eri alalla käytettäviä malleja ja viitekehyksiä. Opinnäytetyössä käytettävät kvalitatiiviset menetelmät ovat kirjallisuuskatsaus, asiantuntija sekä benchmarking eli vertailuanalyysi.

Kirjallisuuskatsauksen avulla saatiin kerättyä tietoa, miten tietoturvapolitiikkaa kehitetään ja toteutetaan. Sen avulla saatiin teoriaa myös oikeanlaisten hyväksi havaittujen mallien ja viitekehysten käyttämiseksi. Kirjallisuuskatsauksessa tutkittiin myös ISO/IEC 27001 standardia tietoturvapolitiikan kehittämisen näkökulmasta. Asiantuntijahaastattelulla saatiin tietoa yrityksen nykyisestä tietoturvan tasosta sekä siihen kohdistuvista ongelmista ja haasteista. Vertailuanalyysiä käytettiin tutkimaan muiden organisaatioiden tietoturvapolitiikoissa olevia parhaita käytäntöjä ja malleja.

Tietoturvapolitiikan julkinen osa toteutettiin Sulavalle sen johtoryhmän hyväksymällä tasolla. Opinnäytetyötä tehdessä löydettiin yrityksen tietoturvapolitiikassa myös kehitettävää kokonaisuutena, vaikka opinnäytetyön lopputuotos eli julkinen tietoturvapolitiikka onkin julkaistavissa. Opinnäytetyön avulla voidaan lisäksi soveltaa erilaisia tietoturvapolitiikan kehittämismalleja.

Yrityksen tietoturvan toteutuksessa seuraavia kehittämiskohteita ovat tietoturvapolitiikan käytäntöön pano eli jalkautus, käyttäjien kouluttaminen sekä tietoturvatietoisuuden lisääminen.

Asiasanat: kontrollit, tietoturva, tietoturvapolitiikka

Laurea University of Applied Sciences **Abstract**

Degree Programme in Security Management

Bachelor's Thesis

Janne Jalava

Developing the Information Security Policy at Sulava

Year 2021 Pages 47

The objective of this thesis was to develop and implement a public information security policy for Sulava. The thesis was performed as a practice-based thesis using qualitative research methods to support the practice-based thesis study. The company had existing documents related to information security and its control, but they lacked a complete information security policy document. Sulava's wish was to have a public version of the security policy, which can be used, for example, on the company's websites. The purpose of the thesis was also to present the issues required for the development and implementation of an information security policy and to support information security development processes.

Although the final product of this thesis was limited to a public information security policy, additional information to improve overall information security was discovered. The theoretical framework in the thesis reviews literature in the information security field, standards and information security policy models. A few models and frameworks for the implementation of information security processes were presented. The qualitative methods used in the thesis are a literature review, an expert interview and benchmarking.

The literature review provided information on how to develop and implement an information security policy. The review also provided a theoretical framework for the use of the right types of well-tried models and frameworks. The literature review also examined the ISO/IEC 27001 standard from the perspective of information security policy development. The expert interview provided information about the current level of information security and the problems and challenges related to the organization's information security posture. Benchmarking was used to compare other organizations' information security policies to learn from and map best practices and models.

The public part of the information security policy was implemented for Sulava at the level approved by its management team. The need for further development of the information security policy as a whole was also discovered during the thesis process. With the help of the thesis, various information security policy development models can also be applied.

Next steps for the company are the implementation of the information security policy, user training and education, and information security awareness training.

Keywords: controls, information security, information security policy

Sisällys

1 Johdanto

Yritykset ovat jatkuvien tietoturvahyökkäyksien kohteena (Moore 2019). Yrityksillä on hallussaan tietoja asiakkaista ja liikesalaisuuksista, joiden vuotaessa yritykselle voi aiheutua valtavia haittoja niin liiketoimintaan kuin imagoonkin. Viime vuosien aikana mediasta on voinut lukea ja nähdä useita tapauksia, jossa yrityksen tietojärjestelmiin on murtauduttu ja hyökkääjät ovat saaneet käsiinsä yrityksen säilyttämää arkaluontoista tietoa. Esimerkiksi viime vuonna 2020 ilmi tullut psykoterapiakeskus Vastaamoon kohdistunut tietomurto herätti osan yrityksistä varmistamaan omaan tietoturvaansa liittyviä asetuksia ja käytäntöjä. (Kumpula 2020; Kärkkäinen 2020.)

Surullinen tosiasia on, että monilla organisaatioilla on valitettavasti puutteellinen tietoturva- ja reagointisuunnittelu. Turvallisuusalalla toimivat tarkkailijat ovat todenneet, että vähittäiskaupan yritys Targetiin kohdistunut tietoturvavuoto joulukuussa 2013 on ollut paljon pahempi, miltä se on aluksi näyttänyt. Jokaisen ilmoitetun tietoturvavuodon jälkeen tietoja vuoti lisää, mikä viittaa siihen, että yritys peitteli ja valehteli tosiasioista, tai ei osannut selvittää ja ratkaista ongelmaa. (Whitman & Mattord 2006, 128.)

Puutteellisilla tietoturvapolitiikoilla ja tietoturvatietoisuudella on vahva yhteys henkilöstöstä lähtöisiin vuotoihin ja rikkomuksiin. Vuonna 2013 tehdyssä tutkimuksessa todettiin, että yli 90 prosentissa yrityksistä, joissa tietoturvapolitiikka ymmärrettiin huonosti, on vastaavanlaisia rikkomuksia. Silti monilta yrityksiltä puuttuu perustasolla tehty tai päivitetty tietoturvapolitiikka. Monilla organisaatioilla tietoturvapolitiikat ovat edelleen tehottomia, koska ne joko puuttuvat kokonaan, ovat epätarkkoja, niitä ei noudateta tai ne ovat epäselviä. (Landoll 2016.)

Tietoturvapolitiikan avulla on tarkoitus luoda selvät käytännöt tiedon turvaamiseksi. Se ohjaa käyttäjien toimintaa ja antaa suuntaviivat tietojärjestelmien ja laitteiden suojaamiseksi. Hyvin suunniteltu ja toteutettu tietoturvapolitiikka luo perustan yrityksen turvalliselle tietojen käsittelylle ja säilytykselle. Sen avulla määritellään tietoturvan käytännöt, vastuualueet ja sanktiot. (Whitman & Mattord 2006.)

Julkisen tietoturvapolitiikan tarkoituksena on viestiä sisäisille ja ulkopuolisille toimijoille yrityksen tavasta hoitaa tietoturvaan liittyviä asioita. Julkisella tietoturvapolitiikalla tarkoitetaan esimerkiksi yrityksen internetsivuilla olevaa tiedotetta, uutista tai muuta artikkelia, joka on julkisesti saatavilla. Julkinen tietoturvapolitiikka ei ole yhtä yksityiskohtainen kuin yrityksen sisäiseen käyttöön tarkoitettu tietoturvapolitiikka.

1.1 Sulava

Sulava Oy on vuonna 2010 perustettu konsultointiyritys, joka tarjoaa konsultointia ja koulutusta, jotka kohdistuvat pääsääntöisesti Microsoftin pilvipalveluihin. Sulavalla on noin 130 työntekijää, joista suurin osa työskentelee yrityksen päätoimipisteessä Suomessa. Työntekijöillä on vapaus tehdä töitä siellä, missä he itse parhaaksi näkevät. Sulavalla on toimipisteet Helsingissä, Kuopiossa ja Dubaissa, jossa sijaitsee myös Sulavan tytäryhtiö. Sulava haluaa auttaa asiakkaitaan hyödyntämään Microsoftin pilviteknologioita liiketoiminnassa. Sulavan arvoihin kuuluu parhaaksi pyrkiminen, osaamisen jakaminen, huolenpito sekä yhdessä menestyminen. (Sulava 2020.)

2 Tutkimusongelma ja kehittämistehtävä

Kananen (2014) toteaa, että opinnäytetyö tarvitsee aina tutkimusongelman, koska ilman sitä tieteellistä tutkimusta ei voida toteuttaa. Ongelma on määriteltävä ja tarvittaessa ongelma pitää muodostaa, jos ongelma puuttuu. Tutkimusongelma on myös määriteltävä ja rajattava tarkasti, koska se ohjaa opinnäytetyön tekemistä alusta loppuun. Tarkan ongelman määrittelyn avulla saadaan muodostettua oikeanlaisia tutkimuskysymyksiä. Tutkimusongelman avulla tuodaan esille opinnäytetyölle tarkoitus sekä sen tavoitteet. (Kananen 2014, 32.)

Kehittämistehtävän kohteena on Microsoftin pilvipalveluita kouluttava ja konsultoiva yritys Sulava Oy, jolla on tarve kehittää yrityksen tietoturvallisuutta sekä viestiä siitä ulkopuolisille toimijoille ja asiakkaille. Yritys tarvitsee yhtenäistä tietoturvapolitiikkaa, jota voi viestiä myös julkisesti. Julkisella viestinnällä tässä tarkoitetaan yrityksen internetsivuja sekä muuta julkiseksi tarkoitettua materiaalia, johon voidaan liittää asioita tietoturvapolitiikasta.

Sulavan tietoturvavastaava Bergius (2020) kertoo, että Sulavalla ei ole olemassa selkeää yhtenäistä tietoturvasuunnitelmaa, jossa olisi eriteltynä tietoturvapolitiikan julkinen osuus. Yhtenäisen materiaalin puuttuminen hankaloittaa työntekijöiden sekä tietoturvallisuudesta vastuussa olevien toimintaa tietoturvaan liittyen. Heidän toiveena on luoda kokonaan yhtenäinen sisäinen ja julkinen tietoturvapolitiikka.

Tätä opinnäytetyötä suunnitellessa on tullut esille, että Sulavalla on useita eri dokumentteja, mutta ne eivät ole helposti työntekijöiden saatavilla. Tämän vuoksi niiden päivittäminen on myös haasteellista. Sulava on toivonut, että julkisen tietoturvapolitiikan avulla voitaisiin käynnistää myös näiden asioiden kehittäminen. (Bergius 2020.)

2.1 Tutkimuskysymykset

Tämän opinnäytetyön suuntaa ohjaavat seuraavat tutkimuskysymykset, joiden avulla pyritään selvittämään seuraavia asioita.

1. Millainen on hyvä julkinen tietoturvapolitiikka, josta asiakkaat, yhteistyökumppanit ja muut ulkoiset toimijat saavat riittävän selkeän kuvan Sulavan tietoturvapolitiikasta?
2. Miten varmistetaan, että tietoturvapolitiikka pysyy ajan tasalla ja on helposti saatavilla?

Näiden tutkimuskysymyksien avulla voidaan ohjata tämän opinnäytetyön suuntaa. Niihin vastaamalla luodaan Sulavalle julkinen tietoturvapolitiikka sekä tietoa tietoturvapolitiikan kehittämisestä ja sen ylläpidosta. Tämän opinnäytetyön tavoitteesta, lopullisesta tuotoksesta sekä menetelmistä, joilla tutkimuskysymyksiin etsittiin vastausta, on kerrottu tarkemmin seuraavissa luvuissa.

2.2 Rajaus ja tavoitteet

Hirsjärvi, Remes ja Sajavaara (2009) toteavat, että aloitteleva tutkija saattaa helposti valita liian laajan aiheen tutkittavaksi. Tutkittavan aiheen rajaaminen on siis tärkeää. Aihe tulisi rajata niin selvästi, että ulkopuolinen lukija pystyy ymmärtämään, mihin tutkimus keskittyy. Kvalitatiivisen tutkimuksen aiheen rajaamista voi joutua tekemään myös tutkimuksen edetessä eli tutkimusaiheen rajaaminen tulisi olla joustavaa. Aiheen rajausta ohjaa myös kirjallisuuskatsauksen pohjalta tutkittu tieto. (Hirsjärvi, Remes & Sajavaara 2009, 81-82.)

Tämä opinnäytetyö keskittyy vain julkiseen tietoturvapolitiikkaan ja sen materiaaliin. Sulavalla on tavoitteena jatkaa tietoturvan kehittämistä ja luoda laajempi tietoturvapolitiikka, joka sisältää sisäisen ja ulkoisen tietoturvapolitiikan. (Bergius 2020.)

Rajaus on tehty yhdessä Sulavan tietoturvavastaavan kanssa. Sen lisäksi on sovittu, että jatkotoimenpiteenä voitaisiin julkista tietoturvapolitiikkaa hyödyntäen tehdä laajempi sisäinen tietoturvapolitiikka sekä siihen liittyvät muut työt, kuten työntekijöiden kouluttaminen ja perehdyttäminen sekä muiden tietoturvamateriaalien luominen. Julkisen tietoturvapolitiikan avulla yritys pystyy osoittamaan oman tietoturvatason muille toimijoille. (Bergius 2020.)

Tämän opinnäytetyön tavoitteena on kerätä tietoa onnistuneen tietoturvapolitiikan toteutuksesta sekä siihen liittyvistä standardeista ja ohjeista. Näiden avulla kehitetään Sulavalle tietoturvapolitiikan julkista osaa ja kerätään tietoa tietoturvapolitiikan kehittämiseksi ja ylläpitämiseksi. Opinnäytetyön lopputuloksena syntyy julkisen tietoturvapolitiikan dokumentti, jota Sulava voi hyödyntää ulkoisessa ja myöskin sisäisessä

viestinnässä. Tavoitteet on määritelty yhdessä Sulavan tietoturvavastaavan kanssa (Bergius 2020.)

3 Toteutus ja tutkimusmenetelmät

Tämä opinnäytetyö toteutetaan toiminnallisena työnä, jonka tuotoksena syntyy julkinen dokumentti yrityksen tavasta hoitaa tietoturvapolitiikkaa. Vilkka ja Airaksinen (2003, 9) kuvaavat toiminnallisen opinnäytetyön olevan konkreettinen tuotos. Sen tavoitteena on ohjeistaa ja opastaa käytännön toimintaa ammatillisella tavalla. Tuotoksena toiminnallisesta opinnäytetyöstä voi syntyä esimerkiksi ohje tai turvallisuusohjeistus, joka on tarkoitettu ammatilliseen käyttöön. Opinnäytetyössä on yhdistettävä käytännön tuotoksen eli produktin toteutus ja sen raportointi käyttämällä tutkimusviestinnän keinoja. (Vilkka & Airaksinen 2003.)

Tässä opinnäytetyössä käytetyt menetelmät ovat kvalitatiivisia eli laadullisia tutkimusmenetelmiä. Kananen (2014) kertoo, että laadullisten tutkimusmenetelmien avulla tutkitaan ja selvitetään ilmiötä syvällisemmin. Laadullisella tutkimuksella saadaan ilmiöstä paljon tarkempi kokonaiskuva ja voidaan kehittää uusia teorioita. Laadullisessa tutkimuksessa tavoitteena on selvittää ilmiötä ilman tilastoja tai määrällistä tietoa. Kvalitatiivisen eli laadullisen tutkimuksen avulla saadaan ilmiöstä mahdollisimman tarkka kuva. (Kananen, 2014.)

Vilkka ja Airaksinen (2003) toteavat, ettei toiminnallinen opinnäytetyö välttämättä vaadi tutkimusmenetelmien käyttöä samalla tavalla kuin tutkimuksellinen opinnäytetyö. Opinnäytetyön rajaaminen ja siihen kohdistuva aineiston ja tiedon keruumenetelmät on myös valittava tarkasti. Toiminnallisen opinnäytetyön laajuus saattaa kasvaa liian suureksi, jos tutkimukseen sisällytetään myös selvitystyötä. Selvitystä voidaan tehdä silloin, kun asiasta ei ole tarpeeksi saatavilla olevaa tietoa. Opinnäytetyön mahdollistamiseksi tarvitaan niitä välttämättömiä tietoja, jotka silloin ovat saatavilla tai mahdollista selvittää. (Vilkka & Airaksinen 2003, 56-57.)

Tähän toiminnalliseen opinnäytetyöhön on sovellettu yllämainittuja Kanasen sekä Vilkan ja Airaksisen oppeja. Tämän opinnäytetyön aihetta tutkittiin myös kirjallisuuskatsauksen kautta. Tätä toiminnallista opinnäytetyötä tuetaan tutkimuksellisilla menetelmillä, jotka ovat kuvattu seuraavissa luvuissa.

3.1 Kirjallisuuskatsaus

Salminen (2011) kertoo, että kirjallisuuskatsauksen avulla kehitetään omaa ymmärrystä aiheeseen kokonaisuutena ja sitä kautta myös rakennetaan osaamisen teoriapohjaa.

Kirjallisuuskatsauksen avulla teorian arvioiminen on mahdollista. Sen avulla voidaan luoda kokonaiskuva jonkin asian ympärille. Kirjallisuuskatsauksen tavoitteena on kerätä tietoja muista tutkimuksista ja koota niistä yhtenäinen tieto, jonka avulla saadaan kehitettyä opinnäytetyön aiheena oleva tuotos. (Salminen 2011.)

Opinnäytetyöhön liittyvään kirjallisuuteen on perehdytty jo ennen itse opinnäytetyön aloittamista ja tutkimuskysymysten muodostamista. Hirsjärvi ym. (2009) kertovat, että varsinkin aloittelevan tutkijan olisi hyvä tutustua tutkittavaan aiheeseen liittyvään kirjallisuuteen hyvissä ajoin (Hirsjärvi ym. 2009). Tämän opinnäytetyön kirjallisuuskatsaus on toteutettu kuvailevana kirjallisuuskatsauksena. Tätä opinnäytetyötä tehdessä on keskitytty tietoturvallisuuteen liittyvään kirjallisuuteen, tietoturvapolitiikkoja käsitteleviin kirjoihin, standardeihin, tiivistelmiin, valmiisiin tietoturvapolitiikkapohjiin ja muihin aiheeseen liittyviin dokumentteihin.

3.2 Asiantuntijahaastattelu

Hirsjärvi ym. (2009) kertovat haastattelun sopivan hyvin laadulliselle opinnäytetyölle. Se on muita tiedonkeruumuotoja joustavampi ja sopii monenlaisiin tutkimustarkoituksiin. Haastattelu mahdollistaa joustavan aineiston keruun. Haastattelussa ei ole välttämätöntä käyttää tarkasti suunniteltua lomaketta vaan ainoastaan. Kysymyksiä ei myöskään esitetä tietyn järjestyksen mukaisesti. Haastattelua voidaan helposti myös ohjata eri suuntiin sen edetessä. (Hirsjärvi ym. 2009.)

Tämän opinnäytetyön asiantuntijahaastattelun tarkoituksena on selvittää yrityksen tämän hetkinen tietoturvapolitiikan tilanne ja kerätä aineistoa opinnäytetyötä varten. Asiantuntijahaastattelun kohteena on Sulavan tietoturvavastaava. Haastatteluita tehtiin useampia, mutta vastaajana oli aina sama asiantuntija, jolla oli tarvittava tieto yrityksen tietoturvaan liittyvistä dokumenteista ja käytännöistä. Haastattelulla pyrittiin selvittämään, millaisia asiakirjoja yrityksellä on jo tehtynä ja miten niitä käytetään, sovelletaan ja päivitetään. Tärkeässä osassa haastattelun aiheena oli myös tietoturvapolitiikkaan liittyvän materiaalin saatavuus.

Haastattelun avulla saadaan kerättyä aineistoa, jota ei voisi saada ilman yrityksen työntekijöiden haastatteluita. Osa haastatteluista saaduista tiedoista olisi voitu kerätä myös lomakehaastatteluna, mutta joustavuuden puuttuminen heikentäisi tiedon laadukkuutta. Osa tiedoista olisi voinut jäädä haastattelijalta pyytämättä, jos lomaketta ei olisi suunniteltu riittävän tarkasti. Joustavammalla haastattelutavalla haastattelua pystytään ohjaamaan teemojen avulla ja haastattelija pystyy vuorovaikutteisesti syventämään kysymyksiä aihealueista haastateltavan antamien vastauksien perusteella. Hirsjärvi & Hurme (2009) toteaa myös lomakehaastattelussa olevan vastaamatta jättämisen riski. Vastaanottaja ei välttämättä vastaa lomakkeeseen tai vastaa vain hyvin lyhyesti. (Hirsjärvi ym. 2009.)

Vilkka & Airaksinen (2003) toteavat, että haastattelu sopii hyvin toiminnalliseen opinnäytetyöhön. Haastatteluita ei ole myöskään välttämätöntä litteroida yhtä tarkasti kuin tutkimuksellisessa opinnäytetyössä. Haastattelun avulla saadut tärkeimmät asiat voidaan kerätä ja keskittyä olennaiseen tietoon. (Vilkka & Airaksinen 2003, 63-64.)

Tämän opinnäytetyön tehdyn asiantuntijahaastattelun litterointia ei tehdä tavallisen tutkimuksellisen opinnäytetyön tasolla, kun otetaan huomioon, mitä Vilkka ja Airaksinen (2003) kertovat haastattelusta toiminnallisessa opinnäytetyössä (Vilkka & Airaksinen 2003). Haastattelun tarkoituksena on kerätä tietoa yrityksen olemassa olevista dokumenteista liittyen tietoturvaan ja tietoturvapolitiikkaan. Haastattelussa saatuja tietoja on kirjattu ylös, mutta haastattelua ei ole litteroitu tarkasti. Itse haastatteluiden sisältö ei ole välttämättä kuvannut tietoturvan nykytilannetta, vaikka osittain sitäkin käsiteltiin.

3.3 Benchmarking

Patterson, Keppler ja Mapson (1996) toteavat benchmarkingin eli vertailuanalyysin sopivan sitä tarvitseville yksilöille ja organisaatioille. Vertailuanalyysin tarkoituksena on oppia muilta ja vertailla muiden kokemuksia ja tuotoksia. Analyysistä saatua tietoa voidaan hyödyntää omassa toiminnassa tai tuotoksessa (Patterson ym. 1996). Myös Tuulaniemi (2011), Kozak (2004) ja Tuominen (2016) kuvaavat vertailuanalyysia samalla tavalla (Tuulaniemi 2011; Kozak 2004; Tuominen 2016).

Patterson ym. (1996) kertoo vertailuanalyysin olevan hyödyllinen tapa kehittää organisaation prosesseja oppimalla muiden kokemuksista. Analyysi aloitetaan arvioimalla ensin omaa toimintaa ja prosesseja. On olennaista löytää prosessin kehityskohteet ja haasteet. Organisaation prosessien vahvuudet tulisi myös selvittää. (Patterson ym. 1996.)

Tuulaniemi (2011) kertoo vertailuanalyysillä olevan paljon hyötyjä. Hän kuvaa vertailuanalyysia vahvasti palvelumuotoilun näkökulmasta. Vertailuanalyysin avulla voidaan hyödyntää muiden löytämiä hyviä käytäntöjä ja toimialariippumatonta logiikkaa omissa toiminnoissa. Vertailuanalyysin avulla voidaan myös löytää ne virheet, joilta voidaan välttyä oppimalla muilta. (Tuulaniemi 2011.)

Analyysiä käyttämällä voidaan selvittää omien prosessien ja toimintatapojen suorituskyky ja vertailla niitä kilpailijoiden prosesseihin (Patterson ym. 1996). Tässä opinnäytetyössä vertailuanalyysin avulla on tarkoitus vertailla muiden yritysten julkisia tietoturvapolitiikkoja sekä löytää niistä toimivimmat ratkaisut.

Tuominen (2011) jakaa vertailuanalyysin kohteet neljään eri kategoriaan, jotka ovat sisäinen, kilpailijat, toimiala ja yleinen. Tämän jaon perusteella voidaan keskittyä vain tietynlaisiin organisaatioihin. Organisaatio voi tehdä vertailuanalyysin sisäisten toimintojen välillä,

keskittyä kilpailijoiden käytäntöihin, valita analyysin kohteeksi samalla toimialalla toimivat organisaatiot tai toimialariippumattomasti valita yleisesti kaikki ne organisaatiot, joissa on parhaat käytännöt. (Tuominen 2011.)

Vertailuanalyysiä tehdessä on huomioitava vertailun kohteena olevan tiedon lähde ja sen arkaluonteisuus. Analyysiä on tehtävä noudattaen lakeja sekä hyviä tapoja. Tarkoitus ei ole kuitenkaan vakoilla muita organisaatioita tai suoraan kopioida heidän tekemiä tuotteita tai käytäntöjä. Käytettäessä julkisesti saatavilla olevaa tietoa, voidaan myös välttyä näistä johtuvia konflikteja. (Tuulaniemi 2011; Kozak 2004.)

Tässä opinnäytetyössä vertailtiin anonyymisti viiden eri toimialoilla toimivien suurien organisaatioiden julkista tietoturvapolitiikkoja, jotka ovat saatavilla organisaatioiden verkkosivuilla tai muussa vastaavassa julkisessa sijainnissa. Kaikki analyysissä käytettävä tieto on siis julkisesti saatavilla olevaa tietoa. Näin vältyttiin arkaluontoisen tiedon käsittelyltä ja siihen liittyviltä haasteilta.

4 Tietoperusta

Toiminnallisen opinnäytetyön aineistona voidaan käyttää jo aiemmin tutkittua tietoa. Tiedonlähteeseen on kuitenkin suhtauduttava kriittisesti. Lähteen valintaa voidaan perustella sen luotettavuuden näkökulmasta. On pohdittava, onko lähde tunnettu ja asiantunteva. Tärkeää on myös tietää muita tietoja lähteestä, kuten lähteen ikä ja laatu. (Vilkka & Airaksinen 2003.)

Myös Hirsjärvi ym. (2009) toteavat lähdekriittisyyden olevan tärkeää tutkimusta tehdessä ja aineistoa valittaessa. Lähteen kirjoittajasta tulisi selvittää, onko hän tunnettu tutkija tai asiantuntija omalla alallaan. Tällä voidaan arvioida, voidaanko kirjoittajaan viitata vedoten hänen asiantuntijuuteen. Kirjoittajan arvostettavuutta voidaan selvittää esimeriksi sillä, että viitataanko hänen tuotoksiin muissa alan tunnetuissa julkaisuissa. Tämän lisäksi olisi syytä huomioida lähteen tuoreus sekä mistä lähteen alkuperäinen tieto on peräisin, kuinka luotettava lähde on, millaisessa asemassa lähteen julkaisija on. (Hirsjärvi ym. 2009.)

Tässä opinnäytetyössä käytettävien lähteiden luotettavuuden selvittäminen on tehty etsimällä tietoa lähteiden kirjoittajasta sekä taustasta. Kirjallisuuskatsauksen avulla selvitetty tietoperusta on useasta eri lähteestä, joissa kaikkien kirjoittajien tunnettavuus ja asiantuntijuus on pyritty selvittämään lähteen luotettavuuden selvittämiseksi.

4.1 Keskeiset käsitteet

Kananen (2015, 105) kertoo, että keskeisten käsitteiden määrittely on ilmiön ymmärtämisen kannalta tärkeää. Määrittelemällä käsitteitä, on helpompi ymmärtää ja hahmottaa alan ilmiöitä. Ilman selkeää käsitteiden määrittelyä asiat saattavat olla kokonaisuutena vaikeita ymmärtää. (Kananen 2015, 105.)

Tietoturvallisuus on tietojen turvaamista. Tietoturvallisuudella tarkoitetaan kolmijakoisesti tiedon luottamuksellisuutta, eheyttä ja saatavuutta. Tiedon on siis oltava saatavilla vain siihen oikeutetuilla henkilöillä. Tieto ei myöskään saa käsittelyn ja säilytyksen aikana muuttua, ellei sitä muuteta siihen tarkoitetuilla valtuuksilla. (ISO/IEC 27000 2017.)

Luottamuksellisuus tarkoittaa sitä, ettei tieto ei ole saatavilla luvattomille henkilöille, yhteisöille tai prosesseille. Tieto on saatavilla vain rajatulle ryhmälle tai yksilölle. Tieto on hyvä rajata vain niille, joilla on tarvetta lukea tai käsitellä tietoa ja se perustuu luottamuksellisuuteen. (ISO/IEC 27001 2017; Alexander, Finch, Sutton & Taylor 2013.)

Eheydellä tarkoitetaan, että tieto ei muutu vaan se säilyy sellaisenaan, ellei sitä tarkoituksenmukaisesti muuteta käyttämällä siihen tarkoitettua lupaa tai oikeutta. Tieto on hyödyllistä ainoastaan, jos se on kokonaista ja oikeaa. Tietoa voidaan muokata, päivittää tai poistaa ainoastaan erikseen annetuilla oikeuksilla. (ISO/IEC 27001 2017; Alexander, Finch, Sutton & Taylor 2013.)

Saatavuudella tarkoitetaan tiedon olevan saatavilla siihen oikeutetuilla henkilöillä silloin kun tietoa tarvitaan. Tieto, joka ei ole saatavilla tarvittaessa ja vaadittaessa, ei ole tietoa vaan pelkkää merkityksetöntä dataa. (ISO/IEC 27001; Alexander, Finch, Sutton & Taylor 2013.)

Tietoturvapolitiikka on johdon toimittama kirjallinen ohjeistus, joka antaa tietoa työntekijöille ja muille työpaikalla oleville henkilöille oikeanlaisesta ja sopivasta tiedon ja tietovarojen käytöstä (Whitman & Mattord 2016, 140). Second Nature Securityn (2020) mukaan tietoturvapolitiikka on yleensä kirjallinen julkinen dokumentti, jossa kuvataan yrityksen tapaa hoitaa tietoturvaan liittyviä asioita. Julkisella osuudella viestitään asiakkaille ja sidosryhmille yrityksen tietoturvallisuudesta. Sen avulla yritys voi näyttää, miten hyvin tietoturvallisuus on otettu huomioon. Hyvällä tasolla oleva tietoturvallisuus on hyödyksi organisaatiolle myös ulospäin. Julkista tietoturvapolitiikkaa on hyvä näyttää asiakkaille ja muille ulkopuolisille toimijoille. Julkinen osuus on myös työntekijöiden saatavilla ja se ohjaa heidän ja yrityksen toimintaa. (Second Nature Security 2020.)

Tietoturvapolitiikkaa käsitellään tarkemmin seuraavissa kappaleissa, joissa esitellään myös tietoturvapolitiikan suunnitteluun ja toteutukseen liittyviä malleja.

4.2 Tietoturvapolitiikka

Whitman ja Mattord (2016) kuvaavat politiikan olevan olennainen perusta toimivalle tietoturvatoiminnalle. Tehokasta tietoturvakoulutusta ja tietoisuutta ei voida aloittaa kirjoittamatta tietoturvapolitiikkaa, koska sen sisältämät politiikat ja käytännöt tarjoavat olennaisen sisällön myös koulutukseen ja tietoisuuden lisäämiseen tarkoitettuihin materiaaleihin. Tietoturvapolitiikan avulla organisaation johto ilmaisee tietoturvaan liittyvät asiat, joilla organisaatio pyrkii hallitsemaan työntekijöiden käyttäytymistä. Tietoturvapolitiikalla ohjataan työntekijöitä käyttämään palveluita ja tietoja asianmukaisesti ja turvallisella tavalla. Politiikan tarkoituksena on luoda tuottava ja tehokas työympäristö, jossa ei ole häiriötekijöitä tai sopimatonta toimintaa. Politiikka on dokumentti tai dokumenttien joukko, jotka sisältävät monia eri politiikkoja eli käytäntöjä. (Whitman & Mattord 2016, 141.)

Myös Alexander, Finch, Sutton ja Taylor (2013) toteavat, että kaikilla organisaatioilla tulisi olla tietoturvapolitiikka tietojen hallitsemiseksi. Politiikan avulla toimitusjohtaja tai organisaation johto ilmaisee tietoturvaan liittyviä riskejä ja toimia, jotka ehkäisevät, pienentävät ja käsittelevät riskejä. Politiikassa kuvataan myös vastuunjakoa eri ryhmien tai tahojen välillä. Organisaatiossa voidaan muodostaa erillinen ryhmä, jonka työnä on varmistaa tiedon suojaukseen liittyvien asioiden taso. (Alexander, Finch, Sutton & Taylor 2013, 45.)

Tietoturvapolitiikka on korkean tason lausunto organisaation arvoista, tavoitteista sekä yleinen lähestymistapa niiden saavuttamiseen. Politiikkoja tulisi päivittää ja tarkistaa säännöllisesti. Tietoturvapolitiikan tarkoituksena ei ole antaa yksityiskohtaisia tai erityisiä ohjeita näiden tavoitteiden saavuttamiseksi. Tämän vuoksi niiden kelvollisuus ja paikkansapitävyys tulisi säilyä, vaikka politiikkaa ei päivitettäisi jatkuvasti. Esimerkiksi käytäntö saattaa kuvata, että jokainen käyttäjä on vastuussa salasanojensa hallinnasta, vaikka siinä ei sanota tarkalleen, miten se tehdään. Politiikkojen noudattaminen organisaatiossa on kaikille pakollista. Politiikat eli käytännöt tulisi olla kaikkien niiden saatavilla, joilla on pääsy organisaation sisäisiin ja ulkoisiin tietoihin ja järjestelmiin. Tietoturvapolitiikan tulee olla sellaisessa käytettävässä muodossa, jonka käyttäjä pystyy myös helposti ymmärtämään. (Alexander ym. 2013, 45-46.)

Whitman ja Mattord (2016) kuvaavat, että suurin osa organisaatioista kehittää ja muodostaa politiikat kuvaamaan hyväksyttyjä ja ei-hyväksyttyjä toimintoja. Oikein määritellyt ja toteutetut politiikat ovat rinnastettavissa lakeihin, koska molempiin sisältyy rangaistuksia, oikeudellisia käytäntöjä ja seuraamuksia. Tämän vuoksi politiikat on laadittava yhtä huolellisesti kuin lait, jotta varmistetaan, että käytännöt ovat täydellisiä, asianmukaisia ja oikeudenmukaisia kaikille työpaikan työntekijöille. Keskeinen ero politiikan ja lain välillä on, että lakia voidaan soveltaa ja teosta rangaista, vaikka henkilö ei tietäisi lain olemassa olosta.

Työntekijä tai muu tietoturvapolitiikan piirin kuuluva voi vedota, ettei tiennyt politiikasta tai ymmärtänyt sen sisältöä. (Whitman & Mattord 2016, 75.)

Tämän vuoksi on olennaista, että tietoturvapolitiikka on jaettu kaikille henkilöille, joiden oletetaan noudattavan niitä. Kaikkien työntekijöiden on myös luettava ja ymmärrettävä sen sisältämät politiikat. Politiikkojen on oltava saatavilla sellaisella kielellä, jonka työntekijä voi ymmärtää. Tietoturvapolitiikasta voi olla saatavilla eri kieliversiona. Kaikkien on myös todettava ymmärtäneensä tietoturvapolitiikan esimerkiksi allekirjoittamalla lomake tai täyttämällä siihen liittyvä kyselymuotoinen testi. Tietoturvapolitiikka pitää myös yhtenäisesti pakottaa kaikille ilman minkään ryhmän, esimerkiksi johtoryhmän, erityiskohtelua. (Whitman & Mattord 2016, 75.)

Vasta kun kaikki ehdot täyttyvät, voidaan kohtuudella odottaa, että käytäntörikkomuksista voidaan rangaista asianmukaisesti pelkäämättä oikeudellista korvausta (Whitman & Mattord 2016, 75).

Oikein kehitettyjen ja toteutettujen politiikkojen eli käytäntöjen avulla voidaan toteuttaa lähes saumattomasti toimiva tietoturva työpaikalle. Tietoturvapolitiikka on yksi halvimpia hallintamenetelmiä, mutta niiden toteuttaminen ja noudattamisen takaaminen ovat usein vaikeita. Politiikkoihin liittyvät kontrollit maksavat vain johtoryhmän käyttämää aikaa ja vaivaa kontrollien luomiseen, hyväksymiseen ja kommunikointiin. Myös työntekijöiltä vaaditaan aikaa ja vaivaa käytäntöjen lukemiseen, ymmärtämiseen ja integroimiseen päivittäiseen toimintaansa. Johtoryhmän palkkaama ulkopuolinen tietoturvakonsultti tulee yleensä halvemmaksi kuin kalliit tekniset ohjaukset, kuten yritystason palomuurit. (Whitman & Mattord 2016, 141.)

Whitman ja Mattord (2016) esittävät seuraavat perussäännöt, joita on noudatettava tietoturvapolitiikkaa kehittäessä:

- Politiikan ei pitäisi koskaan olla ristiriidassa lain kanssa.
- Politiikkaa on kyettävä puolustamaan oikeudessa, jos sitä kyseenalaistetaan.
- Politiikkaa on tuettava ja hallinnoitava asianmukaisesti. (Whitman & Mattord 2016, 141.)

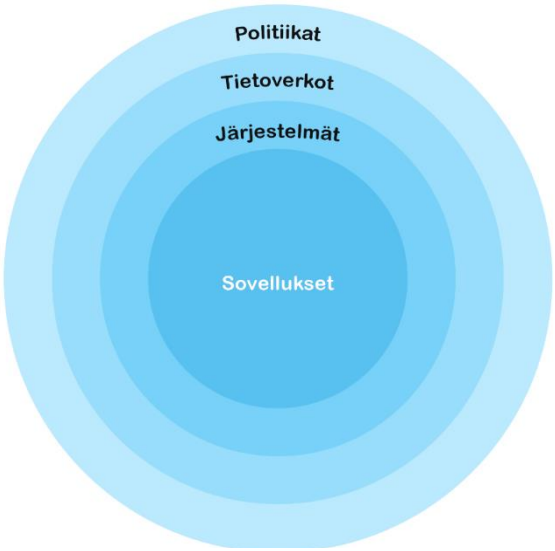
Organisaation on noudatettava omaa politiikkaansa ja sitä on sovellettava johdonmukaisesti (Whitman & Mattord 2016, 141).

Tietoturvapolitiikat on muodostettava organisaation oman tarpeiden mukaisesti. Ei ole järkevää luoda tai käyttää käytäntöjä, jotka eivät ole yhdenmukaisia organisaation linjauksen kanssa. Arkaluontoista tietoa käsittelevillä organisaatioilla ei pitäisi olla lievennettyjä tai kevennettyjä tietoturvapolitiikkoja. Toisaalta organisaatiota, jolla ei ole juurikaan tarvetta

vahvoihin toimenpiteisiin, palvelisi huonosti tiukat käytännöt. Vaikka politiikkojen tulisikin olla mahdollisimman täydellisiä ja kattavia, liian monien tai liian monimutkaisten politiikkojen olemassaolo voi aiheuttaa hämmennystä ja mahdollisesti uuvuttaa työntekijöitä. (Whitman & Mattord 2016, 142.)

Whitman ja Mattord (2016) esittelevät yhden toteutusmallin, joka korostaa politiikan roolia tietoturvaohjelmassa, on bull's-eye-, eli häränsilmämalli. Mallista on tullut laajalti tietoturva-asiantuntijoiden hyväksymä, koska sen avulla voidaan priorisoida monimutkaisia muutoksia. Tässä mallissa ongelmat käsitellään siirtymällä yleisestä yksityiskohtaisempaan, aloittaen aina politiikasta. Toisin sanoen painopiste on yleisissä ratkaisuissa yksittäisten ongelmien sijaan. Kuvio 1 havainnollistaa häränsilmämallin neljää kerrosta, jotka ovat seuraavat:

1. *Politiikat*. Tämä on häränsilmämallin uloin kerros. Se on ensimmäinen yleisnäkymä, joka useimmilla mallin käyttäjillä liittyy tietoturvallisuuteen. Tämä sisältää tietoturvapolitiikan, josta on kerrottu aiemmissa kappaleissa.
2. *Verkot*. Tämä on ympäristö, jossa julkisten verkkojen aiheuttamat uhat kohtaavat organisaation verkkoinfrastruktuurin. Viime aikoihin asti tietoturvan uskottiin usein olevan synonyymi verkkoturvallisuudelle.
3. *Järjestelmät*. Tämä sisältää palvelimet ja muut tietokoneet ja laitteet, ohjelmistot sekä prosessinohjaus- ja tuotantojärjestelmiin käytetyt järjestelmät.
4. *Sovellukset*. Nämä ovat sovellusjärjestelmiä, jotka vaihtelevat paketoiduista sovelluksista, kuten toimistoautomaatio- ja sähköpostiohjelmista huippuluokan yritysresurssipaketteihin ja organisaation kehittämiin mukautettuihin sovellusohjelmistoihin tai prosessinohjaussovelluksiin. (Whitman & Mattord 2016, 142-143.)



Kuvio 1: Häränsilmämalli (Whitman & Mattord 2016. 143.)

Huolimatta siitä, mitä mallia tietoturvapolitiikan kuvaamiseksi käytetään, politiikkoihin liittyviin kontrolleihin ei tulisi käyttää resursseja ennen kuin luotettavat ja oikeanlaiset toimivat tietoturvapolitiikat on kehitetty, tiedotettu ja otettu käyttöön. (Whitman & Mattord 2016, 143.)

Wood (2005) kuvaa politiikkojen olevan tärkeitä viiteasiakirjoja sisäisille tarkastuksille. Ne tukevat johtoa mahdollisten oikeudellisten riitojen ratkaisemiseksi. Politiikat kuvaavat johdon aikomuksia ja tahtotilaa tietoturvaan liittyen. Whitman ja Mattord (2016) kuitenkin huomauttavat, että politiikka ei ole vain hallintatyökalu lakisääteisten vaatimusten täyttämiseksi. On välttämätöntä suojella organisaatiota ja sen työntekijöiden työtä (Whitman & Mattord 2016, 143).

Tietoturvapolitiikka edustaa virallista lausuntoa organisaation tavasta huolehtia tietoturvasta. Sen jälkeen, kun politiikat on suunniteltu, luotu, hyväksytty ja otettu käyttöön, niiden toteuttamiseksi tarvittavat tekniikat ja menettelyt voidaan myös suunnitella, kehittää ja toteuttaa. Toisin sanoen, politiikat muodostavat joukon sääntöjä, jotka kuvaavat hyväksyttävää ja ei-hyväksyttävää käyttäytymistä organisaatiossa. Politiikoissa ei pitäisi määritellä yksityiskohtaisia teknisiä asioita kuten laitteiden ja ohjelmistojen määrittelyjä ja niiden toimintaan liittyviä asioita. Nämä tiedot tulisi sijoittaa muihin asiakirjoihin, kuten standardeihin, menettelyihin, käytännön toimintoihin ja ohjeisiin. Politiikat siis määrittelevät mitä voi tehdä ja mitä ei, kun taas muissa asiakirjoissa keskitytään, miten asioita kontrolloidaan. (Whitman & Mattord 2016, 144.)

Politiikoissa on myös määriteltävä rangaistukset kelpaamattomasta käytöksestä ja määriteltävä muutoksenhakuprosessi. Esimerkiksi organisaation, joka kieltää sopimattomien verkkosivustojen katselun työpaikalla, on pantava täytäntöön joukko ohjeita, jotka selventävät ja määrittelevät tarkalleen, mitä organisaatio tarkoittaa sopimattomana ja mitä organisaatio tekee väärinkäytösten estämiseksi. (Whitman & Mattord 2016.)

4.3 Tietoturvapolitiikan toteutus SDLC-menetelmällä

Kuten minkä tahansa suuren projektin kohdalla, tietoturvapolitiikan kehittämis- tai uudistamisprojektin tulisi olla hyvin suunniteltu, asianmukaisesti rahoitettu ja vahvasti hallinnoitava sen varmistamiseksi, että se valmistuu ajoissa budjetin sisällä. (Whitman & Mattord 2016, 124.)

Landoll (2016) toteaa mallien ja viitekehysten olevan olennainen osa tietoturvaprojektia toteuttaessa. Laajojen ja monimutkaisten tietoturvaprojektien tekeminen ja ylläpitäminen ilman mitään ohjaavaa mallia tai viitekehystä on erittäin haastavaa, ellei jopa mahdotonta. Tämän vuoksi olisi hyvä ottaa käyttöön jokin hyväksi todettu malli, jonka avulla

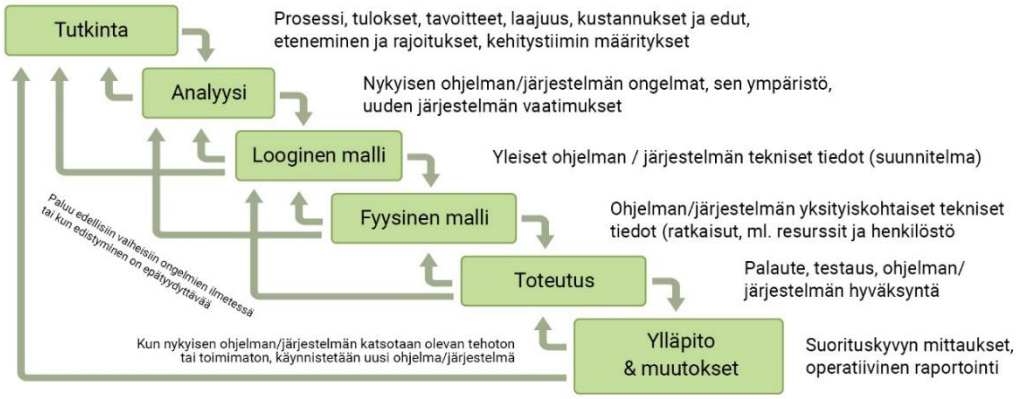
tietoturvaprojektia ohjataan. Landoll (2016) kuvaa neljä erilaista mallia tietoturvaprojektin ympärille. (Landoll 2016, 25-26.)

Vastaavasti Whitman ja Mattord (2016) kertovat yhdestä toimivasta mallista, joka mukautuu hyvin tietoturvaprojektin toteuttamiseen. Heidän kuvaama tapa saavuttaa tämä tavoite on käyttää SDLC-prosessia, joka tulee englannin kielisistä sanoista *systems development life cycle* eli järjestelmien kehittämisen elinkaari. (Whitman & Mattord 2016, 124.)

Järjestelmän kehittämisen elinkaari, jatkossa SDLC, on yleensä menetelmä tietojärjestelmän suunnittelulle ja toteuttamiselle organisaatiossa. Organisaatiot käyttävät usein onnistunutta metodologiaa uudelleen saatuaan siitä kokemusta. Tämä hyväksi havaittu lähestymistapa yhdistetään järkeviin projektinhallintakäytäntöihin projektin keskeisten virstanpylväiden kehittämiseksi, resurssien jakamiseksi, henkilöstön valitsemiseksi ja projektin tavoitteiden saavuttamiseksi tarvittavien tehtävien suorittamiseksi. Joskus järjestelmäkehityksen elinkaarta käytetään mukautettujen sovellusten kehittämiseen tai ostetun ratkaisun käyttöönottoon. Tämän menetelmän muunnelmaa, jota käytetään laajan turvallisuustilan luomiseen, kutsutaan SecSDLC-malliksi (*security systems development life cycle*) eli turvajärjestelmien kehittämisen elinkaareksi. (Whitman & Mattord 2016, 124.)

Järjestelmähankkeet voidaan aloittaa vastauksena tiettyihin ehtoihin tai ehtojen yhdistelmiin. Järjestelmän kehittämisen elinkaaren mukaisen projektin käynnistämisen impulssi voi olla tapahtumavetoinen - toisin sanoen vastaus joihinkin liike-elämän tapahtumiin, organisaation sisällä tai työntekijöiden, asiakkaiden tai muiden sidosryhmien joukkoon. Vaihtoehtoisesti se voisi olla suunniteltua - toisin sanoen huolellisesti kehitetyn suunnittelustrategian tulos. Kun organisaatio tunnistaa projektin tarpeen, SecSDLC-menetelmän tai jonkin muun valitun menetelmän avulla varmistetaan kehityksen hallittu ja kattava eteneminen. Jokaisen vaiheen lopussa suoritetaan tarkistus tai tietojen paikkansapitävyys, jonka aikana tiimi ja sen johtotason tarkastajat päättävät, pitäisikö projektia jatkaa, pitääkö se lopettaa tai ulkoistaa. Projektia voidaan myös lykätä, kunnes lisätuntemus tai organisaatiotieto on hankittu. (Whitman & Mattord 2016, 124.)

Seuraavan sivun kuvio 2 havainnollistaa SecSDLC-menetelmää, joka toteutetaan perinteisellä vesiputousmallilla. Termi "vesiputousmalli" kuvaa, että jokaisen vaiheen tulokset ja löydökset kuuluvat seuraaviin vaiheisiin ja toimivat uuden vaiheen lähtökohtana. Vaikka SecSDLC voi poiketa perinteisestä SDLC-menetelmästä useissa yksityiskohdissa, yleinen menetelmä on kuitenkin sama. SecSDLC-menetelmä sisältää uhkien ja niiden aiheuttamisen riskien tunnistamisen sekä valvontatoimien suunnittelun ja toteutuksen uhkien torjumiseksi ja riskien hallitsemiseksi. Prosessi muuttaa tietoturvan yhtenäiseksi projektiksi tai ohjelmaksi sen sijaan, että löydettäisiin listattuna vastaus useisiin erilaisiin uhkiin ja hyökkäyksiin. (Whitman & Mattord 2016, 124-125.)



Kuvio 2: SDLC-menetelmän vesiputousmalli (Whitman & Mattord 2016, 125.)

Vesiputousmallin lisäksi on olemassa useita muita malleja. Sen avulla on kuitenkin tarkoitus havainnollistaa projektin perusvaatimuksia. Nykyinen suositeltava käytäntö on käyttää menetelmää, joka on jaettu selvästi vaiheisiin. Vaiheistettu menetelmä edellyttää aiempien vaiheiden ja tuloksien säännöllistä tarkastelua. Jokainen vesiputousmallin vaihe mahdollistaa aiempiin vaiheisiin palaamisen, silloin kun havaitaan ongelmia tai edistyminen ei ole toivotulla tasolla. Koko prosessi muuttuu viimeisissä vaiheissa rekursiiviseksi, kun nykyinen lähestymistapa katsotaan tehottomaksi tai kehitystyö aloitetaan uudelleen. Vesiputousmallia ei ole tarkoitettu lopulliseksi lähestymistavaksi. Organisaatiot voivat käyttää myös muita suosimiaan malleja, kuten spiraali, ketterä kehitys tai nopea sovelluskehitys. Vesiputousmalli toimii kuitenkin hyvänä perustana ymmärtää yhteinen lähestymistapa uusien turvallisuusohjelmien kehittämiselle ja toteuttamiselle. (Whitman & Mattord 2016, 125.)

4.3.1 Tutkintavaihe

SecSDLC-mallin tutkintavaihe alkaa ylemmän johdon antamalla ohjeistuksella, jossa täsmennetään projektin prosessi, tulokset ja tavoitteet sekä budjetti ja muut projektin rajoitteet. Usein tutkintavaiheen alussa vahvistetaan ja luodaan organisaation turvallisuusohjelmaan perustuvat tietoturvapolitiikat. Vaiheen alussa määritellään myös ryhmät, jotka kootaan tutkimaan ongelmia ja tekemään tietoturvapolitiikkaan liittyviä määrityksiä. Lopuksi voidaan suorittaa analyysi, joka määrittää, onko organisaatiolla riittävät resurssit ja sitoutuminen onnistuneen tietoturvapolitiikan suunnittelun suorittamiseksi. (Whitman & Mattord 2016, 125.)

Whitman ja Mattord (2016) kertovat, että tutkimusvaiheen aikana politiikan kehittämisryhmän tulisi saavuttaa ainakin seuraavat asiat:

- Ylimmän johdon tuki, koska ilman sitä kaikilla hankkeilla on pienempi onnistumismahdollisuus. Vain ylimmän johdon tuella erityinen politiikka saa

ansaitsemansa huomion johtajien ja käyttäjien keskuudessa. Johtajien on pantava se täytäntöön ja käyttäjien noudatettava sitä.

- IT-hallinnon, erityisesti tietohallintojohtajan, tuki ja aktiivinen osallistuminen. Ainoastaan tietohallintojohtajan aktiivisella tuella teknologia-alueiden johtajat motivoituvat osallistumaan politiikan kehittämiseen ja tukemaan käyttöönottoa sen toteuttamisen jälkeen.
- Selkeiden tavoitteiden määrittely. Ilman politiikan päämäärien ja tavoitteiden yksityiskohtaista määrittelyä, jaoteltuina erillisiin odotuksiin, politiikalta puuttuu rakenne, jota se tarvitsee käyttöönoton saavuttamiseksi.
- Oikeiden henkilöiden osallistuminen ja varsinkin niiden, joihin suositellut käytännöt vaikuttavat. Kokoamalla oikeanlainen tiimi varmistetaan asianmukaisten henkilöiden osallistuminen. Tiimissä on oltava organisaation jokaisen osaston edustajia. Projekti tarvitsee myös oman projektipäällikön, jolla on kyky viedä projekti läpi alusta loppuun.
- Yksityiskohtainen kuvaus politiikan kehittämishankkeen laajuudesta ja perusteelliset arviot projektin kustannuksista ja aikataulusta. (Whitman & Mattord 2016, 166.)

Whitman ja Mattord (2016) toteavat, että valitettavan monet organisaation tietoturvaa kehittävät projektit käynnistetään vasta merkittävän tietoturvamurron tai -tapahtuman jälkeen. Vaikka olosuhteet eivät silloin ole välttämättä ihanteellisimmat organisaation tietoturvatilan kehittämiselle, tulisi sitä tekevän ryhmän kuitenkin korostaa, että parannuksia tietoturvan tilaan on tulossa. (Whitman & Mattord 2016, 125.)

4.3.2 Analyysivaihe

Analyysivaiheessa ryhmä tutkii tutkintavaiheen asiakirjoja. Tutkimusvaiheen aikana koottu kehitystiimi suorittaa alustavan analyysin olemassa olevista turvallisuuspolitiikoista tai ohjelmista sekä dokumentoiduista nykyisistä uhista ja niihin liittyvistä valvontatoimista. Tässä vaiheessa analysoidaan myös asiaankuuluvia oikeudellisia kysymyksiä, jotka voivat vaikuttaa tietoturvaratkaisun suunnitteluun. Yksityisyyden suojaa koskevat lait ovat yhä tärkeämpiä huomioita, kun tehdään päätöksiä henkilötietoja hallinnoivista tietojärjestelmistä. (Whitman & Mattord 2016, 124-15.)

Myös riskienhallinnalliset toimet alkavat tässä vaiheessa. Riskienhallinta on prosessi, jossa tunnistetaan, arvioidaan ja luokitellaan organisaation kohtaamia riskitasoja - erityisesti organisaation turvallisuuteen ja organisaation tallentamiin ja käsittelemiin tietoihin kohdistuvia uhkia. Analyysiprosessi alkaa tutustumalla vihollisiin eli uhkiin ja hyökkäyksiin, jotka kohdistuvat järjestelmiin, palveluihin ja käyttäjiin. Riskienhallinta on osa analyysivaihetta, jossa tunnistetaan haavoittuvuudet organisaation tietojärjestelmässä ja toteutetaan huolellisesti perustellut toimenpiteet kaikkien organisaation tietojärjestelmän

osien luottamuksellisuuden, eheyden ja saatavuuden varmistamiseksi. (Whitman & Mattord 2016, 126.)

Whitmanin ja Mattordin (2016) mukaan analyysivaiheen tulisi tuottaa ainakin uusi tai viimeaikainen riskiarviointi tai IT-auditointi, joka dokumentoi organisaation nykyiset tietoturvatarpeet. Tähän riskiarviointiin tulisi sisältyä kaikki menetykset, samoin kuin aikaisemmat oikeustapaukset, valitukset tai muut tiedot tietoturvaan liittyvistä negatiivisista tuloksista. Toisena asiana analyysivaiheessa pitäisi kerätä kaikki keskeiset viitemateriaalit, mukaan lukien kaikki nykyiset politiikat. Joskus tietoturvaan vaikuttavat poliittiset asiakirjat sijoitetaan organisaation eri osastoihin kuten henkilöstöosastoon sekä kirjanpito-, talous-, laki- tai yritysturvallisuusosastoihin. Näiden dokumenttien kerääminen on analyysivaiheessa olennaista. (Whitman & Mattord 2016, 165.)

Wood (2005) kertoo, että kaikki asiaankuuluvat ja nykyiset organisaatiota koskevat politiikat on kerättävä, jotta lisähuomiota tarvitsevat politiikat voidaan tunnistaa. Asiaankuuluvia politiikkoja ovat mm. sovellusjärjestelmien kehityskäytännöt, tietokoneiden toimintaperiaatteet, it-laitteiden hankintapolitiikat, henkilöstöpolitiikat, tietojärjestelmien laadunvalvontapolitiikat ja fyysisen turvallisuuden politiikat. Saman alan muiden organisaatioiden politiikat voivat tarjota myös hyödyllistä taustatietoa. Myös organisaatiota koskevien eri sidosryhmien politiikat tulisi kerätä. (Wood 2015.)

Organisaatiota saattaa houkuttaa jättää aiemmin mainittu tiedonkeruuprosessi ajan puuteen tai muun resurssin rajoituksen vuoksi. Tiedonkeruuta ei kuitenkaan tulisi lyhentää, koska tuotoksen hylkäämisprosentti kasvaa, jos tiedonkeruuprosessia lyhennetään merkittävästi. Tiedonkeruuprosessin avulla voidaan tunnistaa johdon asettamat odotukset tietoturvasta, olemassa olevat politiikat, politiikat, jotka on lisättävä tai muutettava, miten kontrollit noudattavat politiikkoja, organisaation kohtaamat haavoittuvuudet ja muut olennaiset taustatiedot. Jos näitä taustatietoja ei ole kerätty ja tutkittu, on todennäköistä, että kehitteillä oleva tietoturvapolitiikka ei vastaa organisaation todellisia tarpeita. (Wood 2005.)

Whitman ja Mattord (2016) kuvaavat, että analyysivaiheessa politiikan kehittämiseen keskittyvä ryhmä määrittelee organisaation tapaa suhtautua tai rajoittaa käyttäjien toimintoja. Tällainen jaottelu tehdään yleensä seuraaviin ryhmiin.

Mikä ei ole sallittua, on kiellettyä. Tällainen menetelmä tunnetaan myös termillä "whitelist" eli sallittujen lista. Menetelmä on näistä kahdesta ryhmästä rajoittavampi. Sen avulla kerrotaan kaikki sallitut toiminnot ja käyttäytymiset ja kaikki muut määrittelemättömät toiminnot ovat kiellettyjä tai vaativat jonkin erityisen luvan. Tällä lähestymistavalla voidaan haitata tavallista liiketoimintaa silloin, kun toimintoa ei ole huomioitu politiikkaa luodessa.

Mikä ei ole kiellettyä, on sallittua. Tämä menetelmä tunnetaan termillä "blacklist" eli kiellettyjen lista. Se määrittelee, mitkä toiminnot ja käyttäytymiset ovat kiellettyjä ja kaikki määrittelemättömät asiat ovat oletusarvoisesti sallittuja. Tämä lähestymistapa on helpompi toteuttaa, mutta se voi jättää käyttäjille mahdollisuuksia väärinkäyttäytymiselle. (Whitman & Mattord 2016, 167.)

Alexander ym. (2013) toteavat, että politiikkojen, standardien ja menettelyjen on oltava realistisia ja täytäntöönpanokelpoisia. Voi olla liian tiukkaa vaatia ihmisten pitävän kannettavia tietokoneitaan aina mukanaan. Paljon realistisempaa on vaatia, että kannettavaa tietokonetta ei saa jättää vartioimatta julkisella paikalla. Vastaavasti, jos määritetään teknisesti esimerkiksi kannettavien tietokoneiden salaus, on pohdittava, onko se mahdollista toteuttaa. Joissain tapauksissa politiikan noudattaminen ei ole mahdollista. On myös harkittava poikkeusten sallimista politiikasta erityisluvalla. (Alexander ym. 2013, 46.)

4.3.3 Suunnitteluvaihe

Suunnitteluvaiheen ensimmäinen tehtävä on varsinaisen politiikan sisältävän asiakirjan laatiminen. Yleensä sen tekee yksi henkilö, mutta se voidaan tehdä myös ryhmänä. Asiakirjan tulisi sisältää kaikki määritelmät ja rajoitukset tutkimus- ja analyysivaiheesta alkaen. Asiakirjan laatiminen voi olla haastava prosessi. Asiakirjan laatijan tuoksi on kuitenkin olemassa paljon erilaisia käytettävissä olevia resursseja, joita on kuvattu seuraavassa taulukossa. (Whitman & Mattord 2016, 167-168.)

INTERNET	Verkosta voi etsiä vastaavia tietoturvapolitiikkoja. Tarkoituksena ei kuitenkaan ole kopioida valmiita pohjia tai tuotoksia vaan etsiä ideoita oman politiikan sisältöön. Internetistä ei välttämättä kuitenkaan löydä politiikkoja, jotka liittyvä arkaluontoisiin sisäisiin asiakirjoihin tai prosesseihin.
HALLITUKSEN SIVUT	Sivustot sisältävät lukuisia esimerkkipolitiikkoja ja asiakirjoja niiden laatimiseksi. Yleensä hallituksen käytäntöjä saatetaan soveltaa valtion toimintoihin, mutta ne saattavat sopia joltain osin myös omaan organisaatioon.

AMMATTIKIRJALLISUUS	Useat kirjoittajat ovat julkaisseet aiheesta kirjoja. Näissä vaarana on ottaa liian isoja osia valmiita politiikkoja, jolloin lopputuotoksena on liian laaja asiakirja, jota ei voida julkaista eikä ottaa käyttöön.
VERTAISVERKOT	Muiden tietoturva-asiantuntijoiden on kirjoitettava samanlaisia politiikkoja omille organisaatioilleen. Osallistumalla tietoturva-asiantuntijoille suunnattuihin tapahtumiin voi verkostoitua ja saada sitä kautta tukea omaan projektiin.
AMMATTIKONSULTIT	Politiikka on yksi tietoturvan alue, jota voidaan varmasti kehittää yrityksen sisällä. Jos organisaatiolla ei kuitenkaan ole tarvittavaa asiantuntemusta tai vaikka tiimillä ei yksinkertaisesti ole aikaa oman politiikan kehittämiseen, ulkopuolisen konsultin palkkaaminen voi tällöin olla paras vaihtoehto. Ulkopuolinen konsultti ei kuitenkaan voi tuntea organisaationa niin perusteellisesti kuin organisaation oma työntekijä. Konsultilta voidaan myös pyytää yleiskuvallinen politiikka, jota voidaan muokata organisaation tarpeiden mukaan.

Taulukko 1: Käytettävissä olevia resursseja (Whitman & Mattord 2016).

SecSDLC-suunnitteluvaihe koostuu kahdesta erillisestä vaiheesta: loogisesta suunnittelusta ja fyysisestä suunnittelusta. Loogisessa suunnitteluvaiheessa tiimin jäsenet luovat ja kehittävät suunnitelman turvallisuudesta, ja he tutkivat ja toteuttavat tärkeimmät käytännöt, jotka vaikuttavat myöhempiin päätöksiin. Tässä vaiheessa kehitetään kriittiset varautumissuunnitelmat vaaratilanteiden varalta. Seuraavaksi toteutettavuusanalyysi määrittää, pitäisikö hanketta jatkaa yrityksen sisällä vai pitäisikö se ulkoistaa. (Whitman & Mattord 2016, 167-168.)

Fyysisessä suunnitteluvaiheessa ryhmän jäsenet arvioivat tietoturvasuunnitelman tukemiseen tarvittavan tekniikan, tuottavat vaihtoehtoisia ratkaisuja ja sopivat lopullisesta suunnitelmasta. Turvallisuussuunnitelmaa voidaan tarkistaa, jotta se pysyy synkronoituna

tarvittavien muutosten kanssa, kun fyysinen suunnittelu on valmis. Kriteerit onnistuneelle ratkaisulle valmistellaan myös tässä vaiheessa, samoin kuin teknisten ratkaisujen fyysinen suojaaminen. Tämän vaiheen lopussa toteutettavuustutkimuksen tulisi määrittää organisaation valmius ehdotettuun projektiin ja suunnittelu tulisi esittää. Siinä vaiheessa projekti voidaan hyväksyä tai olla hyväksymättä ennen toteutuksen aloittamista. (Whitman & Mattord 2016, 126.)

Tietoturvan tehtävänä on suojata tietojen luottamuksellisuus, eheys ja saatavuus sekä siirron, varastoinnin että käsittelyn aikana. Tämä tehtävä suoritetaan soveltamalla politiikkaa, koulutusohjelmia ja tekniikkaa. Johdon on määriteltävä kolmentyyppiset tietoturvapolitiikat, kuten National Institute of Standards and Technologyn (NIST) erityisjulkaisussa 800-100 määritellään: yleinen tai yrityksen tietoturvapolitiikka, aihekohtaiset tietoturvakäytännöt (ISSP) ja järjestelmäkohtaiset tietoturvakäytännöt. (Whitman & Mattord 2016, 126-127.)

Toinen olennainen osa tietoturvaohjelmaa on SETA-ohjelma (*Security Education, Training, and Awareness*), joka koostuu opettamisesta, kouluttamisesta ja tietoisuuden lisäämisestä. Osa tietoturvajohtajan vastuista SETA-ohjelmassa on valvontatoimenpide, jonka tarkoituksena on vähentää työntekijöiden tahattomia turvallisuusrikkomuksia. Kuten aiemmin mainittiin, työntekijöiden virheet ovat yksi suurimmista uhista tietovaroille. Tästä syystä on syytä käyttää resursseja ohjelmien kehittämiseen tämän ongelman torjumiseksi. SETA-ohjelmat on suunniteltu täydentämään jo käytössä olevia yleisiä tietoturva-alan koulutusohjelmia. SETA-ohjelma tulisi hyvän käytännön mukaisesti sisältyä SecSDLC-mallin toteutusvaiheeseen. Työntekijöiden koulutusta tulisi hallita sen varmistamiseksi, että kaikki työntekijät koulutetaan asianmukaisesti. (Whitman & Mattord 2016, 127.)

Suunnitteluvaihe jatkuu määrittelemällä kontrollit ja suojaukset, joita käytetään suojaamaan tietoa hyökkäyksiltä ja uhilta. Termejä kontrollit ja suojaukset käytetään usein keskenään. Kontrollit voidaan jakaa kolmeen ryhmään: hallinnalliset kontrollit, operatiiviset kontrollit sekä tekniset kontrollit. (Whitman & Mattord 2016, 127.)

Hallinnalliset kontrollit kattavat strategisten suunnittelijoiden suunnittelemat ja organisaation turvallisuushallinnon suorittamat turvallisuusprosessit. Ne asettavat tietoturvaprosessin suunnan ja laajuuden, ja antavat yksityiskohtaiset ohjeet sen suorittamiseen. Hallinnalliset kontrollit käsittelevät turvallisuussuunnitteluprosessin suunnittelua ja toteutusta sekä turvaohjelmien hallintaa. Ne käsittelevät myös riskienhallintaa ja turvatarkastuksia. Hallinnalliset kontrollit kuvaavat tarkemmin lain noudattamisen ja turvajärjestelmien koko elinkaaren ylläpidon välttämättömyyden ja laajuuden. (Whitman & Mattord 2016, 127.)

Operatiiviset kontrollit käsittelevät organisaation tietoturvan operatiivista toiminnallisuutta. Ne kattavat hallintatoiminnot ja alemman tason suunnittelun, kuten jatkuvuuden suunnittelun

ja haitallisten tapahtumien torjunnan suunnittelun. Lisäksi nämä valvontatoimet koskevat henkilöstön turvallisuutta, fyysistä turvallisuutta sekä tuotannon panosten ja tuotosten suojaamista. Operatiiviset kontrollit tarjoavat myös rakenteen käyttäjien, järjestelmänvalvojien ja johdon koulutus- ja tietoisuusohjelmien kehittämiselle. Ne käsittelevät myös laitteisto- ja ohjelmistojärjestelmien ylläpitoa ja tietojen eheyttä. (Whitman & Mattord 2016, 127.)

Tekniset kontrollit koskevat teknisiä lähestymistapoja, joita käytetään organisaation tietoturvan toteuttamiseen. Operatiiviset kontrollit käsittelevät tiettyjä operatiivisia kysymyksiä, kuten valvonnan kehittäminen ja integrointi liiketoimintoihin, kun taas tekniset kontrollit on valittava, hankittava ja integroitava organisaation it-rakenteeseen. Tekniset kontrollit sisältävät loogisia pääsynvalvontatoimia, kuten niitä, joita käytetään tunnistamiseen, todennukseen, valtuutukseen ja vastuuttamiseen. (Whitman & Mattord 2016, 127.)

Toinen suunnitteluvaiheen osa on olennaisten valmiusdokumenttien luominen. Eri suunnitelmat hyökkäysten, katastrofien tai muun tyyppisten tapahtumien käsittelemiseksi sisältävät liiketoiminnan jatkuvuussuunnitelmat, katastrofien palautumissuunnitelmat ja tapahtumien torjuntasuunnitelmat. Nämä tunnetaan usein yhdessä valmiussuunnitelmina, jotka ovat osa valmiussuunnitteluprosessia. Pienessä organisaatiossa tietoturva- tai järjestelmänvalvojalla voi olla yksi yksinkertainen suunnitelma, joka koostuu suoraviivaisesta joukosta median varmuuskopiointi- ja palautusstrategioita ja muutamasta palvelusopimuksesta yrityksen palveluntarjoajilta. (Whitman & Mattord 2016, 128.)

Suunnitteluvaiheessa käsitellään seuraavaksi fyysistä turvallisuutta, mikä edellyttää vastatoimenpiteiden suunnittelua, toteuttamista ja ylläpitoa organisaation fyysisten resurssien suojaamiseksi. Fyysisiin resursseihin sisältyy ihmiset, laitteet ja niitä tukevat järjestelmäelementit ja resurssit, jotka liittyvät tiedon hallintaan kaikissa sen muodoissa. Monia teknologiapohjaisia ohjauksia voidaan kiertää, jos hyökkääjä saa fyysisen pääsyn hallittaviin laitteisiin. Esimerkiksi, kun työntekijät eivät onnistu suojaamaan palvelinkonsolia, tietokoneessa oleva käyttöjärjestelmä tulee alttiiksi hyökkäyksille. Jotkin tietokonejärjestelmät on rakennettu siten, että kiintolevy ja sen sisältämät tiedot on helppo varastaa. Tämän seurauksena fyysiseen turvallisuuteen tulisi kiinnittää yhtä paljon huomiota kuin loogiseen turvallisuuteen turvajärjestelmien kehittämisen elinkaaressa. (Whitman & Mattord 2016, 128.)

Alexander ym. (2013) toteaa, että kaikkien yrityksen tietovaroja käyttävien on tiedettävä ja ymmärrettävä käytäntörikkomuksen seuraukset, ja tämä on ilmoitettava selkeästi käytännössä, standardissa tai menettelyä koskevassa asiakirjassa. Rikkomuksista ilmoittamista ja käsittelyä varten olisi luotava asianmukaiset prosessit, jotta niitä hallitaan

johdonmukaisesti. Nämä prosessit olisi dokumentoitava ja sovittava asiaankuuluvien sidosryhmien kanssa asiakirjoja laadittaessa. Politiikan rikkominen voi vakavissa tapauksissa johtaa työntekijän kurinpitomenettelyn aloittamiseen, toimittajasopimuksen irtisanomiseen tai tarpeeseen ilmoittaa rikkomuksesta asianomaiselle lainvalvontaviranomaiselle. Siksi säännöt ja prosessit on ymmärrettävä, sovittava ja otettava käyttöön organisaatiossa ennen kuin rikkomuksia voidaan käsitellä. Käytännöllinen politiikka on kuitenkin ajanhukkaa, ellei organisaatio ole valmis toteuttamaan sitä. Ylimmän johdon ja niiden, joiden on noudatettava sääntöjä, on tuettava prosesseja mahdollisten rikkomusten käsittelemiseksi. Jos rikkomuksia ei ole käsitelty asianmukaisesti tai ne ohitetaan, niin myös tätä on pidettävä käytäntörikkomuksena ja kohdeltava vakavasti. (Alexander ym. 2013, 49.)

4.3.4 Toteutusvaihe

SecSDLC-mallin toteutusvaiheessa tietoturvapolitiikka testataan, toteutetaan ja uudelleen testataan. Myös henkilöstölle tehtäviä koulutuksia järjestetään. Lopuksi testattu politiikka esitetään ylimmälle johdolle lopullista hyväksyntää varten. (Whitman & Mattord 2016, 128.)

Whitmanin ja Mattordin (2016) mukaan tärkein osa toteutusvaihetta on projektisuunnitelman hallinta. Projektinhallinta on prosessi, joka tukee kaikkia SecSDLC-mallin vaiheita. Projektisuunnitelman toteutus etenee kolmessa vaiheessa:

1. Projektin suunnittelu
2. Projektisuunnitelman tehtävien ja toimintavaiheiden valvonta
3. Projektisuunnitelman laatiminen (Whitman & Mattord 2016, 129.)

Projektisuunnitelma voidaan kehittää monin eri tavoin. Jokaisen organisaation on määritettävä oma projektinhallintamenetelmänsä tietoturvaprojektille. Tietoturvaprojektien tulisi noudattaa organisaation projektinhallinnan käytäntöjä. (Whitman & Mattord 2016, 129.)

Whitman & Mattord (2016) kertoo tietoturvapolitiikkojen todennuksen olevan tärkeä osa tietoturvapolitiikan toteutusta. Toteutusvaiheessa ryhmän on luotava suunnitelma käytäntöjen jakamiseksi ja todentamiseksi. Organisaation on jollain tavalla todennettava ja varmistettava työntekijöiden vastaanottaneen ja lukeneen politiikan. Muussa tapauksessa työntekijä voi väittää, ettei ole koskaan nähnyt politiikkaa, ellei sitä vastaan pystytä esittämään vahvaa näyttöä. Tällaisessa tapauksessa politiikan rikkomiseen liittyviä sanktioita ei voida välttämättä määrätä. Yksinkertaisin tapa varmistaa työntekijöiden lukeneen politiikan, on liittää dokumenttiin allekirjoitettava kohta, jossa lukee työntekijän vastaanottaneen, lukeneen, ymmärtäneen ja hyväksyneen kyseisen politiikan. Työntekijän allekirjoitus ja päivämäärä vahvistavat työntekijän lukeneen ja sisäistäneen politiikan. (Whitman & Mattord 2016, 168.)

Yksi tapa vahvistaa työntekijöiden lukeneen ja ymmärtäneen politiikan, on arvioida työntekijän osaamista esimerkiksi lyhyellä testillä. Tällä voidaan varmistaa, että työntekijä on oikeasti ymmärtänyt politiikan. Työntekijöiltä vaaditaan tietty pistemäärä testin läpäisemiseksi. (Whitman & Mattord 2016, 170.)

Toteutusvaiheen aikana politiikan kehityksestä vastaava ryhmä varmistaa, että politiikka jaetaan, luetaan, ymmärretään ja hyväksytään asianmukaisesti. Politiikka on jaettava kaikille niille, joihin sitä sovelletaan. Käyttäjiltä vaadittu politiikan hyväksyminen dokumentoidaan. (Whitman & Mattord 2016, 170.)

4.3.5 Ylläpitovaihe

Viimeinen ylläpito- ja muutosvaihe on ehkä tärkein, kun otetaan huomioon monien nykyaikaiseen organisaatioon kohdistuvien uhkien joustavuus ja pysyvyys. Tietoturvapolitikka tarvitsee jatkuvaa seurantaa, testausta, muokkaamista, päivittämistä ja korjaamista. Uusien uhkien tullessa esiin ja vanhojen uhkien kehittyessä organisaation tietoturva vaatii jatkuvaa mukauttamista, jotta estetään uhkien tunkeutuminen arkaluonteisiin tietoihin. (Whitman & Mattord 2016, 131.)

Kun tietoturvapolitiikka on pantu täytäntöön, sitä on käytettävä, hallinnoitava asianmukaisesti ja pidettävä ajan tasalla vakiintuneiden menettelyjen avulla. Politiikan uudelleen arviointi voi olla tarpeen, jos se ei sopeudu riittävästi sisäisen tai ulkoisen ympäristön muutoksiin. Vaikka tietoturvapolitiikka mukautuisi ja kasvaisi, ylläpito- ja muutosprosessit heijastavat SecSDLC-mallin koko prosessia. Kun puutteita havaitaan ja haavoittuvuudet havaitaan, politiikan ylläpitoon, laajentamiseen tai parantamiseen tähtäävät projektit noudattavat SecSDLC-mallin vaiheita. Siksi myös ylläpitoon sisältyy tutkimus, analyysi, suunnittelu ja toteutus. (Whitman & Mattord 2016, 131.)

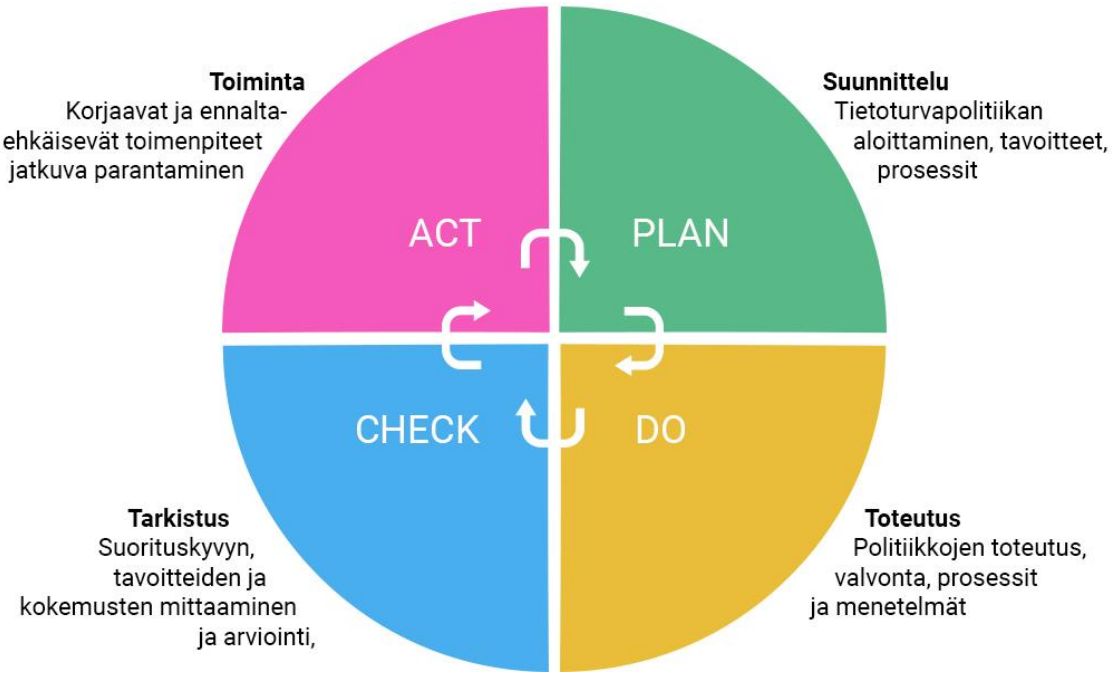
Ylläpitovaiheen aikana politiikan kehittämisryhmä seuraa, ylläpitää ja muokkaa käytäntöä tarpeen mukaan. Tällä varmistetaan, että politiikka pysyy ajantasaisena muuttuvien uhkien torjumisessa. Käyttäjien tulisi olla mahdollista ilmoittaa ongelmista esimerkiksi nimettömän lomakkeen kautta. Tehokkaan politiikan kehittämisen viimeinen osa on toteuttaa tietoturvapolitiikkaa yhtenäisesti. Organisaation tulisi varmistaa, että kaikkien on noudatettava käytäntöä tasavertaisesti, ja että politiikkoja ei toteuteta eri tavoin organisaation eri alueilla tai hierarkioissa. (Whitman & Mattord 2016, 170.)

4.4 PDCA-menetelmä

Allen (2013) kuvaa toimivaa ja tehokasta lähestymistapaa tietoturvan kehittämiseksi sekä sen toteuttamiseksi ja ylläpitämiseksi. Mallista käytettiin ISO 27001 standardin vanhassa versiossa nimeä PDCA, joka tulee sanoista *plan*, *do*, *check* ja *act* (Allen 2013). Kosutic (2014) kuitenkin

toteaa että, PDCA-mallin nimeen ei enää viitata standardin uusimmissa versioissa. Tämä ei kuitenkaan tarkoita sitä, että PDCA-malli olisi kokonaan poistunut standardista. Samat elementit ovat kuitenkin edelleen havaittavissa ja standardi todellisuudessa käyttää PDCA-mallia. (Kosutic 2014.)

PDCA-menetelmää voidaan käyttää organisaation monissa ei toiminnoissa. Tässä opinnäytetyössä keskitytään PDCA-malliin tietoturvapolitiikan kehittämisessä. PDCA-menetelmä vaikuttaa samanlaiselta kuin SecSDLC-malli. PDCA-menetelmä voidaan soveltaa myös muihin malleihin. Allen (2013) määrittelee PDCA-menetelmän kuuluvan SecSDLC-mallin toteutusvaiheeseen (Allen 2013).



Kuvio 3: PDCA-malli (ISO/IEC 27001:2005).

Allenin (2013) ja Kosuticin (2014) mukaan PDCA-mallin suunnitteluvaiheessa on selvitettävä, mitä halutaan tehdä ja missä järjestyksessä. Tehokas ja kestävä tietoturvan kehittäminen vaatii tiettyjä edellytyksiä tai esivaatimuksia ennen kuin tietoturvaa voidaan muuttaa. Allen (2013) on samaa mieltä Whitmanin ja Mattordin (2016) kanssa suunnitteluvaiheen vaatimuksista ja ne ovat myös linjassa ISO/IEC 27001 standardin kanssa. (Allen 2013; Kosutic 2014; Whitman & Mattord 2016; ISO/IEC 27001:2005 2005).

Vaikka standardin uusimmassa versiossa ei enää käytetä PDCA-mallin termiä, Kosutic (2014) kuitenkin korostaa samojen asioiden löytyvän siitä. ISO/IEC 27001 standardin kappaleet 4-7 liittyvät suunnitteluvaiheeseen. Kappaleessa 4 käsitellään organisaatiota ja siihen liittyviä sidosryhmiä, organisaation odotuksia tietoturvasta, tietoturvaohjelman rajausta, johtajien sitoutumista, tietoturvapolitiikan määrittelyä, tietoturvaan liittyvä rooleja ja vastuita,

tietoturvapolitiikan suunnittelua ja siihen liittyvää riskienhallintaa, resursseja ja vaadittavaa tukea. (Kosutic 2014, ISO/IEC 27001:2017 2017).

PDCA-mallin toteutusvaiheessa käydään läpi toteutustapaa ja välttämättömät tietoturvallisuuden käytännöt. Tietoja suojataan erilaisten teknisten ja hallinnallisten kontrollien avulla. (Allen 2013.)

Tarkistusvaiheessa tutkitaan ja mittaan, onko tietoturvaan liittyvät käytännöt riittäviä. Tutkintaan ja valvontaan sisältyy teknisten ratkaisujen lokitietoja, tietoturvatoimenpiteiden analysointi ja raportointi. Tarkistusvaiheessa voidaan toteuttaa myös tietoturvamenetelmiin kohdistuvia testejä, kuten haavoittuvuuden arviointi, penetraatiotestaus, tietoturvariskien arviointi ja auditoinnit. Näiden testien avulla voidaan myös osoittaa, täyttääkö tietoturva säännösten ja standardien vaatimukset. (Allen 2013.)

Toimintavaiheessa määritetään, miten järjestelmien ja ohjelmistojen nykyinen suojaustila voidaan parhaiten ylläpitää ottaen huomioon muutokset ja parannukset. Tarvittavat toimien perusteet pitäisi tulla turvallisuuspolitiikasta, tavoitteista, strategioista, suunnitelmista, tarkastusvaiheen arviointituloksista ja turvallisuustapahtumien analyysistä. Toimintavaiheessa voidaan myös valita tietty viitekehys tai toimintamalli tukemaan tietoturvapolitiikan käyttöönottoa. (Allen 2013.)

PDCA-malli on ylätasolla kevyempi malli verrattuna SDLC-malliin, mutta sen jokaista neljää vaihetta voidaan syventää, vaikka mallissa on määrällisesti vähemmän vaiheita. PDCA-malli on myös yleismallillinen eli sitä voidaan käyttää myös muiden toimintojen kehittämisessä. SDLC-malli taas keskittyy tarkemmin järjestelmien kehittämiseen. (Allen 2013; Whitman & Mattord 2016.)

4.5 Muita menetelmiä

Landoll (2016) kuvaa ISO/IEC 27001 tietoturvan viitekehyksen olevan yksi yleisimmistä tietoturvan kehittämismalleista. Hän esittelee myös muita yleisiä tietoturvan kehittämiseen käytettäviä malleja. Näihin kuuluu FISMA, COBIT ja HMG ISPF. Yritys voi kuitenkin käyttää juuri organisaatiolle parhaiten toimivaksi todettua mallia tietoturvan kehittämiseksi. Eri mallit eroavat toisistaan jonkin verran, mutta kaikkien tarkoitus ja tavoitteet ovat samat.

Landoll (2016) kuvaa FISMA-mallin määrittelevän tietoturvavaatimuksia valtion osastoille, valtion urakoitsijoille ja valtion palveluntarjoajille. Eli sen mallin avulla voidaan täyttää valtion tason tietoturvavaatimuksia. FISMA on yhdysvaltalainen säädös ja lyhenne muodostuu sanoista Federal Information Security Modernization Act. Uusin version FISMA-mallista on vuonna 2014 asetettu säädös. FISMA pohjautuu NIST (National Instititute of Standards and Technology) -organisaation julkaisemaan dokumenttiin SP-800-53: Security and Privacy

Controls for Information Systems and Organizations. FISMA-mallia voidaan hyödyntää tietoturvapolitiikan kehittämisessä. (Landoll 2016, 29-35.)

COBIT-mallin on luonut ISACA (Information Systems Audit and Control Association). COBIT on kehitetty ennen FISMA-mallia. Sen uusin versio on COBIT versio 5, joka on julkaistu vuonna 2021. COBIT-mallin prosessi on jaettu neljään eri vaiheeseen, jotka ovat suunnittelu ja organisointi, hankinta ja toteutus, toimitus ja tuki sekä monitorointi ja arviointi. Jokainen vaihe sisältää monia eri prosesseja. COBIT-malli keskittyy enemmän teknisiin kontrolleihin kuin tietoturvaan itsessään. (Landoll 2016, 46-49.)

5 Opinnäytetyön prosessi

Opinnäytetyö aloitettiin suunnitelman mukaisesti perehtymällä tietoturvapolitiikkaan liittyvään teoriaan alan kirjallisuuden ja standardien kautta, kuten Hirsjärvi ym. (2009) suosittelevat (Hirsjärvi ym. 2009). Teoriaan tutustuessa löydettiin paljon erilaisia malleja tietoturvapolitiikan kehittämiseen. Kirjallisuuskatsaukseen valittiin myös ISO/IEC 27001 – standardi, joka kuvaa vaatimuksia tietoturvan hallintajärjestelmälle (ISO/IEC 27001 2017).

Tietoturvapolitiikan kehittämisprojekti aloitettiin käyttämällä aiemmin kuvatun SecSDLC-mallin mukaisia tutkinta- ja analyysivaiheita, joiden aikana tutkittiin ja selvitettiin Sulavan olemassa olevia dokumentteja liittyen tietoturvapolitiikkaan. Kaikki kommunikaatio käytiin etäkokouksina Teamsin välityksellä maailmalla vallinneen pandemian takia. Haastattelemalla yrityksen tietoturvavastaavaa saatiin kerättyä tietoa yrityksen määrittelemistä teknisistä ja hallinnallisista kontrolleista sekä tietoturvaan liittyvistä vastuualueista. Yrityksen tietoturvavastaavan sekä johdon motivoituneisuus projektia kohtaan tuli jo pelkästään sen tärkeyden ja tarpeen kautta. Motivaatiota ei tarvinnut lisätä kuvaamalla tietoturvapolitiikan tärkeyttä, koska se oli jo valmiiksi tiedossa.

Sulavan tietoturvavastaava arvioi tietoturvapolitiikan dokumenttia sen eri vaiheissa. Sulavan tietoturvavastaavan myös määritteli tiettyjä ehtoja ja vaatimuksia, joita yritys halusi sisältää tietoturvapolitiikkaan. Dokumenttien sisältämän tiedon koonti yhdeksi tietoturvapolitiikaksi muodostui jo suunnitteluvaiheessa, jolloin saatiin ensimmäinen versio yrityksen julkisesta tietoturvapolitiikasta.

Ensimmäistä kehitettyä versiota verrattiin benchmarkingin eli vertailuanalyysin kautta saatuihin tietoihin. Vertailuanalyysin tuloksien avulla tietoturvapolitiikkaa kehitettiin eteenpäin ja myös sen toteutusta suunniteltiin.

Lopullinen tietoturvapolitiikka esiteltiin yrityksen johdolle, joka ei esittänyt korjausehdotuksia tai lisäyksiä politiikalle. Tämä johtuu todennäköisesti hyvin tehdyistä

aiemmista vaiheista eikä suunnitteluvaiheeseen tarvinnut enää tämän version kohdalla palata. Yrityksen johto hyväksytti julkisen tietoturvapolitiikan hallituksella ja se voidaan ottaa käyttöön sellaisenaan. Opinnäytetyön prosessin päätteeksi yrityksen julkinen

5.1 Vertailuanalyysin toteutus

Vertailuanalyysiin otettiin mukaan Tuomisen (2016) kuvaaman yleisen kategorian mukaan viiden eri alan organisaation tietoturvapolitiikat. Yleistä kategoriaa voidaan käyttää, kun vertailussa etsitään parasta toteutustapaa toimialasta riippumatta (Tuominen 2016). Tietoturvapolitiikkoja vertailemalla ei tässä opinnäytetyössä etsitä suoraan kilpailijoiden toimintatapoja, koska tarkoituksena ei ole kehittää suoranaista tuotannollista toimintoa. Tämä ei kuitenkaan estä ottamasta kilpailijoita mukaan analyysiin. Samalla alalla olevat muut yritykset ja kilpailijat oletettavasti käsittelevät vastaavanlaisia tietoja, joten tietoturvapolitiikkaa voidaan verrata jopa paremmin. Vertailuanalyysi voidaan kuitenkin toteuttaa tässä tapauksessa toimialasta riippumatta.

Vertailuanalyysin tuloksia on esitetty Liitteessä 1: Eri organisaatioiden tietoturvapolitiikkojen vertailuanalyysi. Organisaatiot esitetään anonyymisti kirjaimin A-E. Jokaisen organisaation kohdalla on keskitytty tietoturvapolitiikan sisältöön ja sen saatavuuteen.

Kaikkien organisaatioiden tietoturvapolitiikat ovat saatavilla julkisesti organisaatioiden internetsivuilta, joko suoraan leipätekstiin upotettuna tai erillisinä ladattavina dokumentteina. Tietoturvapolitiikka on siis kaikille saatavilla, jos organisaation internetsivuihin ei kohdistu saatavuutta häiritseviä tekijöitä. Jokaisen organisaation kohdalla myös mainitaan, että tietoturvasta ilmoitetaan käyttäjille, joten tietoturvapolitiikka on saatavilla myös sisäisesti sekä perehdytysten tai koulutusten yhteydessä.

Jokaisen tietoturvapolitiikan kohdalla tutkittiin, onko siinä määritelty tietoturva ja siihen liittyvät keskeiset käsitteet. Tietoturva voi olla ulkopuoliselle lukijalle vieras käsite ja kuten Whitman ja Mattord (2016) toteavat, tietoturvapolitiikan sisältö pitäisi olla helposti ymmärrettävää (Whitman & Mattord 2016). Tästä syystä tietoturvan määrittely on otettu yhdeksi vertailukohdaksi.

Myös tietoturvapolitiikkojen tarkoitus ja tarkoituksen kuvaus olivat vertailun kohteena. Käyttäjän on helpompi sisäistää tietoturvapolitiikka, jos sen tarkoitus ja tavoitteet ovat kuvattu selvästi. Tarkoitukseton tai liian hanakala tietoturvapolitiikka saattaa heikentää käyttäjien motivoituneisuutta sen lukemiseen tai sisäistämiseen ja käyttöönottoon (Whitman & Mattord 2016).

Vastuut on jaettu kaikissa julkisissa tietoturvapolitiikoissa hyvin yleisellä tasolla. Vastuita on jaettu tietyille henkilöille aseman perusteella tai ryhmille, jotka liittyvät

tietoturvapolitiikkaan tai tietoturvan toteuttamiseen. Myös palveluiden ja tietojen vastuuhenkilöille eli omistajille on jaettu vastuita tietoturvaan liittyen. Vastuu on myös osittain jaettu käyttäjille ilmoitusvelvollisuuteen sidottuna.

Yhtenä ehkä laajimpana tai tärkeimpänä vertailuna arvioitiin tietoturvapolitiikan sisältämää tietoturvan toteuttamiseen liittyvää kuvausta. Kuten Whitman ja Mattord (2016) toteavat, tietoturvapolitiikan vastaiseen toimintaa tulisi puuttua, joten myös rikkomukset ja seuraamukset otettiin politiikassa huomioon (Whitman & Mattord 2016).

Lopuksi vertailtiin myös tietoturvapolitiikassa esitettyä kommunikointia, politiikan tuoreutta sekä miten tietoturvapolitiikkaa valvotaan ja seurataan.

5.2 Aineiston analyysi

Kananen (2014) toteaa, että laadullisessa tutkimuksessa tiedonkeruuta ja sen analyysia tehdään vuorotellen. Kerätyn aineiston analysoinnin jälkeen uutta aineistoa voidaan kerätä vielä lisää. Uuden tiedon keräämisen tarve voi johtua aiemman tiedon analysoinnissa tulleisiin havaintoihin. Kvalitatiivisessa tutkimuksessa ei voida määritellä tiedon määrän tarvetta etukäteen. Tämän vuoksi tiedonkeruuta ja analyysikertoja voi olla useita yhden tutkimuksen aikana. Analysoimalla kerättyä tietoa pyritään selvittämään tutkimuskysymyksiin vastauksia. Tietoa voi olla niin paljon, ettei sitä voida pelkästään lukemalla analysoida vaan tueksi tarvitaan teknisiä aineiston analyysimenetelmiä. (Kananen 2014.)

Vilkka & Airaksinen (2003) kuitenkin toteavat, ettei toiminnallisessa opinnäytetyössä ole välttämätöntä analysoida kerättyä tietoa niin yksityiskohtaisesti kuin perinteisessä tutkimuksellisessa opinnäytetyössä. Analysointia kuitenkin pitää tehdä, jos aineistoa on kerätty kvantitatiivisten eli määrällisten tutkimusmenetelmien avulla. Aineistoa, joka on kerätty laadullisin tutkimusmenetelmin, voidaan käyttää lähteenä ilman analysointiakin. (Vilkka & Airaksinen 2003.)

Tämän opinnäytetyön aineiston on kerätty kvalitatiivisin menetelmin, jotka on mainittu opinnäytetyön kappaleessa 4. Kuten Vilkka ja Airaksinen (2013) kertovat, opinnäytetyön toiminnallisen luonteen johdosta aineistoa ei varsinaisesti analysoida, mutta esimeriksi asiantuntijahaastatteluilla saatua tietoa käytetään tukemaan argumentointia. Myöskin muuta aineistoa voidaan käyttää teoriapohjan esille nostamisessa. Näiden avulla tuodaan esille opinnäytetyön luotettavuutta. (Vilkka & Airaksinen 2003.)

Opinnäytetyön kirjallisuuskatsaus toteutettiin kuvailevana kirjallisuuskatsauksena. Kirjallisuuskatsauksessa on etsitty tietoa tietoturvapolitiikan eri kehittämismalleista, joista tähän opinnäytetyöhön valittiin SDLC-menetelmä. Menetelmää käytettiin tietoturvapolitiikan kehittämisessä. Opinnäytetyön prosessi on kuvattu aiemmin.

6 Tulokset

Vertailuanalyysissä on löydetty paljon samanlaisuuksia tietoturvapolitiikkojen kesken. Tietoturvapolitiikkojen sisältö on peilattavissa ISO/IEC 27001 standardiin, jossa on myös kuvattu tietoturvapolitiikan sisältö. Tietoturvapolitiikat ovat kaikki saatavilla organisaatioiden internetsivuilla. Osassa kerrotaan tietoturvapolitiikan myös löytyvän käyttäjille sisäisesti sekä koulutusten ja perehdytyksien yhteydessä. Kaikkia käyttäjiä vaaditaan lukemaan, ymmärtämään, sisäistämään ja tottelemaan tietoturvapolitiikassa olevia ehtoja ja käytäntöjä. Käytäntöjen integroimista normaaliin toimintaan vahvistetaan koulutuksilla ja tietoisuuden lisäämisellä. Tietoturvan merkitystä korostetaan kuvaamalla, mitä tietoturvallisuus on, miksi tietoturvapolitiikka on olemassa ja mitä seuraamuksia sen vastaisesta toiminnasta voi koitua.

Yrityksen tietoturvavastaavalle toteutettujen asiantuntijahaastatteluiden avulla löydettiin puutteita yrityksen tietoturvapolitiikan saatavuudesta, sen selkeydestä sekä puutteista. Tietoturvapolitiikasta puuttui julkisesti esiteltävä osuus. Yrityksen tietoturvapolitiikan dokumentit eivät olleet myöskään helposti löydettävissä eikä niistä oltu koostettu selkeää yhtenäistä dokumenttia, jossa olisi kuvattu yrityksen tietoturvapolitiikka kokonaisuutena.

Kirjallisuuskatsauksen tuloksena on tietoperusta, jota on kuvattu luvussa 4. Tietoperustaa käytettiin opinnäytetyön produktin eli tietoturvapolitiikan dokumentin toteutuksen prosessissa. Prosessissa hyödynnettiin kirjallisuuskatsauksen avulla tutkittua SDLC-menetelmää. Lopullisena tuloksena on tämän opinnäytetyön tuotoksena syntynyt julkinen tietoturvapolitiikka, joka löytyy liitteenä 2.

Tutkitun tiedon avulla löydettiin vastauksia tutkimuksen alussa esitettyihin tutkimuskysymyksiin. Opinnäytteen lopputuloksena syntyi julkinen tietoturvapolitiikka, jota Sulava voi käyttää julkisena esityksenä yrityksen tahtotilasta liittyen tietoturvaan. Julkisen tietoturvapolitiikan kehittämisen myötä tietoturvapolitiikkaa tulisi kehittää kokonaisvaltaisesti. Tuotos on esitetty yrityksen tietoturvavastaavalle ja yrityksen johdolle ja se on esitetty hallitukselle hyväksyntää varten.

7 Johtopäätökset

Seuraavissa luvuissa kerrotaan opinnäytetyön johtopäätökset, opinnäytetyön arviointi sekä opinnäytetyön kirjoittajan pohdintaa. Opinnäytetyön prosessi oli toteutettu käyttämällä laadullisia tutkimusmenetelmiä tukemaan opinnäytetyön toiminnallista osuutta. Lopussa on kuvattu myös mahdollisia tulevaisuuden kehityskohteita, joita opinnäytetyön aikana on tullut esille.

7.1 Opinnäytetyön arviointi

Opinnäytetyön toimeksiantaja on arvioinut opinnäytetyön ja sen lopputuotoksena syntyneen tietoturvapolitiikan. Myös opinnäytetyön tekijän yhteistyötä toimeksiantajan kanssa on arvioitu lomakkeen avulla. Arvioinnissa on otettu huomioon lopputuotoksen lisäksi myös opinnäytetyön sisältämät tietoturvan kehittämismallit ja muut tietoturvaan liittyvät teoriat kuten ISO/IEC 27001 standardi. Arviointi on toteutettu Laurea-ammattikorkeakouluin virallisen lomakkeen avulla. Lomake on tämän opinnäytetyön liitteenä 3.

Toimeksiantaja oli tyytyväinen yhteistyöhön opinnäytetyön tekijän kanssa. Yhteistyö oli tiivistä ja opinnäytetyö eteni suunnitelman mukaisesti. Opinnäytetyön lopputuotokseen eli tietoturvapolitiikkaan oltiin tyytyväisiä. Toimeksiantajan kanssa on alustavasti sovittu jatkokehityksen mahdollisuuksista sekä tietoturvapolitiikan kehittämiseksi käytettävän mallin soveltamisesta.

7.2 Työn yhteenveto

Useisiin lähteisiin viitaten voidaan todeta tietoturvapolitiikan olevan edellytys organisaation tietoturvalliselle toiminnalle. Tietoturvapolitiikan on oltava riittävän selkeä ja kaikkien sitä noudattavien saatavilla. Ilman selkeästi rakennettua hallintamallia tietoturvapolitiikan kehittäminen on haasteellista tai jopa mahdotonta. (Whitman & Mattord 2016; ISO/IEC 27001 2017; Landoll 2016; Wood 2005; Allen 2013.)

Yrityksen tietoturvan kokonaisuuden kehittäminen opinnäytetyön pohjalta on vasta alkamassa. Vaikka yritys tulisikin käyttämään julkista tietoturvapolitiikkaa sellaisenaan, tarvitsee tietoturvaprosessi kokonaisuutena vielä kehittämistä ja suunnitelmallisempaa toteuttamista. Opinnäytetyön avulla yritys saa kuitenkin tarvittavaa lisätukea tietoturvakulttuurin, -politiikan ja sen prosessien kehittämiseksi.

Pelkkä julkinen tietoturvapolitiikka ei ole riittävän laaja ja tarkka dokumentti määrittelemään kaikkia vaadittavia toimia tietoturvan edistämiseksi. Yrityksellä on kuitenkin olemassa oleva tietoturvapolitiikka, joka on otettu käyttöön jo ennen tämän opinnäytetyön aloitusta. Julkiselle tietoturvapolitiikalle nähtiin niin suuri tarve, että yrityksen tietoturvan kehitystyö aloitettiin siitä. Opinnäytetyössä on kerätty paljon tietoa tietoturvapolitiikan kokonaisvaltaiseen suunnitteluun, kehittämiseen ja toteutukseen. Näiden tietojen avulla yrityksellä on paremmat mahdollisuudet kehittää laadukas sisäinen ja ulkoinen tietoturvapolitiikka ja saavuttaa haluttu tietoturvan taso.

Toisena tulevaisuuden kehityskohteena tulee todennäköisesti olemaan käyttäjien opettaminen, kouluttaminen ja tietoturvaan liittyvän tietoisuuden lisääminen. Edellä esitetyt

aiheet olivat esillä jo opinnäytetyön aihetta rajatessa. Käyttäjien koulutukseen tarvitaan vielä lisää tutkittua tietoa ja teoriaa, jotta voidaan varmistaa myös sen onnistuvan toivotulla tasolla. Käyttäjien yleisen perehdytyksen lisäksi on esitetty toivomus käyttäjille tehdystä tietoturvakoulutuksesta sekä opinnäytetyössäkin esitetystä käyttäjille kohdistetun lomakkeen suunnittelusta ja toteutuksesta.

Lähteet

Painetut

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2009. Tutki ja kirjoita. 15., uudistettu painos. Helsinki: Tammi

Kananen, J. 2015. Opinnäytetyön kirjoittajan opas: Näin kirjoitan opinnäytetyön tai pro gradun alusta loppuun. Jyväskylä: Jyväskylän ammattikorkeakoulu.

Kananen, J. 2014. Laadullinen tutkimus opinnäytetyönä. Miten kirjoitan kvalitatiivisen opinnäytetyön vaihe vaiheelta. Jyväskylä: Jyväskylän ammattikorkeakoulu.

Kozak, M. 2004. Destination benchmarking, concepts, practices and operations. UK: CABI Publishing.

Landoll, D. 2016. Information Security Policies, Procedures, and Standards. A practitioner's reference. Boca Raton: CRC Press.

SFS-EN ISO/IEC 27000:2017. 2017. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Yleiskuvaus ja sanasto. Helsinki: Suomen Standardisoimisliitto SFS ry.

SFS-EN ISO/IEC 27001:2017. 2017. Information technology. Security techniques. Information security management systems. Helsinki: Suomen Standardisoimisliitto SFS ry.

SFS-EN ISO/IEC 27001:2005. 2005. Information technology. Security techniques. Information security management systems. Helsinki: Suomen Standardisoimisliitto SFS ry.

Tuulaniemi, J. 2011. Palvelumuotoilu. Hämeenlinna: Kariston Kirjapaino.

Vilkka, H. & Airaksinen, T. 2003. Toiminnallinen opinnäytetyö. Helsinki: Tammi.

Whitman, M. & Mattord, H. 2016. Management of information security. Fifth Edition. Boston: Cengage Learning

Sähköiset

Alexander, D., Finch, A., Sutton, D. & Taylor, A. 2013. Information Security Management Principles. Swindon: BCS Learning & Development Limited.

Allen, J. 2013. "Plan, Do, Check, Act". Cybersecurity & Infrastructure Security Agency. Viitattu 5.4.2021. https://us-cert.cisa.gov/bsi/articles/best-practices/deployment-and-operations/plan-do-check-act

Kosutic, D. 2014. Has the PDCA Cycle been removed from the new ISO standards? Viitattu 5.4.2021. https://advisera.com/27001academy/blog/2014/04/13/has-the-pdca-cycle-been-removed-from-the-new-iso-standards/

Kumpula, J. 2020. Monen suomalaisyrityksen tietoturva ontuu pahasti. MTV Uutiset. Viitattu 15.4.2021. https://www.mtvuutiset.fi/artikkeli/monen-suomalaisyrityksen-tietoturva-ontuu-pahasti-asiantuntija-arahtaa-kaikki-ei-ole-mennyt-ihan-putkeen/7963908

Kärkkäinen, H. 2020. Vastaamoon kohdistui kaksi tietomurtoa - näin kymmenientuhansien suomalaisten tiedot varastettiin. Ilta-Sanomat. Viitattu 15.4.2021. https://www.is.fi/digitoday/tietoturva/art-2000006700584.html

Moore, M. 2019. EMEA business ‘under constant cyberattack’. Techradar. Viitattu 8.4.2021. https://www.techradar.com/news/emea-businesses-under-constant-cyberattack

Patterson, J., Keppler, K. & Mapson, R. 1996. Benchmarking Basics: Looking for a Better Way. USA: Course Technology Crisp 1996.

Second Nature Security. Viitattu 4.8.2020. https://www.2ns.fi/tietoturvapolitiikka-liiketoiminnan-tueksi/

Salminen, A. 2011. Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin. Vaasa: Vaasan yliopisto. Viitattu 18.2.2021. http://www.uva.fi/materiaali/pdf/isbn_978-952-476-349-3.pdf

Tuominen, K. 2016. Introducing Benchmarking. The Path to Development. Oy Benchmarking Ltd.

Valtiovarainministeriö. 2011. VAHTI. Johdon tietoturvaopas. Viitattu 5.9.2020. https://www.suomidigi.fi/sites/default/files/2020-06/Ohje_2_2011_etusivu_ohjepdf_2.pdf

Wood, C. 2005. Information Security Policies Made Easy. Information Shield.

Julkaisemattomat

Bergius, K. 2020. Tietoturvavastaavan haastattelu. 6.5.2020. Sulava Oy.

Kuviot

Taulukot

Liitteet

Liite 1: Eri organisaatioiden tietoturvapolitiikkojen vertailuanalyysi

	A	B	C	D	E
Tietoturvan määrittely	Luottamuksellisuus, eheys, käytettävyys	Luottamuksellisuus, eheys ja käytettävyys	Luottamuksellisuus, eheys, saatavuus	Pohjautuu ISO/IEC 27001 standardiin, luottamuksellisuus, eheys ja saatavuus	Luottamuksellisuus, eheys ja käytettävyys
Politiikan saatavuus	Organisaation kotisivut, intranet, julkinen osuus suomeksi ja englanniksi	Organisaation kotisivut	Organisaation kotisivut	Organisaation kotisivut	Organisaation kotisivut
Tarkoituksen kuvaus	Tarkka kuvaus tietoturvan päämäärästä	Kuvattu politiikan ja tietoturvan tarkoitus	Kuvattu kattavasti	Tarkka kuvaus tietoturvan tavoitteista	Tietoturvapolitiikan tarkoitus on kuvattu
Vastuut	Määritelty ylätasolla ryhmille ja tietyssä asemassa oleville henkilöille, tarkemmat määrittelyt sisäisessä dokumentissa	Tietyt tahot vastaavat oman toiminnan osalta tietoturvallisuudesta, tietoturvapäällikkö	Johtaa ja valvoo organisaation hallitus, erillisiä tarkentavia vastuita ryhmille ja henkilöille	Vastuut kuvattu erillisessä dokumentissa, vastuut eritelty tiedon ja palvelun omistajille	Jokaisella käyttäjällä vastuu omista teoistaan
Tietoturvan toteuttaminen	Erikseen mainittu riskien arviointi, tietojen luokittelu ja käsittely, henkilötietojen käsittely, tietoturvavaatimukset kumppaneilta, tietoturvakoulutus, valvonta ja seuranta, poikkeamien käsittely	Käyttäjien toiminnan ohjaus säännöillä ja toimintaohjeilla, sidosryhmien kanssa tehdään sopimukset, sidoksissa tietoturvasuunnitelmaan	Toteutus ja ylläpito kuvattu tarkemmin tietoturvasuunnitelmassa, käytetään hallinnollisia ja teknisiä ratkaisuja	Kontrollit on kuvattu tarkemmin toisessa dokumentissa, korjaavista ja ehkäisevistä toimenpiteistä vastaa palveluiden omistajat, pakollinen tietoturvakoulutus	Riskien arviointi, pääsynhallinta, tietojen luokittelu ja käsittely, tietoverkon ja laitteiden käyttö, jatkuvuuden hallinta
Rikkomukset	Rikkomuksia on kaikki politiikan vastainen toiminta, seuraamukset määritelty erillisessä dokumentissa	Kaikkien tulee ilmoittaa havaitsemistaan rikkomuksista, seuraamukset määritelty erillisessä dokumentissa	Jokainen rikkomus käsitellään erikseen, erillinen toimintaohje määrittelee seuraamukset	Havaituista rikkomuksista tulee ilmoittaa	Havaituista tietoturvaongelmista, rikkomuksista ja riskeistä on ilmoitettava, sanktiot jaettu kolmeen tasoon: huomautus, varoitus ja työsuhteen purkaminen
Kommunikointi	Julkinen tietoturvapolitiikka, politiikasta tiedotetaan intranetissä	Julkisesta ja sisäisestä viestinnästä mainittu niistä vastaavat tahot	Erikseen määritelty henkilö hoitaa ulkoista ja sisäistä tiedottamista	Viestitään organisaation tietoturvan vuosikellon mukaisesti	Ei mainittu
Päivittäminen	Päivitetty viimeksi 2018 lopussa	Ei julkisesti saatavilla	Päivitetty kesällä 2018	Julkaistu kesällä 2019	Ei voida todeta *(metatietojen perusteella 2020)*
Valvonta	Tietoturvapolitiikkan toteutumista valvotaan	Tietoturvasta vastaava varmistaa valvonnan ja seurannan sekä raportoi siitä johdolle	Valvonnan vastuuta jaettu henkilöiden, palveluiden omistajien ja eri ryhmien kesken	Mittarien määrittely, tekniset ja hallinnolliset ratkaisut	Johtoryhmä valvoo toteutusta

Liite 2: Sulavan tietoturvapolitiikan julkinen osa

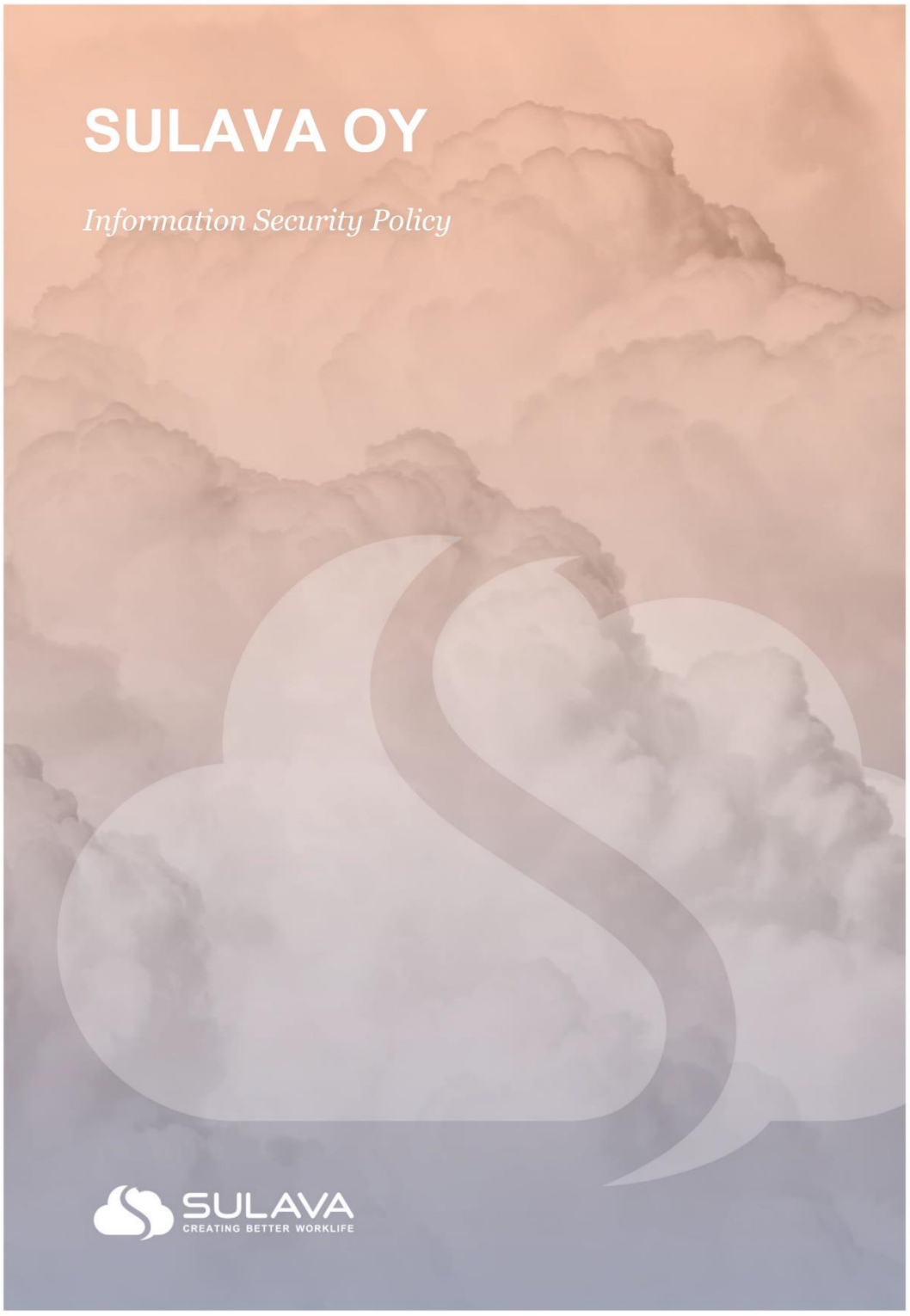


TABLE OF CONTENTS

OBJECTIVES

Information security consists of confidentiality, integrity and availability of information. The primary objective of information security is to ensure the continuity of all operations of the company in all circumstances. Information security ensures the quality of operations, supports Sulava's business, protects the reputation of the company and meets the security requirements set by law, customers and other partners.

The goal is to prevent information and information systems from being accessed by unauthorized third parties, to prevent their unauthorized use, unintentional or intentional destruction or distortion of information and to minimize any damage. Implementation of the information security policy helps Sulava's business to be uninterrupted and making data processing secure.

MANAGEMENT & RESPONSIBLITIES

The Management team and the Board of Directors are responsible for Sulava's risk management and information security, and for the strategic planning and guidance of risk management and information security and keeping the policy updated on regular basis.

Sulava's CEO and Chief Technology Officer are responsible for the operational implementation of risk management and information security. They are also responsible for monitoring and guiding Sulava's internal IT and the development and maintenance of all IT equipment, connections and software.

All employees and users of the services are obliged to comply with the rules, instructions and training given by Sulava.

IMPLEMENTATION METHDOS

All information that concerns Sulava, its customers and partners are always handled responsibly at the various stages of the information lifecycle, taking into account applicable laws, regulations, and guidelines. Information security is part of Sulava's risk management. These methods describe the implementation of information security.

RISK ASSESSMENT

Security risks are regularly assessed and analyzed based on their business impact. The risk assessment takes into account the criticality and confidentiality of the information and the impact of the risk if it occurs. The risk assessment is also conducted always before any major changes that might affect operations and business continuity. These types of changes also include implementing new system or applications. Based on the risk assessment, controls are decided to bring the risk to an acceptable level.

ACCESS RIGHTS & ACCESS CONTROL

Sulava follow the principle of least privilege. Users, programs and processes have only the bare minimum privileges necessary to perform their functions. Access to customer data is granted only for those employees who need to work with customer data.

Sulava's CEO and Chief Technology Officer define licensing policies and access levels. Shared credentials are used only in exceptional cases, which must be approved by Chief Technology Officer.

SECURITY TRAINING & AWARENESS

All new personnel are given information security training during induction. All employees are regularly informed about information security and they must review information security issues at least once a year. Competence and awareness of changing information security requirements is maintained through continuous training and information.

All employees must report security issues and breaches to the CEO or Chief Technology Officer, who will continue to report them to Sulava's Management Team and Board of Directors.

INFORMATION CLASSIFICATION & INFORMATION PROCESSING

The company uses data classification. It defines how the information is classified and how the classification affects the processing of the information. All systems with confidential personal data and their access rights are under special attention and they might be subject to more extensive security audits. Different security controls have been defined for processing different classifications of data. The processing of

personal data, including the personal data of employees and customers, is further specified in the data protection policy and its guidelines.

MONITORING

Improving and maintaining the level of information security requires systematic and continuous monitoring of the operation of information systems. Chief Technology Officer with a help of the Board of Directors are responsible for monitoring the information security, and are bound by professional secrecy by the law for any information they process in their work.

The information security status is reported regularly with internal and external audits. Technical security is continuously assessed and separate security audits are performed on key environments.

ACTIONS DURING AND AFTER INCIDENTS

In case of incidents, Sulava's CEO, Chief Technology Officer and The Board of Directors have the right to take immediate measures to minimize the risk and its impact to the organization or its information.

ACTIONS DURING DISTURBANCE OR EXCEPTIONAL CIRCUMSTANCES

Sulava has prepared for small, medium and large disturbances as well as suitable parts for exceptional conditions in the planning, implementation and monitoring of information security.

COMMUNICATIONS

This information security policy is public. The details of the information security policy with its responsibilities and obligations, as well as the parts describing the information security organization and its appendices are for internal use only. The public part of the information security policy is published on Sulava's website and the part intended for Sulava's internal use on Sulava's intranet.

Sulava's CEO and The Board of Directors make other public and internal briefs and announcements if they are needed.

INFRINGEMENTS & SANCTIONS

Violation of the security policy and guidelines is considered a security breach. All security breaches are reported to the Management Team and to the Chief Technology Officer. Sulava has defined procedures for infringements.

UPDATING & APPROVALING THE POLICY

The Management team and the Board of Directors approve the information security policy. The security policy is updated as necessary, at least once a year.

Liite 3: Työelämän palaute

LAUREA AMMATTIKORKEAKOULU
University of Applied Sciences

Työelämän palaute

8.12.2015/ba

Hyvä työelämän edustaja

Kiitos, että tarjositte Laurea-ammattikorkeakoulun opiskelijalle/opiskelijoille mahdollisuuden tehdä opinnäytetyö yritykseenne/organisaatioonne. Työelämän kehittäminen on tärkeä osa opinnäytetöidemme arvioinnissa. Pyydämmekin näkemystänne.

Yrityksen/organisaation nimi	
Työelämän edustajan/Arvioijan nimi ja tehtävänimike	
Opinnäytetyön ohjaaja yrityksessä/organisaatiossa	
Opinnäytetyön tekijä/t	
Miten yrityksenne/organisaationne hyödyntää tehtyä opinnäytetyötä?	
Mitä uutta ja/tai odottamatonta tuli esille opinnäytetyöprosessin aikana tai tuloksissa?	
Miten kuvailisitte yhteistyötä opinnäytetyöntekijän/-tekijöiden kanssa?	

Haluaisitteko jatkossakin tarjota opiskelijoillemme opinnäytetyön aiheita tai harjoittelupaikkoja? Miten haluaisitte kehittää yrityksenne/organisaationne ja Laurea-ammattikorkeakoulun yhteistyötä?

Paikka ja päivämäärä	
Työelämän edustajan/arvioijan allekirjoitus	
Nimenselvennys	
Voitte palauttaa lomakkeen myös ilman allekirjoitusta sähköpostilla joko suoraan koulun ohjaajalle tai opinnäytetyöntekijälle, joka välittää viestin ohjaajalleen siten, että viestiketjusta näkyy allekirjoittajan sähköpostiosoite.	