Riitta Häkkinen

HENKILÖSTÖN KÄSITYKSIÄ OULUN POLIISILAITOKSEN TIETOTURVALLISUUDESTA

Opinnäytetyö
CENTRIA-AMMATTIKORKEAKOULU
Liiketalouden koulutusohjelma
Kevät 2022

TIIVISTELMÄ OPINNÄYTETYÖSTÄ

Centria-ammattikorkeakoulu	**Aika** Huhtikuu 2022	**Tekijä/tekijät** Riitta Häkkinen
Koulutus Liiketalous		☒ AMK ☐ YAMK
Työn nimi HENKILÖSTÖN KÄSITYKSIÄ OULUN POLIISILAITOKSEN TIETOTURVALLISUUDESTA		
Työn ohjaaja Pekka Paajanen		**Sivumäärä** 50 + 2
Työelämäohjaaja Esa Kylmänen		

Tekemäni opinnäytetyön toimeksiantajana oli Oulun poliisilaitos. Oulun poliisilaitoksen tehtävänä on yleisen järjestyksen ja turvallisuuden ylläpito, rikosten ennalta estäminen, rikostutkinta sekä liikenteenvalvonta ja liikenneturvallisuuden edistäminen. Poliisin tehtävänä on varmistaa ihmisten ja ympäristön turvallisuus kaikissa tilanteissa ja kaikkina aikoina. Lisäksi Oulun poliisilaitoksen tehtäviin kuuluu suorittaa myös muita poliisille määrättyjä tehtäviä, esimerkiksi lupahallinnon tehtäviä.

Tekemäni opinnäytetyön tarkoituksena sekä tavoitteena oli selvittää henkilöstön käsityksiä Oulun poliisilaitoksen tietoturvallisuudesta sekä kartoittaa riskejä eri tietoturvallisuuden osa-alueilla.

Opinnäytetyöni pääteemoiksi teoreettisessa tietoperustassa muodostuivat riskit ja riskienhallinta sekä tietoturvallisuus ja sen osa-alueet.

Empiirisen tutkimuksen tein haastattelemalla kahtatoista Oulun poliisilaitoksen työntekijää. Teemahaastattelujen jälkeen analysoin tutkimustulokset ja laadin johtopäätökset sekä pohdinnan.

Analysoimieni tutkimustulosten mukaan henkilöstön käsitykset tietoturvallisuudesta olivat myönteisiä. Erilaisten koulutusten ja laitehankintojen koettiin olleen onnistuneita. Suurimpina kehittämistarpeina ja myös tietoturvallisuutta heikentävinä tekijöinä koettiin henkilöstöstä sekä toimitiloista johtuvat seikat.

Asiasanat
Fyysinen turvallisuus, henkilöstöturvallisuus, ohjelmistoturvallisuus, riskit, riskienhallinta, tietoturvallisuus

ABSTRACT

Centria University of Applied Sciences	Date April 2022	Author Riitta Häkkinen
Degree programme Business Administration		
Name of thesis PERSONNEL PERCEPTIONS OF THE INFORMATION SECURITY IN THE OULU POLICE DEPARTMENT		
Centria supervisor Pekka Paajanen		**Pages** 50 + 2
Instructor representing commissioning institution or company Esa Kylmänen		

This thesis was commissioned by the Oulu Police Department. The task of the Oulu Police Department is to maintain public order and security, to prevent crime and investigate crimes, to control traffic and to promote road safety. The role of the police is to ensure the safety of people and the environment in all situations and at all times. In addition, the tasks of the Oulu Police Department also include performing other tasks assigned to the police, such as licensing administration tasks.

The purpose of this thesis was to find out the personnel perceptions of the information security On the Oulu Police Department and to map the risks in different areas of information security.

The main themes of my thesis in the theoretical framework were risks and risk management, as well as information security and its components.

I conducted an empirical study by interviewing twelve employees from the Oulu Police Department. After the thematic interviews, I analyzed the results and drew conclusions.

According to the results I analyzed, the personnel´s perceptions on information security were positive. Various trainings and the acquisitions of appliances were considered successful. The biggest needs for development and also the weakening factors were related to personnel and premises.

Key words
Information security, personnel security, physical security, risks, risk management, software security

TIIVISTELMÄ
ABSTRACT
SISÄLLYS

1 JOHDANTO 1

2 RISKIT JA RISKIENHALLINTA 4
2.1 Riskin käsite ja riskien luokittelu 4
2.2 Riskienhallinta ja riskienhallintaprosessi 6

3 TIETOTURVALLISUUS 8
3.1 Tietoturvallisuuden käsite ja tavoitteet 8
3.2 Tietoturvallisuuden laajennettu käsite 10
3.3 Tietoturvallisuuden osa-alueet 12
3.3.1 Hallinnollinen turvallisuus 13
3.3.2 Fyysinen turvallisuus 15
3.3.3 Henkilöstöturvallisuus 16
3.3.4 Käyttöturvallisuus 17
3.3.5 Tietoliikenneturvallisuus 18
3.3.6 Laitteistoturvallisuus 18
3.3.7 Ohjelmistoturvallisuus 19
3.3.8 Tietoaineistoturvallisuus 19

4 TOIMEKSIANTAJAN ESITTELY JA POLIISIN TIETOTURVALLISUUS 21

5 EMPIIRISEN TUTKIMUKSEN TOTEUTUS 26
5.1 Empiirisen tutkimuksen tavoitteet sekä tutkimusongelmat 26
5.2 Tutkimusote, tiedonkeruu sekä aineiston käsittely ja analysointi 27
5.3 Tutkimuksen luotettavuus ja sen arviointi 29

6 TUTKIMUSTULOKSET 33
6.1 Haastateltavien käsityksiä tietoturvallisuuden tasosta 33
6.2 Haastateltavien käsityksiä onnistumisista tietoturvallisuudessa 35
6.3 Haastateltavien käsityksiä tietoturvallisuuden kehittämistarpeista 36
6.4 Haastateltavien käsityksiä tietoturvallisuutta heikentävistä seikoista 38
6.5 Haastateltavien esittämiä keinoja tietoturvallisuuden kehittämiseksi 40

7 JOHTOPÄÄTÖKSET JA POHDINNAT 43
7.1 Vastaukset tutkimusongelmiin 43
7.2 Opinnäytetyön arviointi 46

LÄHTEET 48
LIITTEET

KUVIOT

KUVIO 1. Riskienhallintaprosessi 7
KUVIO 2. Havainnekuva tietoturvallisuuden määrittämisestä 8
KUVIO 3. Tietoturvallisuuden osa-alueet 13
KUVIO 4. Hallinnollisen alueen kyltti 24
KUVIO 5. Turva-alueen kyltti 25

1 JOHDANTO

Tietoturvallisuutta ja tiedonkäsittelyä koskevat nyky-yhteiskunnassamme useat erilaiset haavoittuvuudet, uhat ja riskit. Näiden haavoittuvuuksien, uhkien ja riskien ennalta estäminen sekä mahdollisten syntyneiden vahinkojen minimoiminen vaatii toimia sekä julkishallinnolta että yksityisiltä yrityksiltä ja henkilöiltä. Tietoturvallisuuden kehittäminen ja ylläpitäminen sekä päivittäminen ovat tärkeä osa turvallisuutta ja riskienhallintaa. Lähes kaikki arkaluontoiset tiedot liikkuvat sähköisesti ja digitalisoituminen aiheuttaa tietoturvallisuudelle haavoittuvuuksia ja riskejä. Digitalisoitumisen lisäksi tietoturvallisuutta vaarantavia tekijöitä ovat edelleen myös erilaiset fyysiset haavoittuvuudet, uhat ja riskit.

Tietoturvallisuudella tarkoitetaan tiedon käytettävyyden eli saatavuuden, luottamuksellisuuden sekä eheyden varmistamista ja turvaamista hallinnollisilla ja teknisillä toimenpiteillä. Tietoturvallisuuden tarkoituksena on suojata tietojärjestelmiä ja tietoaineistoa sekä digitaalisilta että fyysisiltä uhkilta ja haavoittuvuuksilta, kuten esimerkiksi luvattomalta pääsyltä, tietojen luvattomalta käytöltä, salaisten tietojen paljastumiselta, tietojen muuntumiselta ja tietojen häviämiseltä. Näiden lisäksi tietoturvallisuuden tarkoituksena on suojata muun muassa tietokoneviruksilta, huijausyrityksiltä, vakoilulta sekä yksityisyyden loukkauksilta.

Opinnäytetyöni tavoitteena ja tarkoituksena on selvittää henkilöstön käsityksiä Oulun poliisilaitoksen tietoturvallisuudesta ja tietoturvallisuuden tasosta eri osa-alueilla. Opinnäytetyön tavoitteena on myös selvittää henkilöstön näkemyksiä niistä tietoturvallisuuden osa-alueista, joissa koetaan onnistuneen hyvin. Tavoitteena on lisäksi selvittää ne tietoturvallisuuden osa-alueet, joissa henkilöstö kokee olevan eniten kehittämistarvetta sekä selvittää henkilöstön ajatuksia ja näkemyksiä toimivista kehittämiskeinoista Oulun poliisilaitoksen tietoturvallisuuden parantamiseksi.

Tutkimuskysymyksen muodossa esitettynä opinnäytetyön päätutkimusongelma on:

- Millaiseksi poliisilaitoksen henkilöstö kokee tietoturvallisuuden tason Oulun poliisilaitoksella?

Päätutkimusongelma jakautuu neljään alaongelmaan. Tutkimuskysymysten muodossa esitettyinä opinnäytetyön alaongelmat ovat:

- Missä tietoturvallisuuden osa-alueissa henkilöstö kokee tietoturvallisuuden onnistuneen hyvin?
- Missä tietoturvallisuuden osa-alueissa henkilöstö kokee olevan eniten kehittämistarvetta?
- Mitkä seikat heikentävät tietoturvallisuutta?
- Millä keinoin tietoturvallisuutta voitaisiin kehittää?

Opinnäytetyössä on seitsemän päälukua. Ensimmäisen eli johdantoluvun jälkeen opinnäytetyön toisessa luvussa käsitellään riskejä, riskienhallintaa sekä eri riskilajeja. Kolmannessa luvussa käsitellään tietoturvallisuuden käsitettä ja tavoitteita, termistöä yleisesti sekä tietoturvallisuuden osa-alueita, jotka opinnäytetyössä on jaettu kahdeksaan osaan.

Luvussa 4 esitellään toimeksiantaja Oulun poliisilaitos sekä käsitellään poliisin tietoturvallisuutta osana organisaatioturvallisuutta. Luvussa 5 käydään läpi empiirisen tutkimuksen toteutusta eli opinnäytetyön suunnittelua, tavoitteita, tutkimusongelmia sekä haastatteluiden toteutusta. Luku 6 esittelee empiirisen tutkimuksen tutkimustuloksia ja luvussa 7, opinnäytetyön viimeisessä luvussa, esitetään haastattelujen perusteella tehtyjä johtopäätöksiä ja pohdintoja.

Tietoturvallisuudesta, tietoturvallisuuden osa-alueista sekä riskeistä on saatavilla kirjallista aineistoa niin sähköisessä muodossa kuin painettunakin. Lisäksi internet tarjoaa runsaasti

erilaisia tieteellisiä julkaisuja tietoturvallisuudesta. Tässä opinnäytetyössä lähteinä on käytetty sähköistä aineistoa sekä painettua kirjallisuutta. Sähköisen ja painetun lähdemateriaalin lisäksi opinnäytetyössä on haastateltu kahtatoista Oulun poliisilaitoksen henkilöstöön kuuluvaa.

2 RISKIT JA RISKIENHALLINTA

2.1 Riskin käsite ja riskien luokittelu

Riski käsitteenä tarkoittaa vahingon mahdollisuutta, tavoitteisiin vaikuttavaa epävarmuutta tai poikkeavuutta odotettuun. Riski mielletään usein negatiiviseksi, mutta riskin vaikutus voi olla myös myönteinen verrattuna siihen, mitä riskin oletettiin ja odotettiin olevan. Ihmisestä johtuvista tai ihmisen aiheuttamilta operatiivisilta riskeiltä, tulevatpa ne organisaation sisä- tai ulkopuolelta, on mahdollista suojautua ja niihin voidaan ennalta varautua ja niihin voidaan vaikuttaa. Usein riskien toteutuminen johtuukin siitä, että riskit pääsevät yllättämään ja uhkaamaan toimintaa, koska riskejä ei ole osattu huomioida riittävän ajoissa. Kun riskeihin varaudutaan ennalta ja suunnitellaan riskeiltä suojautumista, ne eivät pääse yllättämään eivätkä myöskään uhkaamaan toimintaa esimerkiksi keskeytymisellä. Kaikkiin riskeihin, kuten sään tai muiden luonnonilmiöiden aiheuttamiin vahinkoihin, ei pystytä vaikuttamaan, mutta myös niihin pystytään varautumaan ja myös niiltä pystytään suojautumaan. (Suomen Riskienhallintayhdistys 2012a.)

Riskit voidaan luokitella sekä jaotella esimerkiksi sen mukaan, mihin organisaation toimintoihin riski voi vaikuttaa. Riskien luokittelusta on hyötyä, kun suunnitellaan riskienhallintakeinoja sekä myös silloin, kun tunnistetaan riskejä. Luokitteluna voidaan käyttää jakoa, jossa riskit jaetaan strategisiin, operatiivisiin, taloudellisiin sekä vahinkoriskeihin. (Suomen Riskienhallintayhdistys 2021b.) Kun riskien luokittelua käytetään hyödyksi riskienhallintakeinoja suunniteltaessa sekä riskejä tunnistettaessa, on tärkeää määritellä organisaatiokohtaisesti riskin tärkeys ja riskin toteutumisen todennäköisyys. Riskin tärkeyden ja toteutumisen todennäköisyyden lisäksi on olennaista määritellä myös toteutuneen riskin, eli vahingon, vaikutus toimintaan. (Rousku 2017, 25.)

Strategisilla riskeillä tarkoitetaan sellaisia riskejä, jotka vaikeuttavat organisaation strategian toteuttamista. Organisaation täytyy varautua strategisiin riskeihin. Strategisiin riskeihin varautuessa avainasemassa ovat esimerkiksi erilaiset seuranta- ja raportointijärjestelmät. Tämä johtuu siitä, että strategisten riskien varalta ei voi ottaa vakuutuksia. Strategisiin riskeihin kuuluvat muun muassa toiminnan kehittämiseen, toiminnan uudelleenjärjestelyihin, toimintaympäristöön ja sidosryhmiin liittyvät sekä organisaatiorakenteen riskit. (Suomen Riskienhallintayhdistys 2012c.)

Operatiiviset riskit johtuvat organisaation sisäisistä toimimattomista tai puutteellisista tavoista toimia, tietojärjestelmistä, prosesseista tai henkilöstöstä. Operatiivisia riskejä ovat muun muassa henkilö-, tieto-, tuote- sekä projektiriskit ja näihin riskeihin kuuluvat muun muassa johtamisesta, teknologiasta, koulutuksesta ja osaamisesta sekä sopimuksista ja vastuista aiheutuvat riskit. (Suomen Riskienhallintayhdistys 2012d.)

Taloudellisilla riskeillä tarkoitetaan niitä riskejä, jotka liittyvät organisaation kannattavuuteen, maksuvalmiuteen, kustannuksiin ja pääomien riittävyyteen. Taloudellisia riskejä ovat esimerkiksi liike- ja sopimusriskit. Taloudellisten riskien syitä ovat muun muassa valuutta- ja kurssimuutosten sekä korkomuutosten aiheuttamat riskit sekä luotonhallintaan ja verotukseen liittyvät riskit. Osana taloudellista riskiä ovat myös yllättävät muutokset kustannuksissa, jotka koskevat resursseja sekä hyödykkeitä. (Suomen Riskienhallintayhdistys 2012e.)

Vahinkoriskit kohdistuvat organisaatiossa henkilöturvallisuuteen, omaisuuteen tai ympäristöön. Vahinkoriskejä ovat muun muassa toiminnan keskeytykseen liittyvät toiminnan keskeytysriskit, tulipalon aiheuttamat paloriskit sekä rikos- ja ympäristöriskit. (Suomen Riskienhallintayhdistys 2012f.) Kaikille vahinkoriskeille tyypillistä on se, että vaikka itse toteutunut riski, vahinko, ei olisikaan välttämättä kovin suuri, siitä seuraavat vahingot voivat kuitenkin olla merkittävän suuret. Tästä syystä vahinkoriskit ovatkin niitä riskejä, joiden taloudellisia seuraamuksia pyritään siirtämään vakuutusyhtiöille ottamalla erilaisia toiminnan vakuutuksia.

2.2 Riskienhallinta ja riskienhallintaprosessi

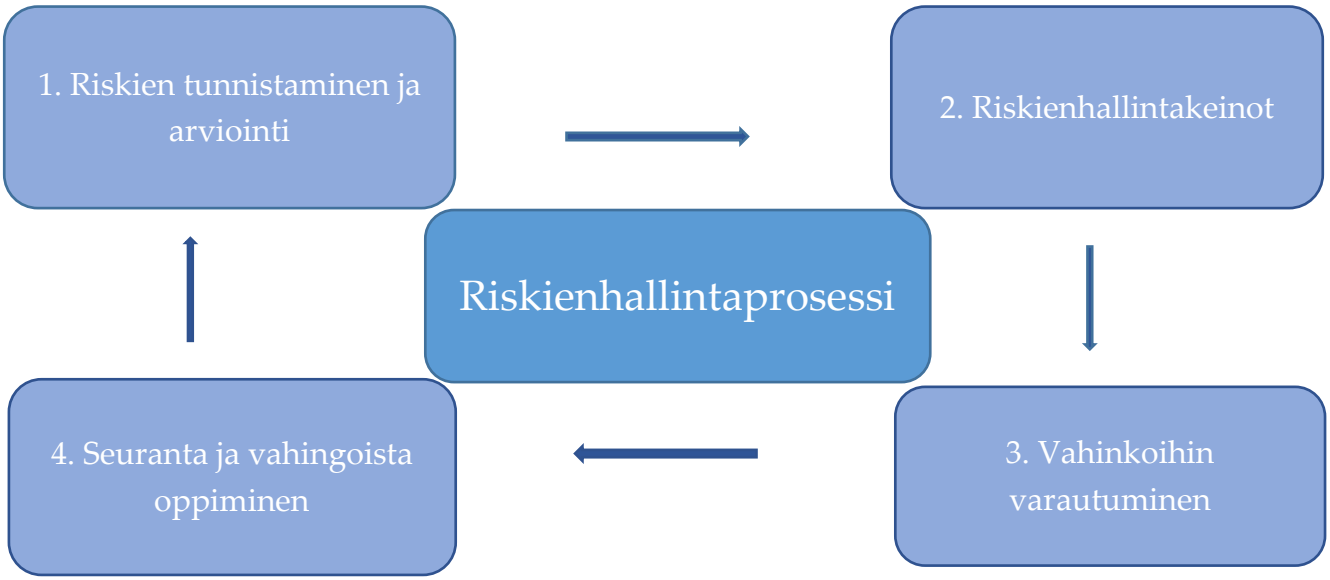
Organisaation riskejä voidaan sekä ohjata että johtaa riskienhallinnalla. Riskienhallinnan pyrkimys ja tarkoitus on varmistaa se, että organisaatiossa toiminta jatkuu sekä päästään tavoitteisiin kaikissa olosuhteissa ja tilanteissa. Riskienhallinnalla pyritään pienentämään toiminnan riskejä sekä niistä aiheutuvia vahinkoja eli toteutuneita riskejä. Tästä syystä riskienhallinnan on tarkoituksenmukaista olla ennakoivaa sekä tavoitteellista, järjestelmällistä ja suunniteltua toimintaa. Tällöin riskienhallinnalla pystytään varmistamaan myös henkilöstön hyvinvointi ja organisaation menestyminen. Riskienhallinnan kannalta on ensiarvoisen tärkeää pystyä tunnistamaan ja arvioimaan riskejä järjestelmällisesti ja selvittämään niitä kattavasti. Organisaation johtamisessa sekä operatiivisessa ja strategisessa suunnittelussa riskienhallinnalla onkin keskeinen rooli. (Suomen Riskienhallintayhdistys 2012g.)

Jotta riskienhallinta saadaan onnistumaan, sitä on toteutettava säännöllisesti, sen on reagoitava muutokseen ja sen on oltava aktiivista. Riskienhallinnan kehittämisessä tärkeää on se, että riskienhallintaa muutetaan ja muokataan tarkoitukseen ja tarpeeseen sopivaksi. Kun riskienhallinta on osa henkilöstön jokapäiväistä työtä, se saadaan aktiiviseksi ja tällöin riskienhallinta reagoi nopeasti tapahtuviin muutoksiin. (Rousku 2017, 18.)

Riskienhallintaprosessi auttaa organisaatiossa johtoa sekä henkilöstöä tunnistamaan niitä riskejä, jotka uhkaavat vaarantaa tavoitteita, joita organisaatiossa on asetettu. Riskien vaikutusten arviointi organisaatiolle, yhtä lailla kuin organisaatiossa tunnistettujen riskien analysointi, helpottuu riskienhallintaprosessin avulla. Riskienhallintaprosessin tavoitteena on muun muassa avustaa organisaation johtoa löytämään sekä päättämään toimivin ja paras keino hallita niitä riskejä, joiden koetaan vaarantavan ja uhkaavan organisaatiota. (Suomen Riskienhallintayhdistys 2012h.)

Riskienhallintaprosessi voidaan jakaa neljään eri vaiheeseen (KUVIO 1). Riskienhallintaprosessin ensimmäisessä vaiheessa riskit täytyy sekä tunnistaa että arvioida. Toisessa vaiheessa

suunnitellaan kaikki tarvittavat toimenpiteet ja vaihtoehdot, joilla riskit saadaan hallittua. Kolmantena vaiheena riskienhallintaprosessissa on sen suunnittelu, kuinka toteutuneen riskin, eli vahingon, sattuessa organisaatiossa toimitaan ja kuinka toteutuneesta riskistä toivutaan. Neljännen eli viimeisen vaiheen aikana tilannetta seurataan, eli mitä vaikutuksia organisaatiossa tehdyillä toimenpiteillä on ollut. Tämän lisäksi neljänteen vaiheeseen kuuluu myös tapahtuneesta oppiminen. Joskus riskienhallintaprosessin viimeisessä vaiheessa voidaan katsoa tarpeelliseksi, että organisaation johtoa raportoidaan riskitilanteen kehittymisestä sekä merkittävimmistä riskeistä. (Suomen Riskienhallintayhdistys 2012h.)

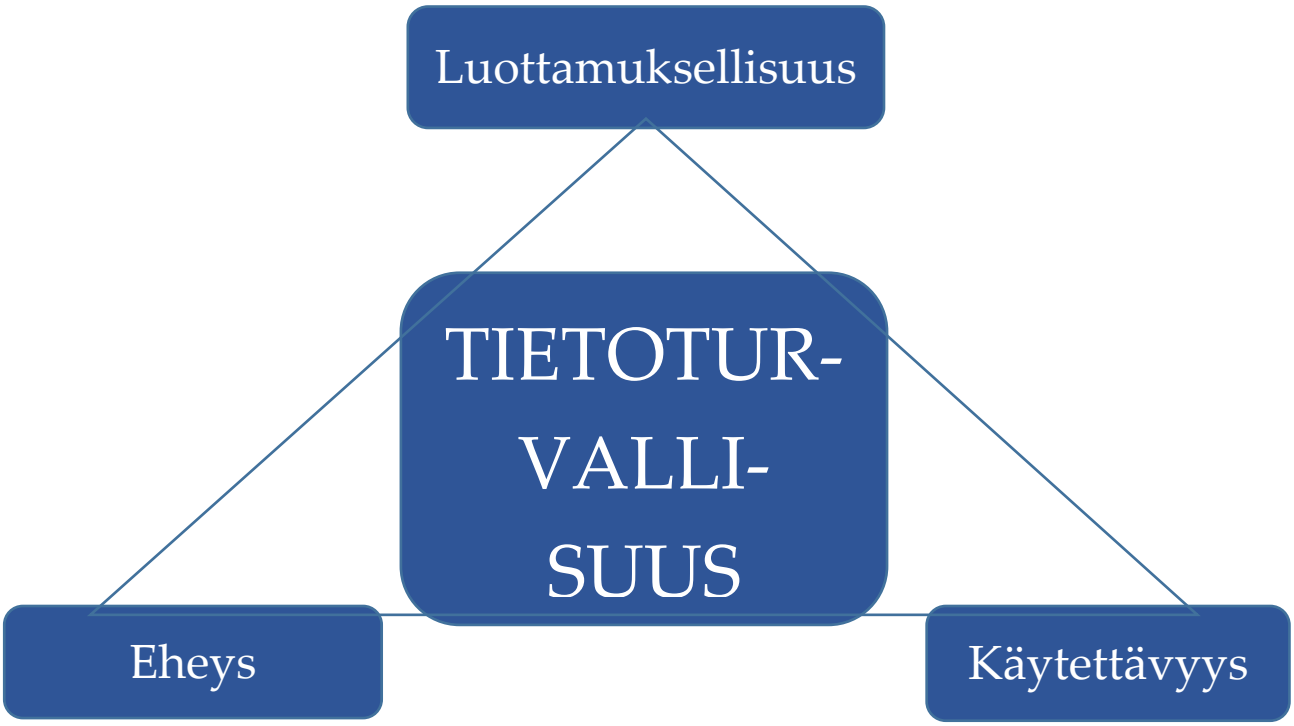


KUVIO 1. Riskienhallintaprosessi (mukaillen Suomen Riskienhallintayhdistys 2012h)

3 TIETOTURVALLISUUS

3.1 Tietoturvallisuuden käsite ja tavoitteet

Tietoturvallisuus tarkoittaa sekä teknisiä että hallinnollisia toimia, joiden tarkoituksena on varmistaa tiedon luottamuksellisuus, eheys sekä käytettävyys (KUVIO 2). Valtiovarainministeriö piti vuoteen 2020 saakka yllä valtionhallinnon yhteistä digitaalisen turvallisuuden kehittäjäverkostoa, VAHTIa. Vuonna 2020 Valtiovarainministeriön tietoturvallisuuteen liittyvä toiminta ja digitaalisen turvallisuuden kehittäjäverkosto siirtyivät Digi- ja väestötietoviraston vastuulle. (Valtiovarainministeriö 2020.)



KUVIO 2. Havainnekuva tietoturvallisuuden määrittämisestä

VAHTI-toiminnan tarkoituksena on kehittää julkisen hallinnon turvallisuutta laajapohjaisella valmistelulla, koordinaatiolla sekä yhteistyöllä ja toiminnassa onkin mukana useiden eri organisaatioiden johtoa sekä digiturvasta vastaavia asiantuntijoita. Toiminnan päätavoitteina ovat muun muassa luottamuksen säilyttäminen julkiseen hallintoon sekä niiden tieto- ja viestintätekniikan palveluiden ja toimintojen turvaaminen, jotka ovat julkiselle hallinnolle elintärkeitä ja olennaisia. (Digi- ja väestötietovirasto 2022.)

VAHTI-toiminnan tavoitteena on tietojen, tietojärjestelmien, tietoliikenteen, laitteiden ja palveluiden suojaaminen sekä teknisillä, hallinnollisella että muilla toimilla uhkia vastaan sillä tavoin, ettei tietojen luottamuksellisuus, eheys tai käytettävyys vaarannu. Sen lisäksi, että tietoturvallisuus koskee erilaisia teknisiä ratkaisuja, tietoturvallisuuden kokonaisuuteen liittyvät keskeisesti yleiset järjestelyt turvallisuusratkaisuissa ja organisaation turvatoiminnassa sekä ihmisten toiminta. Tietoturvallisuuden käsite onkin erittäin laaja ja sillä on merkitystä organisaatiossa myös taloudellisuuteen ja tuottavuuteen liittyvissä osa-alueissa. (VAHTI 2004a, 15.)

Luottamuksellisuudella tarkoitetaan, että tiedot ovat ainoastaan niiden tahojen ja henkilöiden saatavilla sekä käsiteltävissä, jotka ovat niiden käyttöön oikeutettuja. Luottamuksellisuuden varmistamisen tarkoituksena on, ettei tietoja paljastu, paljasteta tai muulla tavoin saateta sivullisten, ulkopuolisten tahojen, tietoon tai käyttöön. (Kyberturvallisuuskeskus 2020.)

Eheydellä tarkoitetaan muun muassa tietojen ja tietojärjestelmien aitouden, luotettavuuden ja väärentämättömyyden varmistamista sekä sisäistä ristiriidattomuutta, kattavuutta ja ajantasaisuutta. Eheyteen kuuluvat tietojen ja tietojärjestelmien oikeellisuus ja käyttökelpoisuus sekä todentaminen, että tietoja ei ole valtuudettomasti muutettu. Eheys sisältää myös sen, että mahdolliset muutokset ovat todennettavissa kirjausketjusta. (Poliisihallitus 2022.) Eheyden varmistamisen tarkoituksena on, että tiedot eivät oikeudettoman inhimillisen toiminnan, laitteisto- tai ohjelmistovikojen tai luonnontapahtumien seurauksena hallitsemattomasti tai

oikeudettomasti tuhoudu tai muutu vaan tiedot ja tiedostot säilyvät totuudenmukaisina (Paavilainen 1998, 10).

Käytettävyydellä eli saatavuudella tarkoitetaan, että tieto, tietojärjestelmä tai palvelu on käyttöön oikeutetuille saatavilla ja käytettävissä (Kyberturvallisuuskeskus 2020). Käytettävyyden varmistamisen tarkoituksena on myös, että tietojärjestelmästä saatavat tiedot sekä eri tietojärjestelmien palvelut ovat oikeassa muodossa, vaaditulla tavalla ja haluttuna aikana hyödynnettävissä (Hakala, Vainio & Vuorinen 2006, 4).

3.2 Tietoturvallisuuden laajennettu käsite

Edellä esitetyn tietoturvallisuuden käsitteen sekä havainnekuvan (KUVIO 2) mukainen tietoturvallisuuden jakaminen kolmeen on koettu nykyajan tarpeisiin nähden riittämättömänä ja kattamattomana. Tästä syystä tietoturvallisuuden määritelmää onkin katsottu tarpeelliseksi laajentaa pääsynvalvonnalla, todentamisella sekä kiistämättömyydellä (Hakala ym. 2006, 4).

Pääsynvalvonnalla varmistetaan, että ainoastaan valtuutetuilla käyttäjillä on oikeus päästä tietojärjestelmiin ja saada tietoa. Pääsynvalvonnalla voidaan määritellä henkilöille erilaisia käyttöoikeuksia tietojärjestelmiin, joilla pystytään säätelemään esimerkiksi luku- tai muokkausoikeuksia tietojärjestelmässä. (Hakala ym. 2006, 5.)

Todentaminen tarkoittaa niitä tapoja, joilla valtuutettu käyttäjä voi todentaa käyttöoikeutensa tiedon saantiin tai tietojärjestelmän käyttöön. Valtuutetun käyttäjän tapoja todentaa käyttöoikeutensa ovat esimerkiksi käyttäjätunnus ja salasana tai sähköinen avainkortti. (VAHTI 2004b, 50.) Käyttäjän käyttöoikeuden todentaminen onkin olennainen osa tiedon luottamuksellisuutta.

Tyypillinen todennus tapahtuu esimerkiksi oikealla tunnuksen ja salasanan yhdistelmällä. Sen jälkeen kun käyttäjä on tunnistettu, voidaan hänelle luovuttaa asianmukaiset käyttöoikeudet eli henkilökohtaiset käyttäjätunnukset sekä salasanat. (Kyberturvallisuuskeskus 2021a.) Erilaiset järjestelmät ja rekisterit mahdollistavat sen, että todentamiseen on mahdollista käyttää esimerkiksi sähköisiä avainkortteja ja omaa henkilökohtaista avainkoodia tai vaihtuvaa koodia.

Kiistämättömyys tarkoittaa sitä, että järjestelmää käyttävän henkilön tiedot sekä tietojärjestelmässä ja tiedonsiirrossa tapahtuneet toimenpiteet pystytään luotettavasti tunnistamaan sekä tallentamaan. Tietojärjestelmä muodostaa valtuutetuista käyttäjistä ja valtuutetun käyttäjän tekemistä muokkauksista lokitiedostoja. (Hakala ym. 2006, 5.) Kun eri tietojärjestelmien käyttöä ja käyttäjien tekemiä muutoksia pystytään seuraamaan lokitiedostoilla, väärinkäytökset vähenevät.

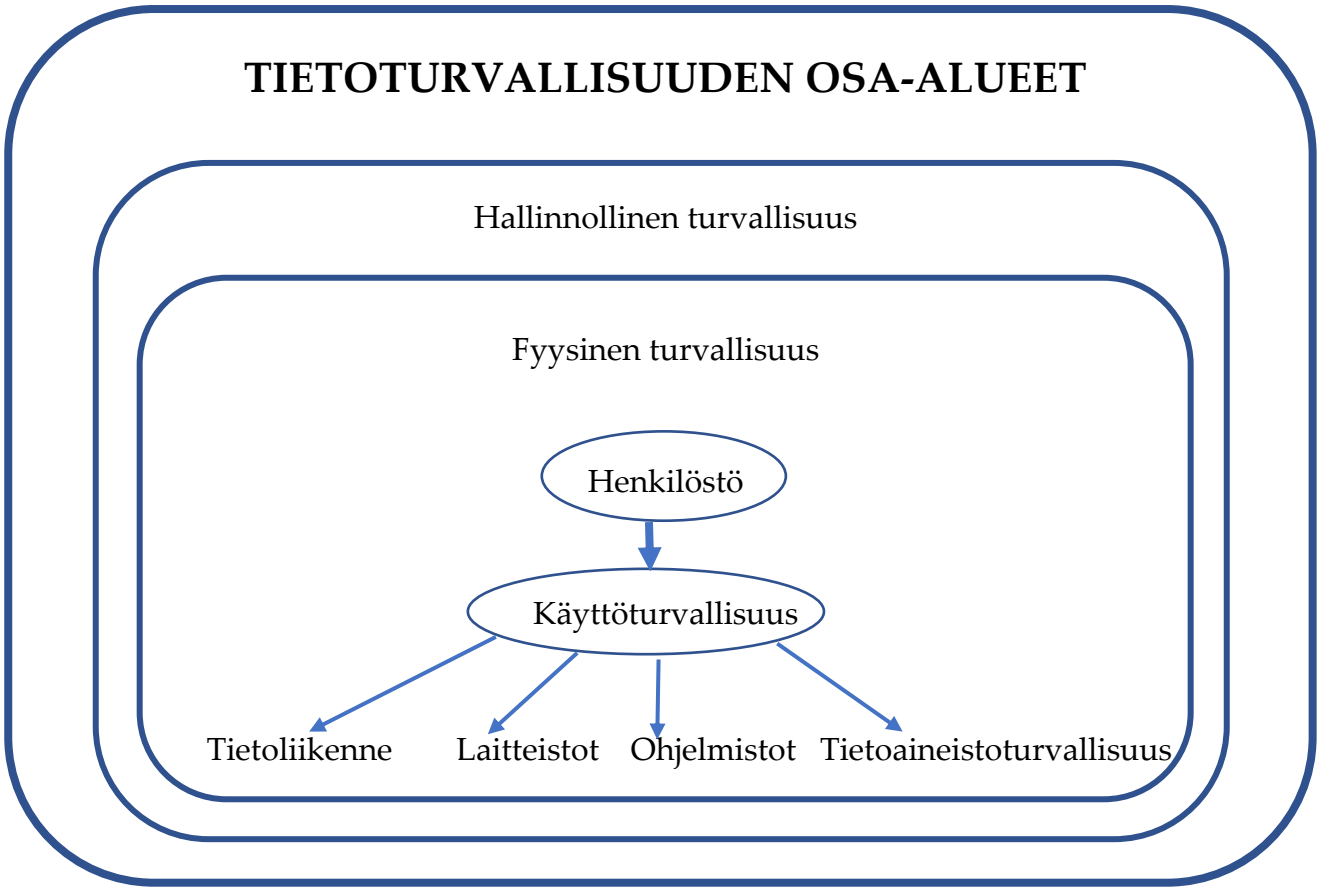
Erilaisia tapoja ja keinoja, joilla voidaan saada estettyä sekä vähennettyä väärinkäytöksiä, on useita. Yksi tavoista on seuranta, joka tarkoittaa sekä järjestelmien käytön että järjestelmissä tehtävien muutosten tarkastelua ja seurantaa. Tapa, jolla tarkastelua ja seurantaa voidaan tehdä, on esimerkiksi tietojen tallentaminen erilliselle lokipalvelimelle. Kun järjestelmien käytöt ja järjestelmissä tehtävät muutokset tallennetaan erilliselle palvelimelle, on mahdollista aukottomasti esittää järjestelmän käyttö tiettynä ajankohtana ja tietyn käyttäjän kohdalla. Tähän kiistämättömyyteen liittyykin hyvin tiiviisti sekä luottamuksellisuus että eheys. Tästä hyvänä esimerkkinä on lokipalvelimella tapahtuva tietomurto, jolloin tietojen kiistämättömyys on hävinnyt eikä luottamuksellisuutta eikä myöskään eheyttä voida varmistaa. (Kyberturvallisuuskeskus 2021b.)

3.3 Tietoturvallisuuden osa-alueet

Tietoturvallisuus jaetaan yleensä useampaan osa-alueeseen (KUVIO 3). Useampaan osa-alueeseen jakamisen tarkoituksena on parantaa tietoturvallisuuden kokonaisuuden hahmottamista sekä auttaa käytännön toimenpiteissä, joita tehdään tietoturvallisuuden suunnittelemisessa ja kehittämisessä.

Valtiovarainministeriön ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa jakaa tietoturvallisuuden kahdeksaan osa-alueeseen (VAHTI 2003, 29):

- hallinnollinen turvallisuus
- fyysinen turvallisuus
- henkilöstöturvallisuus
- käyttöturvallisuus
- tietoliikenneturvallisuus
- laitteistoturvallisuus
- ohjelmistoturvallisuus
- tietoaineistoturvallisuus.



KUVIO 3. Tietoturvallisuuden osa-alueet

3.3.1 Hallinnollinen turvallisuus

Hallinnollinen turvallisuus tarkoittaa tietoturvan johtamista ja hallinnointia. Hallinnolliseen turvallisuuteen sisältyvät johdon hyväksymät periaatteet, vastuunjako ja riskien arviointi sekä käytettävissä olevat resurssit. Tietoturvariskien hallinta perustuu siihen, että organisaation johto on tietoinen tietoturvariskeistä sekä siihen, että johdolla on välineitä käytössään, joilla hallita tiedossa olevia sekä myös tulossa olevia riskejä. Hallinnollisen turvallisuuden osa-alue on laaja ja siihen kuuluvat tietoturvan johtamisen ja hallinnoinnin lisäksi myös hankinnat sekä suhteet sidosryhmiin. (VAHTI 2004b, 27-29.)

Tietoturvallisesti toimiminen organisaatiossa vaatii tietoturvapolitiikkaa. Tietoturvapolitiikan määrittelee organisaation johto. Tämän lisäksi johdon tehtävänä on selvittää ja määritellä eri tavat ja keinot, kuinka voidaan toimia tietoturvallisesti. Hallinnollinen tietoturvallisuus voidaan nähdä yhtenä tuotantotekijänä ja organisaation johdon apuna voidaan käyttää IT-asiantuntijoita. Tällöin tietoturvaa saadaan kehitettyä suunnitelmallisesti. Jos eri järjestelmien tai palveluiden käytössä on joitain rajoituksia, johdon määrittelemän tietoturvapolitiikan tarkoituksena on selvittää sekä selkeyttää, millaisia rajoitukset ovat, mitkä järjestelmien ja käyttäjien toiminnot pitää olla jäljitettävissä sekä minkä tiedon aitous ja muuttumattomuus tulee säilyttää. Tietoturvapolitiikka antaa pohjan yhtenäiselle ohjeistukselle, joka koskee koko henkilöstöä. (VAHTI 2011, 21.)

Johdon vastuulla on analysoida ja arvioida nykyhetken tietoturvatoimintaa ja tietoturvallisuutta organisaatiossa. Analyysien ja arvioiden avulla on mahdollista löytää kriittisiä haavoittuvuuksia sekä niihin liittyviä uhkia. Kriittisen haavoittuvuuden havaitessaan organisaation johdon tehtävänä on reagoida haavoittuvuudesta mahdollisesti aiheutuviin uhkiin ja saada muutettua toimintaa siten, että uhan aiheuttamat vahingot pienenevät, uhan riski pienenee tai poistuu kokonaan. Johdon vastuulla on myös erilaisten tietoturvan edellyttämien hankintojen tekeminen ja se, että hankitut tietoturvallisuuden edellyttämät laitteet sekä ohjelmistot otetaan käyttöön asianmukaisesti. (Poliisihallitus 2022.)

Hallinnolliseen turvallisuuteen kuuluu, että johto vastaa tietoturvan saavuttamiseksi riittävästä henkilöstön osaamisesta ja kouluttamisesta. Henkilöstön tietoturvakäyttäytymiseen vaikuttaa koulutuksen sekä toimintaohjeiden lisäksi myös se, mikä on tietoturvallisuuden edistämiseen vaadittavan työn määrä. Henkilöstölle annettavissa tietoturvaan liittyvissä koulutuksissa ja ohjeissa pitää ottaa huomioon ohjeiden selkeys ja saada osoitettua tietoturvan toteutuksen helppous, jolloin annetuilla ohjeilla voidaan ohjata henkilöstön tietoturvakäyttäytymistä. (Laaksonen, Nevasalo & Tomula 2006, 249-250.)

3.3.2 Fyysinen turvallisuus

Fyysinen turvallisuus tarkoittaa toimitilojen sekä laitteiden fyysistä suojaamista tapaturmilta ja vahingoittamisyrityksiltä. Fyysisen turvallisuuden tarkoituksena on varmistaa kaikissa tilanteissa organisaation häiriötön toiminta ja turvallinen toimintaympäristö sekä estää organisaation tarvitsemien tietojen vahingoittuminen, tuhoutuminen tai niiden joutuminen vääriin käsiin. (Laaksonen ym. 2006, 125.) Jos toimitilat ovat turvallisuuden osalta puutteellisia, se voi olla yksi syistä, joka antaa joko ulkopuoliselle henkilölle tai omaan henkilöstöön kuuluvalle tilaisuuden joko tahalliseen tai tahattomaan tietoturvallisuutta vaarantavaan tekoon.

Fyysiseen turvallisuuteen liittyy olennaisesti erimuotoinen valvonta. Valvonnan tarkoituksena on säilyttää ja ylläpitää turvattava tieto kaikissa tilanteissa eheänä ja luottamuksellisena. Valvonta fyysisen tietoturvallisuuden yhteydessä tarkoittaa esimerkiksi vartiointia ja vahinkojen ennalta estämistä sekä torjumista. Muun muassa murto-, vesi- sekä paloturvallisuus ja teknisten laitteiden ja palvelinten sijainti ovat asioita, jotka on huomioitava fyysisessä turvallisuudessa tietoturvallisuuden varmistamiseksi ja takaamiseksi. (VAHTI 2013, 56-58.)

Toimitiloihin liittyvät turvallisuusasiat ovat olennaisia fyysistä turvallisuutta kehitettäessä ja fyysinen turvallisuus luo perustan koko tietoturvallisuudelle. Fyysistä turvallisuutta voidaan parantaa esimerkiksi sähköavaimilla, jolloin luvatonta liikkumista saadaan vähennettyä. Fyysisen turvallisuuden uhkia voidaan pienentää luokittelemalla tiloja tietoturvallisuuden näkökulmasta sekä sijoittaa huonetilat kiinteistössä niiden toimintojen perusteella. Fyysisen turvallisuuden katsotaan luovan pohjan tietoturvallisuudelle ja sen jokaiselle osa-alueelle. Ilman tätä pohjaa hallinnolliset sekä erilaiset tekniset ratkaisut tietoturvallisuuden säilyttämiseksi ovat hyödyttömiä. (Poliisihallitus 2022.)

3.3.3 Henkilöstöturvallisuus

Henkilöstöturvallisuus tarkoittaa niiden riskien hallintaa, jotka aiheutuvat henkilöstöstä ja koskevat henkilöstöä. Näitä ovat muun muassa vastuihin, rooleihin ja tietoturvaohjeistuksiin sekä annettuihin tehtäviin liittyvät asiat. Henkilöstöturvallisuutta tarvitaan ehkäisemään henkilöstön aiheuttamia tietoturvauhkia, niin tahallisia kuin tahattomiakin. (VAHTI 2007, 57.)

Henkilöstön käytännön toimissa ja päivittäisissä työtehtävissä tietoturvallisuuteen liittyy monia tietoturvallisuusriskejä. Kun käytetään useita eri tietojärjestelmiä sekä käsitellään salassa pidettävää materiaalia, henkilöstöturvallisuudella on iso merkitys. Henkilöstöturvallisuuden merkitys korostuu ja henkilöstön virheelliset toimintatavat sekä henkilöstöstä aiheutuvat riskit on pyrittävä estämään ennalta sekä minimoimaan. (Laaksonen ym. 2006, 143.)

Henkilöstön onnistuneelle riskienhallinnalle luo pohjan tietoisuus uhkista. Käytännössä tämä tarkoittaa riskien kartoitusta sekä osaamista ja koulutusta. Henkilön soveltuvuutta tehtävään voidaan arvioida jo rekrytointivaiheessa aikaisempaan työkokemukseen, koulutukseen ja haastatteluun sekä erilaisiin taustaselvityksiin perustuen. Tapoja henkilöstöturvallisuuteen liittyvien riskien minimointiin ovat esimerkiksi käyttöoikeuksien ja toimenkuvien määrittely, koulutus ja valvonta. Kun rekrytointi on tehty, henkilöstö voidaan jakaa tietoturvan näkökulmasta työtehtävien mukaisiin ryhmiin, jolloin määritellään työtehtävien vaatimusten mukaiset oikeudet tietoihin ja käyttöjärjestelmiin sekä luodaan henkilökohtaiset käyttäjätunnukset sekä salasanat. Näillä rajoituksilla ja ennalta suunnitelluilla järjestelyillä on tarkoituksena pyrkiä sekä suojaamaan että hallitsemaan työntekijöiden mahdollisia tahattomia tai tahallisia tietoturvaloukkauksia. (Poliisihallitus 2022.)

Tietoturvaloukkaukset, joita henkilöstö aiheuttaa, ovat usein tavalliseen työhön liittyviä tahattomia tekoja, vahinkoja. Erilaisia syitä esimerkiksi tietojärjestelmien tahattomiin käyttövir-

heisiin voi olla useita. Näitä voivat olla muun muassa työntekijään liittyvät psyykkiset tekijät, kuten väsymys, ylikuormittuminen tai huolimattomuus. Muita syitä työntekijän tahattomiin tietoturvaloukkauksiin voivat olla väärin ymmärretty annettu työtehtävä, puutteellinen koulutus tai epätarkasti määritellyt toimintatavat, mutta myöskin erilaiset asennetut tai ladatut ohjelmat tai tiedostot, joiden työntekijä on ajatellut helpottavan ja auttavan työtehtävissään. (Poliisihallitus 2022.) Henkilöstöturvallisuuden perustan muodostaa motivoitunut henkilöstö, joka on sekä sitoutunut että osaava. Tietoturvallisuuden toteutumiseen vaikuttavat useat eri henkilöstöön liittyvät tekijät. Esimerkiksi työhön suhteutetulla oikealla henkilöstön määrällä sekä tyytyväisyydellä työhön ja työolosuhteisiin on suuri merkitys. (Vahti 2007, 57.)

3.3.4 Käyttöturvallisuus

Käyttöturvallisuudella tarkoitetaan kaikkia niitä päivittäisen toiminnan menettelytapoja, joilla pyritään säilyttämään ja ylläpitämään hyvä tietoturvallisuuden taso. Käyttöturvallisuus on käsitteenä laaja, koska se ei liity ainoastaan henkilöstön työkäytäntöjä koskeviin tapoihin tai periaatteisiin vaan se kattaa tietotekniikan käytön ja tietojenkäsittelyn lisäksi myös käyttöympäristön turvallisuuteen liittyvien tapahtumien valvonnan. Näiden lisäksi käyttöturvallisuuden piiriin kuuluu vielä sekä toimintojen jatkuvuuden, ylläpidon, kehittämisen, tuen että huoltoon liittyvien toimintojen turvallisuus. (Hakala ym. 2006, 12.)

Yhtenä osana käyttöturvallisuutta on muun muassa henkilöstön työviihtyvyyteen sekä tietojärjestelmien tarpeisiin liittyvä ilmastointijärjestelmän kapasiteetti. Ilmastointijärjestelmän kapasiteetin täytyy sopia sekä henkilöstön että tietojärjestelmien tarpeisiin ja näiden tarpeiden yhteensovittaminen saattaa tietoturvallisuuden kannalta olla joskus haastavaa. Henkilöstön osalta ilmastoinnin mitoittaminen oikein tarkoittaa sitä, että henkilöstöllä ei ole kesällä eikä talvella tarvetta esimerkiksi avata ikkunaa, jolloin tietoturvallisuus ainakaan ensimmäisen kerroksen osalta ei olisi turvattuna. Laitteistojen osalta vikojen todennäköisyys pienenee,

kun ilmastointijärjestelmä on mitoitettu oikein. Tällöin vältytään erilaisilta laitteistojen ylikuumenemiseen liittyviltä katkoksilta. Käyttöturvallisuuteen kuuluu olennaisesti myös sähkökatkoksiin ja tulipaloihin varautuminen. Sähkökatkoksen sattuessa keskeisten turvallisuuteen liittyvien toimintojen tulee säilyä toimintakuntoisena ja erilaisiin sähkönjakeluun liittyviin häiriöihin voi varautua esimerkiksi varavoimalla tai häiriönsuojauksella. (VAHTI 2004b, 49-50.) Tulipalon varalta kiinteistössä tulee olla kunnossa oleva palohälytys- ja tulipalon sammutusjärjestelmä (VAHTI 2004b, 51).

3.3.5 Tietoliikenneturvallisuus

Tietoliikenneturvallisuus käsittää erilaisten tietoliikennelaitteistojen kokoonpanon, ylläpidon sekä muutosten valvonnan. Tietoliikenneturvallisuus käsittää myös ongelmatilanteiden kirjaukset, käytön valvonnan, verkon hallinnan, viestinnän salaamisen ja varmistamisen sekä tietoturvallisuuden kannalta merkityksellisten tapahtumien tarkkailun, kirjaamiset, luetteloinnit ja selvittämiset sekä testaamiset ja hyväksymiset, jotka liittyvät tietoliikenneohjelmiin. Tietoliikenneturvallisuuteen liittyvät myös tiedonsiirtämiseen suunnitellut tietoturvamekanismit. Näillä erilaisilla tietoturvamekanismeilla tarkoitetaan tietoverkoissa liikkuvien tietojen luottamuksellisuuteen, eheyteen ja käytettävyyteen ja näiden varmistamiseen liittyviä toimenpiteitä. (Hakala ym. 2006, 12.)

3.3.6 Laitteistoturvallisuus

Laitteistoturvallisuudella tarkoitetaan tietokoneiden yleistä suojaamista, johon kuuluvat sekä tietoliikenne- ja tietojenkäsittelylaitteiden turvallisuusominaisuudet että asennukset, huoltosopimukset ja yhtenäinen laitteistopolitiikka. Laitteistoturvallisuus käsittää varmistuksen tietojenkäsittely- ja tietoliikennelaitteiden käytettävyydestä, toiminnasta, kokoonpanosta, kunnossapidosta sekä laadusta. Koska ajoittain järjestelmien tietoturvapäivitysten yhteydessä tai

päivitysten asentamisen jälkeen havaitaan erilaisia ongelmia, päivitykset täytyy tarvittaessa saada peruttua. Laitteistoturvallisuus kattaa edellä mainittujen lisäksi myös laitteiston turvallisen poiston sen jälkeen, kun sen käyttö lopetetaan. (VAHTI 2007, 63.)

3.3.7 Ohjelmistoturvallisuus

Ohjelmistoturvallisuus sisältää käyttöjärjestelmien sekä tietoliikenne-, väli- ja sovellusohjelmistojen turvallisuuden. Sillä tarkoitetaan ohjelmistojen tietoturvaan kuuluvia järjestelmien salasanoja sekä erilaisia turvallisuustoimia ja ohjelmistojen laadunvarmistusta. Osana ohjelmistoturvallisuutta ovat myös lokimenettelyt, tarkkailu- ja paljastustoimet, pääsynvalvonta-, varmistus-, tunnistamis- ja eristämismenettelyt sekä ylläpitoon ja päivityksiin liittyvät asiat. Ohjelmistoja valittaessa ja harkittaessa tulee arvioida niiden luotettavuutta sekä sitä, ovatko ne soveltuvia tehtäväänsä usean vuoden ajan. Ohjelmistoturvallisuuteen vaikuttaa vahvasti ohjelmistojen tuleville käyttäjille saatavissa oleva ohjeistus sekä koulutus ennen ohjelmiston käyttöönottoa. (VAHTI 2007, 69.) Ennen kuin ohjelmistoja valitaan organisaation käyttöön, ohjelmistot täytyy testata. Ohjelmistojen testauksissa täytyy tulla esille se, että ohjelmisto tukee vahvaa salausta sekä käyttäjätodennusta. (VAHTI 2007, 71.)

3.3.8 Tietoaineistoturvallisuus

Tietoaineistoturvallisuuteen kuuluvat sekä sähköisten että paperisten dokumenttien käytettävyys, eheys ja luottamuksellisuus. Tietoaineistoturvallisuus koskee ainoastaan tiedostojen ja asiakirjojen käsittelyä ja suojaamista koko niiden elinkaaren ajan. Hyvään tietoaineistoturvallisuuteen sisältyvät tietoaineistojen, tietojärjestelmien sekä tietovälineiden asianmukainen hallinta, käsittely, säilytys ja hävittäminen. (VAHTI 2006, 31-32.) Tietoaineistoturvallisuus on myös tietojen ja tietovälineiden tunnistamista, turvallisuusluokitusta ja varmistamista. Tietoaineistoturvallisuutta parannetaan eri talletusmuodoissa olevien asiakirjojen, tiedostojen ja

muiden tietoaineistojen käytettävyyden, eheyden ja luottamuksellisuuden varmistamisella niiden kaikissa käyttövaiheissa sekä luokittelemalla tieto ja sitä käsittelevä henkilöstö. (Laaksonen ym. 2006, 67.)

Tietoaineisto, joka aiotaan hylätä tai heittää pois, on tuhottava siten, ettei esimerkiksi salassa pidettävä aineisto päädy vääriin käsiin. Aineiston tuhoaminen on tehtävä siten, että aineistossa ollutta materiaalia tai sisältöä ei pystytä uudelleen käyttämään. Tämä tarkoittaa sitä, että aineisto on tuhottava joko fyysisesti, mekaanisesti tai päällekirjoittamalla. Mekaaninen tuhoaminen voi tarkoittaa esimerkiksi silppurilla tuhoamista ja se on suoritettava siten, ettei tuhotun aineiston, esimerkiksi levyjen, levykkeiden tai tulosteiden, uudelleenkokoaminen ole mahdollista. (VAHTI 2006, 27.)

4 TOIMEKSIANTAJAN ESITTELY JA POLIISIN TIETOTURVALLISUUS

Opinnäytetyön toimeksiantaja Oulun poliisilaitos toimii Kainuun ja Pohjois-Pohjanmaan alueella. Pääpoliisiasema sijaitsee Oulussa ja pääpoliisiaseman lisäksi muita poliisiasemia sekä palvelupisteitä on yhteensä 16 kappaletta. (Poliisi 2020a.)

Poliisihallituksen alaisuudessa toimivia poliisilaitoksia on yhteensä yksitoista. Nämä yksitoista poliisilaitosta muodostavat yhdessä paikallispoliisin palveluverkon, eli poliisilaitosten pääpoliisiasemat, poliisiasemat, poliisin palvelupisteet sekä yhteispalvelun asiointipisteet. Myös poliisin valtakunnalliset yksiköt Keskusrikospoliisi ja Poliisiammattikorkeakoulu toimivat Poliisihallituksen alaisuudessa. (Poliisi 2020b.)

Poliisihallitusta johtaa poliisiylijohtaja. Poliisihallituksen tehtävänä on johtaa ja ohjata poliisin operatiivista toimintaa. Operatiivisen johtamisen ja ohjaamisen lisäksi Poliisihallitus suunnittelee, kehittää ja valvoo poliisitoimintaa sekä poliisin tukitoimintoja. Poliisihallituksen vastuulla on tarjota poliisin palveluita kansalaisille eri puolella Suomea siten, että palveluita on tarjolla tasapuolisesti. Poliisihallitukseen kuuluvat Riihimäellä sijaitseva arpajais- ja asehallinto ja Mikkelissä sijaitseva turvallisuusalan valvonta. Suojelupoliisi (SUPO) on suoraan sisäministeriön alainen valtakunnallinen yksikkö. (Sisäministeriö 2022.)

Keskusrikospoliisin (KRP) toimialueena on koko Suomi ja sen tehtävänä on sekä paljastaa että tutkia vakavaa, järjestäytynyttä sekä ammattimaista rikollisuutta. Tämän lisäksi Keskusrikospoliisin tehtäviin kuuluu rikostorjunnan eli esitutkinnan, rikostiedustelun ja rikostutkintamenetelmien kehittäminen. (Poliisi 2020c.) Suomen Rikostekninen laboratorio sekä Kyberrikoskeskus toimivat Keskusrikospoliisissa. Keskusrikospoliisilla on lisäksi vastuu poliisin, Tullin ja Rajavartiolaitoksen rikostiedusteluyhteistyöstä. (Sisäministeriö 2022.)

Tampereella sijaitseva Poliisiammattikorkeakoulu (Polamk) vastaa poliisikoulutuksesta eli poliisikoulutukseen rekrytoinnista sekä opiskelijavalinnoista ja poliisin tutkintokoulutuksesta. Poliisiammattikorkeakoulu vastaa myös johtamiskoulutuksesta, täydennyskoulutuksesta sekä poliisialan tutkimus- ja kehittämistoiminnasta. Poliisiammattikorkeakoulussa toimii myös poliisin tilastopalvelu. Poliisiammattikorkeakoulussa tehdään sisäisen turvallisuuden suunnittelu- ja kehitystyötä sekä poliisitoimintaa palvelevaa soveltavaa tutkimus- ja kehitystyötä. (Sisäministeriö 2022.)

Poliisin organisaatioturvallisuutta johdetaan Poliisihallituksen vahvistaman hallintajärjestelmän mukaisesti. Organisaatioturvallisuuden johtamisella tarkoitetaan ihmisten, menetelmien sekä prosessien johtamista. Poliisin ylijohtona toimii Poliisihallitus, jonka tehtävänä on suunnitella, kehittää, johtaa sekä valvoa poliisitoimintaa ja sen tukitoimintoja alaistensa poliisiyksiköiden osalta. Poliisihallitus antaa koko poliisia koskevat organisaatioturvallisuutta, tietoturvallisuutta ja muuta riskienhallintaa sekä valmiussuunnittelua ja varautumista määrittävät ja ohjaavat turvallisuusohjeet ja turvallisuusmääräykset. (Poliisihallitus 2022.) Tämän lisäksi poliisiyksiköt voivat antaa näitä linjauksia noudattaen turvallisuusohjeita ja turvallisuusmääräyksiä, jotka ovat yksikkökohtaisia.

Poliisin turvallisuusorganisaatioon kuuluvat Poliisihallituksessa toimivat poliisin turvallisuuspäällikkö, valmiuspäällikkö, tietoturvapäällikkö, turvallisuus- ja tietoturva-asiantuntijat sekä poliisiyksiköiden turvallisuuspäälliköt, valmiusvastaavat ja tietoturvavastaavat. (Poliisihallitus 2022.)

Poliisin organisaatioturvallisuudella tarkoitetaan turvallisuuden eri osa-alueista ja niille sijoittuvista tehtävistä ja toiminnoista muodostuvaa kokonaisuutta sekä tämän kokonaisuuden ohjausta, johtamista ja hallintaa. Poliisin organisaatioturvallisuuden päämääränä on toimintaympäristö, jossa poliisi voi suorittaa tehtäviään turvallisesti ja häiriöttömästi. Poliisi varmistaa päämäärän saavuttamiseksi turvallisuusvaatimusten toteutumisen, ennaltaehkäisemi-

sen ja erilaisten turvallisuusriskien torjumisen, jotka kohdistuvat poliisiorganisaatioon. Tämän lisäksi poliisi varautuu toimimaan turvallisuusympäristössä, joka muuttuu ja on monimuotoinen. (Poliisihallitus 2022.)

Poliisin organisaatioturvallisuuden painopisteosa-alueita ovat (Poliisihallitus 2022):

- organisaatioturvallisuuden johtaminen
- henkilöturvallisuus
- henkilöstöturvallisuus
- fyysinen turvallisuus
- tietoturvallisuus
- sidosryhmäturvallisuus
- valmiussuunnittelu ja varautuminen.

Poliisin tietoturvallisuudella tarkoitetaan, että uhat, jotka kohdistuvat poliisin tietojen, tietojärjestelmien ja tietoliikenteen käytettävyyteen, eheyteen ja luottamuksellisuuteen eivät missään olosuhteissa aiheuta merkittävää riskiä poliisissa käsiteltävälle tiedolle tai poliisin tehokkaalle toiminnalle. Kehittämisen ydinalueita poliisin tietoturvallisuudessa ovat poliisin henkilöstön valmiudet sekä prosessit ja teknologia. (Poliisihallitus 2022.)

Henkilöstöturvallisuuden tarkoituksena on pyrkiä vaikuttamaan välttämällä, poistamalla tai minimoimalla turvallisuusriskejä, joita tahallisesti tai tahattomasti, poliisin henkilöstö tai poliisin toimintaympäristössä työskentelevät voivat aiheuttaa poliisille. Fyysisen tietoturvallisuuden tarkoituksena on suojata rakenteellisilla ja teknisillä turvallisuusratkaisuilla poliisin hallinnoimia kiinteistöjä ja toimitiloja. Tämän lisäksi fyysisellä tietoturvallisuudella on tarkoitus suojata poliisin kiinteistöissä ja toimitiloissa työskenteleviä ja asioivia henkilöitä, tiloissa säilytettävää omaisuutta sekä salassa pidettäviä tietoja ja tietoaineistoja. Fyysisen turvallisuuden tarkoituksena on suojata toimintaa onnettomuuksilta, vaaroilta sekä rikoksilta ja ennalta estää, ehkäistä ja havaita vastaavat uhat. Keskeisiä turvallisuusteknisiä järjestelmiä

ovat kameravalvonta-, kulunvalvonta-, rikosilmoitin-, paloilmoitin- ja avainhallintajärjestelmät. Erilaisilla fyysisen turvallisuuden ratkaisuilla saadaan mahdollistettua henkilöstön työ- tai virkatehtävien edellyttämät kulkuoikeudet poliisin hallinnoimien kiinteistöjen ja toimitilojen määritetyille turvallisuusalueille. (Poliisihallitus 2022.)

Tiedonhallintalaki, joka astui voimaan 1.1.2020, toi mukanaan poliisin toimitiloissa tapahtuvaan tiedon käsittelyyn muutoksia. Tiedonhallintalain voimaan astumisen jälkeen poliisin tai poliisiyksikön hallinnoimissa kiinteistöissä ja toimitiloissa tehtiin jako turvallisuusluokitteluasetuksen mukaisiin turvallisuusalueisiin, joita ovat hallinnollinen alue (KUVIO 4) ja turvaalue (KUVIO 5) sekä turvallisuusalueen ulkopuoliset alueet.

KUVIO 4. Hallinnollisen alueen kyltti (Poliisihallitus 2022)

KUVIO 5. Turva-alueen kyltti (Poliisihallitus 2022)

Poliisin toimitilojen turvallisuusalueiden tarkoituksena on osaltaan varmistaa, että salassa pidettävää tietoa käsitellään ja säilytetään asianmukaisesti. Turvallisuusalueen taso määräytyy sen perusteella, mitä toimintaa alueella, toimitilassa tai tilaryhmässä tapahtuu sekä minkälaisia turvallisuusriskejä alueelle, toimitilaan tai tilaryhmään kohdistuu. (Poliisihallitus 2022.)

5 EMPIIRISEN TUTKIMUKSEN TOTEUTUS

Opinnäytetyön aiheen pohtimisen aloitin kesällä 2021. Aiheeksi muodostui henkilöstön käsitykset Oulun poliisilaitoksen tietoturvallisuudesta ja sen tasosta. Teoreettinen viitekehys opinnäytetyöhön rakentui syksyn 2021 aikana ja käytännön osa toteutui kevään 2022 aikana.

5.1 Empiirisen tutkimuksen tavoitteet sekä tutkimusongelmat

Opinnäytetyön ja empiirisen tutkimuksen tavoitteena ja tarkoituksena oli selvittää henkilöstön käsityksiä Oulun poliisilaitoksen tietoturvallisuudesta ja sen tasosta. Tavoitteena oli kartoittaa työhön liittyviä tietoturvallisuutta heikentäviä tekijöitä, joita Oulun poliisilaitoksen henkilöstö kokee tietoturvallisuuden eri osa-alueilla olevan. Opinnäytetyön tavoitteena oli lisäksi selvittää henkilöstön kehittämisideoita Oulun poliisilaitoksen tietoturvallisuuden parantamiseksi.

Tutkimuskysymyksen muodossa esitettynä opinnäytetyön päätutkimusongelma on:

- Millaiseksi poliisilaitoksen henkilöstö kokee tietoturvallisuuden tason Oulun poliisilaitoksella?

Päätutkimusongelma jakautuu neljään alaongelmaan. Tutkimuskysymysten muodossa esitettyinä opinnäytetyön alaongelmat ovat:

- Missä tietoturvallisuuden osa-alueissa henkilöstö kokee tietoturvallisuuden onnistuneen hyvin?
- Missä tietoturvallisuuden osa-alueissa henkilöstö kokee olevan eniten kehittämistarvetta?

- Mitkä seikat heikentävät tietoturvallisuutta?
- Millä keinoin tietoturvallisuutta voitaisiin kehittää?

5.2 Tutkimusote, tiedonkeruu sekä aineiston käsittely ja analysointi

Tutkimusotteeksi tässä tutkimuksessa valikoitui kvalitatiivinen tutkimusote. Tutkimusotetta päätettäessä koettiin, että kvalitatiivisella eli laadullisella tutkimusotteella pystytään saamaan haastateltujen henkilöiden näkökulmat selkeästi, kattavasti ja kuvaavasti esille sanoilla, lauseilla ja merkityksillä (Hirsjärvi & Hurme 2006, 27-28).

Empiirisen tutkimuksen tiedonkeruu suoritettiin haastatteluilla. Ennen haastatteluita laadittiin valmis kysymys- ja haastattelurunko teemahaastattelua eli puolistrukturoitua haastattelua varten. Tutkimuskysymyksen osalta päätutkimusongelma sekä sen neljä alaongelmaa olivat ennalta pohdittu ja teemahaastattelun kysymys- ja haastattelurunko rakentui pitkälti näiden ongelmien ympärille. Haastattelurunko kysymyksineen rakentui siten, että se oli käytettävissä ilman soveltamista jokaiselle haastateltavalle, toimenkuvaan tai työtehtävään katsomatta.

Haastattelurunkoa tehdessä, tai viimeistään sen valmistuttua, on päätettävä, ketä haastatellaan. Myös haastattelujen aikataulusta sekä paikasta on tehtävä päätös. Haastatteluja varten päätettiin valita Oulun poliisilaitoksen jokaiselta sektorilta henkilöitä haastateltavaksi, eli ensimmäisenä kriteerinä haastateltavien valinnassa oli se, että tietoa tutkimuskysymyksiin saatiin mahdollisimman laajasti. Toisena kriteerinä oli, että haastateltavia on Oulun poliisilaitoksen organisaation eri sektoreilta ja hierarkian eri tasoilta. Kolmantena kriteerinä oli, että haastateltavia on Oulun poliisilaitoksen eri poliisiasemilta. Haastateltavien määrä, kaksitoista henkilöä, oli päätetty aikaisemmin opinnäytetyötä suunniteltaessa ja sen arvioitiin antavan riittävällä laajuudella tietoa, käsityksiä ja näkemyksiä tutkittavasta asiasta.

Haastattelujen sopimiseksi valittuihin henkilöihin otettiin yhteyttä joko kasvotusten, soittamalla tai sähköpostitse. Yhteydenotoissa selvitettiin mahdollista halukkuutta osallistua opinnäytetyöhön liittyvään haastatteluun. Kaikki ennakkoon valitut kaksitoista henkilöä suostuivat haastateltaviksi ja tulevan haastattelun ajankohdasta ja paikasta sovittiin samassa tapaamisessa tai yhteydenotossa. Tässä ensimmäisessä kontaktissa haastateltaville kerrottiin myös opinnäytetyön aiheesta, hankitusta tutkimusluvasta sekä tavasta, jolla haastattelu tullaan suorittamaan ja kuinka vastaukset tullaan keräämään käsittelyä ja analysointia varten. Tämän lisäksi haastateltaville kerrottiin, että opinnäytetyötä varten ei kerätä yksilöiviä henkilötietoja.

Kaikille kahdelletoista haastateltavalle sekä haastattelurunko että haastattelukysymykset olivat samat. Koska haastattelutilanne niin sanotusti ”elää”, kysymysten järjestystä voitiin muuttaa haastattelun yhteydessä. Kaikki kaksitoista haastattelua suoritettiin kasvotusten ja vuorovaikutuksessa, puolistrukturoituina haastatteluina. Vuorovaikutustilanteissa keskeisiksi muodostuivat haastateltavien sanavalinnat ja tulkinnat, kehonkieli, sanaton viestintä sekä haastatteluiden tunnelmat ja ilmapiirit. Haastateltavien sanavalinnat ja tulkinnat pystyttiin keräämään käsittelyä ja analysointia varten talteen, mutta haastateltavien kehonkieli, sanaton viestintä sekä haastatteluissa vallitsevien ja välittyvien tunnelmien kerääminen käsittelyä ja analysointia varten ei ollut mahdollista, koska haastatteluja ei tallennettu esimerkiksi videoimalla tai äänittämällä.

Tutkimuksen teemahaastattelut suoritettiin 1.2.-24.3.2022. Kahdestatoista haastatellusta miehiä oli seitsemän ja naisia viisi. Haastateltavat työskentelevät Oulun poliisilaitoksen lupa-, valvonta- ja hälytystoiminta- sekä rikostorjuntasektorilla hierarkian eri tasoilla. Kaikki haastattelut suoritettiin yksilöhaastatteluina. Aluksi haastateltavalle esitettiin kirjallinen tutkimuslupa sekä kerrottiin tarkemmin opinnäytetyön aiheesta, tarkoituksesta sekä tavoitteesta. Haastateltavalle kerrottiin, että hänen haastattelussaan antamat vastaukset kerätään vapaan kerronnan vastauksina sekä haastattelijan tarvittaessa tekemien merkkien, kuten plussien ja miinusten, mukaisesti. Haastateltavalle selvitettiin myös, että haastattelun jälkeen vastaukset

analysoidaan ja analysoinnin jälkeen kaikki haastattelussa käytetty ja kerätty aineisto hävitetään. Haastateltavalle selvitettiin, että haastattelussa ei missään vaiheessa kerätä eikä tallenneta minkäänlaista yksilöivää henkilötietoa.

Varsinaisten haastattelukysymysten osalta, aluksi haastateltavalta selvitettiin yleistä mielipidettä tietoturvallisuudesta ja sen tärkeydestä. Tämän jälkeen haastattelussa edettiin Oulun poliisilaitoksen tietoturvallisuutta koskeviin kysymyksiin. Vaikka haastattelurunko oli kaikille haastateltaville sama, haastattelujen kestot vaihtelivat suuresti. Lyhimmillään haastattelu kesti 21 minuuttia ja pisimmillään yhden tunnin ja kaksi minuuttia. Haastattelujen kestoon vaikuttivat merkittävästi muun muassa haastateltavan innostus ja kiinnostus aiheeseen, luontainen puheliaisuus sekä haastateltavan vireystila.

Haastattelun jälkeen kerätty aineisto analysoitiin välittömästi. Aineisto järjestettiin ja muokattiin käsiteltävään muotoon. Koska haastattelurunko oli jokaisessa haastattelussa sama, muodostettiin haastattelurungon perusteella taulukko, johon kerättiin vapaan kerronnan vastauksista esiin nousevat asiat. Vastausten tulkintojen sekä taulukointien jälkeen kahdentoista haastatellun henkilön vastaukset antoivat analysoinnin jälkeen selvitystä päätutkimusongelmaan sekä neljään alaongelmaan. Analysoinnin jälkeen haastatteluissa käytetty ja kerätty aineisto on kokonaisuudessaan tuhottu. Tämän tutkimuksen johtopäätökset on tehty haastatteluista saatujen vastausten tulkinnoista.

5.3 Tutkimuksen luotettavuus ja sen arviointi

Tehdyn tutkimuksen luotettavuuteen vaikuttavia tekijöitä ovat tutkittava ilmiö, tutkimusmenetelmä sekä tutkija. Tutkittavan ilmiön, eli tietoturvallisuuden ja sen tason selvittämiseksi henkilöstön näkökulmasta, toimeksiantajaorganisaatiosta valittiin haastateltaviksi henkilöitä, joilta odotettiin saatavan tutkittavasta asiasta riittävästi tietoa johtopäätösten tekemiseksi.

Haastatelluilla henkilöillä on omakohtaista kokemusta tietoturvallisuudesta työ- ja virkatehtäviensä hoitamisen yhteydessä. Tästä syystä koettiin, että paras tieto tutkittavaan asiaan oli saatavissa heiltä.

Tutkimusmenetelmäksi valitun teemahaastattelun koettiin tuovan tutkittavaan ilmiöön parhaiten näkökulmia sekä aineistoa. Tutkimusmenetelmä mahdollisti sen, että haastatteluissa edettiin tutkimusongelmittain avoimilla kysymyksillä. Tarvittaessa haastatteluissa esitettiin lisäkysymyksiä tarkennusten saamiseksi sekä tulkinnanvaraisuuksien vähentämiseksi, mutta pääasiassa haastatteluissa edettiin ennakkoon valmistellun haastattelurungon mukaisesti. Haastattelurunko oli toteutettu siten, että sen avulla eri näkökulmat tietoturvallisuuteen liittyen tulivat käsiteltyä jokaisessa haastattelussa tasapuolisesti ja toisaalta mitään olennaista tutkimustuloksiin vaikuttavaa tekijää unohtamatta.

Haastattelut dokumentoitiin tarkasti ja koodattiin haastattelun yhteydessä siten, että haastatteluissa saadut tiedot olivat selkeät ja yksinkertaiset analysoida. Tarkan dokumentoinnin ja koodaamisen päätarkoituksena oli tuottaa tutkimusongelmiin luotettavat tutkimustulokset tehtyjen haastatteluiden antamilla tiedoilla.

Ennen haastattelun aloittamista kerrottiin uudelleen, että haastattelu suoritetaan ilman yksilöivien henkilötietojen keräämistä. Samalla kerrottiin, että kaikki haastattelussa kerätty aineisto tullaan haastattelun jälkeen käsittelemään, analysoimaan sekä tuhoamaan. Sen tarkoituksena, että haastateltavista ei kerätty mitään yksilöiviä tietoja, oli rohkaista heitä kertomaan näkemyksensä tutkittavan asian positiivisista ja negatiivisista puolista rehellisesti ja avoimesti. Haastattelujen aikana tai haastatteluissa saatujen aineistojen käsittely- ja analyysivaiheessa ei ilmennyt mitään seikkoja, jotka olisivat osoittaneet haastateltavien jättäneen kertomatta rehellisiä käsityksiään, näkemyksiään tai mielipiteitään tutkittavasta asiasta.

Haastatteluja ei suoritettu kaavamaisesti pelkästään haastattelurunkoa noudattaen vaan vapaata kerrontaa oli paljon. Tästä huolimatta kaikki haastattelurunkoon suunnitellut kysymykset esitettiin kaikille kahdelle toista haastateltavalle. Haastattelukysymysten laatiminen sekä haastattelutilanteessa oleminen ovat tutkijalle työhön perustuvien tehtävien ja kokemusten kautta tuttuja, joten haastattelutilanteen tai sen mahdollisesti aiheuttaman jännityksen ei koeta vaikuttaneen haastattelutilanteeseen tai tämän tutkimuksen tuloksiin.

Analyysivaiheessa tutkija pyrki siihen, että kerättyä aineistoa tulkittiin siitä näkökulmasta, mitä haastateltava on tarkoittanut. Aineistoa tulkittaessa pyrittiin tarkasti estämään tutkijan omat tulkinnat. Kerätty aineisto käytiin useasti läpi haastattelun jälkeen ja kaikki haastattelussa saadut tiedot ja koodaukset liitettiin taulukkoon, josta ne analysoitiin. Analysoinnin jälkeen kaikki kerätty materiaali hävitettiin heti eikä haastatteluista saatuja tietoja vertailtu toisiinsa kesken tutkimuksen. Vasta siinä vaiheessa, kun kaikki haastattelut oli suoritettu, haastatteluista saadut yksittäiset analyysit ja tulokset yhdistettiin keskenään lopullisten tutkimustulosten saamiseksi.

Kvalitatiivisessa tutkimuksessa muun muassa tutkijan omat tulkinnat vaikuttavat tutkimuksen luotettavuuteen ja aineistoa tulkittaessa pyrittiin tarkasti estämään tutkijan omat tulkinnat. Tutkija saattaa lisäksi tehdä vääriä tulkintoja haastattelussa saamastaan aineistosta. Näihin tulkintoihin, joita tutkija haastatteluissa keräämistään aineistoista tekee, vaikuttavat ne tekijät, joita tutkijalla on tutkittavasta asiasta eli omat näkemyksensä, käsityksensä ja mielipiteensä.

Haastateltavat ja tutkija työskentelevät samassa työorganisaatiossa ja tästä syystä tutkittavan ilmiön asettaminen tutun organisaation toimintakulttuuriin ja toimintaympäristöön oli helppoa. Tutkijan ja haastateltavien välinen tuttavuus auttoi tutkimuksessa tutkijaa ymmärtämään asiaan liittyvää kokonaisuutta, jonka haastateltavat toivat haastatteluissaan esille.

Haastattelut sujuivat keskustelevassa hengessä ja haastattelutilanteet olivat rentoja sekä luottamuksellisia. Koska kaikki haastattelut suoritettiin kasvokkain, vuorovaikutus ei siltä osin ollut rajoittunutta, jos verrataan esimerkiksi puhelimitse tehtäviin haastatteluihin.

Haastatteluissa haasteelliseksi osoittautui aiheen rajaaminen ainoastaan tietoturvallisuutta koskeviin aiheisiin. Tästä syystä olikin hyvä, että pohjana haastatteluissa oli valmiiksi laadittu haastattelurunko ja keskustelun ajauduttua haastattelussa ohi tutkittavana olevasta tietoturvallisuusaiheesta, rungon avulla haastattelu oli helppo ohjata takaisin kohti tutkimusongelmia koskevia asioita. Haastattelurunko helpotti haastattelussa myös siinä, että kaikki tutkimusongelmiin liittyvät kysymykset tuli käytyä läpi ja esitettyä kaikille kahdelletoista haastateltavalle samalla tavalla.

Koen, että tutkimusongelmiin saatiin haastatteluissa vastauksia ja näin ollen tutkimukselle asetettuihin tavoitteisiin päästiin. Tutkimuksessa tuli esille, että haastateltavien vastaukset olivat hyvin samankaltaisia keskenään, mutta eroavaisuuksiakin löytyi, esimerkiksi eri sektoreilla työskentelevien vastauksissa. Pääsääntöisesti eroavaisuudet olivat kuitenkin painotuksissa ja tutkimusongelmien vastauksissa ei tullut esille merkityksellistä eroa tai tietoa. Tässä tutkimuksessa saatuja tutkimustuloksia voidaan hyödyntää esimerkiksi, kun suunnitellaan tietoturvallisuuteen liittyviä ohjeita, kartoitetaan riskejä ja uhkia tai suunnitellaan tietoturvallisuuskoulutuksia ja niiden sisältöä.

Tätä tutkimusta suunniteltaessa haastateltavien lukumäärä päätettiin harkinnanvaraisesti kahdeksitoista henkilöksi ja määrä on koettu riittäväksi ammattikorkeakoulutasoiseen opinnäytetyöhön.

6 TUTKIMUSTULOKSET

Tässä luvussa esitetään tutkimustulokset. Tutkimustulokset on jaettu viiteen osaan päätutkimusongelman ja alaongelmien mukaisesti. Tulosten havainnollistamiseksi esitetään haastateltavien suoria lainauksia.

6.1 Haastateltavien käsityksiä tietoturvallisuuden tasosta

Haastateltavien yleinen käsitys ja mielipiteet tietoturvallisuudesta ja sen tärkeydestä olivat hyvin samankaltaisia keskenään. Tietoturvallisuuden koettiin olevan suuressa roolissa nykyyhteiskunnassamme ja tietoturvallisuuden huomioiminen sekä yksityiselämässä että työtehtävissä koettiin tärkeänä ja erittäin tarpeellisena. Haastateltavat kertoivat, että jatkuva kehittäminen ja seuranta ovat välttämättömiä tietoturvallisuuden hyvän tason sekä luotettavuuden ylläpitämiseksi.

Tietoturvallisuus nähtiin myös merkittävänä osana ammatinhallintaa ja käsitys Oulun poliisilaitoksen tietoturvallisuuden tasosta haastateltavilla oli, että se on kokonaisuudessaan joko riittävällä tai hyvällä tasolla, mutta kehitettävääkin on. Lähes kaikki haastateltavat kertoivat, että tietoturvallisuuden taso on parantunut ja kehittynyt viimeisten 2-3 vuoden aikana. Haastateltavat kokivat tehdyt muutokset sekä tämänhetkisen tietoturvallisuustilanteen myönteisiksi ja olivat tyytyväisiä työnantajan toimiin tietoturvallisuuden edistämiseksi.

> Ei se [tietoturvallisuus] varmaan huonolla tasolla ole, mutta kehitettävää on aina. (Henkilö B)

> Kyllä tietoturvallisuusasiat on kovasti järkeistyneet ja nehän otetaan aivan toisella tavalla työtehtävissä huomioon kuin vaikka kolme vuotta sitten. (Henkilö G)

Haastatteluissa tuli esille, että tietoturvallisuuden tason koettiin parantuneen ja kehittyneen muun muassa järjestelmien ja ohjelmistojen käytettävyyden sekä tehtyjen laitehankintojen ansiosta. Samalla kuitenkin haastateltavat kertoivat, että järjestelmien ja ohjelmistojen parantunut tietoturvallisuus aiheutti käytettävyysongelmia ja niiden koettiin hankaloittavan ja kankeuttavan työntekoa. Erityisesti nopeissa tilanteissa ja kiireisissä työtehtävissä tietojärjestelmien ja ohjelmistojen tietoturvallisuuden huomioimisen koettiin vaikeuttavan ja hidastavan työntekoa. Haastatelluista noin puolet olivat sitä mieltä, että silloin kun järjestelmien ja ohjelmistojen käyttäminen koetaan työlääksi tietoturvallisuussyistä, se aiheuttaa tilanteita, jolloin tietoturvallisuus unohtuu tai jää taka-alalle ja käsillä oleva työtehtävä hoidetaan tietoturvallisuuden kannalta ajatellen harkitsemattomasti ja riskialttiisti.

> No kyllä on tullut vastaan semmosia tilanteita, että työtehtäviä on ollut hankala hoitaa, kun ohjelma on ollut joko vaikea tai sitä ei ole ollenkaan voinut jostain syystä käyttää. (Henkilö A)

Haastateltavat kertoivat, että tietoturvallisuuden kokonaisuutta on vaikea hahmottaa ja ymmärtää. Tietoturvallisuuden ajatellaan, ehkä nimestään johtuen, liittyvän pelkästään tietokoneisiin, ohjelmistoihin ja järjestelmiin. Fyysisen tietoturvallisuuden osa-aluetta, eli muun muassa tiloja, henkilöstön toimintaa tai tietojen suojaamista esimerkiksi taukojen ajaksi, ei välttämättä hahmoteta osaksi tietoturvallisuutta.

> Tietoturvallisuuden kokonaisuutta ja käsitettä ei ymmärretä. Tietoturva mielletään tietokoneisiin ja ohjelmistoihin liittyväksi, fyysisen osuuden roolia ei ymmärretä tai se unohtuu. (Henkilö H)

> Sitä ei vain aina ajattele, että minkälaisessa ympäristössä ja mitä tehtäviä sitä tekee. Tai että miten kovalla äänellä puhuu työkavereitten kanssa tai minkälaisia papereita ja asioita käsittelee. Kai sitä on vaan tullut semmoinen rutiini eikä huomaakaan, että huoneen ovi jää auki, kun lähtee vaikka kahville. (Henkilö I)

Kolmannes haastatelluista oli sitä mieltä, että annetut ohjeet ja määräykset tietoturvallisuuteen liittyen ovat vaikeaselkoisia sekä hankalia ymmärtää ja niiden soveltaminen käytäntöön on työlästä ja vaikeaa. Loput haastatelluista kokivat, että työ- ja virkatehtävissä on mahdollista toimia annettujen ohjeiden ja määräysten mukaisesti, mutta se vaatii itseltä viitseliäisyyttä ja keskittymistä asiaan.

6.2 Haastateltavien käsityksiä onnistumisista tietoturvallisuudessa

Tutkimustulosten mukaan onnistumisia tietoturvallisuuteen liittyvissä asioissa oli saavutettu koulutuksissa ja laitehankinnoissa sekä muutoksissa, joita työtiloihin on tehty fyysistä turvallisuutta ajatellen.

Haastatelluista hieman yli puolet koki tietoturvallisuuteen liittyvien verkkokoulutusten olleen kattavia ja tarpeellisia. Heidän mielestään verkkokoulutuksista oli onnistuttu tekemään mielenkiintoisia ja koulutusten sisällön koettiin olevan riittävän laaja, jotta virkatehtävät saadaan tietoturvallisesti hoidettua. Myös poliisiasemilla kouluttajan johdolla suoritetut tietoturvallisuuteen liittyvät koulutuspäivät koettiin onnistuneiksi, varsinkin kun koulutukset tapahtuivat pienemmissä ryhmissä.

> Verkkokoulutukset on hyviä, jos niistä haluaa saada tietoa irti. Ihtestähän se on kiinni, että kahlaako ne vaan joutusasti läpi loppukokeeseen vai keskittyykö niihin. (Henkilö C)

> Hyvin ollaan onnistuttu TL-II tiedon jakamiseen, säilyttämiseen ja käsittelyyn liittyvissä asioissa valtakunnallisen koulutuksen ja laitoskohtaisen koulutuksen ansiosta. (Henkilö H)

Onnistumisista nousivat esille myös erilaiset laitehankinnat, kuten radioihin liitettävät korvanapit sekä automaattisesti lukittuvat tietokoneet ajoneuvoissa ja henkilökohtaisissa työpisteissä poliisiasemien sisätiloissa.

> Ihan hirveän suuri merkitys on korvanapilla. Nyt ei kaikki ympärillä olevat kuule, minkälainen keikka sieltä tuli. (Henkilö L)

> Ei sitä aina muista, kun kiireellä autosta lähtee, himmentää tai lukita ruutua. Siinä on kyllä apuna ollut nuo lukittuvat koneet. (Henkilö J)

Lisäksi haastateltavat mainitsivat tietoturvallisuutta parantavana tekijänä työ- ja kuulustelu-huoneissa tehdyt muutokset ja parannukset fyysisen turvallisuuden osa-alueella.

> Ne muutokset, mitä huoneisiin tehtiin, oli tarpeellisia. Eikä ne ollut edes kovin isoja, mutta merkittäviä silti. (Henkilö F)

Haastatteluissa oli havaittavissa se, että eri sektoreilla työskentelevät haastateltavat kokivat eri asioiden onnistuneen tietoturvallisuuteen liittyen. Valvonta- ja hälytyssektorilla työskentelevät haastatellut mainitsivat laitteistoihin liittyviä seikkoja, lupasektorilla työskentelevät kokivat, että tietoturvallisuuteen liittyvät saadut koulutukset olivat onnistuneet parantamaan tietoturvallisuutta. Rikostorjuntasektorilla työskentelevät mainitsivat työ- ja kuulusteluhuoneissa tehdyt fyysiseen turvallisuuteen liittyvät muutokset onnistuneiksi ja lisäksi sekä saadut koulutukset että laitteistoihin liittyvät seikat onnistuneiksi.

6.3 Haastateltavien käsityksiä tietoturvallisuuden kehittämistarpeista

Kehittämistarpeina haastateltavat mainitsivat muun muassa ohjelmistojen ja laitteistojen käytettävyyteen, ohjeisiin, määräyksiin ja koulutuksiin sekä toimitiloihin ja henkilöstön toimintaan liittyviä seikkoja.

Usean haastateltavan vastauksessa tuli esille, että käytettävyyden ja tietoturvallisuuden välille pitäisi löytää tasapaino. Moni haastateltavista koki, että jatkuvat kirjautumiset käyttäjätunnuksella ja eri salasanoilla useisiin eri järjestelmiin olivat työläitä ja aikaa vieviä. Tämän

lisäksi haastateltavat kertoivat, että usean eri salasanan ylläpitäminen, muistaminen sekä salasanan vaihtaminen tietyin määräajoin tekivät käytettävyydestä hankalaa. Haastateltavat toivoivat järjestelmien kirjautumisiin yhtenäisyyttä ja sitä, että yhdellä kortilla pääsisi nopeasti ja vaivattomasti kirjautumaan.

> Olisi helppoa, kun laitat kortin koneeseen ja saisit yhdellä kertaa käyttöoikeuden kaikkiin järjestelmiin. Jos oltaisiin yhden kortin varassa kaikkiin kirjautumiseen, se tavallaan parantaisi tietoturvallisuutta, koska se keventäisi salasanataakkaa. (Henkilö H)

Haastateltavat kokivat tarpeelliseksi saada poliisiasemille poliisin verkon ulkopuolisia tietokoneita, joilla pystyttäisiin hoitamaan virkatehtävien edellyttämiä alkutoimia ilman, että ollaan yhteydessä poliisin sisäiseen verkkoon. Esimerkkinä tällaisista alkutoimista haastateltavat mainitsivat asiakkaiden toimittamat muistitikut ja niissä olevan sisällön saamisen tietoturvallisesti poliisin käsiteltäväksi.

Vaikka haastateltavat kokivat, että tietoturvallisuuden osalta verkkokoulutuksissa oli onnistuttu, he toivat esille sen, että tietoturvallisuutta koskevat verkkokoulutukset ovat usein hyvin laajoja sisällöltään ja niiden materiaalimäärä on suuri. Tästä syystä osa koulutuksista koettiin raskaiksi ja työläiksi suorittaa työtehtävien ohessa. Haastateltavat kertoivatkin kehittämistarpeeksi, että verkkokoulutukset tulisi huomioida työvuorosuunnittelussa ja niille pitäisi varata ja antaa työaikaa.

Poliisihallinnon ohjeiden ja määräysten osalta haastateltavat kokivat kehittämistarvetta siinä, että niiden tulisi olla lyhyempiä, kielellisesti helpompia lukea ja ymmärtää sekä selkeämpiä.

> Kyllähän ne [Poliisihallituksen ohjeet ja määräykset] aina pyritään ajatuksen kanssa lukemaan alusta loppuun saakka, mutta ne on pitkiä. Siinä saattaa ajatus harhailla ja taas on luettava sama teksti, uudelleen ja uudelleen. (Henkilö K)

Haastateltavat kertoivat, että kehittämistarpeita tietoturvallisuudessa on myös toimitiloissa. Poliisiasemien kulunvalvonta koettiin nykyajan vaatimuksiin riittämättömäksi vanhemmilla poliisiasemilla ja kehittämistarpeeksi mainittiinkin kulunvalvonnan tarkentaminen. Kulunvalvonnan lisäksi kehittämiskohteiksi mainittiin huono tai olematon äänieristys, asiakkaiden odotusaulan ja poliisin omien tilojen lähekkäisyys sekä tilat, jotka on otettu poliisin käyttöön, vaikka ne eivät käytännössä sovellu uuteen käyttötarpeeseensa.

Yleisten tilojen siisteys oli monen haastateltavan mielestä asia, jossa on kehittämistarvetta. Haastateltavat kertoivat, että pöydillä ja tulostimilla lojuvat paperit unohtuvat helposti, jos tiloissa on muutenkin paljon tavaraa. Koettiin, että tällöin myös tietoturvallisuus vaarantuu, jos työpöydillä olevien papereiden joukkoon jää epähuomiossa salassa pidettävää materiaalia. Haastateltavat kokivat, että henkilöstöön kuuluvien asenteilla ja toiminnalla on suuri merkitys siisteyden kannalta.

> Tuntuu, että jos on epäjärjestystä vaikka kenttähuoneessa, niin sen siivoaminen ei kuulu kellekään. Siellä on sitten kaiken maailman papereita sikin sokin ja ketään ei kiinnosta. Pitääkö se aina järjestää joku virkistysiltapäivä, että saadaan paperit ja muut tavarat oikeilla paikoilleen? (Henkilö L)

Moni haastateltavista oli sitä mieltä, että puhtaan pöydän periaate on unohtunut tai työpiste jää kiireen vuoksi siistimättä. Tästä syntyy hyvin pikaisesti kierre, että työpaikan tiloihin alkaa kerääntyä tavaraa sekä papereita ja yleinen siisteys kärsii.

6.4 Haastateltavien käsityksiä tietoturvallisuutta heikentävistä seikoista

Tietoturvallisuutta heikentävinä seikkoina koettiin erityisesti olevan henkilöstön toimintaan, ohjelmistojen ja laitteistojen käyttävyyteen sekä toimitiloihin liittyvissä seikoissa.

Merkittävimpänä tietoturvallisuutta heikentävänä tekijänä haastateltavat pitivät henkilöstön toimintaa; rutinoitumista ja asenteita sekä henkilöstön aiheuttamia tahattomia tietoturvallisuutta vaarantavia tekoja. Haastateltavien mukaan rutinoituminen tietoturvallisuutta heikentävänä tekijänä näkyy muun muassa siten, että asioita tehdään niin kuin aina ennenkin, vaikka tarvetta toimintatapojen muutokselle on. Tarvittavia toimintatapamuutoksia varten on saatu ja saadaan koulutusta, mutta siltikään toimintatavat ja rutiinit eivät muutu.

Tässä yhteydessä haastateltavat mainitsivat tahattomien tietoturvavirheiden tekemisen, mutta myös välinpitämättömyyden ja laiskuuden. Haastateltavat kokivat, että suurin tietoturvallisuutta heikentävä seikka on ihminen, jolla on vääränlainen asenne tai joka toimii ajattelemattomuuttaan tietoturvallisuutta heikentävästi ja vaarantavasti. Haastateltavista kolmannes mainitsi, että usein toimitaan tietoturvallisuutta sen kummemmin ajattelematta niin sanotusti vanhalla kaavalla, ja koska mitään isoa tietoturvallisuuteen liittyvää katastrofia ei toistaiseksi ole tapahtunut, ei ymmärretä tarvetta toimintatapojen muutokseen ja toimitaan niin kuin ennenkin.

Käytettävyysongelmien koettiin merkittävällä tavalla hankaloittavan ja vaikeuttavan työntekoa, erityisesti kiireessä ja nopeissa tilanteissa. Haastatelluista noin puolet oli sitä mieltä, että silloin kun järjestelmien käyttäminen koetaan työlääksi tietoturvallisuussyistä, se aiheuttaa tilanteita, jolloin tietoturvallisuus unohtuu tai jää taka-alalle ja käsillä oleva työtehtävä hoidetaan tietoturvallisuutta ajatellen harkitsemattomasti ja riskialttiisti.

Toimitiloihin liittyvistä tietoturvallisuutta heikentävistä tekijöistä haastateltavat mainitsivat sekä rakenteelliset ongelmat että huonon äänieristyksen. Rakenteelliset ongelmat korostuvat poliisiasemilla sellaisissa tiloissa, jotka on alun perin tarkoitettu aivan toisenlaiseen käyttöön. Tila on saatettu ottaa esimerkiksi tilanpuutteen vuoksi kuulusteluhuoneeksi eikä se välttämättä sovellu sellaiseen käyttöön. Avokonttoreissa työskentelevät kertoivat, että paitsi työrauhan, mutta myös tietoturvallisuussyiden vuoksi haluaisivat päästä avokonttoritiloista pois.

> Tiloja ei ole ajateltu nykyajan tarpeisiin, osa työhuoneista on vain otettu esimerkiksi tutkinnan käyttöön, vaikka tiloilla ei välttämättä ole edellytyksiä siihen sijaintinsa tai toimintojensa puolesta. (Henkilö F)

> Tyhjän pöydän periaatetta ei olla sisäistetty. Ei uskalleta tai huomata puuttua ja kysyä, kuka on tiloissa ja liikkuu täällä. (Henkilö H)

Kuten kehittämistarpeissa jo tuli esille, toimitilojen yleisellä siisteydellä koettiin olevan suuri merkitys tietoturvallisuuden kannalta, myös heikentävänä tekijänä. Haastateltavat kokivat, että poliisiasemien yleisen järjestyksen tulisi olla paremmassa kunnossa ja että yhteisissä tiloissa pöydillä olevien materiaalien ja tulosteiden pitäisi löytää omat paikkansa, joko silppurista tai lukitusta laatikosta. Papereiden jäämisen pöydille koettiin olevan sekä tahatonta huolimattomuutta tai ajattelemattomuutta ja johtuvan ainakin osittain kiireestä, osa haastatelluista koki, että yleisten tilojen epäjärjestys johtuu välinpitämättömyydestä ja turtumisesta.

Näiden lisäksi haastatteluissa tuli esille tietoturvallisuutta heikentävänä tekijänä liika tieto ja informaatiotulva. Haastateltavat kertoivat, että aika ajoin sähköpostia tulee paljon ja sitä ei välttämättä ehdi heti lukemaan ja käsittelemään kiireisten työtehtävien vuoksi. Tämä saattaa aiheuttaa sen, että tärkeää tietoa ja odottavia toimenpiteitä sisältäviä sähköposteja on lukematta useita ja kun näitä sähköposteja pääsee purkamaan, tietoa tulee yhdellä kertaa liian paljon sisäistettäväksi.

> Liian tiedon kanssa puuroutuu. Sitä väsähdetään liialliseen vaikeuteen tietoturva-asioissa ja silloin tulee välinpitämättömyyttä. Järjestelmien huono osaaminen, liikaa ohjeita eikä enää pysytä kiireen takia kärryillä. Sitten on ongelma. (Henkilö D)

6.5 Haastateltavien esittämiä keinoja tietoturvallisuuden kehittämiseksi

Haastatteluissa tuli esille, että tärkeimpiä asioita tietoturvallisuuden kehittämiseksi ovat johdon ja henkilöstön sitoutuminen ja sitouttaminen tietoturvallisuuteen. Haastateltavista yli

puolet oli sitä mieltä, että kun johdolta saadaan tarkat ja selkeät, ymmärrettävät ohjeet tietoturvallisuuden parantamiseksi ja kehittämiseksi, niitä noudatetaan ja sovelletaan myös käytännössä. Haastateltavat kokivat, että johdon tulee näyttää esimerkkiä omalla toiminnallaan koko henkilöstölle myös tietoturvallisuuteen liittyvissä teoissa.

Yhtenä seikkana tietoturvallisuuden kehittämiseksi haastateltavat mainitsivat palautteen saamisen. Tällä tavalla henkilöstölle tulee ymmärrys siitä, että mitä annetuilla ja noudatetuilla tietoturvallisuusohjeilla ja määräyksillä on saavutettu.

> Tietoturvallisuuden tärkeimpiä asioita ovat johdon sitoutuminen ja henkilöstön sitoutuminen. Kaikki turvallisuuden osa-alueet ovat täysin riippuvaisia näistä toiminnoista. Näihin toimintoihin sisältyy niin johdolta turvallisuustyöhön saatavat resurssit kuin henkilöstön oikea toiminta. Uhkien ja riskien toteutuminen ovat suurimmillaan henkilöstön toimintaan liittyen. (Henkilö H)

> Johdon sitouttaminen eli johto pitäisi saada ymmärtämään asian [tietoturvallisuuden] tärkeys ja kokonaisuus ja että he itse toimivat niin kuin kuuluu ja ovat esimerkkinä muille. (Henkilö H)

> Kyllähän siitä pitäisi joskus palautettakin kuulla, että ollaanko me johtajien mielestä onnistuttu tietoturvallisuudessa. Eihän sitä tiedä muuttaa omaa toimintaansa, jos koulutuksen jälkeen koko asiasta ei enää mitään kuulu. (Henkilö D)

Verkkokoulutusten koettiin onnistuneen hyvin ja haastatteluissa nousi esille, että laadukkailla koulutuksilla saadaan kehitettyä tietoturvallisuutta edelleen. Koulutukset koettiin tärkeiksi, mutta niiden myös koettiin olevan raskaita, osittain siksi, että käsiteltävät tietomäärät ovat suuria. Koulutusten kehittämiseksi haastateltavat esittivät, että koulutuksia kehitettäisiin tiiviimmiksi tai jaettaisiin osioihin, jolloin yhdellä kerralla tuleva tietomäärä on pienempi ja helpommin hahmotettava. Haastatteluissa tulikin esille, että haastateltavat kokevat kouluttajan johdolla suoritetut koulutukset tehokkaammiksi kuin verkkokoulutukset.

> Järjestetään paikalla oleva fyysisen koulutus kohdekohtaisesti ja se dokumentoidaan. Paikalla ollen näytetään ja kerrotaan, mitä tarkoitetaan esimerkiksi tyhjän

> pöydän periaatteella ja sitoutetaan se ihminen tätä kautta tietoturvallisuuteen. (Henkilö H)

Vuosittain suoritettavat tavoite- ja kehityskeskustelut koettiin haastatteluissa olennaisena osana tietoturvallisuuden kehittämistä. Haastateltavat kertoivat, että esimiesten kanssa pitäisi käydä vuosittain läpi voimassa olevat käyttöoikeudet eri järjestelmiin ja punnita niiden tarpeellisuus, jolloin turhat käyttöoikeudet voitaisiin poistaa. Sen lisäksi, että keskustelussa otettaisiin esille ja harkintaan työntekijällä olevat käyttöoikeudet, myös tietoturvallinen käyttäytyminen, sen tärkeys, työntekijän henkilökohtainen asenne ja näkemykset tietoturvallisuudesta tulisi samalla ottaa keskusteltavaksi ja tarvittaessa kirjata myös tietoturvallisuuteen liittyviä ammatinhallintatekijöitä ylös.

> Ihan turhaan niitä käyttöoikeuksia on liikaa. Kyllä se pitäs käydä tavoitekeskustelussa läpi, jos ei nyt vuosittain, niin vaikka parin vuoden välein, että mihin järjestelmiin oikeuksia työtehtävissään tarttee. (Henkilö L)

Yhtenä keinona tietoturvallisuuden kehittämiseksi haasteltavat mainitsivat selkeän ja nopeasti luettavissa olevan ”reisitaskuvihkon”, tietoturvallisuusoppaan, josta on tarpeen vaatiessa yksinkertaista ja helppoa tarkastaa tietoturvallisuuteen liittyviä tiivistettyjä ohjeita ja määräyksiä sekä soveltaa niitä käytäntöön.

> Tietoturvallisuus on jalkautettava päivittäiseen toimintaan. Meille pitää tulla selkeät ohjeet ja toimintamallit, ei pelkästään pitkiä ohjeita hallinnosta. (Henkilö K)

> Siihen työhön [tietoturvallisuuden kehittämiseen] oikeasti sellaiset ihmiset ja asiantuntijat, joilla on hengenpaloa ja ammattitaitoa niin teknisen tietoturvan toteuttamiseen kuin muuhunkin tietoturvaan. (Henkilö H)

Haastateltavien näkemys oli, että tietoturvallisuutta voidaan kehittää saamalla poliisiasemien fyysiset edellytykset kuntoon sekä muuttamalla henkilöstön asenne ja tahtotila vieläkin myönteisemmäksi tietoturvallisuutta kohtaan.

7 JOHTOPÄÄTÖKSET JA POHDINNAT

7.1 Vastaukset tutkimusongelmiin

Opinnäytetyöni tutkimuksen tavoitteena oli selvittää henkilöstön käsityksiä Oulun poliisilaitoksen tietoturvallisuudesta, missä tietoturvallisuuden osa-alueissa koetaan onnistuneen hyvin, missä koetaan olevan eniten kehittämistarvetta, mitkä seikat heikentävät tietoturvallisuutta sekä keinot, joilla tietoturvallisuutta voitaisiin kehittää.

Opinnäytetyön pääongelma:
Millaiseksi poliisilaitoksen henkilöstö kokee tietoturvallisuuden tason Oulun poliisilaitoksella?

Pääongelma jaettiin neljään alaongelmaan. Alaongelmien tavoitteena oli selvittää henkilöstön käsityksiä tietoturvallisuuden onnistuneista osa-alueista ja niistä, joissa on eniten kehittämistarvetta. Lisäksi tavoitteena oli selvittää henkilöstön käsityksiä tietoturvallisuutta heikentävistä osa-alueista sekä tietoturvallisuutta kehittäviä keinoja. Seuraavassa esitetään vastaukset tutkimusongelmaan alaongelmittain.

Missä tietoturvallisuuden osa-alueissa henkilöstö kokee tietoturvallisuuden onnistuneen hyvin?

Tutkimuksen perusteella Oulun poliisilaitoksen henkilöstö kokee tietoturvallisuuden onnistuneen hyvin koulutuksissa ja laitehankinnoissa sekä fyysistä turvallisuutta parantavissa muutoksissa työ- ja kuulusteluhuoneissa. Tutkimuksessa tuli esille, että koetut onnistumiset tietoturvallisuudessa olivat kytköksissä siihen, millä sektorilla haastateltava työskentelee. Valvonta- ja hälytyssektorilla koettiin, että tietoturvallisuudessa oli onnistuttu esimerkiksi

tekemällä tiettyjä laitehankintoja. Lupasektorilla työskentelevät kokivat saadut koulutukset hyvin onnistuneiksi. Rikostorjuntasektorilla koettiin, että fyysisen turvallisuuden osalla oli onnistuttu hyvin tekemällä muutoksia työ- ja kuulusteluhuoneissa, mutta onnistuttu oli myös laitehankinnoissa ja koulutuksissa.

Missä tietoturvallisuuden osa-alueissa henkilöstö kokee olevan eniten kehittämistarvetta?

Tutkimuksen perusteella Oulun poliisilaitoksen henkilöstö kokee eniten kehittämistarvetta olevan ohjelmistojen ja laitteistojen käytettävyyteen sekä toimitilojen ja henkilöstön toimintaan liittyvissä seikoissa.

Tutkimuksessa tuli esille, että jos tietoturvallisuus aiheuttaa ohjelmistojen tai laitteistojen käytettävyydelle hankaluuksia työtehtävää suoritettaessa, työtehtävä saatetaan suorittaa tietoturvallisuuden kannalta riskialttiiksi. Turhien ja käyttämättömien käyttöoikeuksien tarkastamisissa ja poistamisissa koettiin olevan kehittämistarvetta, hyväksi tilaisuudeksi tälle asialle koettiin vuosittain käytävät tavoite- ja kehityskeskustelut.

Kehittämistarvetta haastateltavat kokivat lisäksi toimitilojen ja henkilöstön toiminnan osalta. Kulunvalvonta, äänieristys ja yleinen siisteys olivat ne tietoturvallisuuteen liittyvät kehittämistarpeet, joita haastateltavat kokivat olevan.

Mitkä seikat heikentävät tietoturvallisuutta?

Tutkimuksen perusteella Oulun poliisilaitoksen henkilöstö kokee tietoturvallisuutta heikentäviksi tekijöiksi henkilöstön toimintaan, ohjelmistojen ja laitteistojen käytettävyyteen sekä toimitiloihin liittyvät seikat.

Henkilöstön aiheuttamat tahattomat tietoturvallisuutta vaarantavat teot koettiin merkittävimpinä tietoturvallisuutta heikentävinä tekijöinä. Rutinoituminen ja vääränlainen asenne tietoturvallisuutta koskevissa asioissa sekä myös välinpitämättömyys ja laiskuus mainittiin syiksi. Haastatteluissa tuli esille myös liian suuren tietomäärän ja informaatiotulvan aiheuttavan sen, että saatua tietoa ei ehditä käydä läpi tai se jää sisäistämättä.

Ohjelmistojen ja laitteistojen hyvän tietoturvallisuuden koettiin aiheuttavan sen, että kiiretilanteissa turvatoimet aiheuttavat ongelmia käytettävyyteen ja tuolloin ne saatetaan harkitsemattomasti pyrkiä ohittamaan ajan tai vaivan säästämiseksi.

Huonon äänieristyksen, rakenteellisten ongelmien sekä tilojen epäsiisteyden koettiin merkittävästi huonontavan tietoturvallisuutta. Työskentelytilojen ollessa talon sisällä ja lukittuvien ovien takana, saatetaan esimerkiksi kirjautumiskortti jättää tietokoneeseen taukojen ajaksi. Tietoturvallisuutta vaarantavaa tekijää ei näissä tilanteissa tunnisteta, vaan koetaan vääränlaista turvallisuuden tunnetta lukittujen tilojen vuoksi.

Millä keinoin tietoturvallisuutta voitaisiin kehittää?

Tutkimuksen perusteella tietoturvallisuuden kehittämisessä tärkeää on johdon ja henkilöstön sitoutuminen ja sitouttaminen tietoturvallisuuteen, poliisiasemien fyysisten edellytysten kuntoon saaminen, tietoturvallisuuden ottaminen osaksi tavoite- ja kehityskeskusteluja, palautteen saaminen, koulutusten jatkaminen sekä selkeän tietoturvallisuusoppaan tekeminen.

Tietoturvallisuuden kehittämisessä yhdeksi merkittävimmäksi seikaksi esille nousi poliisiasemien fyysisten edellytysten parannukset ja kunnostamiset. Tietoturvallisuus on tärkeä osa poliisin työtä ja ammatinhallintaa ja vuosittain käytävät tavoite- ja kehityskeskustelut lähiesimiehen kanssa koettiin toimivaksi tilanteeksi, jossa käydään läpi käyttöoikeudet ja päätetään turhien käyttöoikeuksien poistamisesta.

Tietoturvallisuuden saattamisessa päivittäiseen työhön sekä nopeasti ja helposti ymmärrettävään muotoon mainittiin tietoturvallisuusopas, jossa on tiivistettynä olennaisimmat tietoturvallisuusasiat ja josta ne on helppo soveltaa käytäntöön.

Tutkimuksessa tuli esille, että henkilöstön asenteeseen tietoturvallisuutta ja sen tärkeyttä kohtaan koettiin voivan vaikuttaa johdon sitoutumisella ja sitouttamisella sekä esimerkillä. Tietoturvallisuutta kehittäväksi tekijäksi koettiin myös johtaminen, palautteen saaminen sekä sen seuranta, toimitaanko koulutuksissa saatujen oppien mukaisesti. Tutkimuksen mukaan, jos palautteen saaminen johdolta jää kokonaan saamatta, henkilöstö jatkaa toimimistaan samalla tavalla kuin ennenkin, tietämättä ja ajattelematta sitä, toimiiko oikein vai väärin. Tästä syystä palautteen saamisen koettiin auttavan työntekijää kehittämään omaa toimintaansa tietoturvallisemmaksi.

7.2 Opinnäytetyön arviointi

Ennen varsinaisen opinnäytetyöprosessin aloittamista ja aiheen valintaa koin tarpeelliseksi, että tutkimukseni aihe palvelee työorganisaatiotani. Aiheeksi valikoitui omien pohdintojeni sekä esihenkilöideni ja työkavereideni kanssa käytyjen keskustelujen perusteella tietoturvallisuus. Tietoturvallisuus on aiheena hyvin ajankohtainen ja moniulotteinen, joten opinnäytetyöprosessin aikana opin sekä yleisesti tietoturvallisuudesta että toimeksiantajaorganisaation kannalta tärkeistä asioista, jotka vaikuttavat tietoturvallisuuteen ja ovat merkitseviä.

Yhtenä opinnäytetyön haasteena koin aiheen rajaamisen sekä haastateltavien henkilöiden valinnan ja lukumäärän. Jotta tutkimustuloksissa pääsisi tarkempaan analyysiin, aihetta tulisi rajata tarkemmaksi. Kattavampien tutkimustulosten saamiseksi haastateltavien lukumäärän lisääminen ja haastatteluissa saatujen tutkimustulosten jakamiselle sektoreittain voisi myös

olla merkitystä. Jos aloittaisin opinnäytetyöprosessin uudelleen, ottaisin nämä edellä mainitsemani asiat aiheen rajaamisesta sekä tulosten jakamisesta sektoreittain huomioon ja tekisin muutoksia työhöni näiltä osilta.

Tutkimusaiheena tietoturvallisuus on aina ajankohtainen, mutta etenkin tutkimuksen loppuvaiheessa Ukrainan kriisi teki opinnäytetyöni aiheesta vieläkin ajankohtaisemman. Alkujaan opinnäytetyöni aihe valikoitui työelämälähtöisin perustein, mutta maailman turvallisuustilanteen muuttuminen lisäsi opinnäytetyön merkitystä itselleni. Opinnäytetyön tekemisessä ja sen valmistumisessa koen suurta kiitollisuutta ohjaavaa opettajaa, toimeksiantajan edustajaa sekä haastateltavia ja työyhteisööäni kohtaan. Iso kiitos kuuluu myös perheelleni. Kaikki he ovat olleet korvaamattomana apuna sekä tukena ja mahdollistaneet omalla panoksellaan tämän opinnäytetyön.

LÄHTEET

Digi- ja väestötietovirasto. 2022. Digitaalisen turvallisuuden kehittäjäverkosto VAHTI. Saatavissa: https://dvv.fi/vahti. Viitattu 17.2.2022.

Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Porvoo: WS Bookwell.

Hirsjärvi, S. & Hurme, H. 2006. Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö. Helsinki: Yliopistopaino.

Kyberturvallisuuskeskus. 2020. Tietoturva. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva. Viitattu 12.2.2022.

Kyberturvallisuuskeskus. 2021a. Salasanat haltuun. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/salasanat-haltuun. Viitattu 12.2.2022.

Kyberturvallisuuskeskus. 2021b. Katakri 2020-arviointityökalu. https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.kyberturvallisuuskeskus.fi%2Fsites%2Fdefault%2Ffiles%2Fmedia%2Ffile%2FKatakri-2020-arviointity-okalu.xlsx&wdOrigin=BROWSELINK. Viitattu 13.3.2022

Laaksonen, M., Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja - Ohjeistus, toteutus ja lainsäädäntö. Helsinki: Edita.

Paavilainen, J. 1998. Tietoturva. Jyväskylä: Suomen Atk-kustannus Oy, Gummerus.

Poliisi. 2020a. Oulun poliisilaitos. Saatavissa: https://poliisi.fi/oulun-poliisilaitos. Viitattu 24.3.2022.

Poliisi. 2020b. Toimimme koko Suomessa. Saatavissa: https://poliisi.fi/toimimme-koko-suomessa. Viitattu 24.3.2022.

Poliisi. 2020c. Keskusrikospoliisi. Saatavissa: https://poliisi.fi/keskusrikospoliisi. Viitattu 24.3.2022.

Poliisihallitus. 2022. Poliisin organisaatioturvallisuus. Julkaistu 18.02.2022. POL-2021-469. Viitattu 8.3.2022.

Rousku, K. 2017. Ohje riskienhallintaan. Valtiovarainministeriön julkaisuja 22/2017. Saatavissa: https://julkaisut.valtioneuvosto.fi/handle/10024/80013. Viitattu 20.3.2022.

Sisäministeriö. 2022. Poliisin toimijat ja vastuut. Saatavissa: https://intermin.fi/poliisiasiat/toimijat-ja-vastuut. Viitattu 24.3.2022.

Suomen Riskienhallintayhdistys. 2012a. Mitä ovat riskit? Saatavissa: https://pk-rh.fi/riskienhallinta/mita-ovat-riskit.html. Viitattu 18.3.2022.

Suomen Riskienhallintayhdistys. 2012b. Riskien luokittelu. Saatavissa: https://pk-rh.fi/riskien-luokittelu.html. Viitattu 18.3.2022.

Suomen Riskienhallintayhdistys. 2012c. Strategiset riskit. Saatavissa: https://pk-rh.fi/riskien-luokittelu/strategiset-riskit.html. Viitattu 18.3.2022.

Suomen Riskienhallintayhdistys. 2012d. Operatiiviset riskit. Saatavissa: https://pk-rh.fi/riskien-luokittelu/operatiiviset-riskit.html. Viitattu 18.3.2022.

Suomen Riskienhallintayhdistys. 2012e. Taloudelliset riskit. Saatavissa: https://pk-rh.fi/riskien-luokittelu/taloudelliset-riskit.html. Viitattu 18.3.2022.

Suomen Riskienhallintayhdistys. 2012f. Vahinkoriskit. Saatavissa: https://pk-rh.fi/riskien-luokittelu/vahinkoriskit.html. Viitattu 18.3.2022.

Suomen Riskienhallintayhdistys. 2012g. Mistä riskienhallinnassa on kysymys? Saatavissa: https://pk-rh.fi/riskienhallinta.html. Viitattu 18.3.2022.

Suomen Riskienhallintayhdistys. 2012h. Riskienhallintaprosessi. Saatavissa: https://pk-rh.fi/riskienhallintaprosessi.html. Viitattu 18.3.2022.

Valtiovarainministeriö. 2020. Voimassa olevat tietoturvaohjeet ja -määräykset. Saatavissa: https://vm.fi/julkaisut/vahti. Viitattu 15.2.2022.

VAHTI. 2003. Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa. Saatavissa: https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet/vahti-72003-ohje-riskien-arvioinnista-tietoturvallisuuden-edistamiseksi-valtionhallinnossa. Viitattu 12.2.2022.

VAHTI. 2004a. Tietoturvallisuus ja tulosohjaus. Saatavissa: https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet/vahti-22004-tietoturvallisuus-ja-tulosohjaus. Viitattu 15.2.2022.

VAHTI. 2004b. Valtionhallinnon keskeisten tietojärjestelmien turvaaminen. Saatavissa: https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet/vahti-52004-valtionhallinnon-keskeisten-tietojarjestelmien-turvaaminen. Viitattu 17.2.2022.

VAHTI. 2006. Asianhallinnan tietoturvallisuutta koskeva ohje. Saatavissa: https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet/vahti-52006-asianhallinnan-tietoturvallisuutta-koskeva-ohje. Viitattu 22.2.2022.

VAHTI. 2007. Tietoturvallisuudella tuloksia. Saatavissa: https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet/vahti-32007-tietoturvallisuudella-tuloksia. Viitattu 17.2.2022.

VAHTI. 2011. Johdon tietoturvaopas. Saatavissa: https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet/vahti-22011-johdon-tietoturvaopas. Viitattu 12.3.2022.

VAHTI. 2013. Toimitilojen tietoturvaohje. Saatavissa: https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet/vahti-22013-toimitilojen-tietoturvaohje. Viitattu 10.3.2022.

LIITE 1

HAASTATTELURUNKO OPINNÄYTETYÖTÄ VARTEN
Henkilöstön käsityksiä Oulun poliisilaitoksen tietoturvallisuudesta

1. Yleinen mielipide tietoturvallisuudesta ja sen tärkeydestä.

2. Tietoturvallisuuden taso Oulun poliisilaitoksessa

- käsitykset tietoturvallisuuden tilanteesta ja tasosta
- käsitykset tietoturvallisuudesta päivittäisten virkatehtävien hoitamisessa
- ”plussat ja miinukset”.

3. Tietoturvallisuuden onnistuneet osa-alueet

- asiat / teot, joissa onnistuttu
- eniten vaikuttaneet onnistumiset
- vaikutukset päivittäisten virkatehtävien hoitamisessa.

4. Tietoturvallisuuden kehittämistarpeet

- asiat / teot, joissa kehitettävää
- eniten kehitettävää
- syyt, miksi asioissa / teoissa kehitettävää.

5. Tietoturvallisuutta heikentävät tekijät

- asiat / teot, jotka heikentävän tietoturvallisuutta
- tekijät, jotka heikentävät tietoturvallisuutta eniten
- vaikutukset päivittäisten virkatehtävien hoitamisessa.

6. Ideoita tietoturvallisuuden kehittämiseksi

- asiat / teot, jotka kehittävät tietoturvallisuutta
- vaikutukset tietoturvallisuuteen.

7. Muuta asiaa tietoturvallisuudesta, mitä haastateltava haluaa kertoa tai tuoda esille.

LIITE 2

TAULUKKO AINEISTON ANALYSOINTIA VARTEN

1. Tietoturvallisuuden taso

HYVÄÄ	HUONOA

2. Onnistumiset

ASIA / TEKO	ENITEN VAIKUTTANEET	VAIKUTUKSET TYÖHÖN

3. Kehittämistarpeet

ASIA / TEKO	ENITEN KEHITETTÄVÄÄ	SYITÄ KEHITTÄMISTAR-PEESEEN

4. Heikentävät tekijät

ASIA / TEKO	ENITEN HEIKENTÄVÄT	VAIKUTUKSET TYÖHÖN

5. Kehittämisideat

ASIA / TEKO	VAIKUTUKSET