Käsikirja fyysisen turvallisuuden hallintaan tietoliikenneyrityksessä

Juhani Toivonen

2024 Laurea

Laurea-ammattikorkeakoulu

Käsikirja fyysisen turvallisuuden hallintaan tietoliikenneyrityksessä

Juhani Toivonen

Turvallisuus ja riskienhallinta

Opinnäytetyö

Marraskuu,2024

Laurea-ammattikorkeakoulu

Turvallisuus ja riskienhallinta

Tradenomi (AMK)

Juhani Toivonen

Tiivistelmä

Käsikirja fyysisen turvallisuuden hallintaan tietoliikenneyrityksessä

Vuosi 2024 Sivumäärä 53

Tässä opinnäytetyössä käsitellään fyysisen turvallisuuden hallitsemista tietoliikenneyritysten näkökulmasta. Työ tehtiin tutkimuksellisena kehittämistyönä. Työn tarkoituksena oli luoda tilaajayritykselle käsikirja, jossa on koottuna kaikki tärkeimmät lait, ohjeet, sopimukset, säädökset ja standardit liittyen fyysiseen turvallisuuteen. Tärkeimmät vaatimukset valittiin yhdessä tilaajayrityksen kanssa.

Tavoitteena oli, että tämä fyysistä turvallisuutta käsittelevä käsikirja helpottaisi kohteiden turvallisuusvaatimusten tunnistamista ja täyttämistä. Lisäksi käsikirjan esittämien vaatimusten avulla voitaisiin arvioida tilaajayrityksen sen hetkistä vaatimustenmukaisuutta. Opinnäytetyö rajattiin koskemaan fyysistä turvallisuutta ja fyysistä tietoturvallisuutta. Työssä yritettiin löytää metodi, jonka avulla kaikki tärkeimmät vaatimukset saataisiin koottua siten että niiden lukeminen ja käyttäminen olisi aiempaa tehokkaampaa.

Työtä varten tutustuttiin useampaan eri velvoittavaan lähteeseen ja niiden vaatimuksiin. Näitä lähteitä olivat, katakri 2020, finanssialan murtosuoja ohje taso 3, Traficomin määräys 54045 ja valtiovarainministeriön suositus turvallisuusluokiteltavien asiakirjojen käsittelystä.

Työssä tutustuttiin siihen, kuinka turvallisuusjohtaminen ja riskienhallinta liittyvät olennaisesti fyysiseen turvallisuuden hallintaan. Työtä varten haastateltiin kahta tilaajayrityksen turvallisuuspäällikköä. Haastattelussa kartoitettiin tilaajayrityksen fyysisen turvallisuuden tasoa, siihen liittyviä haasteita ja tilaajayrityksen turvallisuuskulttuuria. Kattavan tiedon läpikäymisen jälkeen se analysoitiin ja teemoitettiin. Analysoinnin ja teemoittelun pohjalta alettiin rakentaa tilaajayritykselle käsikirjaa, joka yhdistää tärkeimmät velvoittavat lähteet ja niiden vaatimukset yhteen teokseen. Käsikirjassa otettiin huomioon tiettyjen lähteiden vaatimusten päällekkäisyys. Käsikirjassa käytettiin lähinnä vapaasti saatavilla olevia lähteitä, joten tilaajayritykselle jätettiin mahdollisuus lisätä siihen omia käyttörajoitettuja lähteitä. Käsikirja on salassa pidettävä, joten siitä julkaistaan ainoastaan sisällysluettelo.

Asiasanat: fyysinen turvallisuus, käsikirja, riskienhallinta, turvallisuus

Laurea University of Applied Sciences **Abstract**

Degree Programme in Safety, Security and Risk Management

Bachelor of Business Administration (BBA)

Juhani Toivonen

Handbook for Managing Physical Security in a Telecommunications Company

Year 2024 Pages 53

This bachelor's thesis addresses the management of physical security from the perspective of telecommunications companies. The thesis was carried out as a research-based development project. The objective of the project was to create a handbook for the commissioner company that encompasses the most important laws, guidelines, agreements, regulations, and standards related to physical security. The most important requirements were selected in collaboration with the commissioner company.

The purpose of this handbook was to facilitate the identification and fulfillment of security requirements at different sites. Additionally, the requirements presented in the handbook could be used to assess the current compliance status of the commissioner. The thesis was limited to physical security and physical information security. The thesis aimed at mapping a method to compile all the key requirements in a way that makes reading and using them more efficient than before.

For the project, several sources and their requirements were reviewed. These sources included Katakri 2020, the Financial Sector's Burglary Protection Guideline Level 3, Traficom Regulation 54045, and the Ministry of Finance's recommendation on the handling of security-classified documents.

The work explored how security management and risk management are closely related to the management of physical security. Two security managers were interviewed. The interview assessed the level of physical security at the commissioner, the challenges related to it, and the company's security culture. After a reviewal of this comprehensive information, it was analyzed and categorized. Based on this analysis and categorization, the process of creating the handbook for the commissioner company began, summarizing the key sources and their requirements, now available in one document. The document considered the overlap of requirements from certain sources. The work primarily used only publicly available sources, allowing the commissioner company to add its own restricted-use sources to the handbook if needed. The handbook is confidential and therefore only a table of contents is published.

Keywords: handbook, physical security, risk management, security

Sisällys

1 Johdanto ... 6
2 Tavoite, tarkoitus, keskeiset käsitteet ja yrityksen esittely ... 6
2.1 Keskeiset käsitteet ... 7
2.2 Tilaajayritys ... 8
3 Turvallisuusjohtaminen ... 8
3.1 Turvallisuuden kaksi näkökulmaa safety ja security ... 9
3.2 Riskienhallinta ... 9
4 Fyysinen turvallisuus ... 10
4.1 Finanssialan turvallisuusohjeet rakenteellisesta murtosuojauksesta ... 11
4.2 EN 50600 standardi datakeskusten tiloista ja infrastruktuurista ... 14
5 Fyysinen tietoturva ... 15
5.1 Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä ... 16
5.2 Tietoturvallisuuden auditointityökalu viranomaisille Katakri 2020 ... 29
5.3 Traficomin M54045 ... 30
6 Käsikirjan vaatimukset käytettävyydelle ... 36
7 Opinnäytetyössä käytetyt menetelmät ... 37
7.1 Kehittämistyö ... 37
7.2 Puolistrukturoitu ryhmähaastattelu ja teemoittelu ... 38
8 Opinnäytetyön prosessi ... 39
9 Tulokset ... 43
10 Johtopäätökset ja oman työn arviointi ... 46
10.1 Johtopäätös ... 46
10.2 Oman työn arviointi ... 46
Lähteet ... 49
Kuviot ... 51
Kuvat ... 51
Taulukot ... 51
Liitteet ... 51

1 Johdanto

Tietoliikenneyrityksen fyysisen turvallisuuden hallinnalle on olemassa monia eritasoisia vaatimuksia, joista osa on valtiollisia ja osa yritysten ja organisaatioiden luomia. Suuresta vaatimusmäärästä huolimatta tietoliikenneyritysten on pystyttävä täyttämään kaikki vaatimukset ja suojaamaan yhteiskunnalle kriittiset laitetilat. Kaikki Suomessa toimivat teleyritykset ovat valtakunnallisia toimijoita. Toiminta-alueen suuruus luo haasteita syrjäseuduilla sijaitsevien laitetilojen fyysisen turvallisuuden ylläpitämiseen ja poikkeuksiin reagoimiseen.

Useiden eri vaatimuslähteiden läpikäyminen ja kohteiden tarkastaminen on aikaa ja resursseja vievää työtä. Näiden haasteitten takia tilaajayritykselle syntyi tarve tälle opinnäytetyölle, jonka tavoitteena on helpottaa tietoliikenneyrityksiä koskevien vaatimusten täyttämistä. Tätä työtä varten vaatimuksista rajattiin pois kaikki muut, paitsi kaikista tärkeimmät tietoliikenneyritystä koskevat fyysisen turvallisuuden lähteet. Rajauksessa pyrittiin kiinnittämään huomiota siihen, että jäljelle jääneet lähteet olisivat vapaasti käytettävissä.

Työssä on käytetty lähteinä katakria ja suositusta turvallisuusluokiteltavien asiakirjojen käsittelystä. Näiden lähteiden vaatimukset on suunnattu valtion viranomaisille. Niitä on käytetty tässä työssä, koska valtion viranomaiset käyttävät tilaajayrityksen palveluja ja tiloja. Tilaajayrityksen on siten täytettävä myös nämä viranomaisille suunnatut vaatimukset.

Fyysinen turvallisuus valittiin, koska se nähdään monesti yrityksissä vanhanaikaisena ja hitaasti muuttuvana alana. Fyysinen turvallisuus on ajan saatossa jäänyt uudemman tieto- ja kyberturvallisuuden varjoon, jonka takia sen kehittyminen on hidastunut. Fyysinen turvallisuus tulisi saada jälleen sellaiselle tasolle, ettei alan ammattilaisten tarvitsisi jokaisen ratkaisun tai kehitysehdotuksen kohdalla perustella, miksi suojaus olisi hyvä tehdä tietyllä tavalla. Tälle työlle on siis myös laajempaa tarvetta, jotta fyysinen turvallisuus saataisiin jälleen puheenaiheeksi ja takaisin kehityksen tielle.

2 Tavoite, tarkoitus, keskeiset käsitteet ja yrityksen esittely

Tämä luku on jaettu kahteen osaan. Ensimmäisessä kohdassa käsitellään opinnäytetyön tavoitetta ja tarkoitusta. Toisessa kohdassa selvennetään opinnäytetyössä käytettäviä keskeisiä käsitteitä. Lopuksi luvussa kerrotaan opinnäytetyön tilaajayrityksestä.

Työn tarkoituksena on luoda tilaajayritykselle käsikirja, jossa on koottuna kaikki tärkeimmät lait, ohjeet, sopimukset, säädökset ja standardit liittyen fyysiseen turvallisuuteen. Tärkeimmät vaatimukset valittiin yhdessä tilaajayrityksen kanssa. Tavoitteena on, että tämä fyysistä

turvallisuutta käsittelevä käsikirja helpottaa kohteiden turvallisuusvaatimusten tunnistamista ja täyttämistä. Lisäksi käsikirjan esittämien vaatimusten avulla voidaan arvioida tilaajayrityksen tämänhetkistä vaatimustenmukaisuutta. Yritys itse käyttää näitä kohteita ja vuokraa niitä muille organisaatioille. Tilojen turvallisuusluokitus vaihtelee Traficomin määräyksen korkeimmasta luokituksesta matalimpaan. Käsikirja voisi myös toimia kommunikoinnin välineenä sisäisille sidosryhmille kertoen, mitä turvallisuuden tasoja toimeksiantajan kohteet täyttävät. Opinnäytetyö rajataan koskemaan fyysistä turvallisuutta ja fyysistä tietoturvallisuutta.

Työn tuotoksena on käsikirja, jonka avulla kaikki tärkeimmät vaatimukset saadaan koottua yhteen teokseen. Tämä mahdollistaa vaatimusten lukemisen ja käyttämisen nykyistä tehokkaammin. Käsikirjasta esitellään tilaajayrityksen toiveesta vain sisällysluettelo.

2.1 Keskeiset käsitteet

Käsitteiden merkitystä tutkittaessa on pyritty käyttämään kattavasti eri lähteitä ja niiden luotettavuutta on myös pohdittu. Fyysinen tietoturva tarkoittaa kaikkia niitä keinoja, jolla organisaatio suojaa tärkeätä tietoa fyysisiltä uhilta. Fyysisen tietoturvan perustan muodostaa tiedon käsittely- ja säilytystilojen ympärillä olevat suojaavat fyysiset rakenteet, jotka antavat esimerkiksi tarvittavat äänieristykset kulunvalvonnat ja näköeristykset. (Valtiovarainministeriö 2007.)

Fyysinen turvallisuus on turvatoimien osa, joka koskee henkilöstön ja omaisuuden suojaamiseksi suunniteltuja fyysisiä toimenpiteitä; estää luvaton pääsy laitteisiin, asennuksiin, materiaaleihin ja asiakirjoihin; ja suojella heitä vakoilulta, sabotaasilta, vahingoilta ja varkauksilta. (Yhdysvaltain puolustusministeriö 2005.) Fyysinen turvallisuus on yksi tietoturvan olennaisimmista muodoista. Fyysisen tietoturvallisuuden pääaiheena on yrityksen kyky suojata tuotanto- tai toimitilojaan, dokumentaatiotaan, laitteitaan ja tietojärjestelmiään mahdollisten haitantekijöiden aiheuttamilta hyökkäyksiltä tai muilta fyysisiltä riskeiltä, kuten vesi-, tuli- tai sähkövahingoilta. (Cobb. B, 2021.)

Käsikirja tarkoittaa julkaisua, jossa tuodaan esiin keskeiset tiedot joltakin alalta (Kielitoimiston sanakirja 2022).

Riski tarkoittaa epävarmuuden vaikutusta tavoitteisiin (SFS-ISO 31073:2022,6). Riski voi olla myönteinen, kielteinen tai molempia, ja se voi käsitellä, luoda tai saada aikaan mahdollisuuksia ja uhkia (SFS-ISO 31000:2018,6).

Riskienhallinta on erilaisia yhteensovitettuja toimia, joilla yritys pyrkii hallitsemaan siihen kohdistuvia riskejä. Riskienhallinnan tavoitteena on mahdollistaa yrityksen oman toiminnan jatkaminen ilman häiriötä kaikissa mahdollisissa tilanteissa. Riskienhallinta on tehokkainta

vain, jos yritys on tunnistanut kaikki mahdolliset riskit. Riskeihin ei voi varautua, jos niitä ei ole tunnistettu. (SFS-ISO 31000:2018,5; Vesterinen. P, 2011, 111–114.)

2.2 Tilaajayritys

Tilaajayritys on suomalainen julkinen osakeyhtiö. Tilaajayrityksen toimiala on langattoman verkon hallinta ja palvelut. Yrityksen toimialakuvaus on kaupparekisterissä kirjattu seuraavanlaisesti: Yhtiö harjoittaa yleistä teletoimintaa, jonka tarkoituksena on tarjota tietoliikenne- ja ICT-palveluja Suomessa ja ulkomailla. Yhtiö voi myydä näihin toimintoihin liittyviä laitteita ja harjoittaa näihin toimintoihin kytkeytyvää tai näitä toimintoja tukevaa muuta liiketoimintaa. Yhtiö voi suorittaa ICT:tä ja tietoliikennettä koskevaa tarkastustoimintaa, tutkimustoimintaa sekä konsultointia. Lisäksi yhtiöllä on mahdollisuus tarjota maksupalveluja. Yhtiö harjoittaa toimintaansa sekä välittömästi itse että yhteisyritystensä ja tytäryhtiöidensä välityksellä. Kaksikielisyyden tarve otetaan huomioon liiketoiminnassa. Yhtiö voi omistaa arvopapereita ja kiinteistöjä. Tämän lisäksi yhtiö voi harjoittaa arvopaperikauppaa, sekä yhtiön toimialaa tukevaa sijoitus- ja rahoitustoimintaa. (Patentti- ja rekisterihallitus 2024.)

3 Turvallisuusjohtaminen

Tässä luvussa käsitellään mitä turvallisuusjohtaminen on ja mitä eri asioita tulee ottaa huomioon sitä toteuttaessa ja kehittäessä. Luvussa perehdytään turvallisuuden kahden eri muodon eli safetyn ja securityn eroihin. Luvussa käydään myös läpi, kuinka turvallisuusjohtaminen liittyy organisaation yleiseen kehittämiseen.

Turvallisuusjohtaminen on kokonaisvaltaista, ja siihen kuuluu sekä lakisääteisen että vapaaehtoisen turvallisuuden hallinta. Siinä yhdistyy toimintatapojen, menetelmien sekä ihmisten johtaminen. Turvallisuusjohtamisen tavoitteena on jatkuva organisaation turvallisuuden ja terveellisyyden kehittäminen. (Työsuojeluhallinto 2010.)

Turvallisuusjohtaminen rakentuu useiden keskeisten periaatteiden varaan. Yksi tärkeimmistä työkaluista on riskien arviointi, jonka avulla tarkastellaan työolojen kehittämistarpeita ja arvioidaan työympäristötekijöiden vaikutuksia. Turvallisuuskulttuuri, eli yrityksen toimintatavat liittyen turvallisuuteen, vaikuttaa suoraan turvallisuusjohtamiseen. Jotta turvallisuusjohtamisen ajattelutapa saisi vastakaikua henkilöstöltä, koko johdon on oltava siihen sitoutunut. Vasta kun henkilöstö on mukana, voidaan varmistaa, että tämä ajattelutapa ja siihen liittyvät toimenpiteet edistävät turvallisuuskulttuurin kehittymistä. Turvallisuusjohtaminen edellyttää myös toimivaa palautejärjestelmää, jonka avulla organisaatio voi järjestelmällisesti varmistaa omien käytäntöjensä jatkuvan kehittämisen. Onnistunut turvallisuusjohtaminen parantaa

työilmapiiriä, edistää henkilöstön sitoutumista, nostaa tuotannon laatua sekä auttaa ehkäisemään onnettomuuksia ja tapaturmia. (Työsuojeluhallinto 2010.)

Turvallisuusjohtaminen voi olla reagoivaa tai ennakoivaa. Tämän opinnäytetyön käsikirja pyrkii auttamaan tilaajayritystä olemaan enemmän ennakoiva fyysisen turvallisuuden suhteen. Käsikirjasta on myös hyötyä reagoidessa turvallisuuspuutteisiin.

3.1 Turvallisuuden kaksi näkökulmaa safety ja security

Jos sanat safety ja security käännetään suoraan suomen kielelle niin huomataan, että kummatkin sanat tarkoittavat turvallisuutta. Näin ei kuitenkaan ole vaan, jos perehdytään tarkemmin englanninkielisten termien määritelmiin niin huomataan, että niillä on selkeä ero. Englannin sana safety viittaa järjestelmän toiminnallisen turvallisuuden huomioon ottamiseen. Tavoitteena on suojella ympäristöä järjestelmän toimintahäiriöiltä ja siten säilyttää ympäristön ja ihmisten koskemattomuus. Security puolestaan pyrkii suojaamaan järjestelmää ja siihen tallennettuja tietoja ei-toivotulta pääsyltä ja ympäristön aiheuttamilta vahingoilta. (Turvallisuuskomitea 2017.)

Turvallisuuden käsitteellisten eroavaisuuksien lisäksi näillä kahdella määritelmällä on myös toimialueellisia eroavaisuuksia. Safety erottuu erittäin staattisesta luonteesta. Jos esimerkiksi tuotantokoneelle on kehitetty ja toteutettu turvallisuuskonsepti, tämä järjestelmä ei muutu niin nopeasti, että turvallisuusvaatimuksia ja -toimenpiteitä tarvitsisi mukauttaa usein. Vaikka turvakomponentit voivat vanhentua tai kulua, tämä tapahtuu yleensä pikkuhiljaa melko pitkän ajan kuluessa. (TEPA-termipankki 2024.)

Safetyyn verrattuna security on melko nopeasti muuttuva turvallisuuden ala. Erityisesti verkottuneiden komponenttien lisääntymisen vuoksi security on yhä enemmän keskiössä. Alun perin ensisijaisesti IT-maailmasta tunnetun toimialueen on reagoitava joustavasti ja lyhyellä varoitusajalla järjestelmän uusiin heikkouksiin, koska jokainen heikkous luo välittömästi mahdollisen uhan. (Turvallisuuskomitea 2017.)

Tiivistettynä safety tarkoittaa sitä, että järjestelmä tai siinä tapahtuva virhe ei saa vahingoittaa työntekijää tai ympäristöä. Security taas on järjestelmän suojaamista ulkopuolisilta uhilta, olivat ne sitten ihmisen tai luonnon aiheuttamia. (Turvallisuuskomitea 2017.) Tässä opinnäytetyössä tullaan keskittymään turvallisuuden security -puoleen, sillä tämä opinnäytetyö pyrkii tutkimaan juuri yrityksen fyysistä turvallisuutta ja fyysistä tietoturvallisuutta.

3.2 Riskienhallinta

Riski tarkoittaa epävarmuuden vaikutusta tavoitteisiin (SFS-ISO 31073:2022,6). Riski voi olla kielteinen, myönteinen tai molempia, ja se voi luoda, käsitellä tai saada aikaan uhkia ja mahdollisuuksia (SFS-ISO 31000:2018,6). Riskienhallinta on osa organisaation hallintokäytäntöjä

ja turvallisuusjohtamista. Se on olennainen osa kaikilla tasoilla tapahtuvassa johtamisessa ja tukee johtamisjärjestelmän kehittämistä. Riskienhallinnan tarkoituksena on luoda ja säilyttää arvoa. Se tehostaa suorituskykyä sekä edistää innovointia ja tavoitteiden saavuttamista. Riskienhallinta on jatkuva prosessi, joka auttaa organisaatioita strategian suunnittelussa, tavoitteiden saavuttamisessa ja perusteltujen päätösten tekemisessä tietoon nojaten. Riskienhallinta kietoutuu kaikkiin organisaation toimijoihin ja sisältää myös vuorovaikutuksen sidosryhmien kanssa. Riskienhallinta huomio sekä sisäisen että ulkoisen toimintaympäristön, johon kuuluu esimerkiksi kulttuuriset tekijät ja ihmisten käyttäytyminen. (SFS-ISO 31000:2018,5.)

4 Fyysinen turvallisuus

Tässä luvussa käydään läpi mitä fyysinen turvallisuus on. Luvussa perehdytään myös finassialan kolmannen tason murtosuoja ohjeeseen. Lopuksi luvussa käydään läpi eurooppalaista standardia koskien datakeskuksien turvallisuutta.

Fyysinen turvallisuus on turvatoimien osa, joka koskee henkilöstön ja omaisuuden suojaamiseksi suunniteltuja fyysisiä toimenpiteitä; estää luvaton pääsy laitteisiin, asennuksiin, materiaaleihin ja asiakirjoihin; ja suojella heitä vakoilulta, sabotaasilta, vahingoilta ja varkauksilta. (Yhdysvaltain puolustusministeriö 2005.) Fyysinen turvallisuus on yksi tietoturvan olennaisimmista muodoista. Fyysisen tietoturvallisuuden ytimenä on yrityksen kyky suojata toimitai tuotantotilojaan, laitteitaan, dokumentaatiotaan ja tietojärjestelmiä mahdollisen haitantekijän suorittamilta hyökkäyksiltä tai muilta fyysisiltä uhilta, kuten tuli-, sähkö- tai vesivahingoilta. (Fennelly 2013,339–340.)

Fyysisen turvallisuuden kannalta on erittäin tärkeää toteuttaa huolellinen riskienarviointi. Riskienarvioinnilla määritetään, mitä turvaustoimia voidaan toteuttaa. (Fennelly 2013,12–13.) Suojattavan kohteen sijainti vaikuttaa huomioon otettavien asioiden määrään riskienarvioinnissa. Esimerkiksi: onko suojattava tila jokin tietty kerros vai ulkorakennus? Mitä muita toimijoita rakennuksessa tai sen välittömässä läheisyydessä on? Muiden toimijoiden hätäpoistumisreitit. Suojattavien tilojen seinä-, katto- tai lattiarakenteet voivat mahdollisesti rajoittaa turvallisuusjärjestelyjä. (Fennelly 2013,340–347.)

Kuten aikaisemmin mainittiin, fyysisessä turvallisuudessa tulee ottaa huomioon tilojen suojaaminen eri olosuhteilta kuten vesi ja tuli. Tilojen turvallisuutta voidaan parantaa esimerkiksi palonilmaisu- ja sammutusjärjestelmillä, palokuormaa vähentämällä, riittävällä ilmanvaihdolla ja katkottomalla sähkönsyötöllä. Rakennusautomaatiojärjestelmillä, kuten kosteuden ja lämpötilan säätelyllä, on myös keskeinen funktio fyysisen tietoturvallisuuden ylläpitämisessä palvelintiloissa. Tärkeintä on kuitenkin valita jokaiselle kohteelle sopivimmat ratkaisut rajoitteet ja riskiarviointi huomioon ottaen. (Fennelly 2013,277–283.)

4.1 Finanssialan turvallisuusohjeet rakenteellisesta murtosuojauksesta

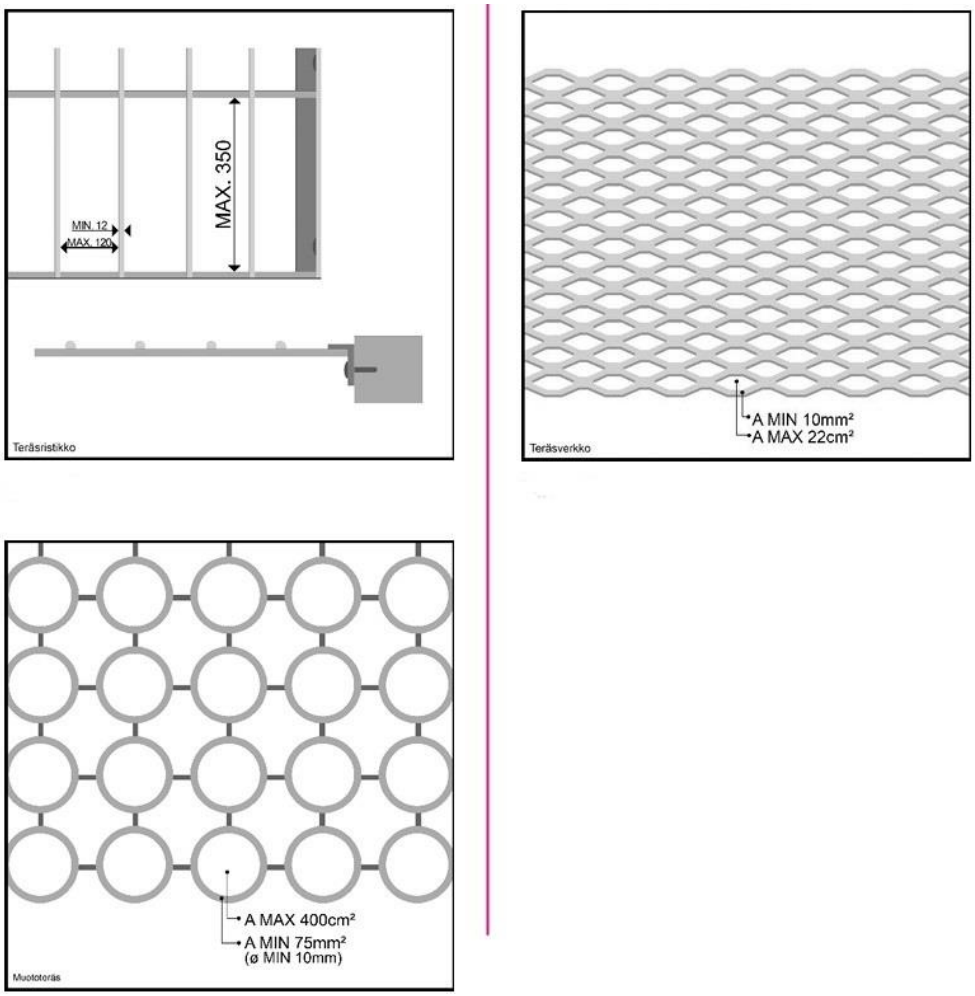
Finanssiala ry on luonut useita eri ohjeita, joita voi käyttää niin yritykset kuin yksityiset henkilöt. Näiden ohjeiden tavoitteena on ehkäistä vahinkojen tapahtumista ja rajata niiden suuruutta. Finanssiala ry muodostuu erilaisista suomalaisista pankeista ja rahoitus- ja vakuutusyhtiöistä.

Dokumentissa ”Rakenteellinen murtosuojaus 3” käsitellään vaatimuksia, jotka koskevat muun muassa seiniä, lattioita, kattoja, ikkunoita, ovia ja lukitusta. Rakenteellinen murtosuojaus 3 on korkein mahdollinen luokka. Mikäli kohde pyrkii saamaan kolmannen tason luokituksen, tulee kaikkien dokumentissa olevien vaatimusten täyttyä. Dokumentissa myös muistutetaan rikoksentorjunnan ja ympäristön huomioon ottamisen tärkeydestä tulevan rakennuksen ja sen ympäristön suunnittelussa. Ympäristö tulisi suunnitella siten, että käyttötarkoituksiltaan ja kulkuoikeuksiltaan erilaiset alueet erotettaisiin toisistaan pensailla, valaistuksella, aidoilla tai muilla arkkitehtuurisilla keinoilla. Edellä mainitut ratkaisut eivät kuitenkaan saisi haitata luonnollista valvontaa. Toisin sanoen ne eivät saisi olla näköesteinä, vaan niiden tulisi helpottaa alueella liikkumisen havaitsemista. Luonnollisella valvonnalla tässä tapauksessa tarkoitetaan oman henkilökunnan valvontaa tai satunnaisten ohikulkijoiden havainnointia. (Finanssiala 2024.)

Suojattavan rakennuksen tai tilan on oltava rakennustavaltaan ja lujuudeltaan sellainen, että tunkeutujan on pakko käyttää rakenteita rikkovia työkaluja sisään pääsemiseksi. Rakenteet ja niiden osat eivät saa olla ulkopuolelta rikkomatta irrotettavissa. Väliseinärakenteiden tulee olla lattiasta kattoon asti rakennettuja. Alakaton yläpuoli suositellaan suojattavan ristikolla. Mikäli tilassa on rakenteellisesti kevyitä seiniä, ne tulee vahvistaa molemmilta puolilta joko 1,0 mm:n metallilevyllä tai 12 mm:n vanerilla. Vahvistuksen tulee olla 4 metrin korkuinen lattia- tai muusta seisomatasosta mitaten. Lasi- ja siirtolasiseinien on oltava vähintään P6B murtosuojalasia. (Finanssiala 2024.)

P6B-lasi koostuu useista lasikerroksista, jotka on laminoitu yhteen käyttäen erityistä polyvinyylibutyraali (PVB) -kalvoa. Tämä kalvo pitää lasin yhtenäisenä iskusta huolimatta, estäen lasin sirpaloitumisen ja murtumisen kokonaan. P6B on suunniteltu kestämään toistuvia iskuja raskailla esineillä, kuten vasaroilla tai kirveillä. (SFS-EN 356:2001,12.)

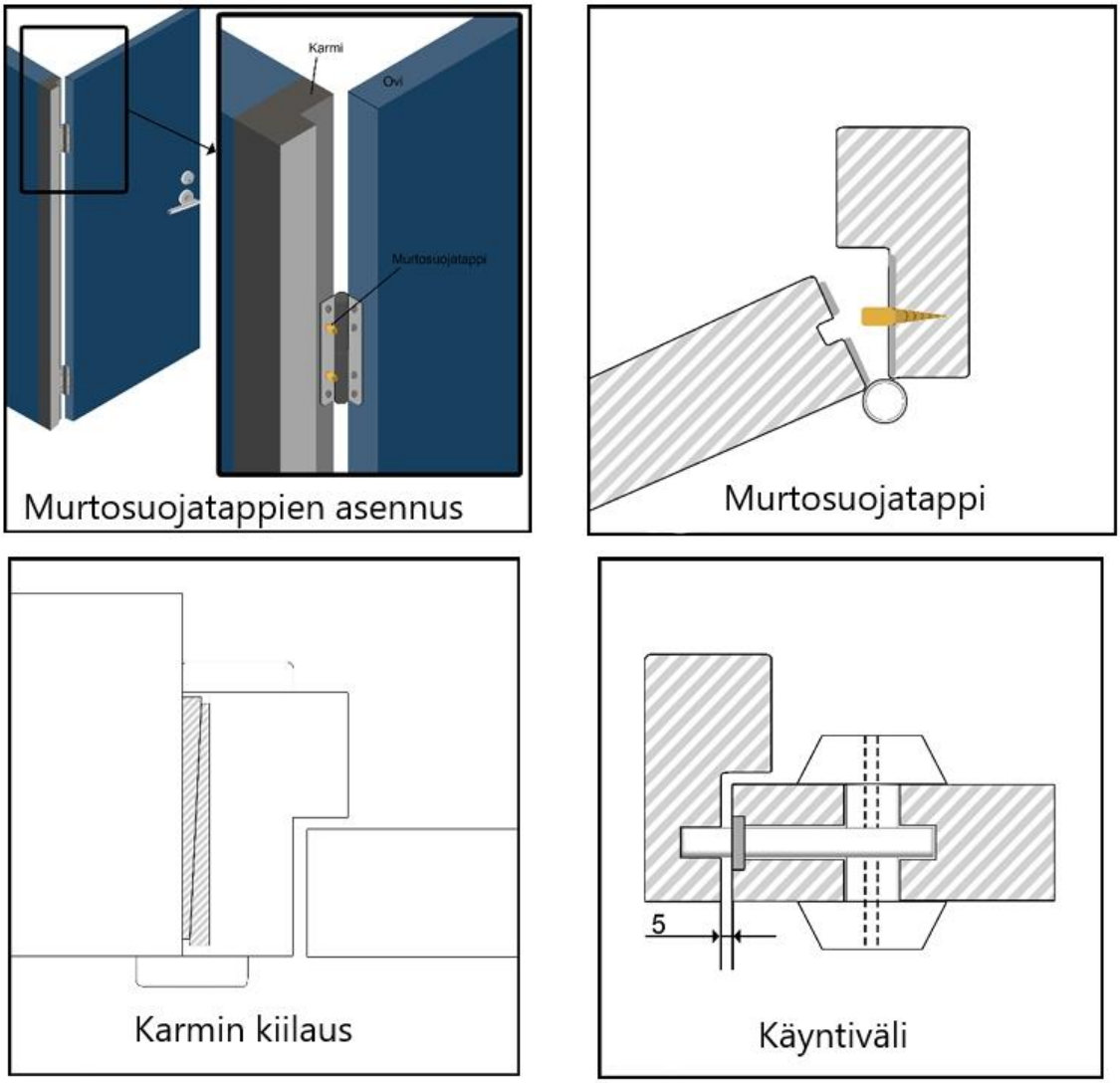
Mikäli P6B-lasin käyttäminen ei ole mahdollista niin lasi tulee suojata siten että ulkopuolinen suojaus on tasoa 4, lasin sisäpuolen suojaus tasoa 3 ja lasi on suojattu rullakalterilla. Kolmas vaihtoehto on suojata lasi teräsverkolla, -ristikolla tai muototeräksellä. Näiden vaihtoehtojen vaatimukset on havainnollistettu kuvassa 1. (Finanssiala 2024.)



Kuva 1: Lasirakenteiden suojaus teräsristikolla, -verkolla tai muototeräksellä (Finanssiala 2024.)

Mikäli rakennuksessa on ikkunoita, ne tulee sulkea ja kiinnittää siten, ettei niitä voi avata tai irrottaa ulkopuolelta ilman rikkomista. Myös ikkunoiden ja kattoikkunoiden on oltava P6B luokan murtosuojalasia tai ne on suojattava samoilla toimenpiteillä kuin edellä mainitussa osiossa. Vaihtoehtoisesti ikkunat ja muut aukot voidaan sulkea suojauslevyllä. Muut aukot, kuten ilmanotto- ja savunpoistoaukot, on suojattava kiinteällä tai lukitulla teräsristikolla. Suojausvaatimus ei kuitenkaan koske sellaisia ikkunoita tai aukkoja, jotka ovat vähintään 4 m:n korkeudessa maan pinnasta tai muusta seisomatasosta. (Finanssiala 2024.)

Rakennuksen ovien on oltava vahvuudeltaan seinärakenteita vastaava. Ovirakenteen saranoiden tai karmin on oltava tapitettu. Saranapuolelle on tarvittaessa kiinnitettävä jokaisen saranan kohdalle murtosuojatappi. Oven karmi on kiilattava rakenteisiin lukkojen ja saranoiden kohdalta. Oven käyntiväli ei saa olla suurempi kuin 5 mm. Mikäli ovessa on lasia niin se on kiinnitettävä siten, ettei sitä voi ulkopuolelta irrottaa rikkomatta. Nämä vaatimukset on havainnoitu kuvassa 2. (Finanssiala 2024.)



Kuva 2: Murtosuoja taso 3 ovien, saranoiden ja karmien vaatimukset (Finanssiala, Rakenteellinen murtosuojausohje 3, 2024)

Lukituksessa tulee käyttää testattuja ja luetteloituja lukkoja. Käyttölukkojen sijasta voidaan käyttää toisen luokan riippulukkoa ja varmuuslukon sijasta kolmannen luokan riippulukkoa. Mikäli ovi lukitaan riippulukoilla, niiden on oltava ulkopuolelta vähintään luokkaa 3 kiinnikkeineen ja sisäpuolelta luokkaa 2 kiinnikkeineen. Lukkojen luokituksessa käytetään SFS:n standardia 7020. Nosto- ja liukuovissa on mahdollista käyttää profiilioven varmuuslukkoja. Aina kun tilassa ei oleskella, on lukkojen oltava takalukossa ja pariovien pikasalpa lukittuna. (Finanssiala 2024.)

Yksilehtisten ovien tulee olla lukittuna käyttö- ja varmuuslukolla. Lukkojen telkien etäisyys toisistaan tulee olla 40 cm. Mikäli kyseessä on lasiovi, niin silloin telkien etäisyys voi olla yli 40 cm. Pariovet lukitaan siten, että käyntipuoli lukitaan samoin kuin yksilehtiset ovet ja oven kiintopuoli suljetaan pikasalvalla, jossa on vähintään luokan 1 riippulukko tai jokin muu

vastaava pikasalvan käytön estävä asia. Vaihtoehtoisesti pariovet voidaan lukita käyttölukon ja lukitun teräspuomin yhdistelmällä tai sisäpuolisilla salvoilla ja riippulukolla. Kippi-, nosto-, taite- ja liukuovet tulee lukita kahdella lukolla. Lukitsimiseen voi myös käyttää profiilioven varmuuslukkoja. Ovet on kuitenkin lukittava myös saranapuolelta, mikäli ovessa on paniikkisaranointi tai se on poistettavissa ylä- tai alaohjauskiskoilta. Siirtolasiseinät ja lasiliukuovet tulee olla lukittuna kahdella lukolla ja niissä käytettävien telkien etäisyys voi olla yli 40 cm. Heiluriovet lukitaan kuten pariovet tai vähintään siten, että toinen ovilehti lukitaan ylä- ja alareunasta varmuuslukolla ja toinen ovilehti lukitaan siihen kuten yksilehtiset ovet. Avattavat rullakalterit ja ristikot tulee lukita kahdella lukolla kuten taitto- tai nosto-ovissa. (Finanssiala 2024.)

4.2 EN 50600 standardi datakeskusten tiloista ja infrastruktuurista

EN 50600 on eurooppalainen standardi, jossa otetaan kantaa datakeskuksien tiloihin ja niihin liittyvään infrastruktuuriin. Standardissa kuvataan yleiset periaatteet tietokeskuksille, joihin EN 50600 -standardin vaatimukset perustuvat. Standardissa määritellään datakeskuksien yhteiset näkökohdat, mukaan lukien terminologia, viitemallit ja parametrit ottaen myös huomioon niiden monimutkaisuus, sekä koko. Standardissa myös kuvataan datakeskuksien tukemiseen vaadittavien laitteiden ja infrastruktuurin yleisiä vaatimuksia. Standardissa täsmennetään tehokkaiden laitosten luokitusjärjestelmää, joka perustuu turvallisuuden, energiatehokkuuden ja saatavuuden kriteereihin, läpi datakeskuksen suunnitellun käyttöiän ajan. Näiden lisäksi standardissa otetaan kantaa muutamaan muuhun asiaan, jotka eivät ole oleellisia tämän opinnäytetyön kannalta. Tiedon luonteen vuoksi opinnäytetyötä varten saatiin käyttöön ainoastaan versio, jossa käytiin läpi standardin yleisiä käsitteitä. Tärkeimmät alueet, joita tästä standardista tarkasteltiin, olivat 6.2 spaces and facilities (tilat ja alueet) sekä 7.3 physical security (fyysinen turvallisuus). (EN 50600 2019,13–20.)

Tiloihin liittyvässä osiossa kerrotaan, että tässä standardissa kaikki datakeskuksen tilat ja kulkuväylät, datakeskuksen koosta tai tarkoituksesta riippumatta, on nimetty tiettyyn suojausluokkaan. Datakeskukseksi määrätyn rakennuksen alueella tilojen tarve ja sisältö riippuu datakeskuksen käyttötarkoituksesta, ennakoidusta virrankulutuksesta ja ympäristön valvonnasta. Tarve tilojen erottelulle riippuu mahdollisista turvallisuusnäkökohdista ja niiden toteutusmahdollisuuksista, ympäristön hallinnan tarpeesta sekä turvallisuusvaatimuksista. Esimerkiksi pienelle yritykselle voi riittää yksi huone, joka toimii tietokonehuoneena ja sähkötilana ilman fyysistä erottelua. Isossa datakeskuksessa voi taas olla useita erillisiä huoneita tietokoneille, sähkönjakelulle ja varavoimalle. (EN 50600 2019,13-16.)

Standardin fyysiseen turvallisuuteen liittyvässä osiossa nostettiin lyhyesti esiin datakeskusalueen suojeleminen luvattomilta sisäänpääsy-yrityksiltä. 50600–2–5 tarkentaa vaatimuksia siten, että sisäänpääsyn estämiseksi tulee käyttää aktiivisia sekä passiivisia menetelmiä. Heti

seuraavassa osiossa mainitaan tunkeutumisien estäminen. Tunkeutumisyritystä pitäisi pystyä hidastamaan niin kauan että tunkeutumiseen ehditään reagoimaan asianmukaisesti. Tunkeutumista voi hidastaa useammalla yksittäisellä esteellä. Tällöin kaikkien näiden yksittäisten esteiden yhteenlaskettu hidastusaika on lopullinen kokonaistunkeutumisen hidastusaika. (EN 50600 2019,19-20.)

5 Fyysinen tietoturva

Tässä luvussa käydään läpi mitä fyysinen tietoturva tarkoittaa. Tämän lisäksi luvussa tutustutaan valtiovarainministeriön suositukseen turvallisuusluokiteltavien asiakirjojen käsittelystä. Luvussa käydään myös läpi tietoturvallisuuden auditointityökalu Katakri ja Traficomin määräys M54045.

Fyysinen tietoturva tarkoittaa kaikkia niitä keinoja, jolla organisaatio suojaa tärkeätä tietoa fyysisiltä uhilta. Fyysisen tietoturvan perustan muodostaa tiedon käsittely- ja säilytystilojen ympärillä olevat suojaavat fyysiset rakenteet. Näiden rakenteiden tulee mahdollistaa tarvittavat äänieristykset, kulunvalvonnat ja näköeristykset. (Valtiovarainministeriö 2007.)

Kaikki yrityksen tilat tulisi luokitella ja sen jälkeen riskienarvioinnin perusteella miettiä miten eri tilat suojataan. Yleensä tilat jaetaan hallinnollisiin- ja turva-alueisiin. Fyysisen tietoturvan kannalta on tärkeää tehdä selkeä rajaus siihen, missä tiloissa saa käsitellä ja tallentaa yrityksen liiketoiminnan kannalta kriittisimpiä tietoja. Yrityksessä tulisi myös rajata työhuoneisiin pääsy, jotta ulkopuoliset tai työntekijät eivät pääse kulkemaan tiloihin, joihin heillä ei ole asiaa. Yrityksessä olisi siis hyvä olla vähimpien oikeuksien käytäntö. Vähimpien oikeuksien periaate tarkoittaa, että työntekijälle annetaan vain välttämättömimmät tietojärjestelmien ja kulkualueiden oikeudet työtehtävän suorittamista varten. (Katakri 2020.)

Tietoturvakriittisten työasemien fyysinen suojelu on olennainen osa organisaation järjestelmien ja tietovarantojen turvaamiseksi. Tähän on olemassa useita eri keinoja kuten fyysisen esteen luominen. Tämä voi olla esimerkiksi lukittava kaappi tai häkki, joka estää pääsyn laitteisiin. Toinen keino on USB-porttien ja muiden liitäntäpisteiden lukitseminen mekaanisella tai jollain muulla erityisellä estolaitteella. Työasemien BIOS- asetuksiin on mahdollista asettaa rajoituksia siten, että se estää tiettyjen laitteiden käynnistämisen. Esimerkiksi jo USB-tikkujen ja muiden ulkoisten laitteiden käynnistämisen estäminen vähentää huomattavasti haittaohjelmien lataamisen riskiä. Niinkin yksinkertainen asia kuin valvontakamera, voi vähentää mahdollisia tunkeutumisyrityksiä, mikäli kamerat on asetettu oikeisiin paikkoihin. (Katakri 2020.)

Avainten ja kulkutunnisteiden käsittely sekä seuranta on tärkeässä asemassa turvallisuuden kannalta. Ei ole väliä kuinka vahva ovi suojattavan kohteen ja tunkeutujan välillä on, mikäli

tunkeutujalla on oveen sopiva avain. Tämän vuoksi kriittisiin tiloihin pääsyyn on hyvä vaatia, avaimen tai tunnisteen lisäksi koodia tai biometristä tunnistautumista. (Katakri 2020.)

5.1 Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä

Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä on valtiovarainministeriön julkaisema asiakirja, jossa kerrotaan mitä toimenpiteitä organisaatioiden täytyy noudattaa käsitellessään turvallisuusluokiteltavia asiakirjoja. Asiakirjassa otetaan kantaa esimerkiksi siihen, kuinka tietoa tulee säilyttää, missä ja miten sitä voi jakaa ja miten tieto tulee lopulta tuhota. Asiakirja ohjeistaa myös tiedon luokittelussa. Asiakirjassa on tuotu esille mitkä lait velvoittavat turvallisuusluokiteltavien asiakirjojen käsittelyä.

Julkisen hallinnon tiedonhallinnasta annetun lain 906/2019 18 §:n mukaisesti valtion virastoissa, laitoksissa ja valtion liikelaitoksissa toimivien viranomaisten, tuomioistuimien ja valitusasioita käsittelemään perustettujen lautakuntien on arvioitava asiakirjojen turvallisuusluokka ja merkittävä ne asianmukaisesti. Tämä tarkoittaa, että heidän on tunnistettava, minkälaisia tietoturvatoimenpiteitä asiakirjan käsittelyyn sovelletaan, ja merkittävä tämä luokka selkeästi asiakirjaan. (Valtioneuvosto 2021,3.)

Turvallisuusluokkaan liittyvä merkintä on tehtävä aina, kun asiakirja tai sen sisältämä tieto on määritelty salassa pidettäväksi viranomaisten toiminnan julkisuudesta annetun lain 1101/2019 24 §:n 1 momentin 2, 5 tai 7–11 kohdassa. Tämä koskee tilanteita, joissa asiakirjan tietojen luvaton paljastuminen tai väärinkäyttö voisi aiheuttaa vahinkoa esimerkiksi maanpuolustukselle, poikkeusoloihin varautumiselle, kansainvälisille suhteille, rikosten torjunnalle, yleiselle turvallisuudelle tai valtion- ja kansantalouden toimivuudelle tai vastaavilla tavoilla Suomen turvallisuudelle. (Valtioneuvosto 2021,9.)

turvallisuusluokan määrittäminen perustuu siihen, kuinka suurta vahinkoa luvaton tietojen paljastuminen voisi aiheuttaa. Vahinkoa arvioitaessa on huomioitava muun muassa seuraavat tekijät: mikä on arvioidun vahingon laajuus, suuruus sekä kesto? Minkälaiset vaikutukset arvioidulla vahingolla voi olla? Mihin laissa mainittuun suojattavaan etuun vahinko kohdistuu? Minkälaiset uhkatekijät vaikuttavat mahdolliseen vahingon toteuttamiseen. Muodostuuko asiakirjojen kasautumisesta riskejä (nk. kasaumavaikutus). Turvallisuusluokitteluasetuksen 1101/2019 3 §:n 1 momentin kohdissa 1–4 on kerrottu, kuinka turvallisuusluokiteltavat asiakirjat jaotellaan eri turvallisuusluokkiin. Nämä eri luokat on kerrottu alla olevassa taulukossa 1. (Valtioneuvosto 2021,12.)

Taulukko 1: Asiakirjojen jakaminen eri turvallisuusluokkiin (Valtioneuvosto 2021)

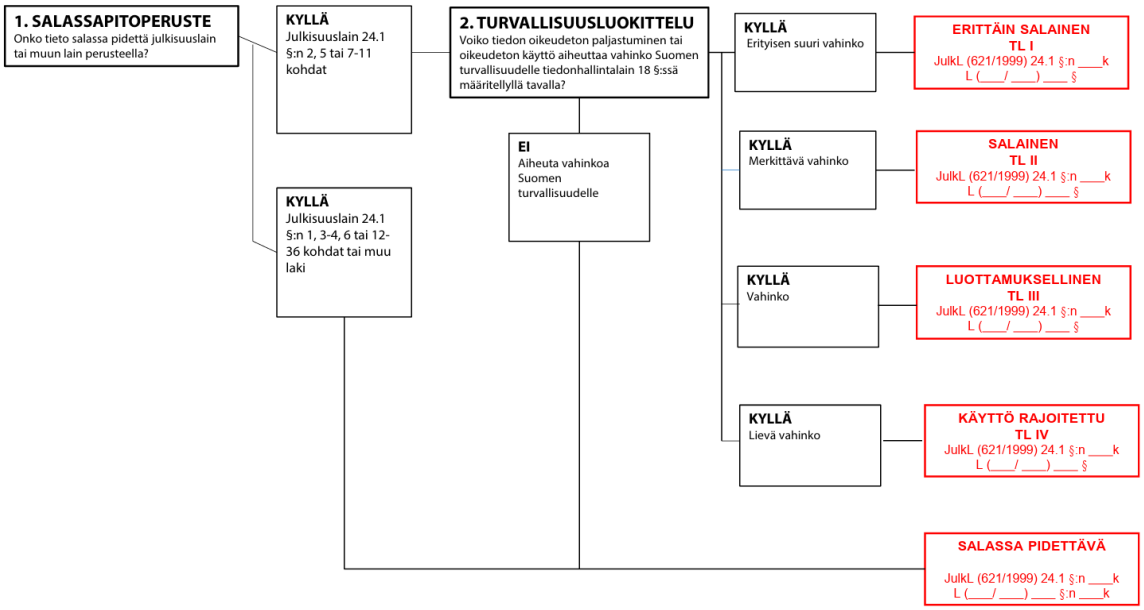
	TL IV	TLIII	TL II	TL I
Kuvaus	Asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa lievää vahinkoa suojattavalle edulle.	Asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa suojattavalle edulle.	Asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa merkittävää vahinkoa suojattavalle edulle.	Asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa erityisen suurta vahinkoa suojattavalle edulle
Tarkempi kuvaus	Tiedon paljastumisesta voi aiheutua seuraus tai tapahtuma, jonka vuoksi ei tarvitse keskeyttää toimintaa, saatetaan joutua muuttamaan toiminnallisia suunnitelmia.	Tiedon paljastumisesta voi aiheutua seuraus taikka tapahtuma, jonka vuoksi toiminta joudutaan keskeyttämään.	Tiedon paljastumisesta voi aiheutua seuraus tai tapahtuma, jonka vuoksi toiminta joudutaan keskeyttämään ja se estyy pitkähköksi ajaksi.	Toiminta keskeytyy, estyy pysyvästi. Vahinko on laajamittaista ja kohdistuu esim. yhteiskunnan toimintakyvyn kannalta keskeisiin kohteisiin/toimintoihin, kuten kriittiseen infrastruktuurin tai elintärkeään toimintaan.
Suojattava etu: Esimerkiksi poikkeusoloihin varautuminen	Mahdollisesti vaarantaa viranomaisen toiminnan. Esim. olennaisten tietojärjestelmien dokumentit kuten turvajärjestelyt, haavoittuvuudet ja auditointiraportit jatkuvuus- ja toipumissuunnitelmat.	Todennäköisesti vaarantaa viranomaisen toiminnan. Esim. elintärkeiden toimintojen turvallisuusjärjestelyt, jatkuvuus- ja toipumissuunnitelmat	Mahdollisesti estää viranomaisen toiminnan. Laajan ihmisjoukon turvallisuutta ei voida taata. Esim. elintärkeiden toimintojen ja niitä tukevien tietojärjestelmien keskeiset dokumentit turvajärjestelyistä, haavoittuvuuksista ja auditoinneista.	Todennäköisesti estää viranomaisen toiminnan ja turvallisuusjärjestelyjen tarkoituksen toteutumisen.

Tiedon saa luokitella se henkilö, jolla on asian ratkaisijana valtuus päättää asiakirjan luokittelusta, joka jakaa aiheeseen liittyvän toimeksiannon tai luo tiedon ensimmäisen kerran. Tiedon luokittelija tekee arvion tiedon mahdollisesta salassapidosta, sekä perustelee mihin säännökseen salassapito perustuu. Luokittelu tulee aina tehdä tapauskohtaisesti riskienarviontiin perustuen. Riskienarvioinnissa tulee ottaa huomioon tietojen yhdistelyn vaikutus sekö tiedon kasaumavaikutus. Nämä kaksi asiaa voivat korottaa riskejä ja näin ollen edellyttää mittavampia tietoturvatoimenpiteitä. Esimerkiksi jos yhdistetään kaksi TL IV- luokan tietoa, niin lopputuloksena voi olla TL I-IV tason kokonaisuus riippuen yhdistetyistä tiedoista. (Valtioneuvosto 2021,13.)

Suomen kriittistä infrastruktuuria ylläpitävissä yrityksissä kuten vaikkapa tilaajayrityksellä, tietyt kerätyt tiedot saattaisivat olla yksittäisinä tietoina liikesalaisuuksiksi tulkittavia. Tässä tapauksessa ne eivät olisi turvallisuusluokiteltavia vaan salassa pidettäviä. Jokin tietty tietojen ryhmä voisi kuitenkin muodostaa yhdistettynä tietokasauman, jonka joutuminen ulkopuolisten käsiin voisi aiheuttaa vahinkoa. Näin ollen tällainen tietokasauma on valtion

turvallisuuden näkökulmasta suojattavaa ja turvallisuusluokittelun perusteet täyttävää. (Valtioneuvosto 2021,35.)

Joissakin yksittäisissä tilanteissa, missä tiedon oikeudeton paljastuminen tai käyttö ei aiheuta vaaraa tiedonhallintalain 906/2019 18§:ssä kuvatulla tai siihen rinnastettavaa tavalla Suomen turvallisuudelle, tieto voidaan silti salata julkisuuslain 1999/621 24§:n 1 momentin 2, 5 tai 7–11 kohtien perusteella. Tällöin tietoon merkitään vain **SALASSA PIDETTÄVÄ.** Kuviossa 1 on tuotu esille myös tämä tiedon salaamisen mahdollisuus. (Valtioneuvosto 2021,34–35.)



Kuvio 1: Salassapito ja turvallisuusluokittelun arviointiprosessi (Valtioneuvosto 2021)

Jotta yli- ja aliluokittelua voitaisiin välttää, tulee organisaation tuntea oman toimialansa erityissääntely sekä varmistaa henkilöstön salassapito- ja turvallisuusluokittelusääntelyn osaaminen. Organisaation on taattava, että asiakirjat turvallisuus luokitellaan lain vaatimusten mukaisesti. Tiedonhallintayksikön johdon tehtävänä on varmistaa tiedonhallinnan vastuiden määritteleminen, huolehtia asianmukaisista työvälineistä, koulutuksesta, ohjeistuksesta ja suoritettava valvontaa. (Tietohallintalaki 4§. 2019.)

Turvallisuusluokitteluasetuksessa (TLA7 §) määrätään myös seuraavanlaisesti monitasoisesta suojauksesta: Monitasoisella suojauksella varmistetaan, että yhden suojauksen murtuessa muut turvatoimenpiteet ennaltaehkäisevät, rajaavat- ja estävät lisävahinkojen syntymistä. Tämän lisäksi tulee suunnitella toimia, joilla voidaan havaita sekä jäljittää turvallisuutta vaarantavia tekoja sekä tapahtumia. Turvatoimien tehtävänä on myös palauttaa toiminta vaarantumista edeltäneeseen turvatasoon mahdollisimman nopeasti. (Valtioneuvosto 2021,33.)

Turvallisuusluokitteluasetuksen 9§ mukaan: tiedonhallintayksikön on määriteltävä fyysisesti suojatut *turvallisuusalueet* turvallisuusluokiteltujen asiakirjojen tietojärjestelmien ja käsittelyn suojaamiseksi. Turvallisuusalueilla tarkoitetaan fyysisesti suojattuja hallinnollisia alueita sekä turva-alueita. Hallinnollisella alueella tarkoitetaan organisaation päivittäiseen työskentelyyn tarkoitettuja tiloja ja alueita, kuten toimistotilaa tai useasta eri kerroksesta muodostuvaa kokonaisuutta. Hallinnollisia alueita voi olla esimerkiksi, yritysten tilat, konesalit tai palvelintilat. Hallinnollisella alueella tulee olla hallitseva toimija, jonka tehtävä on varmistaa, että tiloihin on itsenäinen pääsy ainoastaan viranomaisen ennalta valtuuttamilla henkilöillä. Hallinnollista aluetta rajaavalle rakenteelle ei ole asetettu erityisiä vaatimuksia. Organisaation suorittama riskienarvioinnin tulos vaikuttaa kuitenkin siihen, mitä fyysisiä turvatoimia alueella valitaan. Näiden yksittäisten turvatoimien ja koko turvallisuusjärjestelmän tehokkuutta tulee arvioida uudelleen säännöllisin väliajoin. (Valtioneuvosto 2021,36.)

Vaikka asiakirjassa ei ole annettu vaatimuksia hallinnollista aluetta rajaavalle rakenteelle, niin se asettaa muille fyysisille turvatoimille tiettyjä minimivaatimuksia sekä mahdollisia turvallisuutta parantavia suosituksia. Asiakirjassa olevia minimivaatimuksia on jaettu eri alueisiin.

Alueen rajan on oltava selkeästi määritelty ja näkyvä. Suosituksena ohjeistetaan varmistamaan alueen aukot siten, että ne on mahdollista lukita. Alueen rakenteita suositellaan myös vahventamaan, mikäli alueella säilytetään turvaluokiteltua tietoa tai murtoriski arvioidaan korkeaksi. Pääsyoikeuksien myöntämiseen liittyen minimivaatimuksena on, että vain organisaation asianmukaisesti valtuuttamilla henkilöillä on itsenäinen pääsy alueelle. Tämän lisäksi organisaation on määriteltävä avainten ja pääsyoikeuksien roolit ja menettelyt. Vierailijoihin liittyen minimivaatimus on, että heillä tulee aina olla saattaja. Muutamina suosituksina mainitaan vierailijakortin käyttäminen, vierailun kirjaaminen sekä vierailijoiden valvominen. Äänieristys tulee toteuttaa siten, että se estää asiaan kuulumattomien henkilöiden mahdollisuuden kuulla selväsanaisesti turvallisuusluokiteltuun tietoon liittyviä keskusteluja. Äänieristys tulee ottaa huomioon myös alueen sisällä, mikäli kaikilla alueen sisällä olevilla henkilöillä ei ole tiedonsaantitarvetta turvallisuusluokiteltuun tietoon kuten taulukossa 2 mainitaan. (Valtioneuvosto 2021,36–40.)

Taulukko 2: Hallintoalueen vähittäisvaatimukset osa 1 (Valtioneuvosto 2021)

Turvallisuuden osa-alue	Vähimmäisvaatimus	Lisätietoja ja suosituksia
Alueen raja ja rakenteet (seinät, ovet, ikkunat, lattia- ja kattorakenteet)	Alueella on oltava selkeästi määritelty näkyvä raja. Aluetta rajaavalle rakenteelle ei aseteta erityisiä vaatimuksia.	Alueen aukot, joita ei käytetä kulkemiseen, on voitava lukita, jotta alueelle kulkua on mahdollista hallinnoida asianmukaisesti. Alueen rakenteita tulee vahventaa, mikäli alueella säilytetään turvallisuusluokiteltua tietoa ja murtoriski arvioidaan todennäköiseksi.
Pääsyoikeuksien myöntäminen	Ainoastaan viranomaisen asianmukaisesti valtuuttamilla henkilöillä on itsenäinen pääsy alueelle. Viranomaisen on määriteltävä alueen pääsyoikeuksien ja avainten hallinnan menettelyt ja roolit.	Pääsyn rajaaminen alueelle voidaan toteuttaa joko mekaanisesti, elektronisesti tai henkilökohtaiseen tunnistamiseen perustuen. Alueelle tulee nimetä vastuuhenkilö, joka huolehtii pääsyoikeuksien, kulkutunnisteiden ja avainten hallinnasta. Viranomainen on määritellyt tai hyväksynyt ainakin seuraavat menettelyt ja roolit: • pääsyoikeuksien ja avainten hallinnan menettelytavat ja roolit on luotu, dokumentoitu ja ohjeistettu. • pääsyoikeuksien ja avainten haltijoista on lista. • pääsyoikeudet tarkastetaan säännöllisesti ja ne pidetään ajan tasalla. • avainten ja kulkutunnisteiden lisätilauksia ja muutoksia koskevat toimet on vastuutettu. • avainkortteja, jakamattomia avaimia ja kulkutunnisteita säilytetään asianmukaisesti.
Vierailijat	Muilla kuin viranomaisen asianmukaisesti valtuuttamilla henkilöillä (vierailijoilla) on aina oltava saattaja.	Viranomaisen on täytynyt hyväksyä menettelyohje vierailijoita varten. Viranomaisen hyväksymä vierailijaohje voi käsitellä muun muassa seuraavia asioita: • vieras tunnistetaan ja varustetaan vieraskortilla. • vierailu kirjataan. • vierailijoita ei päästetä tai jätetä tiloihin valvomatta. Vierailun isäntä vastaa ulkopuolisista henkilöistä koko vierailun ajan. • henkilöstö on ohjeistettu vierailijoiden isännöintiä varten • huolehtiminen siitä, ettei vieras pääse oikeudettomasti näkemään, kuulemaan tai muutoin saa haltuunsa turvallisuusluokiteltua tietoa.
Äänieristys	Alueen äänieristyksen tulee estää asiaan kuulumattomia henkilöitä kuulemasta selväsanaisena turvallisuusluokiteltuun tietoon liittyviä keskusteluja. Äänieristys tulee ottaa huomioon myös alueen sisällä, mikäli siellä keskustellaan turvallisuusluokitelluista tiedoista, joihin kaikilla ei ole tiedonsaantitarvetta.	Äänieristysvaatimus kohdistuu ainoastaan alueen niihin tiloihin, joissa keskustellaan turvallisuusluokitelluista tiedoista.

Teknisiin turvallisuusjärjestelmiin liittyen vähimmäisvaatimus on se, että organisaation on varmistuttava, että sen turvallisuusluokiteltujen tietojen fyysistä suojaamista varten käyttöönotetut turvallisuuslaitteet ja järjestelmät ovat toimintakuntoisia ja käyttötarkoitukseen soveltuvia. Suosituksena annetaan, että laitteet olisivat teknisten standardien hyväksymiä sekä niiden toimintakunnosta pidettäisiin huolta korjauksilla ja ajantasaista dokumentaatiota ylläpitämällä. Salaa katselun estäminen täytyy toteuttaa siten että niin ei pääse tapahtumaan vahingossa tai tahallaan. Suosituksena tässä osiossa on mainittu työpisteiden erilainen sijoittelu, sälekaihtimien, tietokoneen näytönsuojien tai verhojen käyttäminen. Tila- ja laitetarkistuksessa mainitaan, että organisaation on tarkistettava kaikki elektroniset laitteet, ennen kuin niitä saa käyttää sellaisella hallinnollisella alueella, jossa käsitellään TL II turvallisuusluokan tietoja tai TL III turvallisuusluokan tietoa, johon kohdistuva uhka arvioidaan korkeaksi. Mikäli kaikkien elektronisten laitteiden tarkastaminen ei ole mahdollista luotettavasti, silloin tarkistamattomat laitteet tulee jättää tilan ulkopuolelle. Mainitsematta jätetyt suositukset voi katsoa taulukosta 3. (Valtioneuvosto 2021,36–40.)

Taulukko 3: Hallintoalueen vähittäisvaatimukset osa 2 (Valtioneuvosto 2021)

Turvallisuuden osa-alue	Vähimmäisvaatimus	Lisätietoja ja suosituksia
Tekniset turvallisuusjärjestelmät	Viranomaisen on varmistuttava, että turvallisuusluokiteltujen tietojen fyysisistä suojaamista varten käyttöönotetut turvallisuusjärjestelmät ja laitteet (esimerkiksi soveltuvaksi arvioidut säilytysratkaisut, paperisilppurit, lukot, elektroniset kulunvalvontajärjestelmät, kameravalvontajärjestelmät, tunkeutumisen ilmaisujärjestelmät ja hälytysjärjestelmät) ovat käyttötarkoitukseen soveltuvia ja toimintakuntoisia.	Suosituksena on, että laitteet ovat hyväksyttyjen teknisten standardien ja vähimmäisvaatimusten mukaisia. Laitteet pidetään toimintakuntoisina huolehtimalla tarvittavista korjaus- ja huoltotoimenpiteistä, toiminnan testauksista sekä dokumentaation ajantasaisuudesta laitevalmistajan ohjeiden ja suositusten mukaisesti. Järjestelmäoikeuksien hallinnassa on suositeltavaa noudattaa vähimpien oikeuksien periaatetta
Tunkeutumisen ilmaisujärjestelmä	Ei vaatimuksia.	Alue tai alueelle johtavat reitit voidaan varustaa tunkeutumisen ilmaisujärjestelmällä (murtohälytysjärjestelmä), mikäli alueella säilytetään turvallisuusluokiteltua tietoa ja murtoriski arvioidaan korkeaksi. Alueen suositellaan olevan valvottu järjestelmän avulla, kun alueella ei työskennellä.
Salaa katselun estäminen	Jos turvallisuusluokiteltuihin tietoihin kohdistuu salaa katselun riski, vahingossa tapahtuva salaa katselu huomioon ottaen, on riskin torjumiseksi tehtävä asianmukaiset toimenpiteet.	Salaa katselun riskiä voidaan pienentää esimerkiksi työpisteiden sijoittelun ja näkösuojasermien avulla sekä käyttämällä sälekaihtimia, verhoja tai tietokoneen näytön suojia.
Tila- ja laitetarkastukset	Viranomaisen on tarkastettava kaikki elektroniset laitteet, ennen kuin niitä käytetään sellaisella hallinnollisella alueella, jossa käsitellään SALAINEN (TL II) turvallisuusluokan tietoja ja riskiarvion perusteella LUOTTAMUKSELLINEN (TL III) turvallisuusluokan tietoja, mikäli tietoihin kohdistuva uhka arvioidaan korkeaksi. Myös alue on tarvittaessa tarkastettava fyysisesti tai teknisesti säännöllisin väliajoin. Tarkastukset tulisi suorittaa myös mahdollisen luvattoman sisäänpääsyn tai sen epäilyn jälkeen.	Mikäli kyseisten elektronisten laitteiden tarkastaminen ei ole mahdollista luotettavasti (esim. matkapuhelimet, älykellot), laitteet tulee jättää tilan ulkopuolelle esimerkiksi tähän tarkoitukseen varattuun säilytysratkaisuun.
Tiedon säilyttäminen	Alueella voi säilyttää KÄYTTÖ RAJOITETTU (TL IV) -turvallisuusluokan tietoa. Tiedot tulee säilyttää soveltuvissa lukituissa toimistokalusteissa. Jos turvallisuusluokan III tai IV sähköisiä asiakirjoja säilytetään päätelaitteessa turva-alueiden ulkopuolella, ne on suojattava turvallisuusluokalle riittävän turvallisella salausratkaisulla. Päätelaitteen tietoturvallisuudesta on huolehdittava.	

Hallinnollisella alueella voi säilyttää TL IV- turvallisuusluokan tietoa. Tieto tulee säilyttää soveltuvassa lukitussa toimistokalusteessa. Mikäli TL III tai TL IV sähköisiä asiakirjoja säilytetään päätelaitteissa turva-alueen ulkopuolella, tulee ne suojata turvallisuusluokalle riittävällä salausratkaisulla. Kyseisen päätelaitteen tietoturvallisuudesta on myös huolehdittava. (Valtioneuvosto 2021,38–40.)

Aiemmin mainittu turva-alue tarkoittaa organisaation työskentelyyn tarkoitettua aluetta, jossa voi myös käsitellä ja säilyttää turvallisuusluokiteltua tietoa. Turva-alueet ovat hallinnollisia alueita paremmin suojattu. Turva-alue on mahdollista rakentaa tilapäisesti hallinnolliselle alueelle, mikäli turva-alueen vähimmäisvaatimukset saadaan kyseiseen tilaan toteutettua. Myös turva-alueen fyysisten turvatoimien valintaa organisaation suorittama riskienarviointi. Turva-alueen koko järjestelmän tehokkuus sekä yksittäisten turvatoimien toimivuus täytyy arvioida uudelleen säännöllisin väliajoin. (Valtioneuvosto 2021,41.)

Turva-alueen fyysisten turvatoimien vähimmäisvaatimuksissa on joitakin samoja vaatimuksia kuin hallintoalueilla, mutta ymmärrettävästi tiukempia lisävaatimuksia on myös asetettu kuten kuvioissa 4, 5 ja 6 käy ilmi. Alueen raja ja rakenteet tulee olla selkeästi määritelty näkyvä raja ja lisäksi mikäli alueella ei ole tiedon säilytykseen riittäväksi arvioitua säilytysratkaisua, on alueen seinien, katon, ikkunoiden, lattian ja ovien tarjottava tietojen säilytykseen edellyttämä turvallisuustaso. Kulunvalvonta täytyy toteuttaa siten, että kaikkea kulkua sisään ja ulos alueelta seurataan kulkulupien avulla tai henkilökohtaisesti tunnistamalla. Tämän lisäksi suosituksena mainitaan, että kulkulupa turva-alueelle tulisi olla vain sellaisella henkilöllä, jolla on oikeus olla alueella. Kulku alueelle tulisi myös myöhemmin olla mahdollista todentaa. (Valtioneuvosto 2021,42–46.)

Itse pääsyoikeuksien myöntäminen toteutetaan siten, että itsenäisen pääsyoikeuden myöntäminen turva-alueelle voidaan myöntää vain sellaiselle organisaation asianmukaisesti valtuuttamalle henkilölle, jonka luetettavuus on varmistettu ja jolla on erityinen lupa tulla alueelle. Suosituksena on, että henkilön luotettavuus tulisi ensisijaisesti varmistaa henkilöturvallisuusselvitysmenettelyn avulla. Alueella pääsemisen perusteena tulisi olla tiedonsaanti tarve tai tapauskohtaisesti erityinen lupa voi tarkoittaa työskentelytarvetta alueella. Tämän lisäksi suosituksena on myös, että alueella on nimetty vastuuhenkilö, jonka tehtävänä on huolehtia pääsyoikeuksien, avainten ja kulkutunnisteiden hallinasta. (Valtioneuvosto 2021,42–46.)

Vierailijoiden osalta vähimmäisvaatimuksena on, että heillä on aina oltava saattaja. Lisäksi, jos pääsy turva-alueelle mahdollistaa välittömän pääsyn turvallisuusluokiteltuihin tietoihin, on otettava huomioon kaksi lisävaatimusta. Alueella säilytettävien tietojen korkein turvallisuusluokka on ilmoitettava selvästi. Henkilöillä, jotka pääsevät alueelle ilman saattajaa, tulee olla asetuksen 8 §1 momentin mukainen oikeutettu tiedonsaantitarve kyseisiin tietoihin. Jos tiedonsaantitarvetta ei ole, on toteutettava tietoturvatoimenpiteitä sen varmistamiseksi, ettei turvallisuusluokiteltuihin tietoihin ole pääsyä. Vierailijoihin liittyvät suositukset ovat samat kuin hallintoalueilla kuten taulukosta 4 huomataan. (Valtioneuvosto 2021, 42–46.)

Taulukko 4: Turva-alueen vähimmäisvaatimukset osa 1 (Valtioneuvosto 2021)

Turvallisuuden osa-alue	Vähimmäisvaatimus	Lisätietoja ja suosituksia
Alueen raja ja rakenteet (seinät, ovet, ikkunat, lattia- ja kattorakenteet)	Alueella on oltava selkeästi määritelty näkyvä raja. Mikäli alueella ei ole tiedon säilytykseen riittäväksi arvioitua säilytysratkaisua, on alueen seinien, lattian, katon, ikkunoiden ja ovien tarjottava tietojen säilytyksen edellyttämä turvallisuustaso.	Alueen aukot, joita ei käytetä kulkemiseen, on voitava lukita, jotta alueelle kulkua on mahdollista hallinnoida luotettavasti. Alueen rakenteita tulee vahventaa, mikäli alueella säilytetään turvallisuusluokiteltua tietoa ja murtoriski arvioidaan merkittäväksi. Mikäli mahdollista, hallinnollisen alueen hätäpoistumistiet eivät saa kulkea turva-alueen kautta. Tämä on otettava huomioon erityisesti uudisrakentamisessa. Hätäpoistumisjärjestelyt eivät saa heikentää turvatoimia.
Kulunvalvonta	Alueen rajalla tulee valvoa kaikkea kulkua sisään ja ulos kulkulupien avulla tai tunnistamalla henkilöt henkilökohtaisesti.	Kulunvalvonta voidaan toteuttaa joko elektronisesti tai henkilökohtaiseen tunnistamiseen perustuen. Turva-alueelle kulkuoikeus on vain alueelle oikeutetulla henkilöllä. Kulku alueelle pitäisi olla myöhemmin todennettavissa.
Pääsyoikeuksien myöntäminen	Itsenäinen pääsyoikeus alueelle voidaan myöntää vain viranomaisen asianmukaisesti valtuuttamalle henkilölle: • jonka luotettavuus on varmistettu. • jolla on erityinen lupa tulla alueelle. Viranomaisen on määriteltävä alueen pääsyoikeuksien ja avainten hallinnan menettelyt ja roolit.	Luotettavuus tulisi ensisijaisesti varmistaa henkilöturvallisuusselvitysmenettelyn avulla. Alueelle pääsemisen perusteena tulisi olla tiedonsaantitarve. Tapauskohtaisesti erityinen lupa voi tarkoittaa myös työskentelytarvetta alueella. Alueelle tulee nimetä vastuuhenkilö, joka huolehtii pääsyoikeuksien, kulkutunnisteiden ja avainten hallinnasta. Viranomainen on määritellyt tai hyväksynyt ainakin seuraavat menettelyt ja roolit: • pääsyoikeuksien ja avainten hallinnan menettelytavat ja roolit on luotu, dokumentoitu ja ohjeistettu. • pääsyoikeuksien ja avainten haltijoista on lista. • pääsyoikeudet tarkastetaan säännöllisesti ja ne pidetään ajan tasalla. • avainten ja kulkutunnisteiden lisätilauksia ja muutoksia koskevat toimet on vastuutettu. • avainkortteja sekä jakamattomia avaimia ja kulkutunnisteita säilytetään asianmukaisesti.
Vierailijat	Muilla kuin niillä henkilöillä, joille on myönnetty itsenäinen pääsyoikeus tilaan (vierailijoilla), on aina oltava saattaja. Jos turva-alueelle tulo merkitsee käytännössä välitöntä pääsyä siellä oleviin turvallisuusluokiteltuihin tietoihin, sovelletaan lisäksi seuraavia vaatimuksia: alueella tavanomaisesti säilytettyjen tietojen korkein turvallisuusluokka on ilmoitettava selkeästi. Mikäli turva-alueelle pääsy tarkoittaa välitöntä pääsyä siellä käsiteltäviin turvallisuusluokiteltaviin asiakirjoihin tai niihin sisältyviin tietoihin, niin alueelle ilman saattajaa pääsevillä henkilöillä tulee olla myös 8 §:n 1 momentissa tarkoitettu tiedonsaantitarve näihin tietoihin. Jos tiedonsaantitarvetta ei ole, niin tulee toteuttaa tietoturvallisuustoimenpiteitä sen varmistamiseksi, ettei turvallisuusluokiteltaviin tietoihin ole pääsyä.	Viranomaisen on täytynyt hyväksyä menettelyohje vierailijoita varten. Viranomaisen hyväksymä vierailijaohje voi käsitellä muun muassa seuraavia asioita: • vieras tunnistetaan ja varustetaan vieraskortilla, • vierailu kirjataan, • vierailijoita ei päästetä tai jätetä tiloihin valvomatta. Vierailun isäntä vastaa ulkopuolisista henkilöistä koko vierailun ajan, • henkilöstö on ohjeistettu vierailijoiden isännöintiä varten, huolehtiminen siitä, ettei vieras pääse oikeudettomasti näkemään tai kuulemaan turvallisuusluokiteltua tietoa.

Turvallisuusohjeiden minimivaatimuksia on, että kullekin turva-alueelle on laadittava turvallisuusmenettelyt, joissa on määräykset seuraavista asioista: Sovellettavat suojaus- ja valvontatoimenpiteet. Turvallisuusluokka turvallisuusluokitelluille tiedoille, joita alueella voidaan säilyttää ja käsitellä. Henkilöt, joilla on pääsy alueelle ilman saattajaa luotettavuuden varmistamisen ja erityisen luvan perusteella. Tarvittaessa menettelyt saattajien käyttämiseksi tai turvallisuusluokiteltujen tietojen suojaamiseksi silloin, kun muille henkilöille myönnetään pääsy alueelle. Muut asiaan kuuluvat toimenpiteet ja menettelyt. (Valtioneuvosto 2021, 42–46.)

Äänieristyksen minivaatimukset ovat samat kuin hallintoalueilla elikkä äänieristyksen tulee estää asiaan kuulumattomien henkilöiden mahdollisuus kuulla selväsanaisesti turvallisuusluokiteltuun tietoon liittyviä keskusteluja. Äänieristys tulee ottaa huomioon myös alueen sisällä, mikäli kaikilla alueen sisällä olevilla henkilöillä ei ole tiedonsaantitarvetta turvallisuusluokiteltuun tietoon. Kummallakin alueella äänieristysvaatimus kohdistuu ainoastaan niihin alueen tiloihin, joissa keskustellaan turvallisuusluokitelluista tiedoista. (Valtioneuvosto 2021, 42–46.)

Teknisten turvallisuusjärjestelmien vähimmäisvaatimukset ovat, että organisaation on varmistuttava, että sen turvallisuusluokiteltujen tietojen fyysistä suojaamista varten käyttöönotetut turvallisuuslaitteet ja järjestelmät ovat toimintakuntoisia ja käyttötarkoitukseen soveltuvia. Tämän lisäksi laitteet ja järjestelmät on tarkastettava ja huollettava säännöllisin väliajoin. (Valtioneuvosto 2021, 42–46.)

Tunkeutumisen ilmaisu järjestelmän kohdassa vaaditaan, että alueella, jossa ei työskentele henkilöstöä vuorokauden ympäri tulee alue tarvittaessa tarkistaa normaalin työajan päätteeksi sekä satunnaisin ajoin työajan ulkopuolella. Poikkeuksena on, jos aluetta valvotaan tunkeutumisen ilmaisujärjestelmällä (murtohälytysjärjestelmä). Suosituksena on, että alue pidetään järjestelmän avulla valvottuna aina kun siellä ei työskennellä. Viimeinen taulukossa 5 käytävä asia on salaa katselu estäminen. Sen estämiseksi on tehtävä asianmukaiset toimenpiteet, jos turvaluokiteltuihin tietoihin kohdistuu salaa katselun riski. Vahingossa tapahtuva salaa katselu tulee ottaa myös huomioon. (Valtioneuvosto 2021, 42–46.)

Taulukko 5: Turva-alueen vähimmäisvaatimukset osa 2 (Valtioneuvosto 2021)

Turvallisuuden osa-alue	Vähimmäisvaatimus	Lisätietoja ja suosituksia
Turvallisuus-ohjeet	Kullekin turva-alueelle on laadittava turvallisuusmenettelyt, joissa on määräykset seuraavista asioista: • turvallisuusluokka turvallisuusluokitelluille tiedoille, joita alueella voidaan käsitellä ja säilyttää, • sovellettavat valvonta- ja suojatoimenpiteet, • henkilöt, joilla on pääsy alueelle ilman saattajaa erityisen luvan ja luotettavuuden varmistamisen perusteella, • tarvittaessa menettelyt saattajien käyttämiseksi tai turvallisuusluokiteltujen tietojen suojaamiseksi silloin, kun muille henkilöille myönnetään pääsy alueelle, • muut asiaan kuuluvat toimenpiteet ja menettelyt.	
Äänieristys	Alueen äänieristyksen tulee estää asiaan kuulumattomia henkilöitä kuulemasta selväsanaisena turvallisuusluokiteltuun tietoon liittyviä keskusteluja. Äänieristys tulee ottaa huomioon myös alueen sisällä, mikäli siellä keskustellaan turvallisuusluokitelluista tiedoista, joihin kaikilla ei ole tiedonsaantitarvetta.	Äänieristysvaatimus kohdistuu ainoastaan alueen niihin tiloihin, joissa keskustellaan turvallisuusluokitelluista tiedoista.
Tekniset turvallisuus- järjestelmät	Viranomaisen on varmistuttava, että turvallisuusluokiteltujen tietojen fyysisistä suojaamista varten käyttöönotetut turvallisuusjärjestelmät ja laitteet (esimerkiksi soveltuvaksi arvioidut säilytysratkaisut, paperisilppurit, lukot, elektroniset kulunvalvontajärjestelmät, kameravalvontajärjestelmät, tunkeutumisen ilmaisujärjestelmät ja hälytysjärjestelmät) ovat käyttötarkoitukseen soveltuvia ja toimintakuntoisia. Järjestelmät ja laitteet tarkastettava ja huollettava säännöllisin väliajoin.	Suosituksena on, että laitteet ovat hyväksyttyjen teknisten standardien ja vähimmäisvaatimusten mukaisia. Laitteet pidetään toimintakuntoisina huolehtimalla tarvittavista korjaus- ja huoltotoimenpiteistä ja dokumentaation ajantasaisuudesta sekä toiminnan testauksista laitevalmistajan ohjeiden ja suositusten mukaisesti. Järjestelmäoikeuksien hallinnassa on suositeltavaa noudattaa vähimpien oikeuksien periaatetta (kts. kpl 7.6).
Tunkeutumisen ilmaisujärjestelmä	Alue, jolla ei ole henkilöstöä palveluksessa vuorokauden ympäri, on tarvittaessa tarkastettava normaalin työajan päätteeksi ja satunnaisiin aikoihin työajan ulkopuolella, paitsi jos aluetta valvotaan tunkeutumisen ilmaisujärjestelmällä (murtohälytysjärjestelmä).	Alueen suositellaan olevan valvottu järjestelmän avulla, kun alueella ei työskennellä.
Salaa katselun estäminen	Jos turvallisuusluokiteltuihin tietoihin kohdistuu salaa katselun riski, vahingossa tapahtuva salaa katselu huomioon ottaen, on riskin torjumiseksi tehtävä asianmukaiset toimenpiteet.	Salaa katselun riskiä voidaan pienentää esimerkiksi työpisteiden näkösuojasermeillä sekä käyttämällä sälekaihtimia, verhoja tai tietokoneen näytön suojia.

Tila- laitetarkastuksiin liittyen minimivaatimuksena on, että tiloissa, joissa käsitellään luokan I tai II tietoa ei saa olla tai tuoda muita laitteita kuin viranomaisen hyväksymiä elektronisia laitteita. Tämän lisäksi alue on tarkastettava teknisesti tai fyysisesti säännöllisin väliajoin. Tarkastus on myös suoritettava mahdollisen luvattoman sisäänpääsyn tai sen epäilyn jälkeen. Mikäli elektronisten laitteiden tarkistaminen ei ole tilaan mentäessä luotettavasti mahdollista niin suosituksena on, että kyseiset laitteet jätetään alueen ulkopuolelle niille tarkoitettuun säilytystilaan. (Valtioneuvosto 2021, 42–46.)

Suurin ero hallinnollisen ja turva-alueen välillä on turva-alueen suurempi mahdollisuus turvaluokitellun tiedon säilyttämiseen. Taulukossa 6 myös mainitaan, että turva-alueella voi säilyttää kaikkiin turvallisuusluokkiin kuuluvia tietoja ottaen huomioon riskien arviointi ja valitut fyysiset turvatoimet. Vaatimuksina kuitenkin on TL III ja sitä korkeammat TL II ja TL I tiedot tulee säilyttää soveltuvaksi arvioidussa säilytysratkaisussa, joka voi olla esimerkiksi kassakaappi. (Valtioneuvosto 2021,46.)

Organisaation on myös määriteltävä säilytysratkaisun numeroyhdistelmien ja avainten hallinnointimenettelyt. Numeroyhdistelmät tulee antaa mahdollisimman harvoille ja se on muistettava ulkoa. Henkilön tulee olla sellainen, jolla on tarve tietää numeroyhdistelmä. Säilytysratkaisun numeroyhdistelmä on vaihdettava mikäli: se siirretään uuteen säilytyspaikkaan, jokin lukoista on korjattu tai huollettu, numeroyhdistelmän tuntevassa henkilössä tapahtuu muutos, tiedon epäillään tai todetaan vaarantuneen tai aikaa numeroyhdistelmän vaihtamisesta on kulunut 12 kuukautta. Mikäli turvallisuusluokiteltu tieto on taso I, silloin on noudatettava jotakin seuraavista lisäehdoista: teknisesti valvottu säilytysratkaisu, ilman teknistä valvontaa oleva säilytysratkaisu, jonka kunto tarkistetaan säännöllisesti, ilman teknistä valvontaa oleva säilytysratkaisu, jossa on tunkeutumisen ilmaisujärjestelmä ja hälytyksiin vastaa koulutettu vasteyksikkö tai tietoa säilytetään erillisessä tilassa, , jossa on tunkeutumisen ilmaisujärjestelmä ja hälytyksiin vastaa koulutettu vasteyksikkö. (Valtioneuvosto 2021,46.)

Taulukko 6: Turva-alueen fyysisten vähimmäisvaatimukset osa 3 (Valtioneuvosto 2021)

Turvallisuuden osa-alue	Vähimmäisvaatimus	Lisätietoja ja suosituksia
Tila- ja laitetarkastukset	Tiloihin, joissa käsitellään turvallisuusluokan I tai II tietoja, saa tuoda ainoastaan viranomaisen hyväksymiä elektronisia laitteita. Myös alue on tällöin tarkastettava fyysisesti tai teknisesti säännöllisin väliajoin. Tarkastukset on suoritettava myös mahdollisen luvattoman sisäänpääsyn tai sen epäilyn jälkeen.	Mikäli kyseisten elektronisten laitteiden tarkastaminen ei ole mahdollista luotettavasti (esim. matkapuhelimet, älykellot), laitteet tulee jättää tilan ulkopuolelle esimerkiksi tähän tarkoitukseen varattuun säilytysratkaisuun.
Tiedon säilyttäminen	Alueella voi säilyttää kaikkiin turvallisuusluokkiin kuuluvia tietoja riskien arviointiin ja fyysisten turvatoimien valintaan perusten. LUOTTAMUKSELLINEN (TL III) ja sitä korkeamman (TL II, TL I) turvallisuusluokan tietoja tulee säilyttää soveltuvaksi arvioidussa säilytysratkaisussa. Viranomaisen on määriteltävä säilytysratkaisun avainten ja numeroyhdistelmien hallinnointimenettelyt. Numeroyhdistelmät tulee antaa mahdollisimman harvoille, sellaisille henkilöille, joiden on tarpeen tietää ne. Kyseisten henkilöiden on osattava numeroyhdistelmät ulkoa. Turvallisuusluokiteltuja tietoja sisältävien säilytysratkaisujen numeroyhdistelmät on vaihdettava • uuden turvallisen säilytyspaikan vastaanoton yhteydessä. • aina, kun numeroyhdistelmän tuntevassa henkilöstössä tapahtuu muutos. • aina, kun tiedot ovat vaarantuneet tai kun niiden epäillään vaarantuneen. • kun jokin lukoista on huollettu tai korjattu. • vähintään 12 kuukauden välein. Turvallisuusluokitellut tiedot, jotka kuuluvat turvallisuusluokkaan ERITTÄIN SALAINEN (TL I), on säilytettävä turva-alueella noudattaen jotakin seuraavista ehdoista: • teknisesti valvottu säilytysratkaisu, • ilman teknistä valvontaa oleva säilytysratkaisu, jonka kunto tarkastetaan säännöllisesti, • ilman teknistä valvontaa oleva säilytysratkaisu, jossa on tunkeutumisen ilmaisujärjestelmä ja hälytyksiin vastaa koulutettu vasteyksikkö, • erillinen tila, jossa on tunkeutumisen ilmaisujärjestelmä ja hälytyksiin vastaa koulutettu vasteyksikkö.	

Hyvinkin turvalliseksi suunniteltu turvallisuusjärjestelmä rapautuu ajan myötä, mikäli järjestelmään tehdään hallitsemattomia muutoksia. Uskottavan turvallisuusjärjestelmän ylläpito edellyttää menettelyjä, jossa järjestelmiin vaikuttavien muutosten turvallisuusvaikutukset arvioidaan huolellisesti. Mahdollisuuksien mukaan nämä muutokset tulisi testata. Mikäli ongelmia tai haavoittuvuuksia löydetään, ne korjataan tai lisäsuojauksia rakennetaan ennen muutosten käyttöönottoa. (Valtioneuvosto 2021,52.)

5.2 Tietoturvallisuuden auditointityökalu viranomaisille Katakri 2020

Katakri 2020 on tietoturvallisuuden auditointityökalu viranomaisille, jonka avulla voidaan arvioida kohdeorganisaation kykyä suojata kansallista tai kansainvälistä turvallisuusluokiteltua tietoa. Katakri on alun perin luotu puolustusministeriön johdolla viranomaisten ja elinkeinoelämän yhteistyössä. Katakri 2020 on asiakirjan neljäs versio ja sen päivitystyöstä on vastannut sisäministeriön alaisuudessa toimiva kansallinen turvallisuus viranomainen. Katakri 2020-versiossa on kiinnitetty huomiota digitaalisen tietojenkäsittelyn kehitykseen sekä paranneltu työkalun käyttöön liittyviä ohjeistuksia. (Katakri 2020.)

Katakriin on koottu kansallisiin lakeihin ja kansainvälisiin velvoitteisiin perustuvat minimivaatimukset. Heti asiakirjan johdannossa kehotetaankin täydentämään siinä mainittuja vähimmäissuojauksia, mikäli tuvallisuusluokiteltua tietoon kohdistuu poikkeuksellisen suuri ulkopuolinen uhka. Katakri itsessään ei aseta tietoturvallisuudelle ehdottomia vaatimuksia, vaan siihen kerätyt vaatimukset pohjautuvat voimassa olevaan lainsäädäntöön ja Suomea sitoviin kansainvälisiin tietoturvavelvoitteisiin. Katakri on jaettu kolmeen eri osa-alueeseen, jotka ovat turvallisuusjohtaminen, fyysinen turvallisuus ja tekninen tietoturvallisuus. Kaikkien näiden osa-alueiden vaatimukset on kuvattu siten, että niille on mahdollista löytää useampia toteutustapoja. (Katakri 2020.)

Opinnäytetyön aiheen takia hallinnolliset vaatimukset rajattiin pois. Tämän lisäksi työssä keskitytään vain turva-alueen vaatimuksiin, jotka ovat korkeampia kuin hallinnollisen alueen vaatimukset. Tämä päätös tehtiin ajan ja työn määrän säästämiseksi. Turva-alue on organisaation työskentelyalue, jossa käsitellään sekä säilytetään turvallisuusluokiteltua tietoa ja on hallinnollista aluetta paremmin suojattu. Turva-alue voidaan perustaa tilapäisesti hallinnolliselle alueelle esimerkiksi turvallisuusluokiteltua kokousta tai muuta vastaavaa tarkoitusta varten. (Katakri 2020.)

Katakri 2020:n F-osa-alue etenee prosessimaisesti: Ensimmäisenä tunnistetaan kohdeorganisaatiossa käsiteltävä turvallisuusluokiteltu tieto ja arvioidaan siihen liittyvät fyysiset turvallisuusriskit. Auditoijan tehtävänä on arvioida riskien arvioinnin riittävyys ja tarvittaessa vaatia niiden uudelleenarviointia. Kun vähimmäisvaatimukset ja monitasoinen suojaus on toteutettu, auditoija tarkastelee fyysisiä turvatoimia ja arvioi, voidaanko jäljelle jäävät riskit hyväksyä. Jos monitasoinen suojaus ei ole riittävä, sitä parannetaan, kunnes auditoija hyväksyy jäännösriskit ja fyysisten turvatoimien tavoite saavutetaan. Monitasoisella suojaamisella tarkoitetaan useiden toisiaan täydentävien suojauskerrosten käyttämistä tietoturvassa ja fyysisessä turvallisuudessa. Sen tavoitteena on varmistaa, että vaikka yksi suojausmekanismi pettäisi, muut tasot edelleen estävät tai hidastavat uhan toteutumista. (Katakri 2020.)

Haittaohjelmariskejä voidaan hallita muun muassa koventamalla järjestelmiä, rajoittamalla käyttöoikeuksia, pitämällä järjestelmät ajantasaisina turvallisuuspäivitysten osalta sekä

tehostamalla poikkeamien havaitsemiskykyä. Henkilöstön turvatietoisuuden varmistaminen ja haittaohjelman torjuntaohjelmistojen käyttö ovat myös keskeisiä keinoja suojautumisessa. Lisäksi riskejä voidaan vähentää erottamalla riskialttiit ympäristöt tuotantoympäristöistä ja rajoittamalla siirreltävien medioiden, kuten USB-muistien, käyttöä. Torjuntaohjelmia ei ole tarpeen asentaa ympäristöihin, joihin haittaohjelmien pääsy on jo muutoin estetty. (Katakri 2020.)

5.3 Traficomin M54045

Traficomin M54045 on määräys viestintäverkkojen ja -palvelujen varmistamisesta sekä viestintäverkkojen synkronoinnista. Määräyksen tavoitteena on yleisten viestintäverkkojen ja -palvelujen toiminnan turvaaminen häiriötilanteissa. Tämän lisäksi määräys asettaa vaatimuksia yleisten viestintäverkkojen synkronoinnille viestintäpalvelujen ja -yhteyksien laadun varmistamiseksi. Tässä työssä on keskitytty vain määräyksen fyysisen turvallisuuden vaatimuksiin. (Traficom 2021a.)

M54:ssa käytetään taulukon 7 mukaista tärkeysluokittelua. Yleisen viestintäpalvelun tai -verkon komponentit luokitellaan viestintäpalvelun käyttäjämäärän, tyypin ja maantieteellisen vaikutusalueen pinta-alan mukaan. Laitetilan tärkeysluokka on sama kuin laitetilaan sijoitetun tärkeysluokaltaan tärkeimmän viestintäpalvelun tai -verkon komponentin tärkeysluokka. Luokkia on viisi ja 1 luokka on kaikista tärkein. Tietoliikenne toimintaa harjoittavan yrityksen tulee määritellä, dokumentoida ja pidettävä ajan tasalla tiedot kaikista omien viestintäpalveluiden ja -verkkojen tärkeysluokitelluista komponenteista sekä tiloista. Teleyrityksen on myös huolehdittava niistä viestintäverkon tai palvelun komponenteista, jotka jäävät tärkeysluokittelun ulkopuolelle. Mikäli tärkeysluokan 1 tai 2 komponentille ei ole sijoituspaikan läheisyydessä kyseisen tärkeysluokan vaatimuksia täyttävää fyysisesti suojattua laitetilaa, niin silloin tila johon komponentti asetetaan, tulee täyttää vähintään tärkeysluokan 3 fyysisen suojaamisen vaatimukset. (Traficom 2021a.)

Taulukko 7: viestintäverkon tai -palvelun komponentin tärkeysluokittelu (Traficom 2021a)

Tärkeys-luokka	**Viestintäverkon tai -palvelun komponentti**
1	Komponentti, joka vaikuttaa viestintäpalveluihin yli 60 000km^2 alueella tai Komponentti, joka vaikuttaa suurusluokaltaan • ≥200 000 käyttäjän yleiseen palveluun tai • ≥200 000 käyttäjän tekstiviestipalveluun tai • ≥200 000 käyttäjän internet yhteyspalveluun tai • ≥500 000 käyttäjän sähköpostipalveluun tai • ≥300 000 käyttäjän joukkoviestintäpalveluun tai • ≥600 000 käyttäjän muuhun viestintäpalveluun

2	Komponentti, joka vaikuttaa viestintäpalveluihin yli 20 000km^2 alueella tai Komponentti, joka vaikuttaa suurusluokaltaan • ≥50 000 käyttäjän yleiseen palveluun tai • ≥50 000 käyttäjän tekstiviestipalveluun tai • ≥50 000 käyttäjän internet yhteyspalveluun tai • ≥200 000 käyttäjän sähköpostipalveluun tai • ≥100 000 käyttäjän joukkoviestintäpalveluun tai • ≥300 000 käyttäjän muuhun viestintäpalveluun
3	Komponentti, joka vaikuttaa • ≥1 000 käyttäjän yleiseen puhelinpalveluun tai • ≥20 000 käyttäjän yleiseen puhelinpalveluun, joka tarjotaan internet-yhteyspalvelun päällä tai • ≥10 000 käyttäjän tekstiviestipalveluun tai • ≥1200 käyttäjän internet yhteyspalveluun tai • ≥2500 käyttäjän internetyhteyspalveluun, joka on tuotettu koaksiaalikaapelipohjaisella kaapelitelevisioverkolla tai • ≥100 000 käyttäjän sähköpostipalveluun tai • ≥50 000 käyttäjän joukkoviestintäpalveluun tai • ≥100 000 käyttäjän muuhun viestintäpalveluun
4	Komponentti, joka vaikuttaa • ≥250 käyttäjän yleiseen puhelinpalveluun tai • ≥10 000 käyttäjän yleiseen puhelinpalveluun, joka tarjotaan internet-yhteyspalvelun päällä tai • ≥250 käyttäjän internet yhteyspalveluun tai • ≥1500 käyttäjän internetyhteyspalveluun, joka on tuotettu koaksiaalikaapelipohjaisella kaapelitelevisioverkolla tai • ≥30 000 käyttäjän sähköpostipalveluun tai • ≥20 000 käyttäjän joukkoviestintäpalveluun tai • ≥500 000 käyttäjän muuhun viestintäpalveluun
5	• Kiinteän puhelinverkon keskitin tai • Kiinteän verkon internetyhteyspalvelu liityntäverkon komponentti, joka palvelee yli 100 käyttäjää tai • Kiinteän langattoman internetyhteyspalvelun tukiasema tai • Maanpäällisen joukkoviestintäverkon komponentti, joka palvelee yli 50 kotitaloutta tai • Kuitukaapelipohjainen kaapelitelevisioverkon komponentti, joka palvelee yli 50 kotitaloutta tai • Koaksiaalikaapelipohjaisen kaapelitelevisioverkon komponentti, joka palvelee yli 4000 kotitaloutta tai • Komponentti, joka vaikuttaa yli 5000 käyttäjän sähköpostipalveluun.

Laitetilojen kulunvalvonnan vaatimukset eivät huomattavasti eroa toisistaan. Tämän takia mainitsen ensimmäisen luokan tilojen vaatimukset, jotka ovat ymmärrettävästi tiukimmat. Tila on varustettava kulunvalvontajärjestelmällä, joka mahdollistaa kulkuoikeuksien määrittelyn yksilöllisen sähköisen avausvälineen tarkkuudella ja rekisteröi jokaisen kulkutapahtuman. Henkilökunnan ja alihankkijoiden tunnistaminen on toteutettava käyttämällä kulkulupia tai kuvallisia henkilökortteja yhdessä virallisen henkilötodistuksen kanssa. Vierailijoiden tiedot

on kirjattava ylös, ja heidän liikkumistaan tiloissa tulee valvoa. Tila täytyy varustaa automaattisella rikosilmoitusjärjestelmällä, jolla on mahdollista havaita tilan ulkopuolelta tapahtuva tunkeutuminen tilaan. Ainoastaan 1 luokan tiloihin vaaditaan kameravalvonta järjestelmä. Alemaan tason kohteisiin kameravalvonnan toteuttaminen on vapaaehtoista. Mainittakoon vielä, että tason 3 vaatimuksissa on erikseen vaadittu, että tunkeutumisesta kohteeseen on järjestettävä hälytys valvontahenkilökunnalle. Taulukossa 8 on kaikkien tärkeysluokkien vaatimuksen kulunvalvontaan liittyen. (Traficom 2021a.)

Taulukko 8: Laitetilojen kulunvalvonnan vaatimukset (Traficom 2021a)

Laitetilan tärkeysluokka	Vaatimukset
1	Tila on varustettava kulunvalvontajärjestelmällä, jossa kulkuoikeudet voidaan määritellä yksilöllisen sähköisen avausvälineen tarkkuudella ja jossa jokainen kulkutapahtuma rekisteröidään. Henkilökunnan ja alihankkijoiden tunnistettavuus on järjestettävä kuvallisella henkilökortilla tai kulkuluvalla ja virallisella henkilötodistuksella. Vierailijat on rekisteröitävä ja vierailijoiden kulku tilassa tulee olla valvottua. Tila on varustettava tallentavalla kameravalvontajärjestelmällä. Tila on varustettava automaattisella rikosilmoitusjärjestelmällä, jolla havaitaan tilan ulkopuolelta tapahtuva tunkeutuminen tilaan.
2	Tila on varustettava kulunvalvontajärjestelmällä, jossa kulkuoikeudet voidaan määritellä yksilöllisen sähköisen avausvälineen tarkkuudella ja jossa jokainen kulkutapahtuma rekisteröidään. Henkilökunnan ja alihankkijoiden tunnistettavuus on järjestettävä kuvallisella henkilökortilla tai kulkuluvalla ja virallisella henkilötodistuksella. Vierailijat on rekisteröitävä ja vierailijoiden kulku tilassa tulee olla valvottua. Tila on varustettava automaattisella rikosilmoitusjärjestelmällä, jolla havaitaan tilan ulkopuolelta tapahtuva tunkeutuminen tilaan.
3	Laitetilan ovien lukitus ja tilan kulunvalvonta on toteutettava vähintään sähköiseen avaimeen perustuvalla ovien lukituksella. Henkilökunnan ja alihankkijoiden tunnistettavuus on järjestettävä kuvallisella henkilökortilla tai kulkuluvalla ja virallisella henkilötodistuksella. Vierailijoiden kulku tilassa tulee olla valvottua. Tilaan tapahtuneesta tunkeutumisesta on järjestettävä hälytys valvontahenkilökunnalle. Laitetilaan liittyvä sähkökaappi, jota asiaankuulumattomat pääsevät esteettä käsittelemään ja jonka kautta syötetään laitetilan viestintäverkon laitteiden tarvitsema sähkö, on lukittava avaimeen perustuvalla mekaanisella tai sähkömekaanisella lukolla.
4 tai *5*	Kaikki tilaan johtavat ovet on lukittava avaimeen perustuvalla mekaanisella tai sähkömekaanisella lukolla. Kaappi tai kotelo, jota asiaankuulumattomat pääsevät esteettä käsittelemään, on lukittava avaimeen perustuvalla mekaanisella tai sähkömekaanisella lukolla.

Laitetilojen rakenteiden vaatimuksissa on jo hiukan enemmän luokka kohtaisia eroja. Ensimmäisen luokan laitetilan on sijaittava maan alla tai sen ympärysrakenteen on oltava vähintään S1-luokan teräsbetonisuojan tasoinen. Maanalaisen laitetilan katon ja seinien tulee olla teräsbetonia tai vastaavaa materiaalia, ja niiden on kestettävä päällä olevan rakennuksen

sortuminen. Lisäksi kaikkien tilan rakennemateriaalien on oltava pääasiassa palamattomia. Laitetilassa ei saa olla ulkoikkunoita ja tilaan johtavien ovien on oltava rakenteeltaan, asennukseltaan ja lukitukseltaan järeiden murtotyökalujen kestäviä. (Traficom 2021a.) Järeillä työkaluilla tapahtuva murto tarkoittaa esimerkiksi murtoa, jossa laitetilaan murtaudutaan käyttäen moottorisahaa, kirvestä, sähkötyökaluja (kulmahiomakonetta, puukkosahaa, poraa jne.) (Traficom 2021b). Mikäli maan alla oleva laitetila on pohjaveden alapuolella tai vesivahinkojen mahdollisuus on todennäköinen, tulee tila varustaa ulkopuolisesta sähkönsaannista riippumattomalla vuotovedenpoistojärjestelmällä. Alemman tärkeysluokan kohteiden suunnittelussa ja rakentamisvaiheessa on myös otettava huomioon vesivahinkojen ehkäisy. (Traficom 2021a.)

2-tason laitetila ei tarvitse olla maanalla, mutta tilojen lattian, katon ja ympärysseinien on oltava kiviaineksesta tai teräksestä. Niiden on myös oltava rakenteeltaan sellaisia, ettei seinäelementtejä voida irrottaa kokonaisina tilan ulkopuolelta. Tilan lattian, katon ja seinien on kestettävä tavanomaisilla käsityökaluilla tehtävää murtoa. (Traficom 2021a.) Tavanomaisilla työkaluilla tapahtuva murto tarkoittaa tilannetta, jossa laitetilaan murtaudutaan käyttäen työkaluina esimerkiksi sorkkarautaa, ruuvitalttaa tai vasaraa (Traficom 2021b). Kaikkien rakennusmateriaalien on oltava pääosin palamattomia. Mikäli tilassa on ulkoikkunoita, niistä ei saa nähdä sisälle. Ikkuna- ja muiden aukkojen on oltava fyysisesti suojattuja. Taajama-alueiden ulkopuolella sijaitsevissa rakennuksissa, joissa ei vakituisesti työskennellä, ei saa olla laitetiloihin johtavia ulkoikkunoita. (Traficom 2021a.)

3-tason tilan lattian, katon ja seinien tulee olla betonista, tiilestä, vahvasta puumateriaalista tai muusta vastaavasta aineesta. Tila on rakennettava siten, ettei seinäelementtejä voi irrottaa kokonaisina tilan ulkopuolelta. Ikkunat, jotka sijaitsevat alle 4 metrin korkeudella maanpinnasta, on suojattava fyysisesti, jos ne kuuluvat laitetiloihin tai tiloihin, joista on pääsy laitetiloihin. Rakennuksissa, jotka sijaitsevat taajama-alueiden ulkopuolella ja joissa ei työskennellä vakituisesti, ei saa olla ulkoikkunoita, jotka johtavat laitetiloihin. 3-tason tilaan johtavien ovien tulee olla käsityökaluilla tehtävän murron kestäviä rakenteen, asennuksen ja lukituksen osalta. (Traficom 2021a.) Ilman erityisiä työkaluja tapahtuva murto tarkoittaa tilannetta, jossa laitetilaan murtaudutaan esimerkiksi ovea nostamalla, potkimalla, repimällä tai olkapäällä työntämällä (Traficom 2021b). Taulukosta 9 voi vielä nähdä, että tason- 4 tai 5 kohteissa riittää, että tilaan johtavien ovien rakenteen, asennuksen, lukituksen ovat ilman erityisiä työkaluja tapahtuvan murron kestäviä. Kaapin tai kotelon, johon asiaankuulumattomat voivat päästä käsiksi tulee olla samalla tavalla murronkestäviä. (Traficom 2021a.)

Taulukko 9: Laitetilojen rakenteelliset vaatimukset (Traficom 2021a)

Laitetilan tärkeysluokka	**Vaatimukset**
1	Laitetilan on oltava maanalainen tai ympärysrakenteeltaan vähintään S1-luokan teräsbetonisuojan mukainen. Maanalaisen laitetilan katon ja ympärysseinien tulee olla teräsbetonista tai vastaavasta materiaalista ja päällä olevan rakennuksen sortuman kestäviä. Kaikkien tilan rakennemateriaalien on oltava pääosin palamattomasta materiaalista. Tilaan johtavien ovien rakenteen, asennuksen ja lukituksen on oltava järeillä työkaluilla tapahtuvan murron kestäviä. Laitetilassa ei saa olla ulkoikkunoita. Tilojen suunnittelussa ja rakentamisessa on otettava huomioon vesivahinkojen ehkäisy. Jos tilan lattia on pohjaveden alapuolella tai vesivahinkojen mahdollisuus on muuten olemassa, tila tulee varustaa ulkopuolisesta sähkönsaannista riippumattomalla vuotovedenpoistojärjestelmällä.
2	Laitetilan katon, lattian ja ympärysseinien on oltava kiviaineesta tai teräksestä ja siten rakennettu, ettei seinäelementtejä voida kokonaisina irrottaa tilan ulkopuolelta. Tilan katon, lattian ja seinien on oltava tavanomaisilla käsityökaluilla tapahtuvan murron kestäviä. Kaikkien tilan rakennemateriaalien on oltava pääosin palamattomasta materiaalista. Tilaan johtavien ovien rakenteen, asennuksen ja lukituksen on oltava tavanomaisilla käsityökaluilla tapahtuvan murron kestäviä. Jos tilassa on ulkoikkunoita, niistä ei saa nähdä sisälle. Ikkuna- ja muiden aukkojen on oltava fyysisesti suojattuja. Taajama-alueiden ulkopuolella sijaitsevissa rakennuksissa, joissa ei vakituisesti työskennellä, ei saa olla laitetiloihin johtavia ulkoikkunoita. Tilojen suunnittelussa ja rakentamisessa on otettava huomioon vesivahinkojen ehkäisy.
3	Tilan katon, lattian ja seinien tulee olla betonista, tiilestä, vahvasta puuaineesta tai muusta vastaavasta aineesta ja siten rakennettu, ettei seinäelementtejä voida kokonaisina irrottaa tilan ulkopuolelta. Tilaan johtavien ovien rakenteen, asennuksen ja lukituksen on oltava tavanomaisilla käsityökaluilla tapahtuvan murron kestäviä. Alle 4 m maanpinnan yläpuolella olevien laitetilojen ikkunat on oltava fyysisesti suojattuja. Lisäksi alle 4 m maanpinnan yläpuolella olevien tilojen, joista on pääsy laitetilaan, ikkunat on oltava fyysisesti suojattuja. Taajama-alueiden ulkopuolella sijaitsevissa rakennuksissa, joissa ei vakituisesti työskennellä, ei saa olla laitetiloihin johtavia ulkoikkunoita. Tilojen suunnittelussa ja rakentamisessa on otettava huomioon vesivahinkojen ehkäisy.
4 tai ***5***	Tilaan johtavien ovien rakenteen, asennuksen ja lukituksen on oltava ilman erityisiä työkaluja tapahtuvan murron kestäviä. Kaappi tai kotelo, jota asiaankuulumattomat pääsevät esteettä käsittelemään, on oltava ilman erityisiä työkaluja tapahtuvan murron kestäviä.

Poikkeuksena edellä mainittuihin vaatimuksiin teleyritys saa kuitenkin sijoittaa tärkeysluokka 1 viestintäverkon tai -palvelun komponenttia varmistavan komponentin laitetilaan, joka täyttää rakenteiltaan luokan 2 vaatimukset.

Olosuhde hälytyksissä **1** & **2** luokan tilat on varustettava automaattisella paloilmoitusjärjestelmällä, jolla saadaan hälytys valvontahenkilöstölle. Tilaan tulee myös asentaa lämpötilojen ylityksistä ja alituksista hälyttävä järjestelmä. Mikäli tilassa on vesivahinkojen mahdollisuus johtuen lattian sijainnista pohjaveden alapuolella tai muista syistä, tulee tila varustaa kosteushälyttimillä, joiden hälytys kulkee valvontahenkilöstölle. 3 ja 4 luokan tiloissa ainoa olosuhdehälytyksiin liittyvä vaatimus on lämpötilojen ylitys ja alitus hälytyksien järjestäminen valvontahenkilöstölle. (Traficom 2021a.)

6 Käsikirjan vaatimukset käytettävyydelle

Parhaat käsikirjat ovat helppokäyttöisiä, informatiivisia oppaita. Ne esittävät käsitteet selkeällä kielellä käyttäen asiaankuuluvia esimerkkejä ja kuvia virheiden vähentämiseksi. Oikein tehtynä hyvästä käsikirjasta tulee luotettava resurssi työntekijöille, esimiehille tai asiakkaille. (Achtelig 2012, 11–13.)

Suunniteltaessa käsikirjaa tulisi kirjoittajan tuntea yleisönsä, ymmärtää käyttäjän tarpeet sekä taso: Kuka käyttää ohjekirjaa? Onko käsikirja tarkoitettu ammattilaisille vai aloittelijoille? Kirjoita ohjekirja heidän lähtötasoaan ja tarpeitaan ajatellen. Aloitat perusasioista ja rakenna looginen eteneminen kohti käsikirjan edistyneempiä osuuksia. (Achtelig 2012, 16–19.) Käytetyn kielen tulisi olla mahdollisimman ymmärrettävää. Käytä yksinkertaisia ja selkeitä lauseita. Vältä ammattislangia ja lyhenteitä, jos kohdeyleisö ei ole alalle suuntautunut. (Weiss 2005, 55–57.) Ohjeet kannattaa kirjoittaa imperatiivia ja aktiivilauseita käyttäen samalla puhutellen lukijaa (Achtelig 2012, 21,38–39).

Yksinkertaisuus on keskiössä käsikirjaa suunniteltaessa ja kirjoittaessa. Dokumentaation täyttäminen monimutkaisilla kuvilla ja tiheillä tekstilohkoilla antaa tunteen, että käsikirja on liian monimutkainen ja saavuttamaton. Tämän tyyppisellä käsikirjalla on suuri todennäköisyys säikäyttää käyttäjäsi ja saada heidät soittamaan tukilinjalle sen sijaan, että yrittäisivät ratkaista ongelman itsenäisesti. (Weiss 2005, 85–89.)

Navigoinnin helpottamiseksi teokseen lisätään sisällysluettelo ja käytetään selkeää otsikoiden ja alaotsikoiden hierarkkista rakennetta. Tämä auttaa lukijaa ymmärtämään, mitä kukin käsikirjan osa käsittelee. Käyttämäsi hierarkian tulisi noudattaa loogista kulkua, jotta lukijat voivat helposti käydä läpi sen, mitä heidän on tiedettävä. Helppokäyttöisyyden lisäämiseksi kirjoita luvut siten että ne on mahdollista lukea vapaassa järjestyksessä. (Achtelig 2012, 32,54.)

Mikäli prosessissa, jota varten käsikirja on luotu, on poikkeuksia tai kohtia missä voi tapahtua virheitä, niin lisää niihin liittyvä tieto mahdollisimman lähelle kuvausta toiminnosta, jossa väärinkäsitys voi tapahtua. Korosta virheet ja poikkeukset esimerkiksi huomiovärillä ja kerro lukijalle virheistä hiukan enemmän kuten miksi virhe tapahtui tai miten sen voi korjata. (Achtelig 2012, 56–57,72–73.)

Käsikirjan visuaalisuuden ohjeena voidaan käyttää ”näytä, älä kerro” periaatetta. Kuvien, kaavioiden ja kuvakaappauksien avulla pystyy havainnollistamaan paremmin monimutkaisia prosesseja tai toimintoja. Mikäli käytät symboleja, kuvakkeita tai koodeja ohjeiden lomassa, niin näiden merkitykset tulisi määritellä mahdollisimman aikaisin. Tällä pystytään välttämään mahdolliset sekaannukset tai lukijan turhautuminen. Visuaalisuus ei ainoastaan riko pitkiä tekstilohkoja, vaan poistaa myös osan tekstistä, jolloin käsikirja ei ole yhtä puuduttava. (Weiss 2005, 85–89.)

Viimeinen vaihe käsikirjan luomisessa on testaaminen. Pyydä joku kohdeyleisöön kuuluva henkilö lukemaan ohjekirja ja kokeilemaan annettuja ohjeita. Tämä auttaa tunnistamaan mahdolliset epäselvyydet tai virheet. Julkaisun jälkeen seuraa paranevatko prosessit ja tulokset? Kerää palautetta käyttäjiltä ja päivitä käsikirjaa säännöllisesti tämän saadun palautteen perusteella tai kun prosessin vaatimukset muuttuvat. (Työterveyslaitos 2021.)

7 Opinnäytetyössä käytetyt menetelmät

Tässä luvussa käydään läpi opinnäytetyössä käytetyt menetelmät. Luvussa kerrotaan miksi jokin menetelmä valittiin. Lisäksi luvussa kerrotaan mitä on tutkimuksellinen kehittämistyö ja kuinka se toteutetaan. Opinnäytetyön tyyppi on kehittämistyö.

7.1 Kehittämistyö

Tutkimuksellinen kehittämistyö yhdistää tutkimuksen ja käytännön kehittämistyön. Tällä pyritään tuottamaan uutta tietoa ja samalla parantamaan konkreettisia käytäntöjä tai ratkaisemaan ongelmia. Tutkijat ja käytännön toimijat voivat työskennellä yhdessä tässä lähestymistavassa, mikä luo siltoja akateemisen tutkimuksen ja käytännön kehittämistyön välille. (Ojasalo, Moilanen& Ritalahti 2015,18–20.)

Tutkimuksellisuus ilmenee usealla eri tavalla kehittämistyössä. Järjestelmällisyydellä varmistetaan, että kehittäminen ei ole vain sarja satunnaisia toimenpiteitä vaan, valinnat dokumentoidaan ja perustellaan. Tiedoksi hankitaan sekä tutkittua että käytännön tietoa. Analyyttisiä menetelmiä käyttäen tunnistetaan, luodaan ja eritellään erilaisia tarkastelutapoja. Tutkimuksellisessa kehittämistyössä arvioidaan kriittisesti hankittua tietoa, omia valintoja, erilaisia

näkemyksiä, prosessia ja tuloksia. Tutkimuksellisuus ilmenee myös uuden tiedon luomisena ja tiedon jakamisena. (Ojasalo ym. 2015,22.)

Tutkimuksellisuus on tärkeässä asemassa kehittämistyössä siksi, että sen avulla kehittämistyöhön vaikuttavat muuttujat otetaan normaalia kattavammin ja suunnitelmallisemmin huomioon. Näin ollen kehittämistyön lopputulokset ovat vakuuttavammin argumentoitavissa. Tutkimuksellisessa kehittämistyössä keskeistä on usein syklisyys, jossa tutkitaan ensin nykytilannetta, suunnitellaan ja toteutetaan muutoksia tai kehitystoimia, arvioidaan niiden vaikutuksia ja sitten tarvittaessa tehdään lisää muutoksia. Tämä prosessi voi toistua useita kertoja, mikä mahdollistaa jatkuvan parantamisen ja oppimisen. (Ojasalo ym. 2015,21–24.)

7.2 Puolistrukturoitu ryhmähaastattelu ja teemoittelu

Tässä työssä on käytetty laadullista tiedonkeruumenetelmää, ryhmähaastattelua sekä laadullista tiedonanalysointimenetelmää, teemoittelua. Tieteellinen haastattelu on menetelmä, jota käytetään tutkimuksessa tietyn ilmiön, ilmiöiden tai aiheen syvälliseen tutkimiseen ja ymmärtämiseen. Se perustuu järjestelmälliseen ja rakenteelliseen lähestymistapaan, jossa tutkija kysyy tarkkaan harkittuja kysymyksiä haastateltavalle. Tieteellisen haastattelun tavoitteena on kerätä tarkkoja, luotettavia ja relevantteja tietoja tutkimuksen kohteena olevasta ilmiöstä. Haastattelijan tehtävänä on myös varmistaa, että haastateltavat ymmärtävät kysymykset samalla tavoin ja että vastaukset voidaan vertailla ja analysoida systemaattisesti. Tieteellinen haastattelu eroaa arkisista keskusteluista siinä, että se on suunniteltu etukäteen, usein perustuen tutkimuskysymyksiin tai -hypoteeseihin. Haastatteluprotokolla voi olla laadittu, ja se ohjaa haastattelijaa käsittelemään tiettyjä teemoja tai aihealueita. (Tietoarkisto 2024b.)

Haastattelu voi kestää muutamasta kymmenestä minuutista useampaan tuntiin. On suositeltavaa nauhoittaa haastattelu, jos haastateltava siihen suostuu. Äänittäminen mahdollistaa haastateltavan paremman tarkkailun, jolloin tietyt kontekstia antavat ilmeet ja eleet eivät todennäköisemmin jää haastattelijalta huomaamatta. Äänittäminen toimii myös jälkeenpäin muistina, jota voi käyttää apuna eri vastausten tulkinnassa. Haastatteluissa ei aina syystä tai toisesta ilmaista asioita suoraan vaan asioiden totuus voi paljastua ”rivien välistä”. (Tietoarkisto 2024b.)

Haastattelut voivat olla strukturoituja, puolistrukturoituja tai avoimia, riippuen tutkimuksen tarpeista. Strukturoidussa haastattelussa kysymykset ja niiden järjestys ovat etukäteen määriteltyjä, kun taas puolistrukturoidussa haastattelussa on tietyt kysymykset, mutta haastattelija voi myös käyttää joustavuutta lisäkysymyksillä. Puolistrukturoituja haastatteluja on hyvä käyttää esimerkiksi silloin, kun tutkittavaa kohdetta ei vielä täysin tunneta ja halutaan välttyä liialliselta vastaajan ohjaamiselta. Avoimissa haastatteluissa haastateltavalle annetaan enemmän tilaa ilmaista itseään ja vastata omalla tavallaan, jolloin on mahdollista saada

selville, miksi haastateltava toimii niin kuin toimii. Avoimiin haastatteluihin tulisi varata paljon aikaa sekä haastattelijan tulisi osata kuunnella, tulkita ja viedä keskustelua eteenpäin. (Ojasalo ym. 2015,41–42.)

Ryhmähaastattelussa käydään läpi tutkimuksen kohteena olevia asioita yhdessä siten, että haastattelija keskustelee samanaikaisesti useammalle haastateltavalle. Ryhmähaastatteluissa on myös mahdollista kysyä yksittäiseltä ryhmänjäseneltä kysymyksiä. Ryhmähaastattelulla voidaan tutkia, esimerkiksi miten henkilöt rakentavat yhteisen näkemyksen jostakin asiasta, tässä tapauksessa fyysisestä turvallisuudesta. Näkemys muodostuu puheenvuoroista ja perusteluista. Ryhmäkeskusteluissa puheteot ja vuorovaikutuksellisuus korostuvat. Puheen lisäksi on mahdollista analysoida nonverbaalista viestintää kuten eleet, ilmeet ja äänenpainot. (KvaliMOTV 2024.)

Tässä opinnäytetyössä käytin puolistrukturoitua ryhmähaastattelua ja haastateltavana oli Henkilöt A ja B. Valitsin tämän haastattelumuodon koska sen avulla sain ohjattua keskustelua haluamiini suuntiin, mutta vastaajilla oli silti mahdollisuus vastata monipuolisesti. Haastateltavien tiukan aikataulun takia päädyimme tekemään ryhmähaastattelun, sillä ryhmähaastattelun yhtenä etuna on nopea tiedonkeruu monelta ihmiseltä samanaikaisesti. Etuna on myös se, että muut haastateltavat voivat auttaa muita muistamaan jotain, mitä ei olisi välttämättä itse muistanut sanoa. (Ojasalo ym. 2015,41.)

Ryhmähaastattelussa on myös tiettyjä haasteita. Ryhmän ilmapiiri vaikuttaa siihen, mitä puhutaan, ketä puhuvat ja milloin puheenvuoroja otetaan. Ryhmässä ei myöskään välttämättä uskalleta kertoa kaikkea mitä vaikkapa kahdenkeskisessä haastattelussa kerrottaisi. Haastattelijalla pitää myös olla taitoa huomata, jos joku haastatteluun osallistuva henkilö uhkaa jäädä syrjään keskustelusta. Ryhmähaastattelun nauhoittaminen voi myös olla ongelma, sillä ryhmähaastatteluissa tapahtuu paljon päälle puhumista. (KvaliMOTV 2024.)

Teemoittelussa aineistosta nostetaan esille tutkimuksen kannalta keskeisiä asiakokonaisuuksia ja piirteitä. Teemoittelu on erinomainen analysointimenetelmä, kun kerätystä aineistosta pyritään jäsentelemään työlle keskeisiä tuloksia ja kehitysehdotuksia. Tyypittelyssä taas pyritään kiteyttämään tutkimusaineistossa useasti ilmeneviä ja tyypillisiä ominaisuuksia, merkitystä ja tapahtumakulkua. (Koppa. 2016.)

8 Opinnäytetyön prosessi

Sain idean tehdä opinnäytetyön silloiselle työnantajalle. Lähestyin esihenkilöäni vuoden 2023 joulukuussa ja sovimme, että hän keksisi minulle opinnäytetyö aiheen joululoman aikana. Vuoden 2024 tammikuun alussa pidimme ensimmäisen kokouksen, jossa keskustelimme opinnäytetyön aiheesta ja rajauksesta. Jo ensimmäisessä kokouksessa alue rajautui fyysisen

turvallisuuteen. Lisäksi ensimmäisessä kokouksessa keskustelimme mitä lähteitä voisin käyttää ja mitä aineistoa tilaajayritys voisi tarjota minulle luettavaksi. Opinnäytetyö sopimus solmittiin 11.1.2024. Opinnäytteen koko prosessi on kuvattuna taulukossa 10.

Taulukko 10: Opinnäytetyön prosessin aikataulu

Kuukausi & vuosi	Mitä on tehty tai mitä on tapahtunut
Joulukuu 2023	• Otin yhteyttä työpaikkani esihenkilöön ja kyselin, voisinko tehdä heille opinnäytetyön • Esihenkilö lupasi keksiä opinnäytetyölle aiheen joululoman aikana
Tammikuu 2024	• Tammikuun alussa pidimme tilaajayrityksen kanssa ensimmäisen kokouksen, jossa keskustelimme opinnäytetyön aiheesta ja rajauksesta • Kokouksessa alue rajautui fyysisen turvallisuuteen • Kokouksessa keskustelimme mitä lähteitä voisin käyttää ja mitä aineistoa tilaajayritys voisi tarjota minulle luettavaksi • Opinnäytetyö sopimus solmittiin 11.1.2024 • Tammikuussa suurin osa ajasta kului tiedon etsimiseen, lukemiseen ja muistiinpanojen tekemiseen • Kirjoitin opinnäytetyössä käytettävistä termeistä ja niiden määritelmistä • Kirjoitin valmiiksi yrityksen esittelyä koskevan osion
Helmikuu 2024	• Aloitin opinnäytetyön alustavansuunnitelman kirjoittamisen ja se valmistui helmikuun puolessa välissä
Maaliskuu 2024	• Maaliskuun loppuun mennessä olin saanut luettua Traficomin M54045:n, Katakrin, valtioneuvoston suosituksen turvallisuusluokiteltavien asiakirjojen käsittelystä sekä EN 50600 standardin • Maaliskuun aikana luin ja kirjoitin myös fyysisen turvallisuuden sekä fyysisen tietoturvallisuuden teoriasta
Huhtikuu 2024	
Toukokuu 2024	• Ensimmäisen puolen vuoden aikana pidimme kokouksia tilaaja yrityksen kanssa kolme kertaa

	• Alkuperäisen suunnitelman mukaan opinnäytetyön olisi pitänyt valmistua toukokuun ja kesäkuun vaihteessa, mutta toukokuun aikana tapahtunut muutto häiritsi sen verran pahasti, että työn valmistuminen venyi syksylle
Kesäkuu 2024	• Alkukesästä kirjoitin valtioneuvoston suosituksen turvallisuusluokiteltavien asiakirjojen käsittelystä ja Finanssialan murtosuoja ohjeen vaatimuksista • Kesän aikana ehdin myös etsiä ja muokata kuvia sekä taulukoita
Heinäkuu 2024	• Loppukesästä pääsin aloittamaan itse työkaluksi tulevan käsikirjan hahmottelua
Elokuu 2024	• Elokuuhun mennessä olin saanut kirjoitettua työtä ja itse käsikirjaa sen verran pitkälle, että pystyin jälleen esitellä työtä tilaajayritykselle • Valitettavasti esittely siirtyi elokuun lopulle • Kirjoitin Traficomin määräyksiä koskevan osion sekä käsikirjan käytettävyyttä koskevan teoria osion valmiiksi • Elokuun viimeisellä viikolla tarkensin vielä työn pienempiä teemoja.
Syyskuu 2024	• Syyskuun alussa tein kysymykset tilaajayrityksen haastattelua varten. • Haastattelu suoritettiin 13.9 ja haastattelu liittyi tilaajayrityksen fyysiseen turvallisuuteen ja turvallisuuskulttuuriin • Haastateltavina olivat tilaajayrityksen turvallisuuspäällikkö A ja tilaajayrityksen tuotannon puolen turvallisuuspäällikkö B • Haastattelun tavoitteena oli selvittää yrityksen sen hetkistä turvallisuuskulttuurin kypsyyttä, kuinka fyysinen turvallisuus otetaan yrityksessä huomioon ja miten yritys voisi kehittää toimintaansa • Syyskuun lopulla kirjoitin kaikki opinnäytetyön ja käsikirjan osiot loppuun asti
Lokakuu 2024	• Opinnäytetyö esiteltiin 1.10

Tammikuussa suurin osa ajasta kului tiedon etsimiseen, lukemiseen ja muistiinpanojen tekemiseen. Etsin tietoa tieteellisestä kirjoittamisesta, kehittämistyön tekemisestä ja fyysisestä turvallisuudesta. Ensimmäisiä asioita, joita kirjoitin opinnäytetyöhön oli siinä käytettävät termit ja niiden määritelmät. Tammikuun aikana kirjoitin myös yrityksen esittelyä koskevan osion.

2024 helmikuun alussa aloitin opinnäytetyön alustavansuunnitelman kirjoittamisen ja se valmistui helmikuun puolessa välissä. Tärkeimpiä palautteita, joita sain, oli aihealueen tarkempi rajaus.

2024 maaliskuun loppuun mennessä olin saanut luettua Traficomin M54045:n, Katakrin, valtioneuvoston suosituksen turvallisuusluokiteltavien asiakirjojen käsittelystä sekä EN 50600 standardin. EN 50600 aiheutti hiukan ongelmia, sillä en voinut käyttää kaikkea siinä mainittuja asioita tilaajayrityksen asettaman käyttörajoituksen vuoksi. Maaliskuun aikana luin ja kirjoitin myös fyysisen turvallisuuden ja fyysisen tietoturvallisuuden teoriasta.

2024 kevään aikana opinnäytetyö eteni työn ohessa, vaikka välillä tuli taukoja kirjoittamiseen. Minulla oli loistava mahdollisuus kirjoittaa ja lukea opinnäytetyöhön liittyvää tekstiä yövuoroissa. Ensimmäisen puolen vuoden aikana pidimme kokouksia tilaaja yrityksen kanssa kolme kertaa. Alkuperäisen suunnitelman mukaan tämän opinnäytetyön olisi pitänyt valmistua toukokuun ja kesäkuun vaihteessa, mutta toukokuun aikana tapahtunut muutto häiritsi sen verran pahasti, että työn valmistuminen venyi syksylle.

2024 alkukesästä kirjoitin valtioneuvoston suosituksen turvallisuusluokiteltavien asiakirjojen käsittelystä ja Finanssialan murtosuoja ohjeen vaatimuksista. Kesän aikana ehdin myös etsiä ja muokata kuvia sekä taulukoita. Loppukesästä pääsin aloittamaan itse työkaluksi tulevan käsikirjan hahmottelua.

2024 elokuuhun mennessä olin saanut kirjoitettua työtä ja itse käsikirjaa sen verran pitkälle, että pystyin jälleen esitellä työtä tilaajayritykselle. Valitettavasti esittely siirtyi elokuun lopulle. Odotellessani kuun loppua kirjoitin Traficomin määräyksiä koskevan osion sekä käsikirjan käytettävyyttä koskevan teoria osion valmiiksi. Elokuun viimeisellä viikolla palasin vielä tarkentamaan työn pienempiä teemoja. Fyysiseen turvallisuuden ja fyysinen tietoturvan alla havaitsin kolme pienempää teemaa, jotka olivat rakenteisiin liittyvät vaatimukset, turvalaitteisiin liittyvät vaatimukset, sekä turvallisuuskulttuuriin liittyvät vaatimukset.

2024 syyskuun alussa tein kysymykset tilaajayrityksen haastattelua varten. Haastattelu suoritettiin syyskuun 13 päivä. Haastattelu liittyi tilaajayrityksen fyysiseen turvallisuuteen ja turvallisuuskulttuuriin. Haastateltaessa tilaajayrityksen kahta edustajaa yhdeksi teemaksi nousi

vielä turvallisuusalan jatkuva nopeatempoinen muuttuminen. Haastateltavina olivat tilaajayrityksen turvallisuuspäällikkö A ja tilaajayrityksen tuotannon puolen turvallisuuspäällikkö B. Haastattelun tavoitteena oli selvittää yrityksen sen hetkistä turvallisuuskulttuurin kypsyyttä, kuinka fyysinen turvallisuus otetaan yrityksessä huomioon ja miten yritys voisi kehittää toimintaansa.

Valitsin puolistrukturoidun ryhmähaastattelumuodon, koska sen avulla sain ohjattua keskusteluaiheita haluamiini suuntiin, mutta vastaajille jäi silti mahdollisuus vastata monipuolisesti. Haastateltavien tiukka aikataulu vaikutti myös ryhmähaastattelun valitsemiseen, sillä ryhmähaastattelun yhtenä etuna on nopea tiedonkeruu monelta ihmiseltä samanaikaisesti. Ryhmähaastattelun etuna on myös se, että muut haastateltavat voivat auttaa muita muistamaan jotain, mitä ei olisi välttämättä itse muistanut sanoa.

Syyskuun lopulla kirjoitin kaikki opinnäytetyön ja käsikirjan osiot loppuun asti ja työ esiteltiin 1.10.2024. Opinnäytteen koko prosessi on vielä kuvattuna taulukossa 10.

9 Tulokset

Opinnäytetyötä varten tehdyssä haastattelussa selvitettiin tilaajayrityksen tämänhetkistä fyysisen turvallisuuden hallintaa ja minkälaiseksi haastateltavat kokivat tilaajayrityksen turvallisuuskulttuurin. Haastateltavina olivat tilaajayrityksen turvallisuuspäällikkö A ja tilaajayrityksen tuotannon puolen turvallisuuspäällikkö B. Kaikkia haastattelun tuloksia ei voida julkaista liikesalaisuuden vuoksi.

Kysyttäessä millaiseksi haastateltavat kokivat tilaajayrityksen turvallisuuden hallinnan, haastateltavat mainitsivat, että heidän fyysisen turvallisuuden hallintamalli vastaa pääpiirteittäin useiden kansallisten ja kansainvälisten turvallisuuskriteeristöjen vaatimuksia. Toinen haastateltavista mainitsi vielä, että yrityksessä näiden kriteeristöjen valuttaminen läpi organisaation on heillä jatkuva prosessi. Vaikka parannettavaa aina löytyy, ovat he kuitenkin siinä hyvällä mallilla. Molemmat heistä kuvailivat yrityksen turvallisuuden hallintaa kypsäksi.

Useassa kysymyksessä kysyttiin asioita, jotka liittyivät jokapäiväiseen fyysisen turvallisuuden hallitsemiseen ja sen haasteisiin. Kysyttäessä kohteen tärkeyden vaikutuksesta arjen työhön Haastateltavat mainitsivat että, kohteiden tärkeysluokitus vaikuttaa heillä kohteeseen rakennettaviin turvallisuuskontrolleihin ja niiden hallintaan. Tärkeysluokitus vaikuttaa myös kohteella käymiseen, turvallisuustarkastusten määrään, turvallisuuspoikkeamien reagointiin ja esimerkiksi vartioinnin määrään kohteella. Haastateltava korosti vielä että, kohteen tärkeysluokitus vaikuttaa suoraan siihen, minkälaisilla resursseilla turvallisuuspoikkeamaa lähdetään tutkimaan ja minkälaisella ilmoituskynnyksellä viranomaisiin ollaan yhteydessä.

Turvalaitteiden teemaan liittyen haastattelussa mainittiin, että erityyppiset luokittelut kohteelle vaikuttavat teknisissä järjestelyissä ja valvontaratkaisuissa. Mitä tärkeämpi kohde, sitä tiukemmat tekniset valvontaratkaisut kohteeseen tulee järjestää.

Turvallisuuskulttuuriin teemaan liittyen keskusteltaessa tilaajayrityksen suuren toimialueen tuomista haasteista haastateltavat myönsivät sen olevan selkeä haaste heidän työssään. Turvallisuushavainnot, jotka tulevat kentältä, ovat ne sitten vartioinnista tai muilta kohteella työskenteleviltä henkilöiltä ovat erittäin tärkeitä. Molemmat haastateltavat kokivat myös johdon tuen olevan vahva mikä mahdollistaa turvallisuuskulttuurin vaatimusten täyttämisen sekä kyvyn ylläpitää korkeaa turvallisuustasoa.

Kysyttäessä fyysisen turvallisuuden jalkauttamisesta, haastateltavat osasivat kertoa, että siinä heillä voisi vielä mahdollisesti olla kehitettävää. Haastateltavat kertoivat, että yrityksessä on jaettu selkeät roolit fyysisen turvallisuuden osalta. Yrityksessä on pakollinen turvallisuuskoulutus, jonka jokainen työntekijä ja alihankkijan työntekijä käy läpi. Yrityksessä käytetään myös paljon turvallisuussopimuksia alihankkijoiden ja yhteistyökumppaneiden kanssa. He lisäsivät vielä, että yrityksessä ei luoteta pelkän sopimuksen olemassaoloon, vaan he jatkuvasti keskustelevat ja muistuttavat turvallisuusasioita kokouksissa, jotta ne pysyisivät mielessä ja jalkautuisivat kentälle asti.

Haastateltavat antoivat kaksi erilaista vastausta, jotka kuitenkin liittyivät toisiinsa kysyttäessä, mikä on heidän mielestä suurin haaste fyysistä turvallisuutta koskien. Ensimmäiseksi vastannut kertoi, että, tämän opinnäytetyön kontekstissa, se olisi se alihankintaketjun viimeisen urakoitsijan kesätyöntekijän turvallisuusymmärryksen ylläpitäminen. Toinen haastateltava taas vastasi, että osaavampien työntekijöiden turvallisuusymmärryksen ylläpitäminen on suurin haaste. Haastateltava vielä lisäsi, ettei hänen mielestä riitä, että asioista ja sopimuksista muistutetaan kerran, vaan se vaatii jatkuvaa muistuttamista. Hänen mielestä turvallisuuskoulutuksia pitää käydä säännöllisin väliajoin uudestaan läpi, koska niiden opit voivat nopeasti unohtua muiden töiden jaloissa.

Kysyttäessä ajankäytöstä molemmat haastateltavat olivat sitä mieltä, että työtä on paljon ja sen jatkuva nopeatempoisuus on merkittävä haaste. Toinen haastateltavista kertoi, jatkuva muutos haastaa turvallisuusalaa ja kenttä työskentelyä. Se luo riskejä, joihin täytyy pystyä reagoimaan. Henkilö B lisäsi vielä omaa pohdintaa, joka avasi hyvin turvallisuusalan nykytilannetta. Hänen mielestä nopeatempoisuus on isossa osassa nykymaailmaa ja turvallisuusalan haasteita. Miten yritykset pystyisivät parhaiten pysymään siinä perässä? Ei pelkästään regulaation osalta, vaan ylipäätänsä. Liiketoiminta ympäristö elää ja siihen liittyvät tarpeet elää jatkuvasti. Se luo haasteita myös ajankäytöllisesti. Miten olisi mahdollista päästä sieltä reaktiivisesta toiminnasta ennakoivaan, proaktiiviseen ja suunnitelmalliseen toimintaan?

Haastattelun lopuksi haastateltaville annettiin mahdollisuus vapaaseen sanaan, jolloin molemmilta tuli erittäin mielenkiintoista pohdintaa fyysisestä turvallisuudesta ja turvallisuuskulttuurista suomessa. Henkilö B kertoi, että hänen mielestään yleisellä tasolla fyysisen turvallisuuden merkitystä ei ymmärretä monessa organisaatiossa. Se nähdään mahdollisesti hiukan vanhakantaisena toimintamallina, jota se varmaan osittain onkin. Vaikka teknologiassa onkin tapahtunut muutoksia niin toimintamallit ovat edelleen osittain sellaisia, että ne elävät sitä vanhaa maailmaa. Tämä johtuu henkilö B:n mielestään siitä, että parempia keinoja, joilla pystyttäisiin varmistamaan esimerkiksi tietty fyysisen turvallisuudentaso ei ole vielä kehitetty.

Henkilö B lisäsi vielä, että fyysiseen turvallisuuteen kytkeytyy ilmeinen haaste. Miten kehittää toimintaa modernimpaan suuntaan ilman, että turvallisuustaso huonontuu? Turvallisuusala on sellainen ala missä on erittäin hankala kokeilla uusia ideoita. Ideoihin ja uudistuksiin liittyy paljon jo olemassa olevia toimintamalleja, jotka asettavat paljon rajoitteita siihen mitä ja miten asioita voidaan uudistaa tai kehittää.

Henkilö B pohti myös fyysisen turvallisuuden ja uudemman kyberturvallisuuden kilpailun vaikutuksia. ” Kun puhutaan kyber- tai tietoturvasta, niin siellähän mennään eteenpäin. Se on paljon seksikkäämpi puheenaihe ja on koko ajan tapetilla, mutta sitten kun fyysisestä turvallisuudesta puhuu, niin sitten joutuukin paljon enemmän perustelemaan miksi tämä on tärkeä asia.”

Henkilö A lisäsi vielä B:n pohdinnan jälkeen, että pilvi on vain jonkun toisen tietokone. Jossain sen tietokoneen on edelleen fyysisesti oltava ja se on paljon tylsempää. Siinä täytyy miettiä minkälaisia ovia ja seinärakenteita tietokoneen säilytyspaikassa on, kuka sinne tietokoneelle fyysisesti pääsee ja minkälaisia henkilöitä siellä tiloissa kulkee? A:n mielestä on harmi, että fyysisessä turvallisuudessa ei pystytä pääsemään ihan sille tasolle, että heidän ei tarvitsisi perustella sen olemassaoloa.

Käsikirjaa tehtäessä tuli esille monen eri lähteen vaatimusten osittainen päällekkäisyys. Sama vaatimus saattoi olla toisessa lähteessä vain hiukan eri tavalla sanoitettu. Missään lähteessä ei ollut täysin samoja vaatimuksia, mutta samoja teemoja selkeästi oli. Lisäksi työhön käytettävää materiaalia oli valtavasti. Osa aineistosta oli helposti saatavilla ja toiset taas käyttörajoitettuja tai maksumuurin takana. Vaatimuksissa oltiin myös hyvin tarkkoja siitä, että kaikkien kohtien tulee täyttyä, jotta tietyn turvallisuusluokituksen voi saada.

10 Johtopäätökset ja oman työn arviointi

Tässä luvussa käydään läpi tuloksista syntyneitä johtopäätöksiä. Johtopäätöksissä arvioidaan työn tarkoituksen ja tavoitteen toteutumista sekä mahdollisia kehittämiskohteita. Lopuksi luvussa arvioidaan omaa työtä.

Tilaajayritykseltä saadun palautteen perusteella työn tarkoituksessa onnistuttiin. Opinnäytetyön tarkoituksena oli luoda tilaajayritykselle käsikirja, jossa on koottuna kaikki tärkeimmät lait, ohjeet, sopimukset, säädökset ja standardit liittyen fyysiseen turvallisuuteen. Koska tilaajayritys on kooltaan huomattava valtakunnallinen toimija, on sen toiminnan vaatimuksenmukaisuuden hallinta hankalaa ja resursseja vievää. Opinnäytetyön fyysistä turvallisuutta käsittelevä käsikirja helpottaa kohteiden tärkeimpien turvallisuusvaatimusten tunnistamista ja täyttämistä keräämällä ne yhteen teokseen. Täten käsikirjalla pystytään opinnäytetyön tavoitteen mukaisesti helpottamaan kohteiden turvallisuusvaatimusten tunnistamista ja täyttämistä sekä tehostamaan tilaajayrityksen toimintaa. Lisäksi käsikirjan esittämien vaatimusten avulla voidaan arvioida tilaajayrityksen tämänhetkistä vaatimustenmukaisuutta.

10.1 Johtopäätös

Turvallisuuspäällikkö A:lle ja Turvallisuuspäällikkö B:lle tehdyn haastattelun perusteella on mahdollista arvioida, että tilaajayrityksessä ollaan erittäin hyvin perillä fyysisen turvallisuuden ja organisaatiokulttuurin onnistumisista ja kehityskohteista. Kummatkin haastateltavat osasivat myös tarjota henkilökohtaista pohdintaa mahdollisille ratkaisuille ja tulevaisuuden haasteille.

Tässä opinnäytetyössä tilaajayritykselle tehty fyysisen turvallisuuden käsikirja tehtiin siis aitoon tarpeeseen. Käsikirjan rakenne ja siihen lisätyt vaatimukset käytiin läpi useaan kertaan yhdessä tilaajayrityksen yhteyshenkilöiden kanssa. Heiltä saadun palautteen perusteella käsikirja sai lopullisen muotonsa. Palautteen ansiosta myös opinnäytetyöntyön tavoitteena ollut kohteiden turvallisuusvaatimusten tunnistamisen ja täyttämisen helpottaminen saavutettiin.

10.2 Oman työn arviointi

Työssä oleva teksti on luotettavaa, sillä aineistona on käytetty lähtökohtaisesti valtiollisia tai asiantuntija lähteitä. Luotettavuutta lisää myös se, että sen keräämiseen ja valitsemiseen sain paljon ohjausta niin tilaajayrityksen yhteyshenkilöiltä kuin opinnäytetyön ohjaajalta. Tässä opinnäytetyössä tehdystä työstä on mahdollista hyötyä myös muiden kuin tilaajayrityksen. Työssä käytetyt lähteet ovat suurimmilta osin julkisia ja vapaasti saatavilla. Työ on siis mahdollista tehdä uudelleen jollekin toiselle organisaatiolle. Jokin toinen suomessa toimiva valtakunnallinen tietoliikenne yritys voi esimerkiksi hyötyä tästä työstä. Ainoastaan itse

käsikirjasta ei muut organisaatiot pääse hyötymään, sillä tilaajaorganisaation pyynnöstä siitä ei julkaista muuta kuin sisällysluettelo.

Suurin osa opinnäytetyöstä kirjoitettiin yövuorojen aikana. Työn laatu ei kuitenkaan kärsinyt tästä liikaa, sillä sen tekemiseen oli varattu paljon aikaa. Työ saattoi venyä ajallisesti turhankin pitkäksi, jonka takia työssä voi olla mahdollista huomata tyylillisiä muutoksia. Työssä käytetyn aineiston suhteen oli tiettyjä haasteita, sillä osa aineistosta oli käyttörajoitettua tai vaikeasti löydettävissä. Toisena haasteena oli tilaajayrityksen yhteyshenkilöiden erittäin kiireelliset aikataulut. Välillä vastausta sähköpostiin joutui odottamaan pitkään

Haastattelussa onnistuttiin itsearvioni perusteella välttämään kaikki mahdolliset ryhmähaastattelun ongelmat. Haastateltava ryhmä oli hyvin pieni vain kaksi henkilöä, jotka tunsivat toisensa hyvin ja työskentelivät keskenään päivittäin. Ennen haastattelun aloittamista sovittiin keskustelu järjestys ja jos toisella henkilöllä oli jotain lisättävää, niin haastateltavat osasivat olla puhumatta toistensa päälle. Vaikka vastausjärjestys oli etukäteen määrätty, niin se ei haitannut vastausten laatua. Kummatkin haastateltavat toivat omia näkökulmia kysymykseen, vaikka usein olivat asiasta pohjimmillaan samaa mieltä. Haastattelun nauhoittamisessa ei myöskään ollut suuria ongelmia pienen ryhmäkoon ja puheenvuorojen kunnioittamisen vuoksi. Haastattelu litterointi saatiin valmiiksi kaksi päivää haastattelun jälkeen, jolloin siitä ei ollut ehtinyt kulua liian pitkää aikaa.

Tietyissä tilanteissa työtä saattaa olla pitkiä kohtia tekstiä, joissa on kaikissa sama lähde. Syynä tälle oli haaste löytää vastaavaa tekstiä muualta, sillä suurin osa tällaisesta tekstistä oli peräisin velvoittavasta lähteistä kuten Traficomista tai standardeista. Toinen syy tiettyjen lähteiden runsaaseen käyttämiseen oli se, että tilaajayritys vaati käyttämään juuri näitä lähteitä. Tiedostan, että tämä aiheutti sen, että tieto saattoi olla yksipuolista ja joitakin asioita saattoi jäädä mainitsematta.

Opinnäytetyön alussa työn ja käytössä olevan materiaalin määrä aiheutti epäselvyyksiä. Työn mittakaava oli yksinkertaisesti liian suuri, joten sitä oli pakko lähteä rajaamaan. Tiukasta rajauksesta huolimatta opinnäytetyöstä tuli tarpeeksi kattava katsaus fyysiseen turvallisuuteen ja sen tärkeimpiin vaatimuksiin koskien tietoliikenne yrityksiä. Tämä sen takia, koska tilaajayrityksen yhteyshenkilö osasi kertoa niiden tärkeydestä ja suositteli käyttämään juuri tässä työssä käytettyjä lähteitä.

Fyysiseen turvallisuuteen liittyvän vaatimusten ja lähteiden määrä, tuli opinnäytetyötä ja käsikirjaa tehdessä erittäin selväksi. Käsikirja, joka yhdistäisi eri lähteistä löytyvät vaatimukset, on ymmärrettävästi kysynnässä. Vaatimusten samankaltaisuus lisää tätä kysyntää, sillä vaatimusten ollessa samassa teoksessa, pystytään välttymään aikaa vievältä lähteiden selailulta ja vertailulta. Tilaajayrityksen suuren kohdemäärän vuoksi, kaikenlainen toiminnan tehostaminen mahdollistaa suuren potentiaalisen ajan säästämisen. Haastattelussa tuotiin esille haaste,

jossa fyysisen turvallisuuden toimenpiteitä joudutaan välillä perustelemaan eri henkilöille. Tämä käsikirja on yksi mahdollinen ratkaisu tähän ongelmaan. Käsikirjan avulla pystyttäisiin osoittamaan, että tietyille turvallisuuden toimenpiteille on olemassa selkeitä vaatimuksia.

Tilaajayritykselle jätettiin mahdollisuus jatkaa työn kehittämistä sen valmistuttua. Mahdollisia kehitystoimenpiteitä voisivat olla yrityksen sisäisten ohjeiden tai jonkin muun käyttörajatun ohjeistuksen lisääminen käsikirjaan. Käsikirjaan voisi myös mahdollisesti lisätä kohdekortin, joka helpottaisi kohteen tarkistamista. Käsikirjan voisi myös mahdollisesti siirtää jollekin toiselle alustalle kuten Excelille, jolloin suuren tietomäärän käsittely voisi mahdollisesti olla helpompaa.

Lähteet

Achtelig, M. 2012. Technical documentation solution series: Writing plain instructions: how to write user manuals, online help, and other forms of user assistance that every user understands. Germany: Indoition Publishing.

Asiakastieto 2024. Viitattu 23.1.2024. https://www.asiakastieto.fi/yritykset/

Cobb, M. 2021. Physical security. TechTarget. Viitattu 23.9.2024. https://www.techtarget.com/searchsecurity/definition/physical-security.

Elinkeinoelämän keskusliitto 2022. Yritysturvallisuus. Viitattu 12.1.2024. https://ek.fi/hyoty-tietoa-yrityksille/yritysturvallisuus/

Fennelly, L. 2013. Effective physical security. E-kirja. UK: Butterworh-Heinemann.

Finanssiala 2024. Rakenteellinen murtosuojaus 3. Viitattu 13.7.2024 https://www.finanssiala.fi/wp-content/uploads/2024/01/rakenteellinen-murtosuojaus-iii.pdf

Jyväskylän yliopisto 2021. KOPPA. Laadullinen tutkimus. Viitattu 5.2.2024. https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/laadullinen-tutkimus

Katakri 2020. tietoturvallisuuden auditointityökalu viranomaisille. Viitattu 27.2.2024. https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246

Kielitoimiston sanakirja 2022. Käsikirja. Viitattu 21.1.2024. https://www.kielitoimistonsanakirja.fi/#/käsikirja

KvaliMOTV 2024. Yhteiskuntatieteellinen tietoarkisto. Ryhmähaastattelu. Viitattu 16.9.2024. https://www.fsd.tuni.fi/menetelmaopetus/kvali/L6_3_4.html

Laki julkisen hallinnon tiedonhallinnasta 906/2019.

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2015. Kehittämistyön menetelmät: uudenlaista osaamista liiketoimintaan. Helsinki: Sanoma Pro.

Patentti- ja rekisterihallitus Virre 2024. Yrityksen tiedot. Viitattu 7.10.2024. https://virre.prh.fi/novus/home?execution=e1s3.

SFS-EN 356:2001. Rakennuslasit. Suojalasitus. Murtautumisyrityksen kestävyyden testaus ja luokitus. Helsinki: Suomen Standardisoimisliitto SFS.

SFS 7020:2022. Rakennushelat. Kiinteästi asennettavat lukot ja riippulukot. Murronkestävyys. Lukitus. Helsinki: Suomen Standardisoimisliitto SFS.

SFS-EN 50600-1:2019. Information technology. Data center facilities and infrastructures. Part 1: General concepts. Helsinki: Suomen Standardisoimisliitto SFS.

SFS-ISO 31000:2018. Riskienhallinta. Ohjeet. Helsinki: Suomen Standardisoimisliitto SFS.

SFS-ISO 31073:2022. Riskienhallinta. Sanasto. Helsinki: Suomen Standardisoimisliitto SFS.

TEPA-termipankki 2024. Safety. Viitattu 3.3.2024. https://termipankki.fi/tepa/fi/haku/safety.

Tietoarkisto 2024a. Laadullisen tutkimuksen ominaispiirteet. Viitattu 6.2.2024. https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/mita-on-laadullinen-tutkimus/laadullisen-tutkimuksen-ominaispiirteet/.

Tietoarkisto 2024b. Haastattelut. Viitattu 24.9.2024. https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/laadullisen-tutkimuksen-aineistot/haastattelut/.

Traficom 2021a. Määräys viestintäverkkojen ja -palvelujen varmistamisesta sekä viestintäverkkojen synkronoinnista. Viitattu 14.3.2024. https://www.traficom.fi/sites/default/files/media/regulation/Määräys_viestintäverkkojen_ja_-palvelujen_varmistamisesta_sekä_viestintäverkkojen_synkronoinnista.pdf.

Traficom 2021b. Määräys viestintäverkkojen ja -palvelujen varmistamisesta sekä viestintäverkkojen synkronoinnista. Perustelumuistio. Viitattu 14.3.2024. *Määräys_viestintäverkkojen_ja_-palvelujen_varmistamisesta_sekä_viestintäverkkojen_synkronoinnista_Perustelumuistio.pdf (traficom.fi).

Turvallisuuskomitea 2017. Kokonaisturvallisuuden sanasto. Viitattu 3.2.2024. https://turvallisuuskomitea.fi/viestinta/kokonaisturvallisuuden-sanasto/.

Työsuojeluhallinto 2010. Turvallisuusjohtaminen. Viitattu 17.9.2024 Turvallisuusjohtaminen_TSO_35.pdf (tyosuojelu.fi).

Työterveyslaitos 2021. Millainen on hyvä ohje? Kahdeksan vinkkiä ohjeiden tekemiseen työpaikalla. Viitattu 24.9.2024. https://www.ttl.fi/tyopiste/millainen-on-hyva-ohje-kahdeksan-vinkkia-ohjeiden-tekemiseen-tyopaikalla.

Valtionneuvosto 2021. Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä. Viitattu 26.2.2024. https://julkaisut.valtioneuvosto.fi/handle/10024/162649

Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa 1101/2019.

Valtiovarainministeriö 2007. Tietoturvallisuudella tuloksia: yleisohje tietoturvallisuuden johtamiseen ja hallintaan. Viitattu 3.2.2024. https://dvv.fi/documents/2252790/13063677/2007_VAHTI_ohje_tietoturvallisuuden_johtaminen.pdf/f605da38-bb4d-ce7b-e2da-49e9a8ee0879/2007_VAHTI_ohje_tietoturvallisuuden_johtaminen.pdf.

Vesterinen, P. 2011. Turvaa logistiikka: kuljetusten ja toiminnan turvallisuus. Helsinki: Kauppakamari.

Weiss, E. 2005. The Elements of International English Style: A Guide to Writing Correspondence, Reports, Technical Documents, and Internet Pages for a Global Audience. UK: Taylor & Francis Group.

Yhdysvaltain puolustusministeriö 2005. Sotilaallisten ja niihin liittyvien termien sanakirja. S174.Fyysinen turvallisuus. Viitattu 21.1.2024. https://irp.fas.org/doddir/dod/dictionary.pdf

Julkaisemattomat lähteet

Turvallisuuspäällikkö A. Turvallisuuspäällikkö B. Tilaajayritys. Haastattelu 13.9.2024

Kuviot

Kuvio 1: Salassapito ja turvallisuusluokittelun arviointiprosessi 18

Kuvat

Kuva 1: Lasirakenteiden suojaus teräsristikolla, -verkolla tai muototeräksellä 12
Kuva 2: Murtosuoja taso 3 ovien, saranoiden ja karmien vaatimukset..... 13

Taulukot

Taulukko 1: Asiakirjojen jakaminen eri turvallisuusluokkiin 17
Taulukko 2: Hallintoalueen vähittäisvaatimukset osa 1 20
Taulukko 3: Hallintoalueen vähittäisvaatimukset osa 2 22
Taulukko 4: Turva-alueen vähimmäisvaatimukset osa 1 24
Taulukko 5: Turva-alueen vähimmäisvaatimukset osa 2 26
Taulukko 6: Turva-alueen fyysisten vähimmäisvaatimukset osa 3 28
Taulukko 7: viestintäverkon tai -palvelun komponentin tärkeysluokittelu 30
Taulukko 8: Laitetilojen kulunvalvonnan vaatimukset 33
Taulukko 9: Laitetilojen rakenteelliset vaatimukset 35
Taulukko 10: Opinnäytetyön prosessin aikataulu 40

Liitteet

Liite 1: Tilaajayrityksen henkilöiden A ja B haastattelu 52
Liite 2: Käsikirjan sisällysluettelo 53

Liite 1: Tilaajayrityksen henkilöiden A ja B haastattelu

Kuka olet?

Kuinka kauan olet ollut nykyisessä tehtävässä?

Millaiseksi koet organisaation fyysisen turvallisuuden hallinnan

Kuinka useasti käytte organisaation kohteissa tarkistamassa vaatimuksenmukaisuuden silmämääräisesti?

Miten organisaation kohteen tärkeys vaikuttaa tarkastusten tiheyteen?

Miten kohteen tärkeys näkyy arjen työssä?

Miten pysyt perillä organisaation ympäri Suomea sijaitsevien kohteiden tapahtumista?

Miten organisaation ylin johto suhtautuu fyysiseen turvallisuuteen?

Miten fyysinen turvallisuus on onnistuttu jalkauttamaan kaikkien organisaation työntekijöiden keskuuteen?

Miten fyysinen turvallisuus on onnistuttu jalkauttamaan organisaation yhteistyökumppaneiden kanssa?

Mikä on suurin haaste työssäsi fyysisen turvallisuuden kanssa?

Millaiset ajalliset resurssit sinulla on käytettävissä työtehtävän kanssa?

Koetko, että yritysturvallisuuden vastuut on jaettu selkeästi?

Mikä yksi muutos parantaisi organisaation fyysistä turvallisuutta?

Tuliko haastattelun aikana mitään muuta mieleen?

Liite 2: Käsikirjan sisällysluettelo

Sisällys

Tämän asiakirjan tarkoitus 2
Mitä on fyysinen turvallisuus ja fyysinen tietoturvallisuus? 2
Traficom määräys 54045 3
Tärkeysluokka 1 laitetilojen Kulunvalvonnan vaatimukset (s.12) 3
Tärkeysluokka 1 laitetilojen rakenteelliset vaatimukset (s.13) 4
tärkeysluokka 1 & 2 olosuhdehälytykset (s.14) 5
Tärkeysluokka 2–5 Kulunvalvonnan vaatimukset (s.12) 5
Tärkeysluokka 2–5 laitetilojen rakenteelliset vaatimukset (s.13) 6
Tärkeysluokka 3 & 4 olosuhdehälytykset (s.14) 8
Rakenteellinen murtosuojaohje taso 3 9
Rikoksen torjunta ja ympäristö (s.2) 9
Säilytyspaikan seinät, lattia ja katto (s.5) 9
Ikkunat ja aukot (s.6) 10
Ovet saranat ja karmit (s.6) 11
Lukitus (s.7- s.10) 12
Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 13
Turva-alueen raja ja rakenteet (s.43) 13
Kulunvalvonta (s.43) 14
Pääsyoikeuksien myöntäminen (s.44) 14
Vierailijat (s.44) 15
Turvallisuus- ohjeet (s.45) 15
Äänieristys (s.45) 16
Tekniset turvallisuus- järjestelmät (s.45) 16
Tunkeutumisen ilmaisujärjestelmä (s.45) 17
Salaa katselun estäminen (s.45) 17
Tila- ja laitetarkastukset (s.46) 17
Tiedon säilyttäminen (s.46) 18
Katakri 2020 19
Fyysinen turvallisuus (F) (s. 22 – s. 62) 19
Lähteet 23