LAUREA AMMATTIKORKEAKOULU Uuden edellä

Geodeettisen laitoksen turvallisuustoiminnan kehittäminen:

Turvallisuuskäsikirja

Kokkonen, Mika

2013 Leppävaara

Laurea- ammattikorkeakoulu
Leppävaara

Geodeettisen laitoksen turvallisuustoiminnan kehittäminen: Turvallisuuskäsikirja

Mika Kokkonen
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Huhtikuu, 2013

Sisällys

1 Johdanto 7
1.1 Tausta ja rajaus 8
1.2 Tarkoitus ja tavoitteet 8
1.3 Kohdeorganisaatio 9
1.4 Keskeiset käsitteet 9
2 Toteutus 10
2.1 Lähestymistapa 11
2.2 Menetelmät 11
2.3 Tietoperustan rakentaminen 12
3 Organisaatioturvallisuus 13
3.1 Johtaminen ja johtajuus 14
3.2 Turvallisuusjohtaminen 16
3.3 Turvallisuusjohtamisen tavoitteet 18
3.4 Turvallisuusjohtamisen kehittäminen 19
3.5 Arviointi, seuranta ja auditoinnit 20
3.6 Oppiva organisaatio 21
4 KATAKRI turvallisuusjohtamisen välineenä 23
4.1 Auditointi 24
4.2 Hallinnollinen turvallisuus 25
4.3 KATAKRI kohdeorganisaatiossa 25
5 Kohdeorganisaation turvallisuustoiminta 25
5.1 Alkukatselmus 26
5.2 Turvallisuuskulttuuri 26
5.3 Turvallisuusjohtaminen ja turvallisuustoiminta 27
5.3.1 Seuranta ja arviointi 27
5.3.2 Raportointi 28
5.4 Turvallisuusryhmä 28
5.5 Turvallisuusdokumentaatio 28
5.6 Opinnäytetyön työprosessi kohdeorganisaatiossa 28
6 Turvallisuuskäsikirjan toteutus 30
6.1 Hyvyyskriteerit 31
6.2 Turvallisuuskäsikirjan rakentaminen 32
6.3 Sidosryhmien vaatimukset 33
6.4 Turvallisuusdokumentaatio 33
7 Arviointi ja palaute 34
7.1 Turvallisuuskäsikirjan sovellettavuus 34
7.2 Tavoitteiden saavuttaminen ja työprosessin arviointi 35

8 Pohdinta 36
Lähteet 38
Kuviot 40
Liitteet 41

Laurea- ammattikorkeakoulu **Tiivistelmä**
Laurea Leppävaara
Turvallisuusalan koulutusohjelma

Mika Kokkonen

Geodeettisen laitoksen turvallisuustoiminnan kehittäminen: Turvallisuuskäsikirja

Vuosi 2013 Sivumäärä 152

Opinnäytetyön tavoitteena oli tuottaa kohdeorganisaatiolle turvallisuuskäsikirja, jonka avulla kohdeorganisaatio voi hallinnoida ja kehittää turvallisuustoimintaansa. Turvallisuuskäsikirjan ohella tarkasteltiin kohdeorganisaation oppimista turvallisuusasioissa. Kohdeorganisaationa tässä opinnäytetyössä oli Geodeettinen laitos, joka on paikkatietoalan tutkimuslaitos. Kohdeorganisaatiossa ei ollut vielä vuoden 2012 alkupuolella suoranaista turvallisuusorganisaatiota, mutta saman vuoden aikana vastuutettiin turvallisuusasioiden hoitaminen ja kevään 2013 aikana muotoutui turvallisuusryhmä opinnäytetyöprosessini aikana. Opinnäytetyön produktina syntynyt turvallisuuskäsikirja toimii kohdeorganisaation tukidokumenttina turvallisuustoiminnassa, auditoinneissa sekä muissa hankkeissa ja projekteissa.

Turvallisuustoiminnan kehittäminen ja ylläpito ovat tärkeä osa jokaisen organisaation toiminnan jatkuvuuden kannalta. Johtaminen ja johtajuus, ja ennen kaikkea ylimmän johdon sitoutuminen, vaikuttaa turvallisuustoiminnan kehitykseen huomattavasti. Johdon tulee ottaa turvallisuustoiminta huomioon kaikilla organisaation tasoilla, jotta turvallisuustoiminta saadaan jalkautettua koko organisaatioon tehokkaasti.

Opinnäytetyön teoreettisessa osassa käsitellään organisaatioturvallisuutta, turvallisuusjohtamista ja minkälainen oppiva organisaatio on. Opinnäytetyön tarkoituksena oli myös tutkia, miten turvallisuusasioita oppivan organisaation on hyvä jatkaa turvallisuustoiminnan kehittämistä turvallisuusjohtamisen ja käytännöllisen turvallisuuden kautta. Turvallisuuskäsikirjalla on tärkeä rooli kohdeorganisaation turvallisuustoiminnan kehittämisessä, sillä se vaikuttaa koko henkilöstön oppimiseen turvallisuustoiminnan osalta.

Produktina syntyneen turvallisuuskäsikirjan rakenteeseen vaikuttivat kansallinen turvallisuusauditointikriteeristö, valtiohallinnon tietoturvatasojen hanke ja Geodeettisen laitoksen eri sidosryhmien vaatimukset. Opinnäytetyölle ja produktille asetettujen hyvyyskriteerien arvioinnin tuloksena voidaan todeta, että toteutettu turvallisuuskäsikirja soveltuu kohdeorganisaation turvallisuustoiminnan parantamiseen ja ylläpitämiseen. Turvallisuuskäsikirjan avulla kohdeorganisaation turvallisuustyötä saatiin helpotettua, sillä turvallisuusdokumentaatio löytyy nyt yhdestä paikasta helposti saatavana.

Turvallisuustoiminta, turvallisuusjohtaminen, turvallisuuskäsikirja

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaara
Bachelor's Degree Programme in Security Management

Mika Kokkonen

Development of the security operations in the Finnish Geodetic Institute: Security handbook

Year 2013 Pages 152

The objective of this thesis was to create a security handbook for the target organization, with which the organization can manage and develop its security operations. Along with the security handbook, the concept of a learning organization was examined. The target organization in this thesis was the Finnish Geodetic Institute, which does research and development in spatial data infrastructures. In the beginning of 2012 the target organization did not have a specific security organization, but during the same year the duties of security management were assigned and in the spring 2013 security organization was formed within the thesis process. The security handbook was developed to serve as a supporting document in the target organization's security operations, auditions as well as in different projects.

Developing and sustaining security operations is an essential part of any organization, so that it can continue its operating. Management and leadership, and most of all the higher management's commitment, affects the development process greatly. The management must pay attention to the security operations at all levels of an organization, so that security operations can effectively be put into practice in the whole organization.

The theoretical section of this thesis examines organizational security, security management and the concept of a learning organization. Another objective of this thesis was to study, how learning organization can continue development of security operations via security management and practical security. A security handbook has a big role in the development process of the security operations, as it affects the learning of security operations of all personnel.

The structure of the developed security handbook was affected by national security auditing criteria, the Finnish government information security development plan and requirements of the Geodetic Institute's different interest groups. Examining the thesis report and the product in the light of the set criteria, it can be stated that the developed security handbook is suitable for developing and keeping up the level of the security operations of geodetic institute. The security handbook facilitates the management of the security and safety work, as the security and safety documentation is in one place and easily available.

Security operations, security management, security handbook

1 Johdanto

Turvallisuusjohtaminen luo perustan turvallisuustoiminnalle ja sen avulla hallitaan kaikkia organisaatioturvallisuuden osa- alueita. Johtaminen ja johtajuus taas vaikuttavat turvallisuusjohtamisen toteutukseen ja siihen, millä tavalla oppiva organisaatio alkaa sisäistämään turvallisuustoimintaan liittyviä asioita. Vaikka turvallisuustoiminnan ja – johtamisen kehittäminen ei olisi tärkeimpiä asioita organisaatiossa, niin silti tulisi pyrkiä ammattimaiseen johtamiseen kaikilla toiminnan osa- alueilla. Turvallisuusjohtamista ja turvallisuuden hallintaa onkin tutkittu paljon aikaisemmin muun muassa Lanteen (2007) ja Simolan (2005) toimesta.

Opinnäytetyön tarkoituksena oli turvallisuustoiminnan kehittäminen kohdeorganisaatiossa ja tavoitteena kattavan turvallisuuskäsikirjan luominen kohdeorganisaation turvallisuustoiminnan tueksi. Työssä kohdeorganisaationa toimi Geodeettinen laitos, jossa tarvittiin apua turvallisuustoiminnan kehittämisessä. Opinnäytetyöprosessin aikana tarkoituksena oli tutkia kohdeorganisaation turvallisuustason nykytilaa, minkälaisia parannustoimenpiteitä tulisi tehdä ja millä tavalla turvallisuustoimintaa pystytään kehittämään vaatimusten mukaiseksi.

Tilanteeseen sopivin ratkaisu muotoutui työharjoittelun ja opinnäytetyön tekemisen aikana konstruktiivisella tutkimuksella ja lopputuloksena syntyi turvallisuuskäsikirja, johon on kerättynä kohdeorganisaation turvallisuusdokumentaatio ja – ohjeistukset sekä muut tarvittavat tiedot turvallisuustoimintaan liittyen. Opinnäytetyöprosessin ja tutkimuksen produktina syntynyttä turvallisuuskäsikirjaa voidaan pitää hyödyllisenä, kun sitä tarkastellaan tietoperustan ja käytännön sekä saadun palautteen valossa, sillä se auttaa turvallisuustoiminnan hallitsemisessa kokonaisvaltaisesti, varsinkin oppivassa organisaatiossa. Turvallisuuskäsikirjaa voidaan yleismaailmallisuutensa puolesta käyttää ja soveltaa myös muissa organisaatioissa.

1.1 Tausta ja rajaus

Aloitin aiheen etsimisen jo syksyllä 2012 ja alustavasti mielessäni oli turvallisuusviestintä. Kävin turvallisuusjohtamisen ja organisaatioviestinnän opintojaksoilla sekä keskustelin opettajien kanssa aiheesta, mutta työharjoittelu johdatti toiseen aiheeseen. Aloitin työharjoittelun valtiokonttorin kautta valtiohallinnon tietoturvatasohankkeessa Geodeettisella laitoksella (jäljempänä ”kohdeorganisaatio”), jossa keskustelin työharjoitteluni esimiehen kanssa mahdollisesta opinnäytetyön aiheesta. Keskusteluissa kävi ilmi, että kohdeorganisaatiossa ei ole suoranaista turvallisuustoimintaa johtavaa organisaatiota tai henkilöä, vaan turvallisuuteen liittyvät työtehtävät on kuvattuna kohdeorganisaation työjärjestyksessä oheistöinä. Tästä sain idean lähteä kehittämään kohdeorganisaation turvallisuustoimintaa ja erityisesti turvallisuusjohtamista.

Opinnäytetyön aiheena oli työharjoittelun alussa turvallisuusjohtamisjärjestelmän kehittäminen ja siihen liittyvä produkti, mutta opinnäytetyön otsikoksi kuitenkin muotoutui ’Geodeettisen laitoksen turvallisuustoiminnan kehittäminen: turvallisuuskäsikirja. Aiheen valinta oli looginen ratkaisu työharjoittelupaikkaan, sillä harjoittelun työtehtävät tukevat myös opinnäytetyön tekemistä. Tällä tavoin pääsin kehittämään samanaikaisesti työelämän turvallisuustoimintaa ja turvallisuusjohtamista käytännössä sekä kehittämään omaa ammatillista osaamista.

Työharjoittelussa esiin tulleista asioista johtuen, päätin rajata opinnäytetyöni aiheen turvallisuustoiminnan ja -johtamisen kehittämiseen ja erityisesti kehittämistyössä tuloksena syntyvään turvallisuuskäsikirjaan, jonka teen kohdeorganisaatiolle. Turvallisuuskäsikirjan sisältö ja rakenne on sovellettu tietoturvatasohankkeen ja sidosryhmien sekä kansallisen turvallisuusauditointikriteeristön (luku 4) vaatimusten mukaiseksi ja siten myös rajasin turvallisuuskäsikirjan käsittelemään organisaatioturvallisuuden osa- alueista vain turvallisuusjohtamista, toimitilaturvallisuutta, henkilöstöturvallisuutta ja tietoturvallisuutta, johon sisältyy tietoaineistojen turvallisuus.

1.2 Tarkoitus ja tavoitteet

Pääasiallisena tarkoituksena oli kehittää kohdeorganisaation turvallisuustoimintaa ja – johtamista, sillä vakituisen turvallisuusorganisaation vähäisyyden takia osaamista turvallisuustoiminnassa oli rajoitetusti. Kevään 2013 aikana työharjoittelun ja opinnäyteyöprosessin mukana tarkoituksena oli myös parantaa kohdeorganisaation turvallisuudesta vastaavan henkilön turvallisuusosaamista ja -johtamista. Tarkoituksena oli myös asettaa selkeät vastuualueet turvallisuustoiminnan hallinnoimisesta kohdeorganisaation työjärjestykseen.

Tärkeimpänä tavoitteena opinnäytetyössä oli tuottaa hyödyllinen turvallisuuskäsikirja kohdeorganisaation turvallisuustoiminnan tueksi, jotta turvallisuusdokumentaatio on kaikki samassa paikassa helposti löydettävissä ja päivitettävissä. Turvallisuuskäsikirjan tuottamisen ohella tavoitteena oli selvittää, miten turvallisuustoimintaa pystytään parantamaan tällaisen käsikirjan kanssa oppivassa organisaatiossa, jossa ei ole varsinaista turvallisuushenkilöstöä.

1.3 Kohdeorganisaatio

Yhteistyökumppanina opinnäytetyöprosessissa toimi Geodeettinen laitos. Se on paikkatietoalan tutkimuslaitos, jonka ydintehtävänä on toteuttaa tutkimus-, asiantuntija- ja palvelutehtäviä. Ydintehtäviä hoidetaan eri osastoilla, jotka ovat; geodesia ja geodynamiikka, geoinformatiikka ja kartografia, kaukokartoitus ja fotogrammetria sekä navigointi ja paikannus. Henkilöstöä kohdeorganisaatiossa on tällä hetkellä noin 85, joista osa on ulkomaalaisia. Kohdeorganisaatio on organisaatioltaan melko pieni, sillä osastojen johtajien yläpuolella ovat vain hallinto- ja tukipalvelut, tutkimusjohtaja sekä kohdeorganisaation ylijohtaja. (Geodeettinen laitos 2013a.)

1.4 Keskeiset käsitteet

Tässä kappaleessa käsittelen opinnäytetyössäni keskeisimpiä käsitteitä. Aiheesta johtuen pääasialliset käsitteet ovat organisaatioturvallisuus, turvallisuuskulttuuri, johtaminen, turvallisuusjohtaminen, turvallisuuskäsikirja sekä kansallinen turvallisuusauditointikriteeristö. Tieto-, toimitila- ja henkilöstöturvallisuuden lisäksi turvallisuuskäsikirjassa käsitellään tietoaineistojen turvallisuutta ja riskienhallintaa.

Organisaatioturvallisuus

Organisaatioturvallisuus tarkoittaa turvallisuustoimintaa, joka sisältää ainakin seuraavat osa-alueet: työ-, henkilö-, ympäristö-, rikos-, tieto-, kiinteistö- ja toimitilaturvallisuuden, pelastustoiminnan, tuotannon ja toiminnan turvallisuuden sekä ulkomaantoimintojen turvallisuuden (Lanne 2007, 11). Näiden osa- alueiden tarkoituksena on suojata organisaation arvoja ja osa- alueiden toimintaa sekä ohjata turvallisuusjohtamista ja riskienhallintaa.

Turvallisuuskulttuuri

Turvallisuuskulttuuri on organisaatiossa turvallisuustoimintaan kohdistuvia tietoisia ja tiedostamattomia uskomuksia, arvojen näkymistä sekä asenteita ja toimintatapoja turvallisuuteen liittyvien asioiden parissa. (Levä 2003, vii.)

Johtaminen
Johtaminen on sosiaalista vuorovaikutusta, jossa henkiöiden toimintaan pyritään vaikuttamaan siten, että asetetut tavoitteet ja päämäärä saavutetaan mahdollisimman hyvin. Johtaminen jaetaan usein organisoitiin, joka on asiajohtamista ja motivointiin, joka on henkilöjohtamista. (Lanne 2007, 12; Levä 2003, v.)

Turvallisuusjohtaminen
Turvallisuusjohtaminen on organisaation järjestelmällistä ja organisoitua ihmisiä, ympäristöä, tietoa, omaisuutta ja mainetta vahingoittavien tapahtumien torjumisen johtamista. Turvallisuusjohtaminen etenee prosessina politiikasta ja tavoitteista suunnitteluun, seurantaan ja arviointiin ja niiden kautta kehitystoimenpiteiden jälkeen jatkuvaan parantamiseen. Turvallisuusjohtaminen on myös osana organisaation normaalia johtamisprosessia (Lanne 2007, 12). Turvallisuusjohtaminen on selkeää ja johdonmukaista yhteistyötä, jossa kaikki tietävät velvollisuutensa ja turvallisuustoiminta on johdonmukaisella päätöksenteolla ja tavoitteellisuudella ohjattua. (Kerko 2001, 38.)

Turvallisuuskäsikirja
Turvallisuuskäsikirja on organisaation turvallisuustoiminnan aputyökalu, jossa on kasattuna kaikki organisaation turvallisuustoimintaan liittyvät ohjeet, menettelyt ja dokumentaatio. Turvallisuuskäsikirjaan linkitetään henkilöstölle perehdytettävää materiaalia dokumentaation löytämisen helpottamiseksi.

Kansallinen turvallisuusauditointikriteeristö (jäljempänä KATAKRI)
KATAKRI on viranomaisten, elinkeinoelämän ja turvallisuusalan toimijoiden yhteistyöllä valmistettu turvallisuuskristeeristö, jonka avulla saadaan yhtenäistettyä yhteisöturvallisuusmenettelyitä ja parannettua eri yhteisöjen omaa valvontaa ja auditointeja. (Kansallinen turvallisuusauditointikriteeristö 2011, 2.)

2 Toteutus

Opinnäytetyön aiheen miettiminen alkoi syksyllä 2012, mutta en päässyt aloittamaan opinnäytetyöprosessia koulun päässä kurssien päällekkäisyyksien vuoksi. Tästä johtuen kunnollinen aloitus siirtyi 2013 tammikuulle, jolloin olin jo aloittanut työharjoitteluni kohdeorganisaatiossa. Kohdeorganisaatiossa työskennellessäni esiintyi tarve kehittää turvallisuustoimintaa, sillä kohdeorganisaatiossa oli ajankohtaisena auditointiprosessi, valtiohallinnon tietoturvatasohanke ja tulevien projektien osalta turvallisuustoimintojen parannustoimenpiteet. Näistä keskustellessani kohdeorganisaation turvallisuuspäällikön kanssa sain ajatuksen tehdä opinnäytetyöni heille, koska sillä tavalla saisin sisällytettyä samaan työprosessiin monta muutakin työprojektia.

Työharjoittelun puolesta olin saanut käyttööni valtiokonttorin IT- palvelukeskuksen työkalupakin, jossa on erilaisia ohjeita, mallipohjia ja muuta neuvoa antavia asiakirjoja tietoturvatasohankkeen osalta. Työkalupakista löysin Kirsi Janhusen (Nurmi 2011) laatiman tietoturvallisuuden hallinnan projektioppaan, jossa on kattavasti kuvattuna tietoturvallisuuden hallinnan suunnittelua ja toteutusta. Projektioppaan pohjalta Janhunen oli tehnyt tietoturvakäsikirjamallin, jonka teksteissä on myös paljon Kari Pohjolan (2013) tuotantoa, jota Janhunen on käyttänyt käsikirjamallissa. Tästä käsikirjamallista sain alustavan pohjan turvallisuuskäsikirjalle, josta sitten muokkasin ja sovelsin kohdeorganisaation tarpeiden mukaisen. Turvallisuuskäsikirjan toteuttamisesta on tarkemmin luvussa 6. Seuraavassa luvuissa kuvailen tarkemmin opinnäytetyön tutkimuksellista taustaa.

2.1 Lähestymistapa

Tämä opinnäytetyö on työelämää kehittävä toiminnallinen opinnäytetyö. Toiminnallisessa opinnäytetyössä on tarkoituksena parantaa käytännön toiminnan ohjeita, opastamista ja toiminnan järjestämistä tai järkeistämistä. Toiminnallisissa opinnäytetöissä raportin lisäksi luodaan työprosessissa syntyvä produkti. Opinnäytetyöraportissa kuvataan produktin syntymisen prosessia ja opittuja asioita, kun taas produkti itsessään on työelämän käyttöön tarkoitettu dokumentti. (Vilkka & Airaksinen 2003, 9, 65.)

Konstruktiivisen tutkimuksen tavoitteena on luoda jokin ratkaisu käytännön ongelmaan. Tutkimuksen konstruktio (produkti) eli jokin tuotos voi olla esimerkiksi tietojärjestelmä, käsikirja, malli tai suunnitelma. Konstruktiivisessa tutkimuksessa muutos on siis jokin konkreettinen kohde. Muutos sidotaan aikaisempaan teoriaan aiheesta. Tiivis vuoropuhelu käytännön ja teorian välillä on konstruktiivisessa tutkimuksessa luonteenomainen piirre. Kehitetyn ratkaisun toteuttaminen ja käytännön toimivuuden arviointi ovat keskeinen osa tutkimusta (Ojasalo, Moilanen & Ritalahti 2009, 38). Seuraavassa kappaleissa kuvailen tarkemmin menetelmiä, joita käytin opinnäytetyössäni.

2.2 Menetelmät

Konstruktiivisessa tutkimuksessa käytetään (ryhmä)keskusteluita ja siinä painotetaan yhteistyötä kohdeorganisaation kanssa, kuten toimintatutkimuksessa (Ojasalo, Moilanen & Ritalahti 2009, 68). Käytin työssä teemahaastattelua tiedonkeruun menetelmänä, sillä teemakohtainen ja avoimempi keskustelu aiheesta vaikutti sopivimmalta opinnäytetyöhön. Haastattelemalla kohdeorganisaation tietohallintopäällikköä ja kysymällä eri asiantuntijoilta palautetta sain tietoa turvallisuuskäsikirjan hyödyllisyydestä ja sovellettavuudesta sekä asetetut hyvyyskriteerit. Haastattelun mallina käytin puolistrukturoitua haastattelua, jonka kysymykset määräy-

tyvät pitkälti KATAKRI:n ja muiden sidosryhmien vaatimusten aihepiirien mukaisesti. (Ojasalo, Moilanen & Ritalahti 2009, 95; Hirsjärvi, Remes & Sajavaara, 208.)

Haastattelun ohella käytin myös havainnointia, joka on tiedonkeruun ja kehittämistyön menetelmä. Havainnoinnilla saadaan tietoa esimerkiksi ihmisten käytöksestä ja toiminnasta eri ympäristöissä. Havainnoimalla voidaan myös todeta, että toimivatko ihmiset sanojensa mukaisesti. Tässä työssä havainnoinnilla todennetaan kohdeorganisaation ympäristössä ja toimitiloissa olevia turvallisuusratkaisuja, jotta dokumentoidut asiat voidaan todentaa. Havainnoin ja tarkastelin myös kohdeorganisaation eri henkilöiden suhtautumista turvallisuusasioihin ja niiden hoitamiseen. (Ojasalo, Moilanen & Ritalahti 2009, 103; Hirsjärvi ym.212- 214.)

Dokumenttianalyysissä pyritään tekemään päätelmiä kirjalliseen muotoon saatetusta materiaalista, kuten verbaalisesta, symbolisesta ja kommunikatiivisesta materiaalista. Materiaali voi olla esimerkiksi dokumentoituja haastatteluja, puheita, keskusteluja, raportteja ja muita kirjallisia dokumentteja (Ojasalo, Moilanen & Ritalahti 2009, 121). Tavoitteenani oli tutkia ja analysoida kohdeorganisaation turvallisuusdokumentaatiota niin, että saan luotua selkeän kuvaus kehitettävästä asiasta. Dokumenttianalyysin tarkoituksena oli auttaa turvallisuuskäsikirjan hyvyyskriteerien asettamisessa ja löytää kaikki tarvittava dokumentaatio turvallisuuskäsikirjaan liitettäväksi.

2.3 Tietoperustan rakentaminen

Olin opinnäytetyöprosessin ajan työharjoittelussa kohdeorganisaatiossa valtiohallinnolle suunnatussa tietoturvatasojen yhteishankkeessa, jonka tavoitteena on saada 2010 voimaan tulleen tietoturvatasoasetuksen velvoitteet perustason osalta saavutettua (Valtiokonttori 2011). Sain harjoittelun puolesta käyttööni kohdeorganisaation käyttöön annettua materiaalia, jota hyödynsin turvallisuuskäsikirjaa luodessani. Valtiokonttorin työkalupakista löytyi paljon hyviä malleja, joista sai kohdeorganisaation turvallisuusdokumentaation hyviä lisäyksiä.

Teoreettista tietoperustaa etsin ensisijaisesti alan ja käsiteltävän aiheen kirjallisuudesta. Teoreettisella tiedolla perustelen, millä tavalla turvallisuusjohtaminen, turvallisuustoiminta ja oppivan organisaation toiminta tulisi hoitaa yleisesti organisaatiossa. Vertaan kohdeorganisaation turvallisuustoimintaa teoriaan ja tarkastelen, millä osa- alueilla olisi parantamisen varaa. Kohdeorganisaatiolta kerään tietoa keskustelemalla eri henkilöiden kanssa ja tutustumalla olemassa olevaan turvallisuusdokumentaatioon.

Pääasiallisina kirjallisuuslähteinä käytin opinnäytetyössäni Marinka Lanteen (2007) tutkimusta ”Yhteistyö yritysturvallisuuden hallinnassa”, Kalevi Mäkisen (2005) tutkimusta ”Strategic security”, Antti Simolan (2005) tutkimusta ”Turvallisuuden johtaminen esimiestyönä”, Kirsi Le-

vän (2003) tutkimusta ”Turvallisuusjohtamisjärjestelmien toimivuus” sekä Pertti Kerkon (2001) teosta ”Turvallisuusjohtaminen”. Näiden teosten pohjalta loin teoreettisen viitekehyksen turvallisuustoiminnan kehittämiseksi.

Keskustelin kohdeorganisaation henkilöiden ja sidosryhmien edustajien kanssa, mitä vaatimuksia heillä on turvallisuuskäsikirjan suhteen. Kohdeorganisaatiosta tulevia vaatimuksia olivat pääasiallisesti projektien ja hankkeiden osalta tarvittavat asiat ja sidosryhmiltä tuli auditointien ja projektien osalta vaatimuksia. Näiden vaatimusten ja tietojen sekä valmiiden mallien pohjalta muokkasin ja sovelsin turvallisuuskäsikirjan rakenteen, jotta kohdeorganisaation kaikki turvallisuustoimintaan liittyvät dokumentit voidaan sijoittaa samaan paikkaan, josta ne ovat löydettävissä helposti.

Opinnäytetyöni tietoperustana toimi myös KATAKRI (luku 4). Kohdeorganisaatiossa oli meneillään FSC (facility security clearance)- auditointiprosessi ja sen aikataulu sopi opinnäytetyöni aikatauluun, joten KATAKRI: n vaatimukset sisällytettiin turvallisuuskäsikirjaan. Tarkastelin kohdeorganisaation kohdalla tarkemmin KATAKRI: n hallinnollisen turvallisuuden toteutumista tässä opinnäytetyöraportissa, sillä työn fokus on turvallisuusjohtamisessa. Opinnäytetyön aiheen osalta rajasin KATAKRI: n muut osa- alueet käsittelyn ulkopuolelle tästä raportista (Kansallinen turvallisuusauditointikriteeristö 2011). En myöskään tarkastellut lainsäädännön ja asetuksien vaatimuksia sen tarkemmin tässä raportissa. Seuraavassa luvussa on tarkasteltuna opinnäytetyön keskeisin tietoperusta, jossa tarkastellaan organisaatioturvallisuutta, turvallisuusjohtamista ja oppivaa organisaatiota.

3 Organisaatioturvallisuus

Turvallisuus on moniulotteinen käsite, joka määritellään hieman eri tavalla toimintaympäristöstä tai henkilöstä riippuen. Turvallisuus kuitenkin tarkoittaa olotilaa tai tunnetta, jossa ei esiinny vaaraa tai riskialtista tilannetta. Kuitenkin, organisaatio-, yhteisö- ja henkilötasolla tämä olotila tai tunne käsitetään hyvinkin eri tavalla (Mäkinen 2005, 89). Turvallisuus on kaikessa mukana oleva asia ja tässä luvussa käsittelen sitä organisaation toiminnan osalta.

Organisaatiot pyrkivät toteuttamaan toimintansa tarkoitustaan ja saavuttamaan asetetut päämäärät jakamalla työtä ja hyödyntämällä resursseja, kuten työvoimaa, pääomaa ja teknologiaa. Toiminnan turvallisuutta ohjaavia velvoitteita löytyy muun muassa turvallisuuteen liittyvästä lainsäädännöstä, asetuksista määräyksistä sekä ulkoisilta tekijöiltä, kuten erinäisiltä sidosryhmiltä, jota vaativat turvallisuustoimenpiteiden parantamista. (Levä 2003, 23; Lanne 2007, 24.)

Organisaatioturvallisuus jakautuu kymmeneen eri osa- alueeseen, joita ohjaa turvallisuusjohtaminen. Nämä osa- alueet ovat kiinteistö- ja toimitilaturvallisuus, henkilöturvallisuus, tietoturvallisuus, valmiussuunnittelu, pelastustoiminta, ympäristöturvallisuus, työturvallisuus, tuotannon ja toiminnan turvallisuus, rikosturvallisuus sekä ulkomaan toimintojen turvallisuus (Elinkeinoelämän keskusliitto 2013). Organisaation toiminnasta riippuen, sen toiminnot saattavat koskea vain osaa edellä mainituista osa- alueista, mutta turvallisuusjohtaminen ohjaa kuitenkin kaikkia osa- alueita, joten organisaatioiden tulisi kehittää ensisijaisesti turvallisuusjohtamista ja turvallisuuden hallintaa.

Organisaatioturvallisuudessa toteuttamiseen tulisi osallistua organisaation ylin johto, linjajohto, henkilöstö, asiantuntijat sekä erinäiset sidosryhmät. Ylimmän johdon roolina on strategisten päätösten tekeminen, sitoutumisen osoittaminen turvallisuustoimintaan, tiedottaminen ja osallistuva työtapa, toimiminen esimerkillisesti, turvallisuusjohtamisen rakenteen luominen sekä turvallisuustoiminnan seuraaminen. Linjaesimiehillä on suuri rooli jokapäiväisessä turvallisuustoiminnassa toimia motivaattoreina kohti turvallisempaa toimintaa ja valvoa turvallisuustoimintaa. Sisäiset tai ulkopuoliset asiantuntijat toimivat organisaatioturvallisuuden osa-alueiden koordinoijina ja analysoijina sekä ylimmän- ja linjajohdon tukena turvallisuustoiminnan kehittämisessä. Turvallisuusorganisaation tehtävänä on johtaa turvallisuutta ja hoitaa riskienhallintaa, jotka ovat keskeisiä prosesseja pyrittäessä kohti parempaa organisaatioturvallisuutta. (Kerko 2001, 26, 45; Lanne 2007, 73,28.)

3.1 Johtaminen ja johtajuus

Hyvää johtamista ja johtajuutta tarvitaan organisaatioiden toiminnan tarkoituksen toteuttamiseksi ja asetettujen päämäärien saavuttamiseksi. Organisaatiot ovat yhä enemmän riippuvaisia inhimillisestä luovuudesta ja jatkuvasta kehittymisestä, joissa johtamisen ja johtajuuden merkitys on erittäin suuri. Organisaatioiden ja ihmisten toimintaa ohjaa pitkälti kaksi lähdettä, joista rakenne ja toimintasäännöt ylläpitävät toiminnallisia rutiineja ja johtajuus on toinen merkittävä ohjauslähde. (Levä 2003, 26; Simola 2005, 106.)

Johtaminen ja johtajuus ovat valtaa ja vallalla vaikutetaan, joten ne ovat olennainen osa organisaatioiden turvallisuustoiminnan kehittämisessä. Ne voidaan määritellä sosiaalisiksi vuorovaikutusprosesseiksi, joissa pyritään saavuttamaan asetetut tavoitteet vaikuttamalla prosessissa työskentelevien toimintaan positiivisesti. Johtaminen voidaan siis käsittää ammattina, joka merkitsee, että sitä voi oppia ja jossain määrin opettaa. Johtaminen ja johtajuus ovat pohjimmiltaan viestintää, sillä ilman kommunikaatiota valtaa ei voi käyttää eli johtaa ja mikään työyhteisö ei toimi ilman viestintää. Hyvään johtamiseen ja johtajuuteen kuuluukin laadukas viestintä kaikilla organisaation tasoilla, joten jokaisen esimiehen tulisi omata viestinnän

perustiedot ja -ymmärtäminen sekä -valmiudet. (Simola 2005, 107,109, 119s; Lanne 2007, 22; Mäkinen 2005, 50.)

Johtajuus on henkilökohtainen kyky vaikuttaa muihin ja se ilmentää organisaation visiota (Mäkinen 2005, 54). Johtajuudella ja johtamisella vaikutetaan myös organisaation kulttuuriin, ja kulttuuria ja johtamista voidaankin pitää saman kolikon kääntöpuolina. Ne sitoutuvat toisiinsa tiiviisti ja niitä on vaikea erottaa selvästi. Simola (2005, 44) toteaakin, että johtajien ainoana tärkeänä tehtävänä saattaa olla kulttuurin luominen ja johtaminen, ja että johtajien taitoihin tulisi kuulua taito työstää (turvallisuus)kulttuuria. Johtajuutta voidaan Mäkisen (2005, 54- 55) mukaan nähdä:

1. Eriävänä työskentelynä olosuhteiden pakosta
2. Voimakkaan viettinä toimia asioiden suhteen
3. Joskus tarpeettomana, sillä hyvä johtaminen ajaa saman asian
4. Vallan käyttönä
5. Asiana, joka vaatii laajaa - alaista osaamista
6. Tehokkaan johtajan kykynä motivoida
7. Mahdollisuuksien analysoimisen ja esittämisen toteuttamisena
8. Riittävän arvostelukyvyn mittarina
9. Vastuuna omista tekemisistä ja sanomisista
10. Riittävänä nöyryytenä

Poikkeukselliset johtajat tähtäävät kontrolloituun ulosantiin ja omaavat mittavasti fyysistä puhtia. Turvallisuusasioita opettelevassa organisaatiossa johtamisella ja johtajuudella on merkitystä, sillä johtajat ovat suunnittelijoita ja opettajia organisaatiossa, jossa henkilöstön turvallisuustiedon ja - taidon tulisi kehittyä. Johtajat ovat siis vastuussa oppimisesta. Inspiroimalla ja motivoimalla henkilöstöä turvallisuudesta vastaavat johtajat saavat henkilöstön löytämään uusia merkityksiä, erikoisuuksia ja haasteita työssään. Yhteiset päämäärät, kokemukset ja palautteen saaminen ja kerääminen kasvattavat organisaation turvallisuustoiminnan tasoa ja yhtenäisyyttä. (Mäkinen 2005, 55, 174.)

Harrastelijamaisesta johtamisesta tulisikin siis suunnata kohti ammattimaisempaa johtamista, johon sisältyy johtamiseen liittyvien käytäntöjen periaatteet ja erilaisten työkalujen hyvä hallinta. Varsinkin muutoksessa ja jatkuvassa oppimisessa johtamisella on tärkeä asema. Johtajuutta tarvitaan, jos halutaan henkilöstön siirtyvän vaiheittain riippuvuudesta kohti yhteistä vastuuta ja sisäistä kurinalaisuutta. Myös organisaation madaltamisessa tarvitaan hyvää johtajuutta, jolloin saadaan lisättyä organisaation aloitekykyä. Näin organisaatiosta tulee riittävän kurinalainen toteuttamaan ideoita, joita matalan organisaatiorakenteen sallima aloitekyky

tuottaa. Tämänkaltainen johtajuus parantaa myös turvallisuutta, joten organisaatiosta tulee tehokkaamman ohella turvallisempi. (Simola 2005, 155, 225.)

Johtoporras ja johtajat ovat kuitenkin usein kykenemättömiä näkemään kuinka paljon turvallisuusasioiden eteen itse tulisi tehdä. Johto saattaa patistaa henkilöstöä tekemään asioita turvallisemmin ja paremmin, mutta ei itse sitoudu esimerkillisesti ongelmiin. Näin ollen paraskaan linjaesimies ei voi korjata ylimmän johdon heikkoa sitoutumista tai huonoa esimerkkiä turvallisuustoiminnassa. Johdon tulee sitoutua turvallisuustoimintaan ja olla esimerkkinä, sillä organisaatiossa oppimista tukee parhaiten ihmisten kanssakäyminen, osallistuminen turvallisuustoimintaan ja itseohjautuvuuteen kannustava johtamistyyli. (Simola 2005, 222; Levä 2003, 27.)

3.2 Turvallisuusjohtaminen

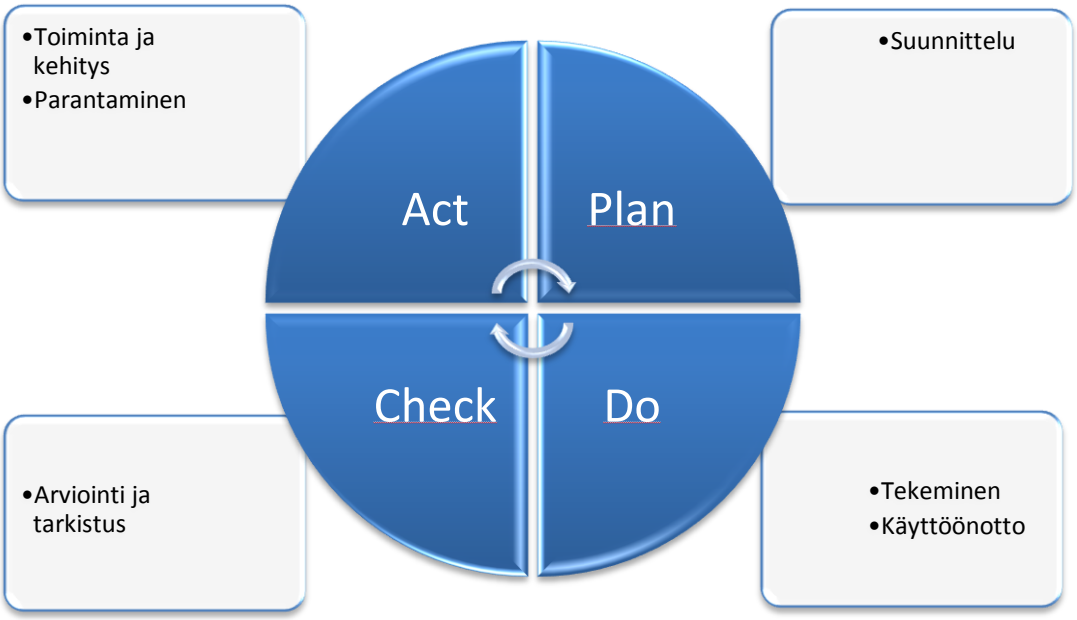
Turvallisuuden johtaminen on luonnollinen osa organisaation kokonaisvaltaista johtamista. Se on osa organisaation taloutta, toimintaa, tavoitteita ja päämääriä sekä olennainen osa vaarojen ja riskien tunnistamista. Turvallisuusjohtamisessa tuetaan organisaation strategioita, periaatteita ja toimintoja. Kuten koko organisaation toiminnan johtamisessa, myös turvallisuuden johtamisessa valtaa käyttävän esimiehen käyttäytyminen, suhtautuminen ja sitoutuminen ovat kehitystoiminnan lähtökohtana. Kuten aikaisemmin on mainittu, niin turvallisuusjohtaminenkin on vuorovaikutteista johtamista ja johtajuutta, jossa viestintä on tärkeässä asemassa. (Lanne 2007, 22; Mäkinen 2005, 152; Simola 2005, 118, 136.)

Turvallisuusjohtaminen on siis ihmisten, toimintaympäristön ja organisaation omaisuuden suojelemista ja turvallisuustoiminnan määrätietoista ohjaamista ja kehittämistä. Turvallisuuden johtamisessa korostuu Simolan (2005, 225) mukaan monimutkaisten riippuvuussuhteiden näkeminen, ymmärtäminen ja kyky ratkaista asioiden ja ihmisten välillä vaikuttavia suhteita, jolloin olennaisimpina asioina ovat vuorovaikutus, johtaminen ja johtajuus.

Turvallisuusjohtamisessa keskeiset välineet edellyttävät johtoasemassa olevilta perustietoja ja – taitoja erilaisista ryhmätyötekniikoista. Järjestelmällisellä ja kokonaisvaltaisella turvallisuusjohtamisella voidaan parhaimmillaan kehittää muutakin johtamistoimintaa. Turvallisuusjohtamisessa korostuu myös koko organisaation yksilöiden vastuu, jossa jokainen on vastuussa omasta sekä muiden turvallisuudesta. (Simola 2005, 214, 219,222.)

Organisaatioiden turvallisuusjohtamisen ja – toiminnan kehittämisen vaiheita voidaan kuvata Demingin PDCA- ympyrän (kuvio 1) avulla. Vuonna 1939 tehty Demingin ympyränä tunnettu jatkuvan kehittämisen malli soveltuu myös turvallisuustoiminnan kehittämiseen. PDCA- malli on järjestelmällinen tapa hakea olemassa oleviin prosesseihin luotettavuutta. Pääsääntönä

kuitenkin on, että organisaatiolla on määriteltynä haluttu turvallisuustaso, millä keinoilla haluttu taso saavutetaan ja millä mittareilla tuloksia mitataan. (Simola 2005, 83; Lanne 2007, 22.)



Kuvio 1: Demingin PDCA- ympyrä

Organisaatioturvallisuuden johtaminen ja organisointi voidaan toteuttaa usealla eri tavalla. Muun muassa organisaation resurssit ja rakenne, toimiala ja verkottuneisuus, toimintaan liittyvät riskit sekä organisaation turvallisuuskulttuuri vaikuttavat turvallisuustoiminnan organisointitapoihin. Kuitenkin ylin johto vastaa organisaatioturvallisuuden toteutuksen puitteista, resursseista, organisoinnista ja linjauksista. (Lanne 2007, 14; Kerko 2001, 48.)

Turvallisuusjohtaminen havainnollistetaan myös muiden määritelmien kanssa, kuten laatujohtaminen, tehtäväorientoituneisuus, lakipainotteinen, sitoutuminen, turvallisuusstrategia ja -periaatteet, turvallisuusorganisaatio ja - vastuut, työ- ja turvallisuusjohtaminen, raportointi sekä kriisien hallinta (Mäkinen 2005, 159). Elinkeinoelämän keskusliiton tekemä yritysturvallisuusympyrä (kuvio 2) kuvaa hyvin turvallisuusjohtamisen asemaa ja otetta organisaatioturvallisuuden osa- alueisiin ja suojattaviin arvoihin nähden. Turvallisuusjohtaminen sitoo organisaatioturvallisuuden osa- alueet ja suojattavat arvot yhteen.

Kuvio 2: Organisaatioturvallisuuden osa- alueet (Sovellettu EK- yritysturvallisuusympyrästä)

3.3 Turvallisuusjohtamisen tavoitteet

Organisaatioturvallisuuden hallinnalla pyritään aktiivisin toimin ja päätöksin saavuttamaan ja ylläpitämään tavoiteltu turvallisuustoiminnan taso. Hallinta kohdistuu organisaatioturvallisuuden tilaan vaikuttamalla ja ottamalla organisaatioturvallisuus järjestelmällisemmin huomioon kaikessa organisaation toiminnassa. Turvallisuuden hallinta toimii sitä paremmin mitä tarkemmin se on liitetty koko organisaation tavoitteisiin ja toteutukseen. Myös koko henkilöstö tulisi ottaa mukaan tavoitteiden visiointiin, sillä luottamus johtoon ja asetettuihin tavoitteisiin parantaa henkilöstön kykyä työskennellä paremmin. (Lanne 2007, 19; Mäkinen 2005, 57.)

Turvallisuusjohtamisen tavoitteet ja turvallisuustoiminnan säännöt ja sen tasoa koskevat vaatimukset tulee tiedottaa koko henkilöstölle, jotta haluttu turvallisuustaso on tiedostettuna koko organisaatiossa ja että sitä voidaan seurata. Tavoitteet ja vaatimukset voivat perustua viranomaisvaatimuksiin tai yrityksen itse asettamiin kriteereihin. Turvallisuustoimintaan liit-

tyvät tavoitteet voivat riippua myös omistajista, asiakaskunnasta ja sidosryhmistä. (Levä 2003, 37; Lanne 2007, 74; Mäkinen 2005, 174.)

Myös strategiset ratkaisut vaikuttavat organisaatioturvallisuuden tavoitetasoon, sillä johdon päätökset luovat pohjan muun muassa riskienhallinnalle. Operatiivisessa johtamisessa turvallisuustavoitteiden toteuttaminen viedään osaksi työprosesseja. Joskus kuitenkin organisaation strategisten ja operatiivisten tavoitteiden ja turvallisuustavoitteiden yhdistäminen on haastavaa. Näin ollen organisaatioturvallisuuden hallinnan yhteistyö tuleekin muodostua tehtävien ja vastuiden jakamisesta eri toimijoille, kuten ylimmälle johdolle, ulkoisille ja sisäisille asiantuntijoille, linjajohdolle, henkilöstölle ja muille toimijoille. (Lanne 2007, 38; Mäkinen 2005, 174.)

Jotta organisaatio saa henkilöstön toimimaan halutulla tavalla turvallisuustoiminnan osalta, on sen tiedotettava ja koulutettava henkilöstöä sekä annettavat selvät tavoitteet turvallisuuden parantamiseksi. Organisaation tulee välittää ainakin seuraavat turvallisuustoiminaan liittyvät tiedot ja niihin liittyvät tavoitteet henkilöstölle:

”- Turvallisuuspolitiikan tavoite ja tarkoitus
- Visiot, arvot ja uskomukset, jotka ovat perustana politiikalle
- Ylemmän johdon sitoutuminen politiikan toteuttamiseen
- Suunnitelmat, standardit, ohjeistukset ja järjestelmät, jotka ovat yhteydessä toteuttamiseen ja suorituskyvyn mittaamiseen
- Ajankohtainen informaatio, joka auttaa varmistamaan työntekijöiden osallistumista ja sitoutumista
- Kommentit ja ideat parannustoimenpiteille
- Vahingoista ja vaaratilanteista saatava oppi”
(Simola 2005, 92.)

3.4 Turvallisuusjohtamisen kehittäminen

Kaikki kehittäminen lähtee suunnittelusta, jossa asetetaan tavoitteet, organisoidaan tehtävät ja kehitysmenetelmät määritellään konkreettisesti. Kaikelle kehittämiselle on myös tärkeää yleinen keskustelu ja yhteisten aikaisempien kokemusten analysointi. Kehittämiseen valittavat mittarit ja niiden laskentaperusteet tulee kaikkien tuntea, jotta henkilöstö voi muodostaa yhteisen ymmärryksen organisaatiolle tärkeistä asioista ja niiden välillä vaikuttavista suhteista. Proaktiivisessa turvallisuustoiminnassa olennaista on mitata ja arvioida sen tasoa, jolloin tason heikkenemisestä saadaan tietoa ennen kuin vahinkoja pääsee tapahtumaan. Näin ollen järjestelmällisen kehityksen perustana ovat ongelmien havaitseminen, määrittäminen ja ratkaiseminen. Kuten laadun tekemisessä, myös turvallisuustoiminnassa kehittämisen pohjana

toimii ylläpitäminen. Turvallisuustoiminnalle tulisi organisaatiossa Levän (2003, 31) mukaan luoda yhteiseksi hyväksytty sisältö, jotta sitä voidaan mitata, arvioida ja kehittää. (Lanne 2007, 93; Simola 2005, 93, 101.)

Organisaation jatkuva oppiminen vaatii vastuullisia ja oma- aloitteisia kehittymispyrkimyksiä kaikilta organisaation jäseniltä. Erityisesti muutoksessa ja siihen liittyvässä oppimisessa on olennaisena osana lähiesimiesten kautta tapahtuva johtaminen, sillä he ovat tärkeässä asemassa turvallisuustoiminnan jalkauttamisessa toimintoihin sekä asenteiden ja käyttäytymisen muutokseen. Turvallisuustoiminnan muutokseen ja kehitykseen tarvitaan siis transformaalisia johtajia ja kaikkien organisaatiossa toimivien oppimista. (Simola 2005, 106, 137, 155; Kerko 2001, 27.)

Turvallisuuskulttuuri vaikuttaa organisaatioturvallisuuden hallinnan onnistumiseen ja varsinkin sen saavuttamiseen ja ylläpitämiseen. Näin ollen täytyy olla olemassa (1) muutoksen käyntiin laittaja, (2) johdon tuki ja (3) rakenne muutosprosessin johtamista varten (Lanne 2007, 38). Kulttuurissa vallassa vaikuttavat asenteet ja arvot vaikuttavat myös turvallisuustoimintaan ja – johtamiseen.

Kuten tavoitteiden asettamisessa, myös organisaatioturvallisuuden suunnittelussa ja toteutuksessa on sisäisten toimijoiden mukana myös ulkoisia sidosryhmiä. Tästä johtuen organisaatioturvallisuuden hallinnan haasteena onkin sisäisten ja ulkoisten toimijoiden yhteistyö, keskinäinen viestintä ja turvallisuustoiminnan oppimisen kehittäminen. Turvallisuustoimintaa voidaankin kehittää ja analysoida johtamislähtöisesti (sisäiset ja ulkoiset auditoinnit), käyttäytymislähtöisesti (havainnointi ja palaute) ja kulttuurilähtöisesti (asenne- ja ilmapiirikyselyt). (Lanne 2007, 14, 33.)

Turvallisuuden johtamisessa kehityksen ongelmana on ollut muun muassa se, miten pystytään osoittamaan hyvän turvallisuustoiminnan merkitys tuloksellisessa toiminnassa. Myöskin, jos päivittäisessä toiminnassa ei noudateta yhteisesti laadittuja sääntöjä ja ohjeita, siitä seuraa ongelmia turvallisuustoiminnan ja –johtamisen kehittämisessä (Simola 2005, 156, 223). Jatkuvan kehityksen takaamiseksi tulee turvallisuustoiminnan olla päivittäistä ja kehittämistä ja ylläpitämistä ei saa keskeyttää, ainakaan liian pitkäksi ajaksi.

3.5 Arviointi, seuranta ja auditoinnit

Turvallisuuden johtamisessa tiedon tarve on yhteydessä turvallisuusmääräyksiin, turvallisuustoiminnan suunnitteluun ja toteutukseen sekä turvallisuuden seurantaan ja arviointiin (Simola 2005, 89). Turvallisuustoiminta koostuu toimenpiteistä, joilla pyritään ehkäisemään vaaroja ja onnettomuuksia, joten näitä toimenpiteitä tulisi arvioida ja seurata. Turvallisuustoiminnan

vaikutuksia voidaan mitata selvittämällä tekniikassa, henkilöstössä ja organisaatiossa tapahtuneita muutoksia ja arvioimalla muutoksien yhteyttä poikkeamatilanteisiin ja onnettomuuksiin. Turvallisuustoiminnan mittaamisessa ja arvioinnissa voidaan käyttää esimerkiksi (OHSAS 18002 2008)

- vaaran tunnistus-, riskin arviointi- ja riskien hallintaprosessien tuloksia
- tarkastuslistojen avulla tehtäviä järjestelmällisiä työpaikkatarkastuksia
- kiertokäyntiperiaatteella tapahtuvia turvallisuuskierroksia
- koneiden ja laitteiden tarkastuksia
- turvallisuuden, työympäristön ja ihmisten käyttäytymisen arvioimista näytteenomaisesti
- henkilöstön asennekartoituksia
- dokumentoinnin ja tiedostojen analysointia
- systemaattista vertailua muiden organisaatioiden hyviin käytäntöihin.

Auditointien tarkoituksena on arvioida organisaation toimintaa ja auditointimenetelmiä on erilaisista tsekkilistoista, kyllä - ei- tyyppisistä, yksityiskohtaisempiin, laadullisiin sekä erilaisiin pisteytyksiin perustuviin menetelmiin. Auditoinnit voidaan jakaa sisäisiin, asiakkaiden ja sidosryhmien tekemiin ja kolmansien osapuolien tekemiin. Säännölliset auditointivälit vaihtelevat kohteesta riippuen päivistä vuosiin. Auditoinneista tarkemmin luvussa 4.1. (Simola 2005, 98.)

3.6 Oppiva organisaatio

Oppivasta organisaatiosta on vaihtelevia teorioita ja määritelmiä. Sillä ei tarkoiteta mitään järjestelmää, vaan se on kehityssuunta toimintojen parantamiseen. Riittävään muutokseen ja oppimiseen vaaditaan se, että koko henkilöstö ottaa vastuuta esiintyvistä ongelmista. Organisaatiot ovat muodoltaan yleensä hierarkkisia, jolloin oppiminenkin on hierarkkista ja siitä johtuen kokonaisvaltaisen oppimisen saavuttamiseksi organisaation eri tasojen tulee kytkeytyä toisiinsa systeemiseksi ja oppivaksi kokonaisuudeksi. Kokonaisvaltainen oppiminen on myös vaiheittaista ja vaiheesta toiseen siirtyminen edellyttää johdolta tietoisia päätöksiä, osaamista ja henkilöstön osallistamista yhteiseen kehittämiseen ja oppimiseen. (Simola 2005, 61, 140- 141; Levä 2003, 67.)

Oppivaksi organisaatioksi voidaan siis kutsua paikkaa, jossa yksilön, yhteisön ja koko organisaation oppimista mahdollistavat ja kannustavat menetelmät ovat organisaation kulttuurissa. Oppivasta organisaatiosta voidaan puhua silloin, kun sen osana on luovuutta, innovaatioita, tilanneherkkyyttä, matala ja joustava organisaatiorakenne, verkostoituneisuus, yksilökohtai-

nen vapaus toimia ja rutiininomainen toiminta (Lanne 2007, 35- 36; Mäkinen 2005, 51). Oppivan organisaation piirteitä ovat myös:

1. Ulkoisen ympäristön, asiakkaiden, kilpailutilanteen seuranta ja tietojen keruu
2. Yhdessä tehty ja hyväksytty visio
3. Organisaatiokulttuuri ja dialogin taito
4. Sisäiset toimintatavat ja rakenteet
5. Systeemiajattelu
6. Henkilöstön osaamisen kehittäminen
7. Tiimioppiminen
8. Johtaminen
9. Palkitsemisjärjestelmät

(Levä 2003, 24- 25.)

Tavoitehakuinen yhteistyö ja henkilöstön jäsenten välinen vuorovaikutus mahdollistavat kokemusten, käsitysten, näkökulmien ja tietojen sekä taitojen jakamisen kautta tapahtuvan oppimisen. Tämänkaltainen oppiminen edesauttaa paremman organisaatioturvallisuuden tason saavuttamista ja ylläpitämistä. Oppimiseen vaikuttaa ympäristön muutokset, organisaatiorakenteen jäykkyys, strategian riittävyys ja turvallisuuskulttuurin vahvuus. Organisaation jatkuvan oppimisen etuina ja hyötyinä voidaan nähdä toiminnan joustavuuden lisääntyminen, organisaation parempi suoriutuminen, kestävämpi kehittyminen, luovuus sekä sidosryhmien tyytyväisyys. (Lanne 2007, 35, 79.)

Henkilöstön käyttäytymistä muuttamalla saadaan muutettu asenteita ja suhtautumista turvallisuustoimintaan liittyvien määräysten ja ohjeiden noudattamiseen. Toteuttamalla turvallisuusmääräykset ja – ohjeistot, riittävät resurssit, henkilöstön osallistamisen, vastuiden selkeyttämisen, turvallisuustoiminnan mittareiden luomisen sekä henkilöstön käyttäytymisperusteisen aktivoimisen, johto saa muutoksia aikaan. Järjestelmällisellä ja pitkäjänteisellä koulutuksella ja harjoittelulla saadaan aikaan uusien tietojen ja taitojen syntyminen. Jokaisen henkilön mahdollisuus jatkuvaan oppimiseen on myös yksi oppivan organisaation piirre. Jatkuva oppiminen käsittää kokonaisvaltaisesti yksilön kehittymisen ja oppimisen, jossa se esiintyy halukkuutena osallistua muutokseen, avoimena asenteena ja aktiivisena tiedonhakuna. (Simola 2005, 147, 222; Mäkinen 2005, 53.)

Erilaisiin tilanteisiin sopeutumisen lisäksi organisaatio muuttaa ja vaikuttaa myös ympäristöönsä. Johtajat tarvitsevat ajatuksia, käsitteitä ja viitekehyksiä organisaation kehittämiseksi ja uuden oppimisen katalysoimiseksi. Johto myös tarvitsee uusista ajatuksista tietoa, jotta se voi hyväksyä ne ja sitoutua niihin. Ideologinen ajattelu muuttuu oppimisen kautta johtamistaidoksi, jonka avulla organisaatio saa käynnistettyä positiivisen oppimisen. Asioiden eteen-

päin viemiseksi johon tärkeimpiä tehtäviä on yhteisten käsitteiden, arvojen ja periaatteiden edistäminen. (Levä 2003, 24, 65- 66.)

Johtajuudella on suuri merkitys varsinkin organisaatiomuutoksien aikana. Johtajuuteen liittyviä tärkeitä osia ovat johtajan ja alaisen tasapuolinen suhde, henkilökohtainen johtajuus sekä vuorovaikutus johtajan, alaisen ja asioiden välillä. Johtajuus organisaation muutoksessa voisi olettaa olevan lineaarista, vaikka se onkin ei- lineaarista johtamista. Kulttuuri vaikuttaa oppivan organisaation johtamistyyliin, kuten myös alaisten toiveet, tarpeet, arvot, uskomukset ja asenteet. (Mäkinen 2005, 53, 209.)

Johtajuus- termin käyttö johtamisen sijasta kuvaa organisaation oppimista. Johtajuus voidaan luokitella kolmeen ulottuvuuteen, jotka ovat syväjohtaminen, kontrolloiva ja korjaava johtajuus sekä passiivinen johtajuus. Syväjohtamisessa tärkeimmät osa- alueet syntyvät rakentamalla luottamusta ja luotettavuutta, inspiroivaa motivointia, älyllistä stimulointia sekä yksilöllistä harkintakykyä. (Mäkinen 2005, 171- 172.)

Organisaation yhteinen oppiminen tulee organisoida, jotta organisaatioturvallisuuden hallinta toimisi kaikilla organisaation tasoilla. Turvallisuustoiminta tulee liittää organisaation normaalin toiminnan johtamiseen ja jokapäiväiseen toimintaan, jotta se ei eriydy liikaa organisaation muusta johtamisesta ja perustehtävän toteutumisesta. Organisaatiossa toimivat sisäiset ja ulkoiset asiantuntijat tuovat erityistietoja ja – taitoja sekä osaamista turvallisuustoiminnan kehittämiseen, mutta loppujen lopuksi turvallisuuden merkityksen ymmärtäminen ja sisäistäminen koko organisaatiossa, ja erityisesti johtotasolla, ratkaisee turvallisuustoiminnan tason. (Lanne 2007, 85.)

Yhteenvetona voikin todeta, että muutoksen ja kehityksen perimmäinen kysymys on organisaatiossa toimivien henkilöiden oppiminen. Tässä korostuu nimenomaan se, että esimiehet kaikilla organisaation tasoilla ovat kriittisessä asemassa henkilöstön ja koko yhteisön kollektiivisen oppimisen ja osaamisen kehittäjinä ja tukijoina. Myös turvallisuuden osittaisen abstraktiuden takia organisaation paras tapa kehittää turvallisuustoimintaa on pitää koulutuksia, harjoituksia ja muita harjoitteita järjestelmällisesti vuosittain. Tämä vaatii kuitenkin sen, että organisaatiosta löytyy riittävästi tietoa ja taitoa turvallisuustoiminnan implementoinnista sekä verkostoitumista. (Simola 2005, 155; Mäkinen 2005, 198.)

4 KATAKRI turvallisuusjohtamisen välineenä

KATAKRI valmistui vuonna 2009 osana hallituksen sisäisen turvallisuuden ohjelmaa. Tarkoituksen oli luoda yhtenäinen turvallisuuskriteeristö yhteisöturvallisuusmenettelyn yhtenäistämiseksi sekä omavalvonnan ja auditoinnin kehittämiseksi. KATAKRI valmistettiin viranomaisten,

elinkeinoelämän ja turvallisuusalan toimijoiden yhteistyöllä. KATAKRI: n toinen versio julkaistiin vuonna 2011 ja siinä on paranneltu ensimmäisen version kriteeristöä ja kysymyksiä. (Kansallinen turvallisuusauditointikriteeristö 2011, 2.)

KATAKRI:n päätavoitteena on yhtenäistää viranomaistoimintoja silloin, kun viranomainen suorittaa yrityksessä tai muussa kohteessa kohteen turvallisuustason arvioinnin eli auditoinnin. Toisena päätavoitteena on auttaa yrityksiä ja muita yhteisöjä sekä viranomaisia sidosryhmineen parantamaan omaa sisäistä turvallisuustoimintaa. KATAKRI: ssä esitetyt kriteerit eivät saa olla perusteena sellaiselle toiminnalle, joka saattaa vahingoittaa ihmishenkiä. Esimerkiksi pelastustoimintaan liittyviä toimenpiteitä ei saa estää kriteeristön vaatimuksiin vedoten. (Kansallinen turvallisuusauditointikriteeristö 2011, 3.)

KATAKRI jakautuu neljään pääosioon, jotka ovat: hallinnollinen turvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus ja tietoturvallisuus. Viranomaisvaatimukset noudattavat jokaisessa osiossa kolmiportaista luokittelua, joka vastaa myös valtiohallinnon tietoturvallisuusasetusta. Luokittelun luokat ovat perustaso, korotettu taso ja korkea taso, joiden lisäksi ovat erilliset suositukset elinkeinoelämälle. (Kansallinen turvallisuusauditointikriteeristö 2011, 3.)

4.1 Auditointi

Turvallisuusauditointi on vuorovaikutteinen tapahtuma, jossa auditoija tutustuu auditoinnin kohteena olevan kohteen turvallisuusdokumentaation, jota kautta auditoija pyrkii selvittämään kohteen turvallisuuden tason, varsinkin hallinnollisen turvallisuuden osalta. Auditointiprosessin alkuvaiheessa auditoija tiedottaa selvistä puutteista kohteelle, jotta räikeimmät poikkeamat saadaan korjattua mahdollisimman pian. Yleensä pääauditoija kiertää auditointiryhmän kanssa tarkastettavat kohteet etukäteen tehdyn suunnitelman pohjalta ja kirjaa auditonnin tulokset joko täytettyinä vaatimuksina tai poikkeamine vaatimuksista. (Kansallinen turvallisuusauditointikriteeristö 2011, 4.)

Auditoinnista annetaan välitön suullinen palaute tuloksista. Kirjallinen raportti toimitetaan myöhemmin kohteelle mahdollisimman pian, jotta kohde pääsee korjaamaan poikkeamia. Auditointeja tehdään lisää tarpeen mukaan niin kauan, että vaatimukset täyttyvät. Auditoinnin yhteydessä on yleensä kohteen turvallisuudesta vastaavien henkiöiden kannattavaa kouluttaa henkilöstö ymmärtämään omat turvallisuusvastuunsa. (Kansallinen turvallisuusauditointikriteeristö 2011, 4.)

4.2 Hallinnollinen turvallisuus

KATAKRI: n hallinnollisen turvallisuuden osiossa tarkastellaan hallinnollista turvallisuustyötä turvallisuuden johtamisena. Turvallisuuden johtamista voidaan arvioida eri suojaustasoilla, joita ovat aikaisemmin mainitut perustaso, korotettu taso ja korkea taso. Näiden kolmen tason lisäksi kriteeristössä on myös elinkeinoelämän antamia omia suosituksia, joita voidaan myös käyttää turvallisuusjohtamisessa. Tarkoituksena käyttää korotettua tasoa vertailukohteena kohdeorganisaation turvallisuustyöhön, varsinkin suojattujen tilojen osalta. (Kansallinen turvallisuusauditointikriteeristö 2011, 7.)

4.3 KATAKRI kohdeorganisaatiossa

Geodeettisella laitoksella tavoitellaan KATAKRI: n korotettua tasoa suojattujen tilojen osalta, sillä tietyt projektit ja hankkeet vaativat sen tason tiettyjen tilojen osalta, jotta kohdeorganisaatio voi toimia yhteistyössä erinäisten sidosryhmien kanssa. Kohdeorganisaatiossa on käynnissä FSC- auditointi, jota kohdeorganisaatiossa on audioimassa toimivaltainen viranomainen. Auditointiprosessi jatkui säännöllisinä väliauditointeina koko kevään 2013 ajan ja tuloksena turvallisuusratkaisuja ja dokumentaatiota saatiin toteutettua aktiivisesti.

KATAKRI: n vaatimukset kohdeorganisaatiossa ovat nähtävillä turvallisuuskäsikirjassa sijoiteltuna niitä vastaaviin lukuihin. Auditoijat löytävät helposti tarvittavat kohdat turvallisuuskäsikirjasta ja se toimii näin ollen myös tarkastuslistana vaatimusten täyttämisen osalta. Tällä tavoin on myös tehty turvallisuuskäsikirjan liitteenä olevan soveltamissuunnitelman osalta, vaikkakin siinä esitettyjen vaatimusten perässä on viittaus käsikirjaan lukuun, jossa se esiintyy.

5 Kohdeorganisaation turvallisuustoiminta

Aloittaessani työharjoittelua kohdeorganisaatiossa tietoturvatasohankkeessa aloin tarkastelemaan ja havainnoimaan kohdeorganisaation turvallisuustoimintaa kokonaisuutena, jotta saisin selvän kuvan siitä taustatiedoksi. Kävi ilmi, että kohdeorganisaatiolla ei ole suoranaista turvallisuusorganisaatiota, joka hoitaisi ja ylläpitäisi kokonaisvaltaisesti turvallisuustoimintaa. Turvallisuuteen liittyvät roolit ja tehtävät olivat merkittynä kohdeorganisaation työjärjestyksessä tai muuten vastuutettu niin sanotusti oman toiminnan ohella - menettelyn mukaisesti.

Haastattelin (Geodeettisen laitoksen turvallisuus- ja tietohallintopäällikkö 2013) kohdeorganisaation turvallisuus- ja tietohallintopäällikköä turvallisuustoiminnan ja turvallisuusjohtamisen osalta. Haastattelun perusteella pyrin saamaan paremman kuvan turvallisuustoiminnan kehittämisen lähtökohdista sekä silloisesta nykytilasta kohdeorganisaation turvallisuusjohtamisessa

ja – toiminnassa. Haastattelun tuloksista kerron tarkemmin seuraavissa luvuissa, jotka toimivat myös teemahaastatteluni teemoina alkukatselmusta lukuun ottamatta.

5.1 Alkukatselmus

Alkukatselmuksessa kerätään tietoa missä ollaan menossa, jotta ymmärretään organisaatiota kohtaavat ongelmat ja mahdollisuudet sekä sen hetkinen turvallisuustoiminnan taso. Keskeisimpien uhkien ja vaarojen selvittäminen on myös olennaista tässä vaiheessa. Esille nousseista asioista tulee keskustella johdon ja muun organisaation kesken sekä päättää alkukatselmuksen tulosten perusteella jatkotoimenpiteistä. Tämä on tärkeimpiä vaiheita organisaation kehittämisessä, sillä siinä valitaan sopivin malli organisaation ymmärtämiselle ja analysoinnille. Tässä vaiheessa annetaan myös palautetta yrityksen johdolle ja muulle henkilöstölle ongelmista ja mahdollisuuksista. Määrittelyvaiheessa tärkeintä onkin tiedon keräys ja sen analysointi sekä palautteen antaminen. Esimerkiksi haastattelut ovat hyvä tapa kerätä tietoa eri henkilöiltä tai kohderyhmiltä, jotka kannattaa valita organisaation eri tasoilta. (Kerko 2001, 40; Simola 2005, 150- 151; OHSAS 18002, 26, 28, 56.)

Haastattelin (Geodeettisen laitoksen turvallisuus- ja tietohallintopäällikkö 2013) alkukatselmuksessa kohdeorganisaation turvallisuus- ja tietohallintopäällikköä. Ylijohtajaa en päässyt erinäisistä syistä haastattelemaan, joten ylimmän johon näkemys turvallisuustoimintaan jäi puuttumaan tästä työstä. Haastattelu oli aikaisemmin kuvattuun tapaan avoin teemahaastattelu, jossa pyrin keskustelemaan avoimemmin henkilön kanssa turvallisuustoimintaan liittyvistä asioista. Itselleni olin laatinut kysymysrungon teemoittain, jotta keskustelu ohjautuisi loogisesti teemojen sisällä ja teemasta toiseen.

5.2 Turvallisuuskulttuuri

Haastattelun aluksi kysyin, minkälainen turvallisuuskulttuuri kohdeorganisaatiossa on ja kävi ilmi, että kohdeorganisaatiossa on melko vapaa ympäristö turvallisuuden suhteen. Tutkimustoiminnasta johtuen, turvallisuuskulttuuri on samankaltainen kuin esimerkiksi yliopistoilla. Kokonaisvaltainen turvallisuustoiminta lähti käyntiin vasta vuonna 2012, jolloin kohdeorganisaatio alkoi rakennuttamaan turvallisuusluokiteltuja tiloja projektien ja hankkeiden takia. Aikaisemmin kukaan ei ollut suoranaisesti vastuussa turvallisuustoiminnasta, vaikka nykyistä ylijohtajaa edeltävä ylijohtaja ja projektipäälliköt sitä hoitivat oman toimen ohella.

Turvallisuus- ja tietohallintopäällikkö aloitti työskentelyn kohdeorganisaatiossa 2008 ja siitä lähtien hänellä on ollut vastuu tietoturvallisuudesta vahvasti, sillä se on olennainen osa tietohallintopäällikön tehtäviä. 2012 hän otti edellä mainittujen turvatilojen osalta vastuuta ja

alkoi hoitamaan muitakin organisaatioturvallisuuden osa- alueita oman toimen ohella. Tästä lähti myös kokonaisvaltainen turvallisuustoiminnan kehittäminen.

5.3 Turvallisuusjohtaminen ja turvallisuustoiminta

Turvallisuusjohtaminen lähti myös pyörimään kokonaisvaltaisemmin vuonna 2012 projektien ohella. Aikaisemmin vastuu oli ollut kohdeorganisaation ylijohtajalla, mutta 2012 tietohallintopäällikkö otti tehtäväkseen alkaa johtamaan turvallisuustoimintaa. Tehtävä on ollut kuitenkin haasteellinen ja esimerkiksi riskienhallinta ei ole kovin kattavaa, vaikka sitä on säännöllisesti tehty vuosittain. Uusittu riskienhallintapolitiikka auttaa tässä tapauksessa asiaa ja uudet käytänteet otetaan käyttöön kevään 2013 aikana.

Kokonaisvaltainen turvallisuusjohtaminen on ollut tietohallintopäällikölle haastavaa, sillä hänellä on paras osaaminen tietotekniikassa ja sen myötä pääasiallisesti tietoturvallisuudessa. Resurssien puute on vaikeuttanut turvallisuustoiminnan kehittämistä ja hidastanut parannustoimenpiteiden toteutusta. Kehitystä on kuitenkin tapahtunut ja tietohallintopäällikkö on työtehtäviä tehdessään oppinut paljon kokonaisvaltaisesta turvallisuusasioiden hoitamisesta. Myös nykyinen ylijohtaja on ottanut turvallisuusasiat paremmin huomioon kuin edellinen ylijohtaja.

Turvallisuustoiminta kokonaisuutena on ollut kohdeorganisaatiossa pienimuotoista, pois lukien erilaiset hankkeet ja projektit. Turvallisuuteen ei ole nähty tarpeellista kehittää johtamisjärjestelmää, sillä kohdeorganisaatio on pieni organisaatio. Kuten aikaisemmin mainittu, turvallisuustoiminnan resurssit ovat rajalliset, vaikka kohdeorganisaatiossa on käynnissä FSC- sertifiointi ja esimerkiksi hankkeiden osalta Galileo- hanke (Geodeettinen laitos 2013b) asettaa vaatimuksia turvallisuustoiminnan parantamiseksi. Myös tulosohjaus turvallisuustoiminnan tueksi olisi tarpeellista tietohallintopäällikön mukaan.

5.3.1 Seuranta ja arviointi

Turvallisuustoimintaa ja sen kehittymistä ei seurata systemaattisesti, joten sen seuraamiseen ei ole asetettu mitään mittareita. Turvallisuustoimintaa kuitenkin arvioidaan edellä mainittujen FSC- sertifioinnin ja hankkeiden osalta, joista on kevään 2013 aikana ollut käynnissä auditointiprosessi toimivaltaisen viranomaisen toimesta. Kohdeorganisaatiossa ei ole myöskään tapahtunut suurempia onnettomuuksia tai muita vakavia poikkeamatilanteita. Kevään 2013 aikana kehitteillä oli menettelyt poikkeamatilanteiden ja niiden raportoinnin osalta.

5.3.2 Raportointi

Turvallisuusasioista on raportoitu johdolle säännöllisesti aina, vaikka turvallisuustoiminta ei aikaisemmin ole johdettu kokonaisvaltaisesti. Turvallisuuspoikkeamista ja niiden raportoinnista oli kevään 2013 aikana kehitteillä toimintaperiaatteet, jonka jälkeen raportointia tapahtuu koko organisaation laajuudella. Poikkeamatilanneraportointi kattaa koko turvallisuustoiminnan työtapaturmista tietoturvaloukkauksiin.

5.4 Turvallisuusryhmä

Turvallisuutta ei siis aikaisemmin ole organisoitu sen tarkemmin, vaan ylijohtaja ja projektipäälliköt vastasivat turvallisuudesta. Suojelupäällikkö on kuitenkin ollut pitkään kohdeorganisaatiossa ennen vuotta 2012. Tietohallintopäällikkö sai 2012 tietoturvallisuuden hoitamisen lisäksi vastuulleen kokonaisturvallisuuden kehittämisen ja projektipäälliköt ovat edelleen projektikohtaisessa turvallisuustoiminnassa mukana. Turvallisuusryhmälle on ollut tarvetta, sillä turvallisuustoiminta on haluttu kohdeorganisaatiossa vastuuttaa tietyille tahoille ja näin saada selvä turvallisuusorganisaatio kohdeorganisaatioon. Nykyisellään turvallisuusryhmään kuuluu tietohallintopäällikkö turvallisuuspäällikkönä ja hänen kanssaan siinä on suojelupäällikkö. Laajempaan turvallisuusfoorumiin tarvittaessa osallistuvat kohdeorganisaation luottamusmiehet, työsuojelupäällikkö sekä työsuojeluvaltuutettu.

5.5 Turvallisuusdokumentaatio

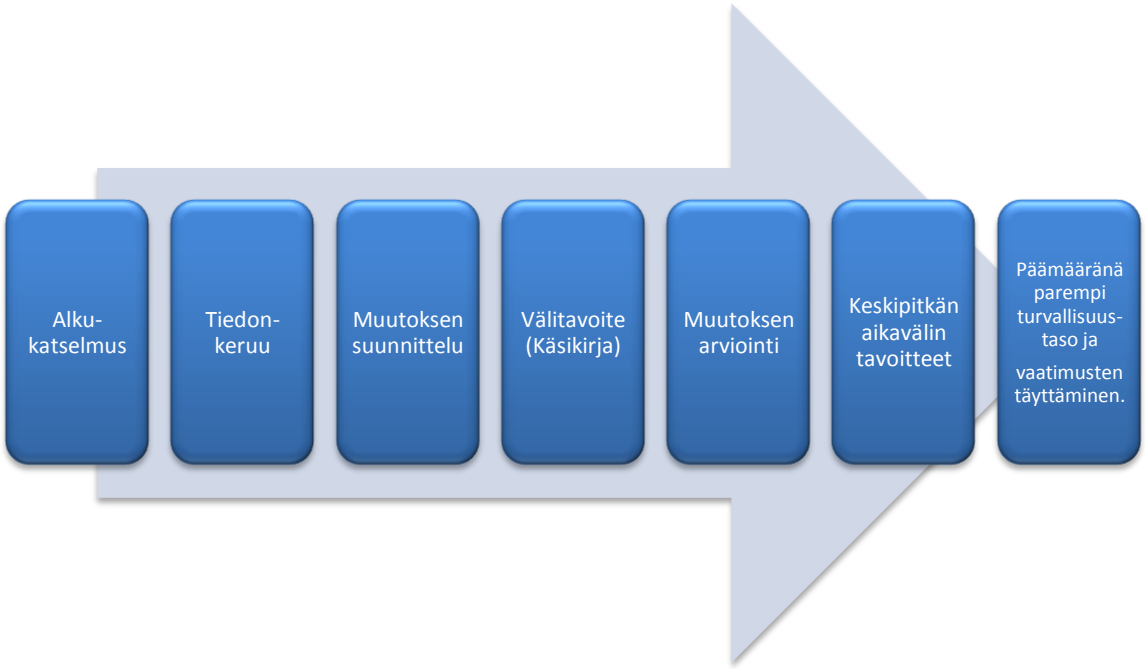
Turvallisuusdokumentaation osalta lakisääteiset asiat ovat hyvällä mallilla ja esimerkiksi pelastussuunnitelma ja työsuojelun toimintaohjelma ovat ajan tasalla. Dokumentaatio itsessään on kuitenkin ollut vaikeasti saatavilla Intranetissä ja paperilla tai ei ole löytynyt ollenkaan jostain syystä. Tästä johtuen kevään 2013 aikana oli tarkoitus kerätä tätä dokumentaatiota eri paikoista samaan paikkaan, tekemääni turvallisuuskäsikirjaan. Dokumentaation keräämisessä oli omat haasteensa sen levinneisyyden takia, sillä kohdeorganisaation henkilötkään eivät oikein tienneet, missä kaikkialla mitäkin on. Seuraavassa alaluvussa tarkastelen tarkemmin opinnäytetyön työprosessia ja sen etenemistä kohdeorganisaatiossa.

5.6 Opinnäytetyön työprosessi kohdeorganisaatiossa

Opinnäytetyöprosessi alkoi jo 2012 syksyn aikana, jotta aikaa ei kuluisi aiheen etsimiseen enää kevään 2013 aikana. Työskentelemään aloin heti opinnäytetyöopintojakson aloituksen jälkeen opinnäytetyön parissa ja produktia aloin tekemään ennen opinnäytetyön aiheen lopullista valintaa. Pääsin myös alustavan suunnitelman mukaan työstämään opinnäytetyön doku-

mentteja ennen orientaatiota. Orientaatioseminaarissa sain lopullisen vahvistuksen aiheelleni ja pääsin aloittamaan työskentelyn opinnäytetyön parissa aktiivisesti.

Työprosessin (kuvio 4) aikana tarkoituksena oli, kuten aikaisemmin todettu, kehittää kohdeorganisaation turvallisuustoimintaa. Kehittämisprosessin tavoitteena oli luoda kohdeorganisaatioon turvallisuuskäsikirja, joka oli välitavoite kohdeorganisaation turvallisuustoiminnan kehittämisessä kevään 2013 aikana. Kohdeorganisaation tulee arvioida tämän opinnäytetyöprosessin ja työharjoittelun aikana ja jälkeen tapahtuneita muutoksia turvallisuustoiminnassa ja jatkaa sen parantamista itsenäisesti. Asetettuaan välitavoitteita ja saavutettuaan ne, kohdeorganisaation päämääränä on kokonaisvaltaisesti parempi turvallisuustaso ja eri turvallisuusvaatimusten täyttäminen ja niiden todentaminen.



Kuvio 3: Turvallisuuden kehittämisen prosessi (Sovellettu Simolan (2005, 158) mallista)

Työprosessin (kuvio 4) olisi pitänyt alkaa alkukatselmuksella (luku 5.1) välittömästi työharjoittelun alussa, mutta opinnäytetyön aiheen valinnan ollessa kesken se lykkäytyi myöhempään ajankohtaan. Alkukatselmus saatiin tehtyä ja siinä haastattelin kohdeorganisaation turvallisuus- ja tietohallintopäällikköä. Alkukatselmus oli osa tiedonkeruuta kohdeorganisaatiosta ja muista lähteistä. Tiedonkeruun aikana tein dokumenttianalyysiä kohdeorganisaation olemassa olevasta turvallisuusdokumentaatiosta ja aloin luomaan tietoperustaa opinnäytetyöhön. Tässä vaiheessa alkoi myös turvallisuuskäsikirjan suunnittelu ja miten se kehittäisi kohdeorganisaation turvallisuustoimintaa.

Välitavoitteen eli turvallisuuskäsikirjan tuottaminen alkoi tammikuun lopulla ja sen julkisuuden osalta oli paljon miettimistä. Aluksi tarkoituksena oli perehdyttää se koko henkilöstölle kohdeorganisaation turvallisuusryhmän lisäksi, joten olisi pitänyt laatia perehdytyssuunnitelma. Sain työn alkupuolella palautetta käsikirjan julkisuudesta ja perehdyttämisestä, josta kävi ilmi, että käsikirjan olisi hyvä olla vain kohdeorganisaation turvallisuusryhmän käytössä, joten rajasin perehdytyksen pois. Kuitenkin auditointiprosessin aikana toimivaltainen viranomainen totesi, että käsikirjan tulisi nimenomaan olla julkinen asiakirja. Myöhäisestä ajankohdasta johtuen en sisällytä perehdytyssuunnitelmaa tai – koulutusta tähän työhön. Myös turvallisuusdokumentaation laajuuden ja opinnäytetyön julkisuuden takia liitteenä olevassa turvallisuuskäsikirjassa on sisältönä turvallisuusasioita vain yleisellä tasolla ja esimerkkiliitteinä vain julkisia dokumentteja, kuten turvallisuuspolitiikka.

Opinnäytetyön nimi vaihtui noin puolessa välissä työprosessia ja työ keskittyi tarkemmin turvallisuusjohtamiseen ja turvallisuustoiminnan kehittämiseen. Helmi- ja maaliskuu menivät pitkälti tietoperustan luomisessa ja turvallisuuskäsikirjan rakenteen ja sisällön tuottamisessa sekä KATAKRI: n vaatimusten merkitsemisessä käsikirjaan auditointiprosessin edetessä. Kohdeorganisaatiossa edenneen auditointirposessin aikana sain toimivaltaiselta viranomaiselta ja muilta tahoilta palautetta turvallisuuskäsikirjan rakenteesta ja sisällöstä, joita sitten muutin palautteen mukaisesti.

Huhtikuu meni opinnäytetyön raportin ja turvallisuuskäsikirjan viimeistelyssä arvioitavaan kuntoon. Palautteen saaminen eri tahoilta jäi viime hetkeen, vaikka olin ollut ajoissa ja aktiivisesti yhteydessä näihin tahoihin arvioinnin tiimoilta, jotta saisin luotettavuutta opinnäytetyön tuloksien arviointiin. Sain kuitenkin huhtikuun lopulla hyvää ja rakentavaa palautetta Kirsi Janhuselta valtiovarainministeriöstä, Matti Aitalta ja Erja Kinnuselta valtiokonttorilta, toimivaltaiselta viranomaiselta sekä tietenkin kohdeorganisaation tietohallinto- ja turvallisuuspäälliköltä ja ylijohtajan sijaiselta. Saamaani palautetta käsittelen tarkemmin luvussa 7. Seuraavassa luvussa tarkastelen tarkemmin itse turvallisuuskäsikirjan toteutusta.

6 Turvallisuuskäsikirjan toteutus

Opinnäytetyön produktina syntyi turvallisuuskäsikirja (liite 1), jonka tarkoituksena on tukea geodeettisen laitoksen turvallisuusjohtamista ja turvallisuustoimintaa. Turvallisuuskäsikirjassa on kuvattuna kohdeorganisaation nykyinen tila turvallisuustoiminnassa ja siihen kootaan kaikki tarvittava ja olemassa oleva turvallisuusdokumentaatio. Käsikirjaan laitetaan myös linkitys henkilöstön ohjeistuksiin, jotka sijoitetaan geodeettisen laitoksen Intranetiin. Tämän opinnäytetyön liitteenä olevassa turvallisuuskäsikirjassa on esimerkkinä liitettynä vain turvallisuuspolitiikka, riskienhallintapolitiikka ja tietoturvapolitiikka, sillä kaiken dokumentaation liittäminen tai linkittäminen ei ole mahdollista tai julkista.

Turvallisuuskäsikirjan tarkoituksena on olla kohdeorganisaatiolle työkalu ja tukidokumentti, johon organisaatio, erityisesti turvallisuusryhmä (liite 1, 2.2), voi lisätä ja päivittää uutta sekä vanhaa dokumentaatiota. Kohdeorganisaatio pystyy osoittamaan turvallisuuskäsikirjan avulla täyttävänsä eri tahojen vaatimukset turvallisuustoiminnan osalta, joten käsikirja helpottaa kohdeorganisaation ja turvallisuusryhmän työskentelyä sidosryhmien kanssa työskennellessä, varsinkin turvallisuustoiminnan päivittämisen tullessa ajankohtaiseksi.

Eri organisaatioilla on erilainen painopiste organisaatioturvallisuuden osa- alueissa toimialan mukaan ja tässä tapauksessa turvallisuuskäsikirja on rakennettu kohdeorganisaation tarpeiden mukaisesti. Käsikirjan rakenteessa on otettu huomioon lähtökohtaisesti KATAKRI, sillä geodeettisella laitoksella sillä on ollut suurin vaikutus turvallisuustoiminnan kehittämisessä. Seuraavissa luvuissa tarkastelen turvallisuuskäsikirjan toteutukseen vaikuttaneita tekijöitä.

6.1 Hyvyyskriteerit

Opinnäytetyössä tuotettavana produktin, tässä tapauksessa turvallisuuskäsikirjan, hyvyyden osalta tulee asettaa jonkinlaiset kriteerit. Arvioinnin kohteena on ensin työn tarkoitus, kuten idean tai ongelman kuvaus tai ratkaisu. Opinnäytetyötä lukevan tulee ymmärtää, mitkä työssä on tehty ja millaiset tavoitteet. Tavoitteiden saavuttamisen arviointi on tärkein osa työtä. (Vilkka & Airaksinen 2003, 154- 155.)

Kokonaisuutena turvallisuuskäsikirjan hyvyyttä voidaan tarkastella sillä, että täyttääkö se KATAKRI: n ja sidosryhmien asettamat vaatimukset ja löytyykö sieltä tarvittavat tiedot ja dokumentaatio turvallisuustoiminnan osalta. Asiantuntijoiden kommenttien ja arvioinnin sekä käsillä olleen materiaalin pohjalta sain tietoa, minkälainen sen tulisi olla ja näiden pohjalta sain luotua kattavan sisällön ja rakenteen käsikirjalle. Myös kohdeorganisaation vaatimukset tuli ottaa huomioon käsikirjan rakenteessa ja miten helppokäyttöinen se on kohdeorganisaation ja sen turvallisuusryhmän apuna. Turvallisuuskäsikirjan hyödyllisyydestä keräsin palautetta (luku 7) eri tahoilta, jotta kykenin arvioimaan tämänkaltaisen tuotoksen soveltuvuutta muualla ja käytännöllisyyttä sekä hyvyyttä turvallisuustoiminnan parantamisessa organisaatiossa, jossa ollaan opettelemassa kokonaisvaltaisempaa turvallisuuden hallintaa.

Turvallisuuskäsikirjan tarve oli ajankohtainen, sillä kohdeorganisaatiossa on meneillään aikaisemmin mainitut tietoturvatasohanke, FSC- auditointi sekä projekteja ja hankkeita, jotka asettavat vaatimuksia turvallisuustoiminnan parantamiselle ja turvallisuusdokumentaation löytymiselle. Näin ollen turvallisuusdokumentaation kokoava käsikirja oli tarpeellinen. Turvallisuuskäsikirjan sisältö on käyty läpi kohdeorganisaation turvallisuuspäällikön kanssa, joten se on sisällöltään paikkansa pitävä sekä se tehdään ymmärrettäväksi myös henkilöstölle. Käsikir-

ja tullaan perehdyttämään henkilöstölle, joten turvallisuusasioista vähemmän tietävän tulee kyetä ymmärtämään käsikirjassa olevat asiat. Turvallisuuskäsikirja on helposti saatavilla koko henkilöstölle Intranetissä, joten jokainen pystyy myös itsenäisesti tutustumaan käsikirjan sisältöön ja kertaamaan sitä perehdytyksen jälkeen.

Turvallisuuskäsikirjasta ja siihen liitettävien asiakirjojen hallinnasta ja ylläpitämisestä vastaa pääasiallisesti turvallisuusryhmä (liite 1, 2.2). Turvallisuusryhmä laatii dokumentaatiota ja hyväksyttää sen kohdeorganisaation ylimmällä johdolla, jotta saadaan hyväksyntä niiden julkaisemiselle ja toteuttamiselle. Kevään 2013 aikana laadittujen dokumenttien soveltuvuuden arviointiin osallistui muun muassa auditointien osalta toimivaltainen viranomainen, joka voi todeta myös jatkossa asiakirjat vaatimusten mukaisiksi. Tulevaisuudessa turvallisuuspäällikön olisi hyvä saada koulutusta, että hän kykenee arvioimaan turvallisuusasiakirjojen kattavuutta ja hyvyyttä ennen niiden esittämistä ylimmälle johdolle julkaisemista varten.

6.2 Turvallisuuskäsikirjan rakentaminen

Turvallisuuskäsikirjan rakentamien alkoi tiedon, tarpeiden ja vaatimusten kasaamisella ja miten nämä saataisiin koottua samaan paikkaan. Tietoturvatasohankkeen työkalupakissa oli Kirsi Janhusen tekemä tietoturvallisuuskäsikirjamalli, josta sain alustavan rungon tietoturvallisuuden osalta. Tästä lähdin lisäämään sidosryhmien vaatimuksia otsikkotasolla, jonka jälkeen tarkastelin, miten KATAKRI: n osa- alueet ja muut vaatimukset näkyivät siinä vaiheessa olevassa turvallisuuskäsikirjassa ja lisäsin puuttuvia asioita otsikkotasolla.

Tämän jälkeen käsikirjan rakenne tuli muokata ymmärrettäväksi ja loogisesti eteneväksi. Alla (kuvio 3) on kuvattuna turvallisuuskäsikirjan rakentamisprosessin eri vaiheet. Tietoperustan rakentamisen jälkeen alkoi turvallisuuskäsikirjan luominen, johon kului eniten aikaa prosessissa. Arvioinnin saaminen kaikilta tahoilta oli haastavaa, mutta sain tarpeeksi palautetta tuloksien arvioinnin osalta. Lopuksi tuloksissa tarkasteltiin ilmenneitä johtopäätöksiä ja miten turvallisuuskäsikirja ja työprosessi ovat auttaneet kohdeorganisaatiota.

Kuvio 4: Turvallisuuskäsikirjan rakentamisprosessi

Turvallisuuskäsikirjan rakenne etenee (1) hallinnollisesta turvallisuudesta (2) Tieto- ja tietoaineistoturvallisuuteen, siitä (3) toimitilaturvallisuuteen ja (4) henkilöstöturvallisuuteen, joiden jälkeen on (5) riskien- ja jatkuvuuden hallintaa sekä (6) itse dokumentaatiota. Turvallisuuskäsikirjan lopussa on liitteinä esimerkkinä kohdeorganisaation turvallisuus-, riskienhallinta- ja tietoturvapolitiikka kuvaamassa millä tavalla loputkin dokumentit liitetään käsikirjaan.

Tiedon hankinta turvallisuuskäsikirjaan kohdeorganisaatiosta ja muualta oli opettavaista, mutta joissain tapauksissa myös haastavaa. Esimerkiksi auditointeja ajatellen tiedon etsiminen oli ammatillisesti rakentavaa, sillä jokaisessa auditoinnissa joutuu etsimään olemassa olevasta materiaalista oikeat dokumentit, jotta auditoinnin viitekehyksessä esitetyt vaatimukset pystytään täyttämään ja osoittamaan toteen. Turvallisuuskäsikirjan luomisessa onkin pyritty helppokäyttöisyyteen, jotta dokumentaatio löytyisi aina vaivattomasti.

Turvallisuuskäsikirjaa ei siis ole tarvinnut luoda tyhjästä, vaan se on voitu rakentaa kohdeorganisaatiolle yhdistämällä ja soveltamalla eri tahoilta saatuja tietoja samaan pakettiin. Tällä tavoin on pystytty minimoimaan ylimääräisten ja erillisten dokumenttien syntyminen ja hajaantuminen eri puolille. Näin voitiin myös välttää niin sanottu pyörän uudelleen keksiminen ja säästin paljon aikaa käyttämällä olemassa olevaa materiaalia.

6.3 Sidosryhmien vaatimukset

Organisaation toimialasta riippuen sillä saattaa olla sidosryhmiä, jotka esittävät vaatimuksia turvallisuustoiminnan ylläpitämiseksi tai parantamiseksi. Tämä saattaa joissain tapauksissa aiheuttaa melko suuriakin kustannuksia, sillä varautumaton organisaatio joutuu esimerkiksi hankkimaan uutta turvallisuustekniikkaa ja mahdollisesti myös muuttamaan toimitilojensa rakenteita vaatimusten mukaisiksi.

Kohdeorganisaatiossa on tehty vuodesta 2012 lähtien paljonkin muutoksia turvallisuusratkaisujen osalta aikaisempaan verrattuna. Erilaiset projektit ja hankkeet ovat asettaneet melko suuriakin investointivaatimuksia kohdeorganisaatiolle turvallisuustoiminnan parantamiseksi. Sidosryhmiltä tulleiden vaatimusten osalta turvallisuuskäsikirjan rakennetta muokattiin, jotta ne saatiin sisällettyä siihen. Turvallisuuskäsikirjasta löytyy tiedot, miten eri vaatimukset ja turvallisuusratkaisut on toteutettu kohdeorganisaatiossa, varsinkin turvaluokiteltujen tilojen osalta.

6.4 Turvallisuusdokumentaatio

Turvallisuusdokumentaatio tulisi arkistoida aina samaan paikkaan, osaksi laajempaa kokonaisuutta, kuten turvallisuusjärjestelmäarkistoon. Onnistunut dokumentaatio hyödyttää organi-

saatiota, sillä se edesauttaa ja ylläpitää turvallisuustoiminnan toimivuutta. Dokumentaation suunnittelussa on otettava huomioon myös viranomaistarpeet, jotta vaadittavat dokumentit löytyvät vaivattomasti. (Kerko 2001, 86.)

Turvallisuuskäsikirjan tarkoituksena on toimia turvallisuusdokumentaatiota kokoavana asiakirjana, jotta kaikki dokumentit löytyisivät samasta paikasta vaivattomasti. Kun aloitin työharjoittelun, niin suuri osa turvallisuusdokumentaatiosta oli hajallaan joko paperilla jossain tai Intranetissä eri paikoissa taikka tietokoneen syövereissä. Näiden kerääminen käsikirjaan oli melko työlästä, mutta nyt kun suurin osa dokumentaatiota on samassa paikassa, niin jatkossa dokumenttien lisääminen ja päivittäminen on helppoa.

7 Arviointi ja palaute

Pyysin arviointia työstäni koko työprosessin ajan, jotta etenin oikeaan suuntaan työssäni. Pääasialliset työn arvioijat olivat kohdeorganisaation esimieheni, opinnäytetyötä ohjaava opettaja sekä muut työelämän edustajat, kuten työharjoittelun puolesta valtiokonttorin IT-palvelukeskuksen asiantuntijat, tietoturvakäsikirjan tekijä Kirsi Janhunen valtiovarainministeriöstä sekä toimivaltainen viranomainen.

Kuten aikaisemmin mainitsin, niin sain palautetta käsikirjasta melko myöhään lähellä palautusta, joten sen osalta tuli kiire saada lisättyä sekä palaute että palautteessa esiintyneet parannukset käsikirjaan ennen työn palautusta. Arviointi ja palaute olivat kuitenkin tärkeä saada, jotta sain parannettua sekä oman opinnäytetyöni sisältöä ja kohdeorganisaation menevää turvallisuuskäsikirjaa. Palautteessa nousi esille paljon asioita, joita turvallisuuskäsikirjan laatimisen aikana ei osannut omilla tiedoilla ja taidoilla tarkastella. Seuraavissa luvuissa tarkastelen turvallisuuskäsikirjan soveltuvuutta muualla ja miten saavutin tavoitteet.

7.1 Turvallisuuskäsikirjan sovellettavuus

Opinnäytetyön tuloksena syntynyt turvallisuuskäsikirja luotiin tietoperustassa käytettyjen tutkimusten tulosten, tietoturvatasohankkeen työkalujen, KATAKRI: n viitekehyksen, sidosryhmien vaatimusten sekä saadun palautteen pohjalta. Vaikka turvallisuuskäsikirja luotiin kohdeorganisaation vaatimuksia ajatellen, niin sitä voidaan soveltaa rakenteen osalta myös muissa organisaatioissa, sillä sitä voidaan muokata erilaisten organisaatioiden tarpeiden ja toiminnan mukaiseksi. Otsikkotasolla turvallisuuskäsikirja on sopivan yleinen ja kuitenkin kattava, joten se on sovellettavissa hyvinkin erilaisiin kohteisiin. Turvallisuuskäsikirjan käytännön testaaminen tapahtui pitkälti auditointiprosessin aikana, jossa viitekehyksenä toimi KATAKRI.

Janhuselta (valtiovarainministeriö) saadun palautteen mukaan turvallisuuskäsikirjaa voidaan soveltaa hyvin, sillä siihen on liitettynä KATAKRI:n ja soveltamissuunnitelman (VAHTI) vaatimustaulukot. Näin ollen jossain toisessa organisaatiossa käsikirjaa voidaan tarkastella esimerkkinä, miten turvallisuusratkaisut vaatimusten suhteen voidaan käytännössä toteuttaa. Liitteinä olevien taulukoiden avulla myös auditoijat löytävät helposti kohdat turvallisuuskäsikirjasta, jossa otetaan kantaa tarkasteltavana olevaan vaatimukseen. Myös Aitan (valtiokonttori) mukaan käsikirjaa voi hyödyntää varsinkin turvallisuustoiminnan kehittämisessä hyvin alkuvaiheessa olevissa organisaatioissa, sillä se voisi toimia niin sanotusti tsekkilistana turvallisuusasioiden tarkastelussa. Seuraavassa luvussa tarkastelen asetettujen tavoitteiden saavuttamista ja täyttyivätkö ne raportin ja produktin osalta.

7.2 Tavoitteiden saavuttaminen ja työprosessin arviointi

Opinnäytetyöni tarkoituksena oli kehittää yhteistyökumppanin turvallisuustoimintaa ja tavoitteena oli luoda turvallisuustoiminnan tueksi turvallisuuskäsikirja. Tavoitteena olleen turvallisuuskäsikirjan luominen onnistui kohtalaisen hyvin, vaikka aikataulu olikin melko tiukka. Toimin tiiviissä yhteistyössä kohdeorganisaation ja eri tahojen kanssa, ja heidän asettamat vaatimukset ja ehdotukset saatiin sisällettyä turvallisuuskäsikirjaan. Kohdeorganisaation ylijohtajan sijainen hyväksyy turvallisuuskäsikirjan 06.05.2013 ja se otetaan saman tien käyttöön, sillä erinäiset projektit ja auditointi vaativat dokumentaation toteen osoittamista ennen kesää.

Alkukatselmuksessa olisi voinut tehdä kyselyn henkilöstölle turvallisuustoiminnan tasosta heti alkuun, että olisi saanut myös heidän mielipiteensä turvallisuustoiminnasta. Alkukatselmus olisi pitänyt tehdä myös heti työharjoittelun alkuvaiheessa, mutta opinnäytetyön aiheen puuttumisen ja muiden kiireiden takia se lykkääntyi pidemmälle kevääseen ja lähtötilannetta piti tarkastella takautuvasti. Turvallisuuspäällikön haastattelun perusteella sain kuitenkin hyvän tietopohjan turvallisuustoiminnan kehittymisestä vuodesta 2012 nykyiseen hetkeen.

Oman työprosessin tarkastelun ja kerätyn palautteen perusteella lopputuloksena syntynyt turvallisuuskäsikirja onnistui kohtalaisen hyvin. Turvallisuuskäsikirja täytti sille asetetut hyvyyskriteerit, jotka sille oli asetettu, joten siltä osin tavoite saavutettiin. Opinnäytetyön rajauksen osalta turvallisuuskäsikirjan sisältöä saattaisi pitää suppeana, mutta turvallisuuskäsikirjaa voidaan soveltaa otsikkotasolla myös muissa organisaatioissa, sillä siitä voi poistaa tai lisätä halunsa ja toiminnan mukaan organisaatioturvallisuuden osa- alueita.

Turvallisuuskäsikirja itsessään ei ole mikään lopullinen ja viimeistelty tuotos, vaan tästä eteenpäin kohdeorganisaation turvallisuusryhmän vastuulla on päivittää käsikirjaa. Tästä johtuen käsikirjan sisältöä ei ole täysin viimeistelty opinnäytetyöni liitteenä olevassa versiossa,

joka saattaa vaikuttaa sen hyvyyden arviointiin. Käsikirjan perehdyttäminen henkilöstölle jäi turvallisuusryhmän tehtäväksi ja tästä eteenpäin kohdeorganisaation tulee seurata ja arvioida säännöllisesti käsikirjan päivittämisen tarvetta.

Loppujen lopuksi aikataulun kireyden ja muiden haasteiden osalta onnistuin kokonaisvaltaisesti opinnäytetyössäni hyvin. Käytetyt menetelmät tukivat opinnäytetyöprosessia ja tietoperustana ollut aineisto tuki turvallisuuskäsikirjan luomista ja kohdeorganisaation turvallisuustoiminnan tarkastelua ja kehittämistä. Turvallisuuskäsikirjan tekeminen olisi ollut melko haastavaa ilman käsillä olleita laadukkaita työkaluja ja malleja, joita pääsin käyttämään ja soveltamaan. KATAKRI: n tarkastelu jäi melko vähäiseksi tässä raportista, mutta sen käsittely oli tarkempaa työharjoittelun ja auditoinnin puolella.

8 Pohdinta

Joskus turvallisuustoiminnan kehittämisen lähtötilanteessa olosuhteet pakottavat jonkun henkilön tai ryhmän alkamaan suorittamaan turvallisuustoiminnan hoitamista ja kehittämistä, vaikka kyseisellä henkilöllä tai ryhmällä ei olisi aikaisempaa kokemusta tai koulutusta asiasta. Tämä saattaa johtua pääasiallisesti säästämisen halusta, sillä aina ei ole resursseja tai halukkuutta palkata täysin uutta, mutta osaavaa henkilöä palvelukseen, varsinkaan jos työtehtävää tai toimintaa ei nähdä tarpeellisena tai joku nykyinen henkilö tai ryhmä voi hoitaa sen myös oman toimen ohella. Turvallisuustoiminnan kehittämisen ja organisaation oppimisen kannalta tämä ei ole kuitenkaan aina paras vaihtoehto.

Opinnäytetyössä käytetyn tietoperustan perusteella turvallisuustoiminnan johtaminen vaatii organisoidumpaa toimintaa, sillä esimerkiksi lainsäädännön asettamien vaatimusten täyttämistä tulee valvoa tarkasti. Turvallisuustoimintaa opettelevan organisaation koko henkilöstön tulee sitoutua toiminnan kehittämiseen ja ylläpitämiseen. Opinnäytetyössä keskeisenä tarkoituksena ollut turvallisuustoiminnan kehittäminen saavutettiin ainakin turvallisuusryhmän osalta, mutta organisaation kokonaisvaltaista turvallisuustoiminnan kehittymistä en ehtinyt arvioimaan. Opinnäytetyöprosessissa luodun turvallisuuskäsikirjan apu nähtiin jo kevään auditointiprosessin aikana, mutta tarkemmat vaikutukset esiintyvät vasta pitemmällä aikavälillä sen kunnollisesta käyttöönotosta. Turvallisuuskäsikirjan täyttää kuitenkin sille asetetut hyvyyskriteerit ja vaatimukset sekä siitä saatu palaute tukee sen hyödyllisyyttä ja sovellettavuutta myös muualla.

Tietoperustaan ja omaan havainnointiin perustuen kohdeorganisaatiossa turvallisuusasiat ovat siis vielä oppivan organisaation tasolla, mikä oli myös havaittavissa työharjoittelun puolesta muuallakin valtiohallinnossa. Tietoperustan mukainen turvallisuusjohtamisen ja yleisesti johtamisen ja johtajuuden kehittäminen sekä halukkuus kehittyä turvallisuustoiminnassa ovat

jatkossa kohdeorganisaation vastuulla, sillä turvallisuuskäsikirja auttaa pääasiallisesti turvallisuusdokumentaation hallitsemisessa. Aikaisemmin tarkastellun sovellettavuuden osalta turvallisuuskäsikirjaa voitaisiin käyttää valtiohallinnon tietoturvatasohankkeeseen osallistuvissa virastoissa ja laitoksissa, joissa on tarvetta kokonaisvaltaisemmalle turvallisuuden hallitsemiselle.

Opinnäytetyöprosessissa nousi esille turvallisuusjohtamisjärjestelmän puuttuminen kohdeorganisaatiosta ja tämä jättääkin tilaa jatkotutkimukselle, jossa voidaan tutkia turvallisuusjohtamisjärjestelmien tarpeellisuutta pienissä organisaatioissa. Turvallisuuskäsikirjan hyödyllisyyden arviointi ja soveltaminen muualla, varsinkin toisessa valtiohallinnon organisaatiossa tai yksityisen sektorin yrityksessä voisi auttaa eri organisaatioita hallitsemaan turvallisuusdokumentaatiota paremmin. KATAKRI- auditointien osalta turvallisuuskäsikirjan rakennetta voitaisiin testata, miten hyvin sen rakennetta voidaan hyödyntää auditointiprosessin tukena.

Lähteet

Kirjallisuuslähteet:

Geodeettisen laitoksen Turvallisuus- ja tietohallintopäällikkö. 2013. Alkukatselmus haastattelu. 22.03. 2013. Masala.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2007. Tutki ja kirjoita. 15- 17. Helsinki: Tammi.

Kerko, P. 2001. Turvallisuusjohtaminen. Porvoo: WS Bookwell Oy.

Ojasalo K., Moilanen T. & Ritalahti J. 2009. Kehittämistyön menetelmät: Uudenlaista osaamista liiketoimintaan. Helsinki: Sanoma Pro Oy.

Tuomi, J. 2007. Tutki ja lue: Johdatus tieteellisen tekstin ymmärtämiseen. Helsinki: Tammi.

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

Sähköiset lähteet:

Elinkeinoelämän keskusliitto. 2013. Yritysturvallisuuden osa- alueet. Viitattu 24.03.2013 http://www.ek.fi/ek/fi/tyomarkkinat_ym/Yritysturvallisuus/osa-alueet/Osa-alueet.php

Geodeettinen laitos. 2013a. Tietoa meistä. Viitattu 2.2.2013 http://www.fgi.fi/fgi/fi/me/tietoa-meist%C3%A4

Geodeettinen laitos. 2013b. Lehdistötiedote 03.04.2012: Geodeettinen laitos panostaa Galileo- tutkimukseen. Viitattu 22.03.2013. http://www.fgi.fi/fgi/sites/default/files/current_topics/GeodeettinenLaitos_Galileon_vastaanotto_lehdistotiedote.pdf

Kansallinen turvallisuusauditointikriteeristö. 2011. Puolustusministeriö. Viitattu 20.1.2013. http://www.defmin.fi/files/1870/KATAKRI_versio_II.pdf

Lanne, M. 2007. Yhteistyö yritysturvallisuuden hallinnassa. Tutkimus sisäisen yhteistyön tarpeesta ja roolista suurten organisaatioiden turvallisuustoiminnassa. Espoo: VTT. Viitattu 13.02.2013. http://www.vtt.fi/inf/pdf/publications/2007/P632.pdf

Levä, K. 2003. Turvallisuusjohtamisjärjestelmien toimivuus: Vahvuudet ja kehityshaasteet suuronnettomuusvaarallisissa laitoksissa. Viitattu 15.02.2013. http://www.tukes.fi/Tiedostot/julkaisut/1_2003.pdf

Merivirta, M-J. 2011. Turvallisuusviestintä rakennusalalla. Viitattu 07.02.2013. https://jyx.jyu.fi/dspace/bitstream/handle/123456789/26694/URN%3aNBN%3afi%3ajyu-201103221913.pdf?sequence=1

Mäkinen, K. 2005. Strategic security: A constructivist investigation of critical security and strategic organizational learning issues: Towards a theory of security development. Viitattu 15.02.2012. http://www.defmin.fi/files/350/3011_Kalevi_MAkinen_Strategic_Security.pdf

Nurmi, K. 2011. Tietoturvallisuuden hallinnan suunnittelu ja toteutus: Projektiopas valtiohallinnon organisaation tietoturvallisuudesta vastaavalle. Viitattu 25.4.2013. www.tietoturvatalkoot.fi/Projektiopas.pdf

OHSAS 18002. 2008. Työterveys- ja työturvallisuusjohtamisjärjestelmät: ohjeita OHSAS 18001 soveltamiseksi. Viitattu 24.03.2013. http://sales.sfs.fi/sfs/servlets/ProductServlet?action=productInfo&productID=231608

Pohjola, K. 2013. Claritas security consulting. Viitattu 25.4.2013.
http://www.claritas.fi/

Simola, A. 2005. Turvallisuuden johtaminen esimiestyönä. Tapaustutkimus pitkäkestoisen kehittämishankkeen läpiviennistä teräksen jalostustehtaassa. Viitattu 15.02.2013
http://herkules.oulu.fi/isbn9514277619/isbn9514277619.pdf

Valtiokonttori. 2011. Valtiokonttorin uutiskirjeet. Viitattu 07.02.2013.
http://www.valtiokonttori.fi/uutiskirjeet/public/default.aspx?contentid=38073

Kuviot

Kuvio 1: Demingin PDCA- ympyrä 17
Kuvio 2: Organisaatioturvallisuuden osa- alueet (Sovellettu EK-yritysturvallisuusympyrästä) 18
Kuvio 3: Turvallisuuden kehittämisen prosessi (Sovellettu Simolan (2005, 158) mallista) 29
Kuvio 4: Turvallisuuskäsikirjan rakentamisprosessi 32

GEODEETTINEN LAITOS

Mika Kokkonen
15.01.2012

Liitteet

Liite 1

Geodeettisen laitoksen TURVALLISUUSKÄSIKIRJA

KUVAILUTIEDOT		PVM	Allekirjoitus
Laatija	Turvallisuusasiantuntija Mika Kokkonen	15.01.2013	
Tarkastaja	Turvallisuuspäällikkö	x.x.2013	
Hyväksyjä	Ylijohtajan sijainen, tutkimusjohtaja	x.x.2013	
Versio n:o	2.0		
Tiedoston nimi	Turvallisuuskäsikirja_geodeettinen_laitos_2013		
Tallennuspaikka	Intranet		
Omistaja	Turvallisuuspäällikkö		
Avainsanat	*Turvallisuuskäsikirja, turvallisuusjohtaminen, organisaatioturvallisuus*		

JAKELU

Turvallisuusryhmä

Henkilöstö

(152)
MUUTOSHISTORIA

Versio	Päiväys	Laatija	Muutoksen kuvaus
0.1	15.01.2013	Mika Kokkonen	Luonnos
0.2	04.03.2013	Mika Kokkonen	Väliversio, KATAKRI: n lisäyksiä
1.0	13.03.2013	Mika Kokkonen	KATAKRI: n vaatimukset, viimeistelyversio
1.1	18.03.2013	Mika Kokkonen	Laitoksen turvallisuuspäällikön läpikäynti
1.2	08.04.2013	Mika Kokkonen	KATAKRI- taulukot ja soveltamissuunnitelman viittaukset
1.3	22.04.2013	Mika Kokkonen	Sisällön päivitys
2.0	24.04.2013	Mika Kokkonen	Hyväksyttäväksi lähtevä versio

(152)

Sisällys

1 Johdanto 46
1.1 Keskeiset käsitteet 46
2 Turvallisuustoiminnan päämäärä, tavoitteet ja organisointi 47
2.1 Turvallisuustoiminnan päämäärä ja tavoitteet 48
2.2 Turvallisuuden organisointi 49
2.3 Turvallisuuden vastuut ja tehtävät 50
3 Turvallisuustoimintaa ohjaavat tekijät 53
3.1 Tulosohjaus 54
3.2 Velvoitteet 54
3.3 Työjärjestys 54
3.4 Turvallisuuspolitiikka 54
3.5 Turvallisuuden kehitysohjelma 55
4 Turvallisuuden sidosryhmät ja yhteistyö 55
4.1 Sisäinen turvallisuusyhteistyö 56
4.2 Ulkoinen turvallisuusyhteistyö 56
4.3 Turvallisuus hankittavissa palveluissa 60
5 Turvallisuuden ylläpito ja kehittäminen 60
5.1 Turvallisuuden vuosikello 60
5.2 Turvallisuuden ylläpito- ja kehittämissuunnitelma 61
6 Turvallisuusviestintä ja -raportointi 61
6.1 Raportointi johdolle 61
6.2 Raportointi sidosryhmille 62
6.3 Raportointi turvallisuusvastaavalle 63
7 Turvallisuusohjeistus 63
7.1 Turvallisuusohjeet ja -koulutus 63
7.2 Vierailumenettelyt 64
7.3 Etä- ja matkatyöskentely 64
7.4 Tiedottaminen ja turvallinen tiedonhallintatapa 64
8 Seuranta, valvonta ja auditointi 65
9 Tärkeiden toimintojen, tieto-omaisuuden ja turvakontrollien hallinta 66
10 Tietoturvallisuus 67
10.1 Verkkojen ja järjestelmien valvonta 68
10.2 Tietojen luokittelu 70
10.3 Asiakirjaturvallisuus 71
10.4 Pääsyn rajoitus 71
10.5 Pääsynvalvonta 71

(152)

10.6 Istunnonhallinta....72
10.7 Käyttövaltuushallinto ja varmenteiden myöntäminen....72
10.8 Puhtaan pöydän ja näytön periaate....73
10.9 Tietovälineet....73
10.10 Tietojärjestelmäturvallisuus....73
10.11 Jäännöstiedot....74
10.12 Kalenterikutsut....75
10.13 Salaus....75
10.14 Tietojen tallennuspaikka ja varmistukset....75
10.15 Arkistointi....75
10.16 Yksityisyyden suoja....76
10.17 Tietojen luovutus....76
10.18 Tietovälineen kierrättäminen ja käytöstä poisto....76
11 TIETOAINEISTOTURVALLISUUS....76
11.1 Tietojen säilytys....77
11.2 Tietojen käsittely....77
11.3 Tietojen lähettäminen ja välittäminen....78
11.4 Lähetysten kirjaaminen, postikirja ja diaarikirja....78
11.5 Tietojen kopiointi....78
11.6 Tietojen hävittäminen....79
11.7 Materiaalin tuhoaminen....79
12 Teknisen tietojenkäsittely- ympäristön turvallisuus....79
12.1 Teknisten ympäristöjen dokumentointi....79
12.2 Ohjelmistoturvallisuus....80
12.3 Laitteistoturvallisuus....81
12.4 Tietoliikenneturvallisuus....82
13 Tietojärjestelmien ylläpito ja kehittäminen....85
14 Tietotekniikkahankinnat....87
15 Laitteet....87
15.1 Luettelo ohjelmistoista....87
15.2 Luettelo laitteista....87
16 Toimitilaturvallisuus....87
16.1 Yleistä....88
16.2 Rakennukset ja tilat tarkennettuna....88
16.3 Ulkoalueet....88
16.4 Pääsyoikeudet....89
16.5 Tilojen lukitus....89
16.6 Yleisavaimet ja niiden käyttö....89
16.7 Avainten ja kulkuoikeuksien hallinta....90

16.8 Ikkunat....90
16.9 Rikosilmoitinjärjestelmä....90
16.10 Kassakaapit....91
16.11 Vartiointi....91
16.12 Kulunvalvonta....91
16.13 Muutokset kulunvalvontaan....91
16.14 Kameravalvonta....92
16.15 Huoltotoimenpiteet....92
16.16 Rakenteet....92
16.17 Aukot rakenteissa....94
16.18 Ovet....94
16.19 Laite- ja palvelintilojen valvonta....95
16.20 Tilojen äänieristys....95
16.21 Varautuminen hajasäteilyyn ja salakuunteluun....95
16.22 Toimitilojen pohjapiirrokset....95
17 Henkilöstöturvallisuus....96
17.1 Henkilöstöluettelo ja muutokset henkilöstössä....96
17.2 Rekrytointivaiheeseen liittyvät turvallisuusjärjestelyt....96
17.3 Toimenkuva....97
17.4 Työtehtävien eriyttäminen....97
17.5 Turvallisuusselvitykset....97
17.6 Vaitiolo- ja salassapitositoumus....98
17.7 Perehdyttäminen....98
17.8 Osaamispääoman hallinta....98
17.9 Turvallisuuskoulutus....99
17.10 Jaksaminen ja työkyky....99
17.11 Turvallisuuden ohjeistus ja turvalliset käytännöt....100
17.12 Avainhenkilöiden kartoitus ja varahenkilöjärjestelyt....100
17.13 VAP- varaukset....100
17.14 Kolmas osapuoli ja tukihenkilöstö....100
17.15 Palvelussuhteen päättymiseen liittyvät turvallisuusjärjestelyt....101
17.16 Sanktiomenettelyt....101
18 Riskienhallinta ja jatkuvuuden varmistaminen....101
18.1 Riskienhallinnan menettelyt....102
18.2 Toiminnan jatkuvuuden varmistaminen ja ennaltaehkäisevä toiminta....103
19 Dokumentaatio....107
20 Liitteet....109

1 Johdanto

Tämän turvallisuuskäsikirjan tarkoituksena on toimia laitoksen turvallisuustoiminnan tukena ja kuvata turvallisuusasioihin liittyvät käytännöt sekä niihin liittyvän dokumentaation. Turvallisuuskäsikirjan tarkoituksena on myös toimia tiiviinä tietolähteen turvallisuusasioiden johtamisessa. Käsikirjaa tarkastetaan säännöllisesti vuosikellon mukaan ja päivitetään tarpeen mukaan, jotta turvallisuustoiminnan tiedot ja taso pysyvät ajan tasalla.

Käsikirjan alkuosa käsittelee turvallisuustoiminnan hallinnollista puolta, jossa tarkastellaan tavoitteita, yhteistyökumppaneita, turvallisuustoiminnan kehittämistä, turvallisuusviestintää ja – ohjeistuksia sekä seurantaa ja arviointia. Tämän jälkeen käsitellään tietoturvallisuutta ja tietoaineistoturvallisuutta sekä tietojenkäsittely-ympäristöjä ja laitoksen tietoteknistä laitteistoa. Loppupuoliskolla tarkastellaan toimitilaturvallisuutta, henkilöstöturvallisuutta sekä riskienhallintaa. Käsikirjan liitteistä löytyy kaikki laitoksen turvallisuusdokumentaatio.

1.1 Keskeiset käsitteet

Tässä kappaleessa kuvaillaan turvallisuuskäsikirjassa käytetyt keskeiset käsitteet. Käsitteiden selventäminen on olennaista turvallisuusjohtamisen ja turvallisuusasioiden hallinnoimisen kannalta. (VAHTI 8/2008)

1.1.1 Kansallisen turvallisuusauditointikriteeristön turvallisuustasot

Toimivaltaiset viranomaiset suorittavat KATAKRI- auditointeja turvallisuustason tarkastamiseksi. Tarkastuksesta myönnetään erillinen todistus, jotta voi toimia esimerkiksi kansainvälisissä hankkeissa (Facility Security Clearance, FSC). Turvallisuustason todentamiseen käytetään eri vaatimuksia, jotka jaetaan kolmelle eri turvallisuustasolle: perustaso, korotettu taso ja korkea taso. Tilojen osalta käytetään termiä ”suojaustason I, II tai III- tila” ja tietoaineistosta käytetään termiä ”turvallisuusluokiteltu- aineisto”. Tässä dokumentissa KATAKRI: n vaatimukset ovat taulukoituna sitä vastaavassa luvussa ja liitteestä X löytyy listaus vaatimuksista.

1.1.2 Tietoturvallisuus

Tietoturvallisuuden tarkoituksen on suojata tietoa, joka on organisaation tärkeää omaisuutta ja jonka luotettavuus, eheys ja saatavuus tulee turvata kaikissa tilanteissa. Tietoturvallisuus on osa organisaatioturvallisuutta ja riskienhallintaa. Tietoturvallisuuden ratkaisut ovat fyysisiä, teknisiä ja hallinnollisia toimenpiteitä. (VAHTI 8/2008)

1.1.3 Tietoaineistoturvallisuus

Tietoaineistoturvallisuuteen liittyy kaikki tietoturvallisuuden toimenpiteet koskien asiakirjoja, tiedostoja ja muita tietoaineistoja. Toimenpiteillä ylläpidetään käytettävyyttä, eheyttä ja luottamuksellisuutta. Toimenpiteitä ovat muun muassa aineistojen luettelointi ja luokitus, hallinta, käsittely, säilytys ja hävittäminen. Tietoaineistojen suojaaminen oikealla tavalla ja riittävällä turvallisuustasolla (KATAKRI) on tietojen suojaamisen ja tietojenkäsittelyn jatkuvuuden kannalta tärkeää. (VAHTI 8/2008)

1.1.4 Kiinteistö- ja toimitilaturvallisuus

Toimitilaturvallisuuden tarkoituksena on suojata ja ylläpitää organisaation omistamia tai hallinnoimia kiinteistöjä ja toimitiloja sekä niiden turvallisuutta. Kiinteistöjä ja toimitiloja voidaan suojata erilaisilla toimenpiteillä ja ratkaisuille, jotka voidaan jakaa rakenteellisiin ja teknisiin ratkaisuihin, kuten kulunvalvonnalla, vartioinnilla sekä palo-, vesi-, sähkö-, ilmastointi- ja murtovahinkojen torjunnalla. (VAHTI 8/2008)

1.1.5 Henkilöstöturvallisuus

Henkilöstöturvallisuuden toimenpiteiden tarkoituksena on suojata organisaation henkilöstöä onnettomuuksilta ja vaaroilta. Henkilöstöturvallisuudessa kiinnitetään myös huomiota henkilöstön luotettavuuteen ja soveltuvuuteen, oikeuksiin, varamiesjärjesteltyihin sekä työsuhteeseen liittyviin järjestelyihin. Henkilöstöturvallisuuteen liittyy muidenkin organisaatioturvallisuuden osa- alueita ja niihin liittyviä ohjeistuksia. (VAHTI 8/2008)

2 Turvallisuustoiminnan päämäärä, tavoitteet ja organisointi

Turvallisuustoiminnan päämäärän ja turvallisuusorganisaation asettaminen ovat olennaisia turvallisuustoiminnan toimivuuden kannalta. Päämäärät ohjaavat turvallisuusorganisaation toimintaa, jolloin tavoitteet ovat konkreettiset ja saavutettavissa. Riskienhallinnan avulla laitos pystyy priorisoimaan tärkeimmät tavoitteet turvallisuustoiminnassa.

KATAKRI	Liite
A501.0	

(152)

A502.0	
A503.0	
A506.0	
A605.0	
A702.0	
A704.0	

2.1 Turvallisuustoiminnan päämäärä ja tavoitteet

Turvallisuustoiminnan päämääränä on turvata laitoksen häiriötön toiminta kaikissa tilanteissa. Turvallisuustoiminnan pääpaino on ennaltaehkäisevässä toiminnassa, jonka avulla tunnistetaan suurimmat riskit ja reagoidaan nopeasti potentiaalisimpiin uhkiin. Tällä tavoin pystytään hallitsemaan riskejä sekä estämään ja pienentämään niiden seurauksia. Riskienhallinta kaikilla organisaatioturvallisuuden osa- alueilla mahdollistaa päämäärien ja tavoitteiden asettamisen ja toteutumisen. Keskeisimpänä tavoitteena on kehittää ja ylläpitää tavoiteltua turvallisuuden tasoa hallita tunnistettuja riskejä. Turvallisuuden tasoa pyritään mittaamaan vuosittain. Tavoitteille ja niiden saavuttamiselle laaditaan realistinen aikataulu.

Tässä turvallisuuskäsikirjassa on kuvattuna hallinnollinen, fyysinen ja tietotekninen turvallisuus, joka koskee tieto-, toimitila- ja henkilöstöturvallisuutta. Tässä käsikirjassa otetaan huomioon myös toimintaa koskeva lainsäädäntö ja asetukset. Turvallisuustoimintaa koskevat ohjeistukset on kuvattuna tarkemmin kappaleessa 7.

KATAKRI	Liite
A102.0	
A204.0	
A301.0	
A302.0	
A303.0	
A304.0	
A305.0	
A404.0	

2.2 Turvallisuuden organisointi

Turvallisuustoiminnan organisointi on tärkeää vastuiden jakamiseksi ja toimintojen sujuvuuden varmistamiseksi. Turvallisuusorganisaation tehtävänä on ottaa vastuu turvallisuustehtävistä, laatia ohjeistuksia ja toimintaohjeita henkilöstölle sekä perehdyttää uusi henkilöstö ja muut sidosryhmäläiset organisaation turvallisuusasioihin. Alempana on kuvattuna tarkemmin laitoksen turvallisuusvastuut ja tehtävät

Kokonaisvastuu turvallisuudesta ja sen johtamisesta on laitoksen ylimmällä johdolla. Laitoksen turvallisuustoiminta organisoidaan toiminnan luonteen ja laajuuden edellyttämällä tavalla. Laitoksen osastojen osalta vastuu on osaston johtajalla. Jokaisella henkilökuntaan kuuluvalla on vastuu turvallisuudesta omien tehtäviensä osalta. Turvallisuuspäällikkö vastaa turvallisuuden kehittämisen, ylläpitämisen ja valvonnan koordinoinnista.

Tehtäviin liittyvät työtehtävät määritellään työjärjestyksessä (liite x). Turvallisuustyöhön on varattava riittävät resurssit ja tarvittaessa käytetään ulkopuolista asiantuntemusta. Organisointi, vastuut ja tehtävät määritellään selvästi ja viestitetään kaikille asianomaisille ja henkilöstölle.

Turvallisuusryhmä edustaa organisaation turvallisuustoiminnan johtamista. Sen tehtävänä on sovittaa turvallisuusvaatimukset ja turvallisuustoimenpiteet palvelemaan laitoksen toimintaa. Esimerkiksi tietoturvaryhmä ohjaa tietoturvatoimenpiteitä laitoksen eri osa- alueilla. Alempana on kuvattuna turvallisuusryhmän roolit ja vastuut.

Ryhmä kokoontuu kaksi kertaa vuodessa sekä tarvittaessa. Kokoontumisen tarkoituksena on tarkastella turvallisuustoiminnan tasoa, kehitystoimenpiteiden tarvetta, edistymistä ja tavoitteiden saavuttamista. Laitoksen turvallisuushenkilöstöstä koostuvan turvallisuusryhmän tehtävänä on:

- laatia ja päivittää turvallisuusperiaatteet
- laatia ja päivittää turvallisuuden ylläpito- ja kehittämissuunnitelma
- järjestää auditoinnit
- laatia ja päivittää turvallisuuden ja riskienhallinnan päälinjaukset
- vastata turvallisuuden ja riskienhallinnan toteutumisesta
- auttaa liittämään turvallisuus osaksi johtamistoimintaa
- varmistaa riittävien resurssien saatavuus turvallisuuden toteutumiselle
- raportoida johtoryhmälle vuosittain ja esittää kehitysehdotuksia turvallisuustoimintaan liittyen
- laatia ja päivittää vaatimukset turvallisuuden ja riskienhallinnan huomioon ottamisesta toiminnoissa.

(152)

Turvallisuusryhmän jäsenet:

- Turvallisuuspäällikkö
- Suojelupäällikkö
- Tarpeen mukaan erikseen määriteltävä projekti- ja hankehenkilöstö

2.3 Turvallisuuden vastuut ja tehtävät

Tässä kappaleessa on kuvattuna rooli ja tehtäväkohtaiset vastuut ja tehtävät turvallisuustoiminnassa.

Ylijohtaja

- Laitoksen toimintaa koskevan lainsäädännön seuranta ja turvallisuutta koskevien vaikutusten arviointi.
- Säädösten edellyttämien toimenpiteiden toimeenpano.
- Toimialansa turvallisuuden kehittämistoimenpiteiden hyväksyntä.
- Turvallisuustoiminnan valvonta.
- Turvallisuusvastuiden omistajien nimeäminen ja toimialansa turvallisuuden tulosohjaus.

Osastonjohtajat

- Toimeenpanevat turvallisuustoiminnan vaatimuksia ja ohjeita asetettujen turvallisuustavoitteiden mukaisesti.
- Seuraa valtionhallinnon ja omien turvallisuuden ohjeiden noudattamista ja raportoi riskeistä ja turvallisuudesta sekä havaituista turvallisuuspoikkeamista ylijohtajalle ja turvallisuuspäällikölle.

Tietohallinto

- Ylläpitää tietojärjestelmäkuvaukset.
- Toteuttaa tietojärjestelmiinsä liittyvät turvallisuustoimenpiteet.
- Seuraa tietoturvallisuutta tietojärjestelmässä ja palvelujen sopimuksenmukaisuutta.
- Raportoi johdolle tietoturvallisuudesta sekä havaituista tietoturvapoikkeamista sekä vastaanottaa poikkeamailmoituksia.

Turvallisuuspäällikkö

- Johtaa turvallisuustoimintaa ja kehittää turvallisuusjohtamista.

- On vastuussa laitoksen jatkuvuus- ja toipumissuunnittelusta yhteistyössä laitoksen johdon ja osastojen johtajien kanssa.
- Raportoi turvallisuutta vaarantavista tapahtumista ja häiriöistä johtoryhmälle.
- Onnettomuuksien, vaaratilanteiden ja turvallisuuspoikkeamien käsittely ja tutkinta.
- Poikkeamatilanteiden johtaminen.
- Viranomaiskontaktien hoitaminen poikkeamatilanteissa.
- Johtaa hyväksyttyjen periaatteiden ja suunnitelmien toteutumista.
- Valvoo turvallisuusmenettelyjä tietojärjestelmissä.
- Seuraa järjestelmien toimintaa tietoturvallisuuden kannalta.
- Vastata turvallisuuden vuosikellon laatimisesta ja seurannasta.
- Turvallisuuskoulutusten järjestäminen.
- Turvallisuusselvityspyyntöjen käsittely

Suojelupäällikkö

- Suojelupäällikkö valmistelee laitoksen suojelusuunnitelman ylijohtajan hyväksyttäväksi ja huolehtii laitoksen suojeluvalmiudesta.
- Johtaa, kehittää ja ylläpitää laitoksen suojelu- ja pelastustoimintaa.
- Vastaa pelastussuunnitelman laadinnasta ja ajan tasalla pitämisestä.
- Tekee tarvittava ilmoitukset viranomaisille ja osallistuu viranomaisten tekemiin tarkastuksiin.
- Toimii turvallisuuspäällikön sijaisena tarvittaessa.

Työntekijä

- Tuntee turvallisuudesta annetut ohjeet ja noudattaa niitä sekä parantaa omaa turvallisuustoimintaansa.
- Raportoi havaitsemistaan poikkeamista, ongelmista, uhista ja ohjeiden vastaisesta menettelystä.
- Osallistuu järjestettäviin koulutuksiin.

Henkilörekisterien hoitajat ja tietopalveluhenkilöstö

- Huomioi turvallisuudesta ja tietoturvallisuudesta annetut määräykset ja ohjeet tietoaineiston käsittelyssä ja hallinnassa.
- Arkistosääntö/ arkistonmuodostussuunnitelma

Tutkimusosastojen tietojärjestelmäomistajat

Osastojen tietojärjestelmäomistajien tehtävänä on seurata ja arvioida osaston omistamien tietojärjestelmien soveltuvuutta, toimivuutta ja kehittämistarpeita yhdessä tietohallinnon kanssa. Heidän vastuullaan on viedä kehitysehdotukset ja - suunnitelmat osastonjohtajien käsiteltäväksi.

Tietotekniikan yhdyshenkilötehtäviin kuuluu ehdotusten tekeminen osaston laite- ja ohjelmistokannan parantamisesta. Näiden tarpeiden välittäminen tietohallinnolle ja käyttötuen palvelutason seuranta on osastolla. Lisäksi he tiedottavat tarvittaessa toimintahäiriöistä tietohallintoon.

KATAKRI	Liite
A504.0	
A505.0	
A602.0	
A603.0	

Rooli	Turvallisuuspäällikkö
Vastuuhenkilö	
Mistä turvallisuusprosessista tai toimenpiteestä vastaa:	Kokonaisturvallisuuteen, tietohallintoon ja tietotekniikkaan liittyvän turvallisuuspolitiikoiden valmistelu ja esittely • Valvoo turvallisuustoimintaan liittyvät vuosikellon mukaiset asiat osana talouden- ja toiminnansuunnittelua. • Vastaa turvallisuuteen liittyvien asioidenperehdyttämisestä ja koulutuksesta henkilöstölle. • organisaation turvallisuuden kehittämistoimenpiteiden ohjaus • turvallisuuden tulosohjaus • turvallisuuden toteutumisen varmistaminen • turvallisuuden toteutumisen valvonta ostetuissa palveluissa • avustaa johtoa ja yksiköitä riskienhallinnan toimeenpanossa • tulosohjaustavoitteiden mukaisesti seuraa ja kehittää riskienhallintaa • järjestää riskienhallinnan seurannan ja rapor-

	toinnin riskeistä johdtoryhmälle • osallistuu erinäisten turvallisuustoimintaan liittyvien politiikkojen suunnitteluun • kehittää turvallisuutta turvallisuuspolitiikan mukaisesti • ohjaa turvallisuuden käytännön toteutusta henkilöstön, toiminnan ja omaisuuden turvaamiseksi ja niihin kohdistuvien riskien hallitsemiseksi • seuraa merkittävimpiä riskejä ja ohjaa niiden hallitsemiseksi suunniteltujen toimenpiteiden toteutumisesta. • huolehtii henkilöstön turvallisuustietoisuuden lisäämisestä ja turvallisuuskoulutuksen järjestelystä • raportoi ylimmälle johdolle turvallisuudesta, riskeistä ja uhista.
Rooli	Suojelupäällikkö
Vastuuhenkilö	
Mistä turvallisuusprosessista tai toimenpiteestä vastaa	• Ohjaa ja sovittaa yhteen laitoksen poikkeusoloihin varautumista • varautumistoimenpiteiden huomioon ottaminen organisaation toiminnassa • laitoksen poikkeusolojen valmiuden kehittäminen • poikkeusoloissa turvattavien toimintojen selvittäminen ja esittely johtoryhmälle • toiminnan kannalta kriittisten järjestelmien valmiuden kehittäminen yhdessä turvallisuusryhmän ja muun johdon kanssa. • Toimii turvallisuuspäällikön sijaisena tarvittaessa

Taulukko 1: Turvallisuusryhmän roolit

3 Turvallisuustoimintaa ohjaavat tekijät

Tässä kappaleessa on kuvattuna laitoksen turvallisuustoimintaa ohjaavia tekijöitä. Eri tekijät vaikuttavat turvallisuustoimintaan ja tavoitteisiin eri tavoin, joten on oleellista tunnistaa riskienhallinnan avulla kriittisimmät tekijät, jotta näiden tekijöiden vaikutukset ja todennäköisimmät riskit voidaan ottaa huomioon turvallisuustoimintaa suunniteltaessa. Tunnistamisessa ja tavoitteiden asettamisessa käytetään riskienhallintaprosessia, joka on kuvattuna tarkemmin riskienhallintapolitiikassa (Liite x).

KATAKRI	Liite
A305.0	

3.1 Tulosohjaus

Turvallisuustoiminnan taloudellinen ohjaus perustuu laitoksen sisäinen toiminnan ja talouden ohjaukseen. Keskeiset turvallisuustavoitteet viedään johdon toimesta tulosohjaukseen. Tulostavoitteet määritetään osastoittain ja henkilöittäin. Turvallisuustyössä otetaan huomioon toiminnan tehokkuus ja kustannukset. Turvallisuusjärjestelyjen suunnitteluun ja toteutukseen vaikuttavat varsinaisen toiminnan tavoitteet ja tarpeet, niistä johdetut turvallisuusvaatimukset sekä laitoksen koko ja rakenne. Tulosohjauksessa otetaan huomioon myös oman toiminnan ja talouden vaatimukset.

3.2 Velvoitteet

Laitoksen toimintaa ohjaavat lainsäädäntö, asetukset, säädökset sekä valtionhallinnon ja hallinnonalan määräykset ja ohjeet. Ulkoisten velvoitteiden lisäksi laitoksen turvallisuustoiminnassa noudatetaan laitoksen johdon vahvistamaa turvallisuuden kehitysohjelmaa ja – politiikkaa sekä hyväksyttyjä sopimuksia. Ulkoiset ja sisäiset velvoitteet yksilöidään sopimus- ja hankekohtaisesti ja ne dokumentoidaan asianmukaisesti.

Turvallisuuteen liittyvät merkittävimmät säädökset on kuvattu Intranetissä.

(Liite X)

3.3 Työjärjestys

Laitoksen työjärjestyksessä on kuvattuna organisaation eri työtehtävien vastuut, joihin sisältyy turvallisuustoiminnan huomioon ottaminen työtehtävästä riippuen. Riskienhallinta ja turvallisesti työskenteleminen ovat olennainen osa jokaisen työntekijän työtehtäviä, koska tutkimustehtävät ovat hyvin projektiluontoisia ja tutkimusta suoritetaan myös paljon kenttätyönä, jolloin työturvallisuus on otettava huomioon.

Työjärjestys löytyy Intranetistä.

(152)
3.4 Turvallisuuspolitiikka

Virastolla on johdon hyväksymä turvallisuuspolitiikka, jossa määritellään turvallisuustoiminnan päämäärä ja tavoitteet, riskienhallinnan periaatteet, turvallisuustoiminnan organisointi ja vastuut, dokumentointi, turvallisuuskoulutuksen ja viestinnän sekä valvonnan periaatteet. Turvallisuuspolitiikan ajanmukaisuus tarkistetaan säännöllisesti johdon katselmuksen yhteydessä. Geodeettisen laitoksen turvallisuuspolitiikka on julkinen ja sen on henkilöstön nähtävillä Intranetissä. (liite x)

KATAKRI	Liite
A101.0	
A103.0	
A105.0	
A105.1	
A106.0	
A107.0	
A108.0	
A301.0	
A401.1	
A703.0	
A801.0	

3.5 Turvallisuuden kehitysohjelma

Laitoksella on laadittuna vuosikello, jossa kuvataan toimintaohjelma turvallisuuden johtamisen ja turvallisuustoiminnan osalta. Vuosikellosta ilmenee myös turvallisuustoiminnan ydintavoitteet ja sen avulla voidaan kuvata turvallisuuden kehitystarpeet. Menetelmät, vastuut ja aikataulu merkitään vuosikelloon ja tähän turvallisuuskäsikirjaan. Vuosikellon ohella tässä käsikirjassa on kuvattuna turvallisuuden nykytila, tavoitteet, kehittämistarpeet ja mittaristo. Vuosikelloa seurataan ja päivitetään vuosittain.

KATAKRI	Liite
A201.0	
A202.0	

(152)

A203.0	

4 Turvallisuuden sidosryhmät ja yhteistyö

Tässä kappaleessa on kuvailtuna turvallisuuden sidosryhmät ja yhteistyö turvallisuusasioissa eri tahojen kanssa. Sidosryhmien kanssa työskennellessä tulee olla tarkat ohjeet, miten turvallisuustoiminnot jaetaan. Turvallisuustavoitteiden asettamisessa tulee ottaa huomioon myös sidosryhmien vaatimukset. Sopimuksilla saadaan kontrolloitua sidosryhmien toimintaa esimerkiksi tietoturvallisuuden osalta salassapitosopimuksin.

4.1 Sisäinen turvallisuusyhteistyö

Turvallisuusryhmä ja ylin johto tapaavat kaksi kertaa vuodessa tai tarpeen mukaan. Tapaamisessa käydään läpi havaittuja riskejä, asetettuja turvallisuustavoitteita, niiden saavuttamista ja tulevaisuuden tarpeista aiheutuvia muutoksia sekä resurssitarpeiden riittävyyttä. Johdon tapaamisessa tarkastellaan myös turvallisuuden ylläpito- ja kehittämissuunnitelmaa.

Tapaaminen ajoitetaan niin, että suunnitelmassa esitetyt resursointitarpeet pystytään huomioimaan organisaation tulevassa toiminta- ja taloussuunnittelussa. Tapaamisista pidetään pöytäkirjaa, jotta sovittujen asioiden toteutumista pystytään seuraamaan. Tarpeen mukaan laitoksella osallistutaan myös turvallisuustilanteen seuranta- ja yhteistyöryhmiin.

4.2 Ulkoinen turvallisuusyhteistyö

Ulkoisilta yhteistyökumppaneilta saattaa tulla vaatimuksia turvallisuustoiminnan osalta, joten organisaation oman toiminnan kannalta haastavaa on täyttää eri yhteistyökumppaneiden vaatimukset turvallisuustoiminnan osalta. Laitoksella tämä on kuitenkin otettu huomioon ja resurssit on saatu sijoitettua tarpeiden mukaisesti. Liitteessä X (alla olevat taulukot) on kuvattuna kriittisimmät yhteistyökumppanit.

Tärkeimmät tai kriittisimmät palvelutuottajat sekä alihankkijat

Nimi	
Palvelu	Vartiointi
Palveluntuottajan yhteys-henkilö	

(152)

Viraston yhteyshenkilö	
Turvallisuusraportointi	Turvallisuusraportointi laaditaan jokaisesta käynnistä kohteessa ja jos kohteessa on havaittu jotain poikkeamia.
Erityiset turvallisuusvaatimukset?	Määriteltynä erikseen sopimuksessa.
Turvallisuus-/tietoturvasopimus	Toimeksiantosopimuksessa on määriteltynä erikseen tietojen salassa pitämisestä.

Nimi	
Palvelu	Kiinteistöhuolto
Palveluntuottajan yhteyshenkilö	
Viraston yhteyshenkilö	
Miten usein raportoidaan, mistä asioista, kenen toimesta	
Erityiset turvallisuusvaatimukset	
Turvallisuus-/tietoturvasopimus	

Nimi	
Palvelu	Kulunvalvonta
Palveluntuottajan yhteyshenkilö	
Viraston yhteyshenkilö	
Miten usein raportoidaan, mistä asioista, kenen toimesta	
Erityiset tietoturvavaatimukset	
Onko tehty turvallisuus-/tietoturvasopimus	

(152)

Nimi	
Palvelu	Kiinteistöjen omistaja
Palveluntuottajan yhteys-henkilö	
Viraston yhteyshenkilö	
Miten usein raportoidaan, mistä asioista, kenen toimesta	
Erityiset tietoturvavaati-mukset	
Onko tehty turvallisuus-/tietoturvasopimus	

Tärkeimmät yhteistyökumppanit

Nimi	
Yhteistyön tehtävä	
Kumppanin yhteyshenkilö	
Viraston yhteyshenkilö	
Miten usein raportoidaan, mistä asioista, kenen toimesta	
Minkä suojaustason tieto- ja pääasiallisesti käsitel-lään, onko muuta turvalli-suusluokitusta?	
Erityiset tietoturvavaati-mukset	
Turvallisuus-/tietoturvasopimus	

Nimi	
Yhteistyön tehtävä	
Kumppanin yhteyshenkilö	

(152)

Viraston yhteyshenkilö	
Miten usein raportoidaan, mistä asioista, kenen toimesta	
Minkä suojaustason tieto- ja pääasiallisesti käsitellään, onko muuta turvallisuusluokitusta?	
Erityiset tietoturvavaatimukset	
Turvallisuus-/tietoturvasopimus	

Tärkeimmät viranomaisyhteydet

Nimi	
Viranomaisyhteyden luonne/tehtävä	
Viranomaisen yhteyshenkilö	
Viraston yhteyshenkilö	
Miten usein raportoidaan, mistä asioista, kenen toimesta	
Minkä suojaustason tieto- ja pääasiallisesti käsitellään, onko muuta turvallisuusluokitusta?	
Erityiset tietoturvavaatimukset	
Tehty turvallisuus-/tietoturvasopimus	

Nimi	
Viranomaisyhteyden luonne/tehtävä	
Viranomaisen yhteyshenkilö	

Viraston yhteyshenkilö	
Miten usein raportoidaan, mistä asioista, kenen toimesta	
Minkä suojaustason tieto- ja pääasiallisesti käsitellään, onko muuta turvallisuusluokitusta?	
Erityiset tietoturvavaatimukset	
Turvallisuus-/tietoturvasopimus	

4.3 Turvallisuus hankittavissa palveluissa

Hankinnoissa ja ulkoistamisessa otetaan huomioon turvallisuustoiminnan vaatimukset. Sopimuksia tehdessä tulee lisätä liitteiksi tarkennukset tietyt turvallisuustoiminnan kannalta tärkeät asiat. Esimerkiksi salassapitovaatimukset määritellään ja kirjataan palvelusopimukseen. Palvelutoimittajan kanssa tehdään kirjallinen sopimus, jossa määritellään hankinnan kohteen turvallisuusvaatimukset sekä miten turvallisuuden valvonta, seuranta, auditointi ja raportointi tapahtuu.

Oikeus sitoutua hankintaan on sillä, jolla työjärjestyksen tai tehtäväksi annon mukaan on toimivalta kyseisessä asiassa. Menojen hyväksyjänä toimii ylijohtaja tai hänen sijaisekseen merkitty henkilö. Hankintaa suorittavan tehtävänä on huolehtia siitä, että palvelutoimittajalle asetetaan tarvittavat turvallisuusvaatimukset jo tarjouspyyntö- tai kumppanuusneuvotteluvaiheessa yhdessä turvallisuuspäällikön kanssa. Sopimuksessa määritellään mitä turvallisuustasoa kumppanin ja mahdollisen kumppanin alihankintaverkoston on kohteen luonteen huomioon ottaen noudatettava. Turvallisuustaso määräytyy sen mukaan, minkä turvallisuusluokan tietoja palvelussa pääasiallisesti käsitellään ja millaisia riskejä palveluun liittyy. Turvallisuuspoikkeamille ja – loukkauksille tulee olla sanktiot.

Ennen sopimuksen solmimista laitos voi auditoida tai pyytää kirjallisen selvityksen kumppanin yhteistyön kohteeseen liittyvistä turvallisuusmenettelyistä.

Palvelutoimittajien tehtävänä on

- noudattaa hyvää tietojenkäsittely- ja tietoturvatapaa
- ylläpitää ja valvoa toiminnassaan valtionhallinnon tietoturvallisuuden yleisohjeistuksen mukaista ja ohjeistettua tietoturvallisuutta
- raportoida hankkeiden tai palveluiden tietoturvallisuudesta ja siihen vaikuttavista tekijöistä.

5 Turvallisuuden ylläpito ja kehittäminen

Turvallisuustoiminnan ylläpito ja kehittäminen ovat tärkeitä toiminnan jatkuvuuden varmistamisen kannalta. Johdon asettamaa turvallisuustasoa tulisi pysty pitämään yllä ja parhaassa tapauksessa kehittämään aktiivisesti. Tässä kappaleessa on kuvattuna toimenpiteet turvallisuustoiminnan ylläpitämisen ja kehittämisen osalta.

5.1 Turvallisuuden vuosikello

Turvallisuuden vuosikellon avulla pystytään seuraamaan vuosineljänneksittäin kalenterivuoden aikana suoritettavien turvallisuustoimintojen tekemistä. Vuosikelloon lisätään myös sen itsensä päivittämisen ajankohta, joka tehdään turvallisuustoimintojen päivittämisen rinnalla. Laitoksen turvallisuuden vuosikello on liitteessä X. Keskeiset turvallisuustavoitteet viedään johdon toimesta tulosohjaukseen.

5.2 Turvallisuuden ylläpito- ja kehittämissuunnitelma

Turvallisuuspäällikkö ylläpitää vuosittain tai tarpeen mukaan päivitettävää turvallisuuskäsikirjaa. Turvallisuuskäsikirjassa on esitetty:

- Turvallisuustoiminnan ja – johtamisen toiminnot ja vastuut
- Tietoturvallisuus ja tietoaineistojen turvallisuus
- Henkilöstöturvallisuus
- Toimitilaturvallisuus
- Riskienhallinnan perusasiat
- toteutettaviksi valittujen turvallisuustoimenpiteiden ja –prosessien organisointi ja vastuu.
- suunnitellut auditoinnit

Suunnitelman toteutumista tarkastellaan puolivuosittain johdon ja tietoturvaryhmä yhteisessä tapaamisessa. Suunnitelmassa esitetyt resursointitarpeet huomioidaan johdon toimesta organisaation toiminta- ja taloussuunnittelussa.

6 Turvallisuusviestintä ja -raportointi

Turvallisuusviestinnän tarkoituksena on olla väylänä johdon ja henkilöstön välillä turvallisuusasioista, toimia kanavana kriisi- ja poikkeamatilanteissa sekä ylläpitää sisäisten ja ulkoisten tekijöiden tietoisuutta laitoksen turvallisuusasioista. Turvallisuustoimintaan liittyvistä asioista, kuten turvallisuuspoikkeamista, raportoidaan ja viestitään ohjeistuksen mukaan. Laitoksen omassa viestintästrategiassa on kuvattuna yleisen viestinnän periaatteet, tarkoitus ja tavoitteet.

KATAKRI	Liite
A604.0	
A903.0	

6.1 Raportointi johdolle

Turvallisuuspäällikkö vastaa vuosittaisen johdon turvallisuusraportin laatimisesta. Turvallisuusraportti esitetään puolivuosittaisessa turvallisuusryhmänryhmän ja johdon tapaamisessa. Poikkeamatilanteessa raportoidaan poikkeamatilanteiden raportointimenettelyllä (tehostettu raportointi).

Turvallisuusraportin sisältö:

- Ajankohtaista turvallisuudesta
    - trendit, organisaation toimintaa koskevat lait ym. (lyhyesti, mitä ne merkitsevät organisaation kannalta)
    - merkittävät turvallisuuden kannalta tapahtuneet muutokset
- Tuvallisuustoiminnan resurssien käyttö
- Turvallisuustoiminnan tavoitteiden toteutuminen
- Turvallisuuspoikkeamat ja niiden johdosta tehdyt korjaavat toimenpiteet
- Resurssien riittävyys
    - Turvallisuuspäällikön ajankäytön riittävyys
    - organisaation turvallisuushenkilöstön määrän riittävyys
- Kehittämisehdotukset alustavine kustannus- ja työmääräarvioineen (millä ennaltaehkäistään ongelmia, korjataan havaittuja puutteita ja kehitetään tietoturvallisuutta)

Laitoksen johdolle esitetään turvallisuusryhmän tapaamisissa vähintään kahdesti vuodessa yhteenveto toteutetuista toimenpiteistä, auditointien tuloksista, sattuneista vahingoista ja turvallisuuteen ja riskeihin vaikuttavista muutoksista. Lisäksi katselmuksessa esitetään päätösehdotukset tarvittavista toimenpiteistä. Johto tekee tarvittaessa päätökset muutoksista turvallisuuspolitiikkaan, organisointiin ja resursseihin.

KATAKRI	Liite
A901.0	

6.2 Raportointi sidosryhmille

Raportoinnista sovitaan eri sidosryhmien kanssa organisaatiokohtaisesti. Raportointia kehitetään palautteen perusteella huomioiden salassapitovaatimukset. Ellei toisin ole sovittu, sidosryhmäraportoinnissa käydään läpi seuraavat asiat:

- Ajankohtaista turvallisuudesta (palveluihin liittyvät lait ym.)
- Yhteisten turvallisuustavoitteiden toteutuminen (mikäli niistä on sovittu)
- Havaitut kehittämiskohteet ja näihin liittyvät välittömät korjaavat toimenpiteet
- Turvallisuuteen liittyvät kehittämishankkeet (miten turvallisuutta on kehitetty, huomioitava salassapitovaatimukset)
- Kehittämisehdotukset alustavine kustannus- ja työmääräarvioineen (kuvataan tarvittaessa, millä ennaltaehkäistään ongelmia, korjataan havaittuja puutteita ja kehitetään turvallisuutta)

6.3 Raportointi turvallisuusvastaavalle

Turvallisuustoiminnan hallinnasta vastaavalle turvallisuuspäällikölle raportoidaan kaikki turvallisuustoimintaan liittyvät asiat raportointiohjeen mukaisesti. Vakavista tapahtumista raportoidaan viivytyksettä ja niistä luodaan poikkeamatilaraportti ohjeistuksen mukaan.

IT- järjestelmien ja niiden hallinnasta raportoidaan turvallisuuspäällikölle. Vakavista tietoturvatapahtumista kerrotaan viivytyksettä ja niistä laaditaan poikkeamatilaraportti ohjeistuksen mukaan.

7 Turvallisuusohjeistus

Turvallisuusohjeistuksen tarkoituksena on ohjata kaikkia laitoksella työskenteleviä turvalliseen työskentelyyn. Ohjeistukset ovat näkyvillä henkilöstölle Intranetissä ja niitä päivitetään tarpeen mukaan ja ne tarkastetaan säännöllisesti vuosikellon mukaan. Tässä osiossa on yleiset tiedot turvallisuusohjeistuksesta ja tähän osioon lisätään uudet ohjeistusten kuvaukset ja linkit niihin.

KATAKRI	Liite
A105.0	
A803.0	

(152)

A805.0	
A806.0	

7.1 Turvallisuusohjeet ja -koulutus

Henkilöstöllä on mahdollisuus tutustua keskeisimpiin turvallisuusohjeisiin Intranetissä. Turvallisuusohjeita käydään myös läpi kouluttamalla ja varsinkin uusille työntekijöille selvitetään organisaation turvallisuustoiminnan periaatteet. Turvallisuusohjeiden kouluttamisesta pidetään rekisteriä, jotta voidaan todeta koko henkilöstön käyneen vaaditut ohjeistukset. Riskienarviointi antaa perustan turvallisuuskoulutukselle.

Laitoksen koko henkilöstölle koulutetaan henkilöstö-, toimitila- ja tietoturvallisuuden vaatimukset ja periaatteet tasovaatimusten mukaisesti. Projektihenkilöstö koulutetaan projektikohtaisesti ja myös sidosryhmien henkilöt koulutetaan. Henkilöstölle myös selvitetään omiin työtehtäviin kohdistuvat keskeisimmät turvallisuusriskit.

KATAKRI	Liite
A406.0	
A801.0	
A802.0	
A804.0	

7.2 Vierailumenettelyt

Laitoksella on oma vierailumenettelynsä, joka löytyy liitteestä X. Vierailumenettelyn tarkoituksena on suorittaa kulunvalvontaa ja tarpeen vaatiessa voidaan selvittää mahdolliset poikkeamatilanteet, kuten laittomat kulut toimitiloissa. Turvaluokiteltuihin tiloihin on olemassa erillinen ohje, joka on liitteessä x.

KATAKRI	Liite
P104.0	
P606.0	
F209.2	

(152)

7.3 Etä- ja matkatyöskentely

Laitoksella on laadittuna Intranetiin ohjeet etätöiden tekemiseksi.

(liite x)

KATAKRI	Liite
I704.0	

7.4 Tiedottaminen ja turvallinen tiedonhallintatapa

Laitoksella on laadittuna viestintästrategia, jossa on kuvattuna viestinnän yleiset periaatteet ja niihin liittyvät vastuut. Tiedottamisella pyritään vaikuttamaan tiedon laatuun ja määrään. Tiedottaminen tapahtuu pääsääntöisesti Intranetin kautta.

(viestintästrategia liite x)

8 Seuranta, valvonta ja auditointi

Laitoksella on suoritettavana kansallisen turvallisuuden auditointiprosessi, joka sisältää auditointikohteet, ajankohdat ja auditointiresurssit. Auditoinnilla tarkistetaan ja varmistetaan, että (turvallisuus)politiikat ovat ajan tasalla ja että lakia ja säädöksiä noudatetaan sekä sitä, että suunnitellut menettelytavat ovat käytössä ja että ne ovat riittäviä ja tehokkaita. Arviointi suoritetaan riippumattoman ulkopuolisen virnaomaisen puolesta. Puutteet ja heikkoudet dokumentoidaan, korjataan ja raportoidaan. Laitoksen vastuuhenkilön on ryhdyttävä tarvittaviin toimenpiteisiin ja korjaavien toimenpiteiden toteutuminen tarkistetaan. Turvallisuusryhmä voi tehdä turvallisuuteen ja sen hallintaan liittyviä tarkastuksia omien suunnitelmiensa mukaisesti.

Turvallisuustoiminnan tasoa ja tehokkuutta mitataan säännöllisesti, jotta voidaan todeta nykytilanne ja muutoksen suunta sekä tehdä tarvittaessa päätökset korjaavista ja parantavista toimenpiteistä.

Laitoksessa tehdään turvallisuuden auditointeja tai arviointeja vuosittain. Auditoinnit tai arvioinnit kuvataan johdon puolivuosittain tarkastelemaan sekä hyväksymään turvallisuuskäsikirjaan. Kerran kolmessa vuodessa käydään läpi avaintoiminnot.

Auditointi- ja arviointiprosessin kulku pääpiirteittäin:

1. Auditointisuunnitelma
2. Suunnitelman hyväksyttäminen johdolla

3. Auditoinnin suorittaminen ja raportin laatiminen
4. Turvallisuuspäällikkö tai johdon osoittama muu vastuuhenkilö arvioi auditoinnin suositukset.
5. Auditoinnin tai arvioinnin tulokset raportoidaan toiminnon tai kohteen omistajalle. Samalla pyydetään mahdolliset kommentit ja oikaisut havaintoihin.
6. Sovitaan korjaavista toimenpiteistä kohteen vastuuhenkilön kanssa. Vastuuhenkilö määrittelee ja vastuuttaa parannustoimenpiteet. Tarvittaessa parannustoimenpiteet esitetään hyväksyttäväksi johdolle. Mikäli korjaavat toimenpiteet vaativat erillistä projektointia, tehtävät kirjataan tietoturvallisuuden ylläpito- ja kehittämissuunnitelmaan.
7. Raportoidaan auditointihavainnot toimenpide-ehdotuksineen johdolle.
8. Turvallisuuspäällikkö tai muu sovittu vastuuhenkilö tarkistaa ja hyväksyy korjaavat toimenpiteet. Merkittävissä poikkeamissa johto hyväksyy toimenpiteet.

Auditoinnin suorittajalla tulee olla tehtävään riittävä pätevyys ja työkokemus. Tarvittassa tehtävään käytetään ulkopuolista asiantuntijaa. Mikäli auditointi suoritetaan tiettyyn viitekehykseen nähden, tulee auditoijan olla riittävästi perehtynyt lähteeseen. Teknisen auditoijan tulee lisäksi olla riittävästi perehtynyt tekniseen (tieto)turvallisuuteen.

KATAKRI	Liite
A104.0	
A902.0	
A904.0	
A905.0	

9 Tärkeiden toimintojen, tieto-omaisuuden ja turvakontrollien hallinta

Laitoksen työtehtävät sekä ydintoiminnot ja -prosessit on kuvattu työjärjestyksessä. Laitoksella määritellään johdon vahvistamana turvallisuuden kannalta tärkeät kohteet ja niiden vastuuhenkilöt (omistajat). Kunkin vastuuhenkilön tulee varmistaa, että oman suojattavan kohteensa osalta turvallisuusasiat kunnossa. Tärkeiden toimintojen tieto-omaisuus ja turvakontrollit kuvataan taulukon 1 (Liite X) mukaisesti.

Yksikön/toiminnon nimi	Vastuuhenkilö(t)
Kuvaa lyhyesti toiminta/vastuualueet (kuvaa myös tietoturvavastuut)	

(152)

Mitkä ovat toimintaan kohdistuvat erityisvaatimukset (säädökset, sopimukset, tietoturvavaatimukset)?	
Mitkä ovat toiminnan tietoturvatavoitteet? Miten niitä mitataan?	
Mitkä asiat ovat toiminnan kannalta välttämättömiä, mitä ilman toimintaa ei pystytä tekemään (perustele)? Miten välttämättömät asiat on suojattu?	
Jos toiminnassa on häiriöitä, mihin/keihin se ensisijaisesti vaikuttaa?	
Mitä vaikutuksia on tietojen joutumisella ulkopuolisten tai asiattomien käsiin? Mistä tiedoista tällöin on kyse?	
Arvioi vakavuus 1-5 (1=ei erityistä merkitystä, 5=erittäin kriittinen)	
Arvioi todennäköisyys 1-5 (1=ei todennäköinen, 5=erittäin todennäköinen)	
Onko joitakin asioita, jotka erityisesti altistavat tällaiselle vahingolle? Jos on, niin kerro, mitkä:	
Miten tähän on varauduttu?	
Mitä vaikutuksia on 1) tietojen puutteellisuudella tai 2) sillä, että niiden todenperäisyydestä ei ole varmuutta tai 3) ne ovat muuttuneet virheellisiksi? Kerro, millaisista tiedoista olisi kyse.	
Arvioi vakavuus 1-5 (1=ei erityistä merkitystä, 5=erittäin kriittinen)	
Arvioi todennäköisyys 1-5 (1=ei todennäköinen, 5=erittäin todennäköinen)	
Onko joitakin asioita, jotka erityisesti altistavat tällaiselle vahingolle? Jos on, niin kerro, mitkä:	
Miten tähän on varauduttu?	
Mitkä järjestelmät tai palvelut ovat kriittisiä, jos ne ovat pois päältä tai eivät ole käytettävissä? Kerro vaikutuksista.	
Alle 2 tuntia	
Päivä	
Viikko	
Miten tähän on varauduttu?	
Tietoturvapäällikkö täyttää: Tietoturvallisuuden ylläpito- ja kehittämissuunnitelmassa huomiotavat erityisvaatimukset ja tavoitteet Suojattavien kohteiden turvallisuusluokittelu	

Taulukko 1. Tietoturvakortti

10 Tietoturvallisuus

Laitoksella tietoturvallisuus on tietojen, palvelujen, järjestelmien ja tietoliikenteen suojaamista ja varmistamista. Tavoitteena on taata tietojen luottamuksellisuus, eheys ja käytettävyys sekä saatavuus kaikissa olosuhteissa. Laitoksella on tietoturvallisuuspolitiikka, joka löytyy liitteestä x. Laitoksen tietoturvallisuutta arvioidaan vuosittain ja havaintojen perusteella tietoturvallisuuden tasoa kehitetään jatkuvasti. Tässä kappaleessa tarkastellaan laitoksen tietoturvallisuuden hallintaan liittyviä osa- alueita.

KATAKRI	Liite
A408.0	
A409.0	
A410.0	
A501.1	
A608.0	

10.1 Verkkojen ja järjestelmien valvonta

Verkkoliikenteestä tiedetään normaali tila, liikennemäärä ja käytetyt protokollat. Riskienarvioinnilla on mitoitettu resurssit järjestelmien toimivuuden takaamiseksi kaikissa olosuhteissa. Verkkoliikennettä myös tarkkaillaan ja sieltä havaitaan merkittävät poikkeamat, poikkeavat protokollat ja luvattomien yhteyksien yritykset. Verkoissa ja järjestelmissä olevat asetukset on dokumentoitu siten, että poikkeamatilanteet pystytään hoitamaan ja korjaamaan toimintavaatimusten mukaisesti. Dokumentaatio pidetään ajan tasalla, jotta se on yhdenmukainen toteutuksen kanssa ja eroavaisuuksia käsitellään turvallisuuspoikkeamina. Alempana on kuvattuna suojattujen tilojen tietojärjestelmien suojaustoimenpiteitä.

KATAKRI	Liite
I408.0	
I410.0	
I508.0	
I702.0	
I706.0	

10.1.1 Verkkolaitteet

Suojatun tilojen verkon laitteet on kovennettu.

KATAKRI	Liite
I405.0	

10.1.2 Tulostimet

Suojatussa tilassa kopiointia voi suorittaa vain suojaustasoa vastaavalla hyväksytyllä laitteella eikä niistä lähde ulkoisia tiedonsiirtoyhteyksiä.

KATAKRI	Liite
I604.0	

10.1.3 Menettelyt oikeuksien luomiselle, poistamiselle ja muutoksille

Suojattujen tilojen oikeuksien luomisesta ja poistamisesta päättää turvallisuuspäällikkö projektipäällikön esityksestä.

(liite x)

10.1.4 Käyttäjän tunnistaminen

Suojatuissa tiloissa työskentelevien henkilöiden tunnistaminen tehdään laitoksen virallisesta henkilökortista.

(liite x)

10.1.5 Käyttäjätunnustasot

Suojatuissa tiloissa käytettävissä tietojärjestelmissä käytetään erillisiä käyttäjätunnuksia kuin muissa laitoksen tietojärjestelmissä.

(liite x)

10.1.6 Palvelimien suojaus

Suojattavien tilojen palvelimet sijoitetaan suojaustasoa vastaavaan tilaan.

(liite x)

10.1.7 Tallennusvälineiden salaus

Kaikkien tallennusvälineiden salaus toteutetaan AES-256- menetelmällä. Tarkempi menettely tapauskohtaisesti.

(liite x)

10.1.8 Tietojärjestelmien ylläpito ja konfigurointi

Tietohallinto vastaa suojattavien tilojen tietojärjestelmien ylläpidosta ja konfiguroinnista.

(liite x)

10.1.9 Lokitietojen seuranta

Tietohallinto vastaa lokitietojen seurannasta.

(liite x)

10.1.10 Virustorjunta

Tietohallinto vastaa suojatuissa tiloissa sijaitsevien työasemien virustorjunnan ajantasaisuudesta viikoittain.

(liite x)

10.1.11 Toiminta poikkeustilanteissa

Poikkeustilanteissa toimitaan normaalien ohjeiden mukaan, ellei toisin mainita.

(Pelastussuunnitelma liite x)

(152)

10.2 Tietojen luokittelu

Laitoksen arkistonmuodostussuunnitelmasta vastaa X. Arkistonmuodostussuunnitelma käy ilmi tiedonhallinnan periaatteiden lisäksi arkistonmuodostuksen periaatteet. Julkisuuslain mukaista luetteloa käsiteltäviksi tulleista ja käsitellyistä asioista ylläpidetään järjestelmässä, jonka pääkäyttäjänä toimii X. (Arkistonmuodostussuunnitelma liite x)

Henkilöstölle tarkoitetut tietoaineistojen käsittelyohjeet ovat olemassa ja ne julkaistaan Intranetissä. Tietoaineistojen käsittelyohjeistus kuuluu osana henkilöstön perehdytykseen. Sidosryhmille tarkoitettu tietojenkäsittelyohjeistus liitetään sopimuksiin.

Dokumenteista käy ilmi, kuka dokumentin on laatinut, milloin sekä asiakirjan hyväksymisen tila. Dokumenttien hyväksyminen, katselmointi, luokitus ja salassapito on kuvattu laitoksen tietoaineistojen käsittelyohjeessa.

Laitoksella määritellään menettelytavat, joilla varmistetaan, että laitoksella noudatetaan aineistoihin ja ohjelmistoihin liittyviä tekijän ja muita aineettomia oikeuksia. Vastaavasti laitoksella huolehditaan siitä, että sille tulee ja sillä säilyy tarkoituksenmukaiset oikeudet laitoksella tai sen toimeksiannosta laadittuihin aineistoihin ja ohjelmistoihin. Hankkeen tilaajan turvaluokiteltua materiaalia käsitellään ja säilytetään suojaustasoa vastaavassa tilassa.

KATAKRI	Liite
I601.0	

10.3 Asiakirjaturvallisuus

Asiakirjat säilytetään arkistomuodostussäännön mukaisesti. Työntekijöiden on säilytettävä rajoitetun käytön tutkimusaineisto lukitussa tilassa ja luottamuksellinen tietoaineisto säilytetään kassakaapissa. Tarvittaessa asiakirjat säilytetään laitokselle hankituissa kassakaapeissa. Myös sähköistä tietoaineistoa käsitellään ohjeistuksen mukaisesti.

10.3.1 Asiakirjojen tunnistetiedot

Asiakirjoihin merkitään riittävät tunnistetiedot. Ne löytyvät suoraan asiakirjapohjasta tai merkinnät tehdään manuaalisesti.

(152)

10.4 Pääsyn rajoitus

Laitoksella on pääsynvalvontapolitiikka, jossa on kuvattu mm. eri turvatasoilla hyväksyttävät tekniset tunnistusmenetelmät, tunnusten lukitus- ja avausperiaatteet sekä salasanan tai muiden tunnisteiden laatuvaatimukset ja vaihtoperiaatteet. Sen ylläpidosta vastaa turvallisuuspäällikkö.

Tiedot ja tietojärjestelmät suojataan siten, että pääsy sallitaan vain niihin tietoihin ja järjestelmiin, jotka ovat tarpeen työtehtävien hoitamiseksi. Käyttövaltuudet ovat henkilö- tai roolikohtaisia. Valtuuksia myönnettäessä tai muutettaessa kiellettyjen työyhdistelmien syntymistä seurataan ja estetään. Huonolaatuisten salasanojen käyttöä estetään.

KATAKRI	Liite
P505.0	

10.5 Pääsynvalvonta

Tietoihin, järjestelmiin ja palveluihin pääsyn valvontaa koskevat vaatimukset määritellään työtehtäviin perustuen. Käyttäjät tunnistetaan ja todennetaan, ellei nimenomaisesti ole tarkoitus tarjota anonyymipalvelua. Uuden henkilön tullessa organisaatioon ensimmäinen tunnistus tehdään valokuvallisesta henkilöllisyystodistuksesta tai sähköiseen palveluun rekisteröitymisen osalta käyttäen samantasoista todennusmenetelmää.

Kaikilla käyttäjillä on yksilöllinen käyttäjätunnus ja siihen soveltuva todennusmenettely käyttäjän henkilöllisyyden varmistamiseksi. Salasanoihin perustuvassa todentamisessa käyttäjiltä edellytetään hyvää salasanakäytäntöä salasanan valinnassa ja käytössä.

Sekä onnistuneet että epäonnistuneet sisään kirjautumiset kirjoitetaan lokiin niin, että yksittäisen käyttäjän kirjautumiset järjestelmään voidaan selvittää ja yhdistää hänen henkilöllisyyteensä luotettavasti. Pääsynvalvontalokit säilytetään niin, että niitä ei päästä jälkikäteen muuttamaan. Niiden säilyttämisestä vastaa tietohallinto. Tunnistuksen epäonnistuminen liian monta kertaa peräkkäin tärkeimpiin järjestelmiin tai palveluihin aiheuttaa tunnuksen lukittumisen.

KATAKRI	Liite
I501.0	

(152)

10.6 Istunnonhallinta

KATAKRI: ssa esitettyä vaatimusta tämän osion osalta toteutetaan sillä tavalla, että suojaustaso III tietojärjestelmät eivät ole yhteydessä laitoksen muuhun verkkoon, joten tällä tavoin estetään istuntojen kaappaus ja kloonaus.

KATAKRI	Liite
I511.0	

10.7 Käyttövaltuushallinto ja varmenteiden myöntäminen

Laitoksella on määritelty ja dokumentoitu käyttöoikeuksien ja – valtuuksien hallintaprosessi sekä -periaatteet. Kukaan ei voi hyväksyä, päättää tai teknisesti toteuttaa itseään koskevia oikeuksia ja valtuuksia. Myöntöprosessista jää jälki, millä perusteella käyttäjälle on myönnetty käyttövaltuus.

Jokaisella käyttövaltuudella on henkilökohtainen omistaja. Kaikki lisäykset, muutokset ja poistot käyttövaltuuksia koskien dokumentoidaan. Yksittäisen käyttäjän käyttövaltuudet voidaan selvittää rekisteristä. Ylläpito- ja pääkäyttäjäoikeuksien määrää seurataan ja tilastoidaan.

Käyttövaltuudet perustuvat työtehtäviin (ks. luku 9.4) tai muuhun kirjalliseen sopimukseen ja järjestelmien käyttö estetään teknisesti ilman tarpeetonta viivytystä perusteen päätyttyä. Käyttöoikeuksien ja – valtuuksien ajantasaisuus tarkistetaan säännöllisesti tai työtehtävien muuttuessa. Järjestelmien käyttövaltuudet katselmoidaan vähintään kerran vuodessa ja tarpeettomat tunnukset, roolit ja valtuudet suljetaan tai poistetaan. Varmenteiden myöntämisestä, käytöstä ja uusimisesta on kirjallinen ohjeisto ja käytössä olevista varmenteista ajantasainen lista. Ohjeistoa ylläpitää tietohallinto ja turvallisuuspäällikkö.

10.8 Puhtaan pöydän ja näytön periaate

Henkilöstöä on ohjeistettu toimimaan työasemien kanssa siten, että työasemat lukitaan kun laitteelta poistutaan, istunnot päätetään töiden loputtua tai pitkillä tauoilla, laitteista kirjaudutaan ulos töiden päätteeksi sekä suojattavaa tietoa sisältäviä laitteita ei saa viedä suojaustason vaatimusten tasoisen fyysisen tilan ulkopuolelle.

Laitoksella noudatetaan puhtaan pöydän ja näytön periaatteita. Turvallisuusluokiteltu aineisto säilytetään suojaustason mukaisesti käsittelyn päätyttyä. Näyttö lukitaan tai tietokone sammutetaan laitteen äärestä poistuttaessa siten, etteivät tiedot, sovellukset ja yhteydet jää avoimiksi asiattomalle käyttäjälle. Tietokoneen sammuttamisesta annetaan tarvittaessa poikkeavat ohjeet (mm. tietoturvapäivitykset).

KATAKRI	Liite
F219.0	
I707.0	
I708.0	

10.9 Tietovälineet

Suojausluokiteltua tietoa sisältävien tallennusvälineiden (kuten USB- muistitikut, muistikortit, CD-/DVD- levyt, levykkeet, nauhakasetit) käyttö ohjeistetaan projektiohjeessa. (Liite x)

10.10 Tietojärjestelmäturvallisuus

Laitoksen tietoverkkojen ja – järjestelmien hallintaliikenne on eriytettyä ja salattua. Tietojärjestelmissä suojattavat tiedot on eritelty käyttöoikeusmäärittelyllä. Järjestelmien käytön aikana syntyvät suojatun tiedon väliaikaistiedostot hävitetään säännöllisesti. Kaikissa tallennusvälineissä palvelimista ja työasemista muistitikkuihin suojattava tieto salataan ja suojataan AES- 256 menetelmällä. Jos useamman projektin tai hankkeen saman tason suojattavaa aineistoa säilytetään samassa paikassa, niin ne eritellään käyttöoikeuksien mukaan eri hakemistoihin tai alueisiin.

Kehitys- ja testaus- sekä tuotantojärjestelmät ovat erilliset ja niissä olevat tiedot, tilit ja vastaavat poistetaan niiden mennessä poistoon tai huoltoon. Suojattavaa tieto ei kopioida alemman tason ympäristöihin.

KAKAKRI	Liite
I404.0	
I505.0	
I506.0	
I705.0	

(152)

10.10.1 ST IV tietojärjestelmät

Turvallisuusluokiteltua (käyttö rajoitettu) aineistoa säilytetään erillään muista suojaustasoista eikä sitä käsitellä mobiililaitteilla (älypuhelimet).

10.10.2 ST III tietojärjestelmät

Turvallisuusluokiteltua (luottamuksellinen) aineistoa säilytetään erillään muista suojaustasoista eikä sitä käsitellä mobiililaitteilla (älypuhelimet).

10.11 Jäännöstiedot

Henkilöstöä ohjeistetaan varomaan toimistosovellusten jäännöstietoja (esimerkiksi käytettäessä vanhoja asiakirjoja uuden pohjana). Jäännöstiedot poistetaan tarkoitukseen sopivalla välineellä/menettelyllä valmiista ja erityisesti Viraston ulkopuolelle toimitettavista asiakirjoista.

(liite x)

10.12 Kalenterikutsut

Suojattavia tiedostoja ei liitetä kalenterikutsuihin. Suojaustasoiset liitteet tulee lähettää erikseen salatun sähköpostin liitetiedostona tai viitata dokumentin sijaintipaikkaan.

10.13 Salaus

Tietojen salauksessa käytetään Utimacon ohjelmistoja, välineitä ja algoritmejä, jotka ovat vahvoiksi tunnettuja, tarkastettuja ja hyväksyttyjä asianomaiselle suojaustasolle. (liite x)

Salausavainten hallinta on vain valtuutettujen käyttäjien ja prosessien käytössä. Hallintaprosessit ja – käytännöt ovat dokumentoitu ja asianmukaisesti toteutetut.

KATAKRI	Liite
I509.0	
I510.0	

10.14 Tietojen tallennuspaikka ja varmistukset

Tiedot talletetaan suojaustason vaatimusten mukaiseen ympäristöön ja sellaiseen paikkaan, että se tukee varmuuskopiointimenettelyä. Varmuuskopioinnista vastaa projektikohtainen henkilöstö. Tietohallinto vastaa turvaluokitellun tietojärjestelmän lokitietojen varmuuskopioinnista. (jatkuvuus- ja toipumissuunnitelma liite x)

Virastossa on varmuuskopiointiprosessi, joka on muodostettu ottaen huomioon toiminnan vaatimukset ja joissa ohjeistetaan varmuus- ja suojakopioiden käsittely siirron ja varastoinnin aikana. Laitoksella kartoitetaan säännöllisesti varmuuskopioinnin kannalta tärkeät suojattavat kohteet ja niistä otetaan varmuuskopioita suunnitelman mukaisesti. Myös varmuuskopioiden palauttaminen on suunniteltu ja niiden palautusta testataan säännöllisesti. Laitoksella otetaan tärkeimmistä järjestelmistä suojakopioita, joita säilytetään eri palotilassa kun varsinaisia varmuuskopioita.

KATAKRI	Liite
I710.0	

10.15 Arkistointi

Arkistoinnissa noudatetaan tiedonhallintasuunnitelmaa ja arkistolaitoksen voimassa olevaa ohjeistoa.

10.16 Yksityisyyden suoja

Laitos kerää ja ylläpitää vain henkilötietolain sallimia toiminnalleen välttämättömiä rekistereitä, jotka suojataan asianmukaisesti. Henkilötietoja sisältävistä rekistereistä laaditaan asianmukaiset rekisteriselosteet, jotka ovat henkilöstön saatavilla. Henkilötietojen käsittelyssä noudatetaan lakien ja säädösten vaatimuksia. Hallintosihteeri vastaa henkilörekistereiden ylläpidosta.

KATAKRI	Liite
A701.0	

10.17 Tietojen luovutus

Tietojen luovutusta koskevat menettelytavat ja päätöksenteko on kuvattu tietoaineistojen käsittelyohjeessa.

(liite x)

10.18 Tietovälineen kierrättäminen ja käytöstä poisto

Aineiston siirto pyritään tekemään sähköisenä tiedonsiirtona, turvallisuusluokan edellyttämällä tavalla. Fyysistä tietovälinettä käytettäessä varmistutaan siitä, ettei tietovälineellä siirry vahingossa muuta aineistoa. Siirrettäessä tietoa fyysisellä tietovälineellä laitoksen ulkopuolelle on aina käytettävä luotettavasti tyhjennettyä tietovälinettä tai kokonaan uutta tietovälinettä ennen tarkoitetun aineiston siirtoa välineelle. Tarpeettomat ja vialliset tietovälineet hävitetään luotettavalla tavalla.

11 TIETOAINEISTOTURVALLISUUS

Tietoaineistoturvallisuudella tarkoitetaan tässä hyvää tiedonhallintatapaa, joka koskee tiedon koko elinkaarta. Esimerkiksi henkilötietojen käsittelyssä on otettava huomioon henkilötietolaki ja sen säännökset. Viranomaisten on myös huomioitava käytössään olevat tietovarannot ja niitä käyttävät tietojärjestelmät sekä tietoaineiston käsittelyprosessien ajantasaisuus. Tässä kappaleessa kuvaillaan, miten laitoksella on hoidettuna tietoaineistoturvallisuuden osa- alueita ja miten niistä on tiedotettu henkilöstölle.

KATAKRI	Liite
A105.1	
A306.0	
A807.0	

11.1 Tietojen säilytys

Tietojen säilytykseen liittyy toimenpiteet, joita esiintyy tiedon tallentamisessa, valmistelussa ja käyttövaiheessa. Julkinen ja turvaluokiteltu materiaali pidetään erillään. Vain käyttöoikeudet omaava pääsee käsittelemään luokiteltua tietoa. Autentikaatiodataa ei säilytetä selväkielisenä tietojärjestelmissä. Suojausluokitelluista tiloista luokiteltu aineisto säilytetään kassakaapissa.

KATAKRI	Liite

(152)

I512.0	
I602.0	

11.2 Tietojen käsittely

Tietojen käsittelyssä toimitaan huolellisesti ja erityisesti turvallisuusluokiteltujen tietojen käsittelyssä. Lait, asetukset ja sopimukset asettavat tiettyjä vaatimuksia tietojen käsittelyn osalta. Turvaluokitellusta tietoaineistosta käsittelystä erillinen ohje (tiedonkäsittelyohje liite x). Hanke- ja projektikohtaisia tietoja käsitellään vain suojatuissa tiloissa.

11.2.1 Menettelyt turvallisuusluokitellun tiedon käsittelyssä

ST IV ja ST III

kirjelähetys

kirjeiden vastaanotto

Elektronisen materiaalin lähettäminen

Elektronisen materiaalin vastaanottaminen

(tiedonkäsittelyohje liite x)

AES- 256 kryptattuja.

11.2.2 Perehtymisoikeus materiaaliin

Henkilöillä on oltava työtehtäviin liittyvä ja määritelty oikeus perehtyä (suojattuun) materiaaliin.

11.3 Tietojen lähettäminen ja välittäminen

Laitoksella tietoa siirretään eri muodoissa ja asiakirjat ovat yleisin muoto. Suojaustasoille I-III luokitellut asiakirjat osoitetaan tietylle henkilölle, tehtävää hoitavalle tai organisaatiolle ja lähettäjä varmistuu siitä, että vastaanottajalla on riittävät oikeudet käsitellä tietyn turvallisuustason asiakirjaa. Lähettämisestä, välittämisestä ja luovuttamisesta tehdään dokumentti.

KATAKRI	Liite
I602.0	

(152)

I605.0	
I606.0	

11.4 Lähetysten kirjaaminen, postikirja ja diaarikirja

Lähetykset kirjataan tarpeen mukaan. EU: n turvallisuusluokiteltu tieto diarioidaan.

KATAKRI	Liite
I607.0	

11.5 Tietojen kopiointi

Tietoja voidaan kopioida ottamalla esimerkiksi asiakirjoista jäljennöksiä. Suojaustasosta riippuen kopioita käsitellään kuten alkuperäistä, identtisyys varmistetaan, jäljitettävyys tulee varmistaa sekä kopiot leimataan alkuperäistä vastaavalla leimalla.

11.6 Tietojen hävittäminen

Tarpeeton tietoaineisto hävitetään luotettavalla, turvallisuusluokan edellyttämällä tavalla. Sähköiset tiedostot tuhotaan välineiltä, työasemilta, palvelimilta ja muilta laitteilta. Paperiset asiakirjat hävitetään polttamalla, silppuamalla tai kerätään tietosuojasäiliöön ja viedään asianmukaiseen ja valvottuun paikkaan tuhottavaksi. Kaikki projektien tai hankkeiden käytössä olleet laitoksen laitteet puhdistetaan (kovalevyt ylikirjoitetaan), ennen siirtoa muuhun käyttöön (tai käytöstä poistoa). Turvaluokiteltu tieto tuhotaan silppurilla.

KATAKRI	Liite
I603.0	

11.7 Materiaalin tuhoaminen

Kaikki projektien käytössä olleet laitoksen laitteet puhdistetaan (kovalevyt ylikirjoitetaan), ennen siirtoa muuhun käyttöön (tai käytöstä poistoa). Poistetut laitteet lähetetään kierrätykseen ja kovalevyt irrotetaan erikseen tuhottavaksi.

(liite x)

11.7.1 Puhelin ja langattomat viestimet

Suojattua materiaalia ei käsitellä puhelimilla eikä langattomilla viestimillä. Suojatuissa tiloissa ei ole edes mahdollista käyttää puhelinta eikä sinne saa viedä puhelinta ja kannettavissa tietokoneissa on estetty langattoman verkon käyttö.

12 Teknisen tietojenkäsittely- ympäristön turvallisuus

Tietojenkäsittelyverkot on eritelty fyysisesti ja loogisesti sekä niistä ei ole liittymiä alemman suojaustason ympäristöihin.

KATAKRI	Liite
I401.0	

12.1 Teknisten ympäristöjen dokumentointi

Tietoteknisen ympäristön kuvauksesta vastaa tietohallinto. Tietojärjestelmäkuvauksia ylläpidetään Intranetissä. Suojatun tilan kuvaukset katselmoidaan kerran vuodessa. Tekniset ja fyysiset turvallisuusjärjestelyt on dokumentoitu järjestelmäkorttiin (tietohallinnon tiloissa, ei julkinen).

12.2 Ohjelmistoturvallisuus

Ohjelmistot hankitaan vain luotettavista ja luvallisista lähteistä ja ohjelmien asennus tapahtuu tietohallinnon kautta. Uudet asennettavat ohjelmat ja niiden päivitykset tarkistetaan. Ohjelmiston toimittajalta vaaditaan selvitys ohjelman turvallisuudesta.

KATAKRI	Liite
I513.0	

Sovelluskontrollit ja jäljitettävyys

Uuden ja olemassa olevan järjestelmän tietoturvavaatimukset analysoidaan ja määritellään. Määrittelyjen perusteella ohjelmistoihin suunnitellaan ja toteutetaan riittävät sovelluskontrollit ja jäljitysominaisuudet. Sovelluskontrolleissa otetaan huomioon mm. järjestelmään pääsy ja käyttövaltuudet, tiedon syöttö, käsittely, säilytys, liittymät ja tiedonsiirto sekä raportointi ja tulostus.

Laadunvarmistus ja katselmoinnit

Ohjelmien kehitys- ja ylläpitotyössä sovelletaan laadunvarmistusmenettelyitä, joilla todetaan tehdyn työn asianmukaisuus, määritysten mukaisuus, vaadittujen tehtävien tekeminen sekä dokumentointi.

Testiaineistojen suojaus

Testiaineistot suojataan asiattomalta muuttumiselta, paljastumiselta ja häviämiseltä.

Lisenssien hallinta

Ohjelmistolisenssit ovat ajan tasalla ja hallinnassa. Käytössä on vain laillisesti hankittuja ohjelmistoja ja niiden lisenssiehtoja noudatetaan.

Asentaminen

Laitoksella vain tietohallinto saa asentaa ohjelmistoja, tietoliikenneyhteyksiä ja oheislaitteita. Turvallisuusasetusten muokkaaminen on vain tietohallinnon tehtävänä. Uusien järjestelmiin, päivityksiin ja muihin vastaaviin on hyvyyskriteerit, jotka nykyiset ohjelmistot ym. Täyttävät.

Kaikissa ohjelmistoasennuksissa otetaan huomioon tietoturvallisuusvaatimukset. Ohjelmiston turvallisuusominaisuudet selvitetään ja otetaan harkitusti käyttöön. Oletustunnukset ja -salasanat muutetaan.

KATAKRI	Liite
I703.0	

Huolellinen ylläpito

Ohjelmistoja ylläpidetään suunnitellusti ja dokumentoidusti.

12.3 Laitteistoturvallisuus

Turvallisuusasiat otetaan huomioon laitehankinnoissa.

KATAKRI	Liite
I514.0	

Rekisteröinti ja turvamerkinnät

Kaikki tietotekniset laitteet merkitään henkilökohtaisesti ja luetteloidaan laiterekisteriin.

Asennusvaatimusten noudattaminen

Tietohallinto huolehtii kaikista laiteasennuksista ja lopputuloksena on kovennettu asennus suojatuissa tiloissa. Laitteet asennetaan suunnitelmallisesti ja vakioidulla tavalla. Yhteiskäyttöiset laitteet (mm. palvelimet, verkon aktiivilaitteet) asennetaan suojattuihin tiloihin. Tietojärjestelmään saadaan asentaa tai liitää vain järjestelmän omistajan hyväksymiä ohjelmia ja laitteita.

KATAKRI	Liite
I502.0	
I703.0	

Säännöllisen ylläpidon suunnittelu

Laitteiden ylläpito tehdään suunnitelmallisesti. Tietohallinto huolehtii laitteiden ja tietojärjestelmien päivitysten tarpeen seurannasta, päivityspäätösten teosta ja päivitysten asennuksesta. Tietohallinnolla on kirjalliset periaatteet, jotka kertovat, millaiset päivitykset tai muutokset asennetaan välittömästi ja millaisiin päivityksiin ja muutoksiin käytetään riskitason huomioon ottavaa tarveharkintaa. Päivitykset ja muutokset testataan mahdollisuuksien mukaan ennen kuin ne otetaan tuotantokäyttöön.

Laitoksen tietohallinto seuraa säännöllisesti päivitysten ajantasaisuutta ja mittaa niiden onnistumista. Sopimuksissa on huomioitu, että muut kuin päivitys- ja muutos-

hallintaperiaatteiden perusteella kiireellisinä toteutettavat päivitykset tai muutokset tehdään vain etukäteen sovittuna aikana.

Laitteistojen kunnossapito ja huolto

Laitteistojen kunnossapidosta huolehditaan valmistajan suositusten mukaisesti ja laitteistoilla on käytettävyysvaatimusten mukaisesti harkitut huoltosopimukset. Kriittisessä käytössä ei pidetä kolmea vuotta vanhempaa laitteistoa, ellei sitä kahdenneta tai se voidaan siirtää vähemmän kriittiseen käyttöön. Tietosisältö ei saa tavanomaisen huollon yhteydessä siirtyä laitoksen ulkopuolelle vioittuneellakaan medialla vaan laitteet tyhjennetään tai tuhotaan poiston tai huollon yhteydessä. Suojattavaa materiaalia sisältäviä kiintolevyjä ei luovuteta vaihdon yhteydessä, vaan ne hävitetään itse.

KATAKRI	Liite
I507.0	

Käytöstä poisto ja kierrättäminen

Laitteiden käytöstä poisto tehdään suunnitelmallisesti. Ennen laitteen mahdollista siirtoa muuhun käyttöön, myyntiä, lahjoittamista tai romuttamista huolehditaan tarvittaessa tietosisällön ottamisesta talteen. Tämän jälkeen käytöstä poistettavalta laitteelta hävitetään kaikki tiedot ja ohjelmat luotettavalla tavalla. Lisenssihallinnollisesti otetaan huomioon ohjelmistojen poistaminen sekä käyttöjärjestelmän mahdollinen jääminen laitteelle. Vastaavasti käytöstä poisto otetaan huomioon laite- ja käyttöomaisuusrekistereissä.

12.4 Tietoliikenneturvallisuus

Tietoliikennettä suojaavien ja suodattavien laitteiden, kuten palomuurien, säännöstöt ja haluttu toiminta varmistetaan säännöllisin tarkastuksin. Eri turvatasojen tietoverkot ja verkkosegmentit eriytetään toisistaan suojaustarpeen (suojaustasovaatimuksen) kannalta tarkoituksenmukaisella ratkaisulla (esim. kytkin, VLAN, palomuuri, fyysinen eriyttäminen). Eri suojaustason verkkojen välistä liikennettä ei ole ollenkaan.

Julkisesta verkosta organisaatioon sisäänpäin tulevaa liikennettä rajoitetaan ja suodatetaan ”kaikki liikenne on kielletty ellei erikseen sallittu” - periaatteella. Myös organisaatiosta julkiseen verkkoon lähtevää liikennettä suodatetaan. Langaton vierasverkko on erillään laitoksen sisäverkosta.

Palomuurien ja muiden tietoliikennelaitteiden sääntöjen lisäämisestä, muuttamisesta ja poistamisesta vastaa tietohallinto. Palomuurien tai muiden suodatuslaitteiden suodatussäännöt on dokumentoitu tietohallinnossa.

(152)

KATAKRI	Liite
I402.0	
I403.0	
I406.0	
I407.0	
I409.0	

Kiinteistövalvontaverkon eriyttäminen

Kiinteistönvalvontaverkko eriytetään tietoverkoista loogisesti ja fyysisesti.

Tietoliikenneyhteyksien ja turvajärjestelyiden dokumentointi

Tietoliikenneyhteydet ja niiden turvajärjestelyjen dokumentoinnista huolehtii tietohallinto. Palomuuri- ja liikenteensuodatuspolitiikka ovat kirjalliset. Suojattujen tilojen sääntöjen päivitysprosessi on kirjallinen. Palomuurien tai muiden suodatuslaitteiden säännöstöjen ajantasaisuutta katselmoidaan säännöllisesti.

Kaapeloinnin suojaus

Tietoverkon kaapelointi sijoitetaan ja suojataan asiattomalta irrottamiselta, katkeamiselta, kulumiselta, häiriöiltä ja salakuuntelulta. Mahdollisuuksien mukaan käytetään materiaaleja, jotka ovat immuunimpia häiriöille ja salakuuntelulle.

Aktiivilaitteiden suojaukset ja asetukset

Verkon aktiivilaitteet sijoitetaan fyysisesti turvattuihin tiloihin ja ne konfiguroidaan siten, että tunkeutumisen riskit minimoidaan.

Ulkoisten yhteyksien turvaaminen

Ulkoisissa tiedonsiirtoyhteyksissä pyritään vikasietoisuuteen. Tarvittaessa järjestetään fyysisesti erilliset varayhteydet.

Lokien hallinta

Lokien keräämiseen, hälytyksiin ja lokien seurantaan on laadittu prosessi, joka huomioi toiminnan vaatimukset. Laitoksella varmistetaan, että laitteet, ohjelmistot se-

kä tietojärjestelmät tekevät riittäviä lokeja ja kirjausketjuja toiminnastaan. Lokien seurannan perusteella muodostetaan tilannekuvaa ja havaitaan turvallisuuspoikkeamia sekä kehitetään toimintaa. Lokitietojen käsittelyssä huolehditaan Sähköisten viestien, tunnistamistietojen sekä paikkatietojen luottamuksellisuudesta ja oikeasta käsittelystä.

KATAKRI	Liite
I504.0	

Tunkeutumien havaitsemis- ja estämisjärjestelmät

Toimiminen turvallisuuspoikkeamatilanteissa on kuvattu liitteessä x.

KATAKRI	Liite
I504.0	

Haittaohjelmilta suojautuminen

Laitoksella on asennettuna kaikkiin järjestelmiin haittaohjelmatorjuntaohjelmisto. Haittaohjelmakuvaukset päivittyvät säännöllisesti ja automaattisesti. Haittaohjelmistokuvausten ajantasaisuutta valvotaan. Haittaohjelmasuodatuksen kattavuutta mitataan ja seurataan.

Toimiminen turvallisuuspoikkeamatilanteissa on kuvattu liitteessä x ja se on ohjeistettu henkilöstölle. Työasemia ja muita välineitä ei kytketä korkean tietoturvallisuustason verkkoihin.

KATAKRI	Liite
I503.0	

Monitoimikone

Monitoimikone on sijoitettu suojattuun tilaan käyttötarpeen perusteella. Luokitellun materiaalin tulostuksen vastaanottoon käytetään nimettyjä ja ilmoitettuja laitteita ja näiden laitteiden tulostaminen on valvottua.

Etäkäyttöyhteydet

(152)

Yhteyksien avaamisessa käytetään vahvaa tunnistusta ja todentamista sekä liikenteen salausta. Etäkäyttömahdollisuus rajataan etäkäyttöohjeen mukaan. Etätyöohje liitteessä x.

KATAKRI	Liite
I402.0	

13 Tietojärjestelmien ylläpito ja kehittäminen

Laitoksella on järjestelmien ja sovellusten hankintaan, kehitykseen, käyttöönottoon, ylläpitoon ja käytöstä poistamiseen turvallisuusvaatimukset huomioon ottava ohje. Ohjeen ylläpidosta vastaa tietohallinto.

Järjestelmiin kohdistetaan riskianalyysi, jolla pyritään löytämään turvallisuusvaatimukset tarjouspyyntöön, vaatimusmäärittelyyn tai uuden version asennuksen projektisuunnitelmaan. Järjestelmän omistaja hyväksyy, mitä tietoturvallisuustasoa järjestelmän tulee valmiina tai muutosten jälkeen noudattaa, kunhan se on arkkitehtuurilinjauksen mukainen. Laitoksella tulee olla turvallisuusvaatimuksia sisältävä tietojärjestelmien arkkitehtuurilinjaus, jonka mukaisia hankittavien tai kehitettävien järjestelmien tulee olla.

Järjestelmän toimivuus testataan ennen tuotantokäyttöön ottamista. Jos yksikkö hankkii räätälöityjä tietojärjestelmiä tai kehittää niitä itse, sillä tulee olla käytössään dokumentoitu tietojärjestelmän kehitysprosessi, jonka eri vaiheissa on otettu tietoturvallisuus huomioon.

Osana hankinta- tai kehitysprojektia järjestelmästä valmistuu kirjallinen turvallisuussuunnitelma ja käyttäjän ohje, joissa kerrotaan miten järjestelmä suojataan tuotantokäytössä ja millaiset ovat käyttäjiltä vaadittavat turvallisuustoimenpiteet. Järjestelmän määritykset ja toteutukset auditoidaan turvallisuuden osalta. Turvallisuuspäällikkö tarkastaa järjestelmän tietoturvakuvauksen, -suunnitelman tai -suunnitelmat. Kehitys- tai räätälöintityön aikana järjestetään katselmointeja tietoturvallisuuden kannalta kriittisiin osiin ja katselmoinneista valmistuu pöytäkirja.

Dokumentointi

Tietojärjestelmät dokumentoidaan käytettävän systeemityömallin ja laitoksen dokumentointistandardin mukaisesti. Kirjanpitoon ja sen esikäsittelyyn liittyvistä järjestelmistä ylläpidetään menettelytapakuvausta, jossa esitetään mm. sovelluskontrollit, kirjausketju ja täsmäytykset. Dokumentaatio suojataan luvattomalta käytöltä.

Järjestelmän hyväksyntä

Uudet järjestelmät ja versiot testataan ja hyväksytään tietohallinnossa ennen käyttöön ottoa.

Standardiratkaisujen ja – rajapintojen käyttö

Valittavat ratkaisut, tuotteet ja palvelut ovat keskenään yhteensopivia. Yleisesti hyväksyttyjä standardeja suositaan ja niiden käyttöä vaaditaan.

Arkkitehtuuriyhteensopivuus

Ohjelmistot sopivat laitoksen verkko-, sovellus-, laite- ja turvallisuusarkkitehtuuriin.

Käyttäjätietojen hallinta, käyttäjien todennus ja pääsyoikeudet

Ohjelmistojen vaatimat käyttäjätiedot ja pääsyoikeudet säilytetään ja hallitaan huolellisesti ja turvallisesti. Käyttäjien todennuksen tietoturvataso valitaan suojattavien tietojen turvaluokituksen perusteella.

Muutosten hallinta

Kaikki korjaus- ja kehitystoimenpiteet käsitellään muutoshallintamenettelyn kautta ennen toimenpiteisiin ryhtymistä. Hätämuutokset tositetaan jälkikäteen vastaavan menettelyn kautta.

Tukipalvelut

Ohjelmistojen osalta huolehditaan siitä, että saatavilla on riittävät tuki- ja päivityspalvelut.

Koulutus

Ylläpitäjät ja käyttäjät saavat riittävän koulutuksen ohjelmiston hallintaan ja käyttöön. Sovellushankintaan ja – kehitykseen osallistuville järjestetään riittävä tietoturvakoulutus.

(152)

Tietotekniikan hankinnat hoitaa keskitetysti tietohallinto. Tämä koskee sekä tietotekniikan laitteistoja että laitoksen yhteiskäyttöisiä toimisto-ohjelmistoja ja tietojärjestelmiä. Projektikohtaisia erityisohjelmia hankitaan osastojen omista määrärahoista. Osastojen hankinnat tulee tehdä yhteistyössä tietohallinnon kanssa, jotta voidaan varmistaa soveltuvuus laitoksen työasemaympäristön kanssa ja järjestää keskitetty lisenssihallinta palveluntarjoajan kautta.

Työasemahankinnat

Laitoksen työasemat ja tulostimet ovat ostettuja. Hankinnat toteutetaan laitteistojen elinkaaren mukaisesti suurehkoina kokonaisuuksina. Kaikki laitteet hankitaan Hanselin puitesopimustoimittajilta.

15 Laitteet

Laitoksella on laitteina pääasiallisesti työasemia, kannettavia ja muita tietojärjestelmien osia.

15.1 Luettelo ohjelmistoista

Laitoksella käytetään vain tiettyjä ohjelmistoja laitteistossa. Luettelo ohjelmistoista on liitteessä X.

15.2 Luettelo laitteista

Kaikista hankittavista laitteista laaditaan luettelo, josta ilmenee ID- numeron tarkkuudella kaikki sen tiedot sekä kenelle se on menossa. Luettelo laitteista löytyy laiterekisteristä.

16 Toimitilaturvallisuus

Toimitilaturvallisuus sisältää kaikki kiinteistöön, alueeseen ja tiloihin liittyvän turvallisuuden. Laitoksella otetaan huomioon kehäajattelulla alue-, kuori-, tila- ja kohdesuojaus. Kriittisimmät tilat on suojattu suojaustason mukaan ja niiden suojaamisessa on noudatettu myös sidosryhmien vaatimuksia.

16.1 Yleistä

(152)

Laitoksen toimitilat jaetaan suojaustason mukaan turvallisuus- ja käyttötarpeiltaan erilaisiin vyöhykkeisiin ja asetetut tasot dokumentoidaan. Vyöhykkeiden välistä kulkemista rajoitetaan ja valvotaan. Suojattujen tilojen kulunvalvontamenettely on dokumentoitu.

Kulkuoikeudet ja kulunvalvontatoimet määräytyvät henkilö- ja roolitasolla, jotka määritellään työtehtäväkohtaisesti. Eri suojaustasovyöhykkeille ja turva-alueille luodaan ja ylläpidetään tarvittavat lisäturvallisuusjärjestelmät ja – menettelyt.

Suojattavat tietoaineistot, niiden käsittely ja tietojen käsittelyyn tarkoitetut laitteistot ja käyttötoiminnot sijoitetaan suojaustason mukaan valitulle turvallisuusvyöhykkeelle tai – tilaan. Ulkopuolisten henkilöiden toimintaa tiloissa valvotaan projektikohtaisesti ja pääsyoikeudet määritellään myös ulkopuolisille henkilö-, rooli- ja työtehtäväkohtaisesti.

Kaikki asiakaspalvelu ja neuvonpito ulkopuolisten vieraiden kanssa järjestetään aina yleisellä tai rajoitetulla alueella ja henkilöstölle on ohjeistettu vierailukäytänteet. Ylimääräistä asiointia ja vierailuja toimistotiloissa ja työhuoneissa pyritään välttämään.

16.2 Rakennukset ja tilat tarkennettuna

Päärakennuksen lisäksi on yksi erillinen toimistorakennus sekä autokatos. Laitoksella on toimitiloja 3122 neliömetriä kolmessa kerroksessa, joista 2,5 kerrosta maan päällä. Toimitilat on jaettu laboratoriosiipeen, kirjastosiipeen ja entiseen asuntoon, jossa tietohallinto työskentelee.

16.3 Ulkoalueet

Laitoksen lähiympäristössä ulkoalueena on pääosin metsää, tietä ja parkkipaikkoja. Alueen aitaamista ei ole katsottu tarpeelliseksi.

KATAKRI	Liite
F101.0	
F102.0	
F103.0	

16.4 Pääsyoikeudet

(152)

Kulunvalvontajärjestelmän pääkäyttäjänä toimii hallintosihteeri ja pääsyoikeudet kiinteistöön määritellään kaikille henkilöille työtehtäväkohtaisesti ja projektien osalta tarpeen mukaan. Kaikkien henkilöiden pääsy – ja käyttöoikeuksia hallitaan hyvän tiedonhallintatavan mukaisesti. Kiinteistössä vierailevien henkilöiden tiedot merkitään vieraskirjaan vierailuiden yhteydessä.

Suojausluokiteltuihin tiloihin on vain asianomaisilla pääsy, jotka on perehdytetty suojatussa tiloissa työskentelyyn. Suojattuihin tiloihin pääsyoikeudet myöntää turvallisuuspäällikkö projektipäällikön esityksestä.

KATAKRI	Liite
F209.0	
F209.1	

16.5 Tilojen lukitus

Toimitilojen lukitus on toteutettu pääosin sekä mekaanisella avaimella että kulunvalvontajärjestelmällä. Toimistohuoneisiin on pääsääntöisesti kuitenkin vain mekaaninen avain. Suojausluokiteltuihin tiloihin johtavat kulkuaukot pidetään aina lukittuina ja käyttölukon lisäksi aukoissa on varmuuslukko. Suojausluokiteltuihin tiloihin käyvät avaimet säilytetään turvallisuuspäällikön toimesta kassakaapissa.

KATAKRI	Liite
F210.0	

16.6 Yleisavaimet ja niiden käyttö

Kiinteistön yleisavainta käyttää pääsääntöisesti vahtimestari. Suojausluokiteltuihin tiloihin on eri mallia olevat yleisavaimet, joten alemman suojaustason tilan yleisavain ei käy ylemmän suojaustason tilaan. Suojaustason III tilan yleisavainta ei saa viedä toimitilojen ulkopuolelle.

KATAKRI	Liite
F213.0	

16.7 Avainten ja kulkuoikeuksien hallinta

Avaimia ja kulkuoikeuksia hallitaan henkilöstöhallinnosta, jossa hallintosihteeri on vastuussa näiden jakamisesta. Avaimia ja kulkutunnisteita luovutettaessa avaimesta, tunnisteesta ja näiden saajasta otetaan tiedot ylös, jotta vahinkojen tai väärinkäytösten sattuessa voidaan selvittää tapahtumia. Vastuuhenkilöllä on myös luettelo lukostokaaviosta ja avainkorteista. Suojattuihin tiloihin saa olla avain/kulkutunniste vain nimetyllä henkilöllä hankekohtaisesti. Vartiointi- ja huoltohenkilöstölle jaettavat avaimet sinetöidään ja niitä saa käyttää vain poikkeustilanteissa.

KATAKRI	Liite
F211.0	
F212.0	
F214.0	

16.8 Ikkunat

Laitoksella on ikkunoita lähellä maantasoa alle neljässä(4) metrissä ja kattoikkunoita. Toimitilojen ikkunoita valvotaan lasirikkoilmaisimilla.

KATAKRI	Liite
F202.0	
F203.0	

16.9 Rikosilmoitinjärjestelmä

Laitoksella on käytössä rikosilmoitinjärjestelmä, joka valvoo ovia, aukkoja ja tiloja. Järjestelmän toiminta ja ilmoituksen siirto testataan kerran kuukaudessa vartioimisliikkeen kanssa. Rikosilmoitinjärjestelmän hälyttäessä toimistoajan ulkopuolella paikalle tulee vartiointiliikkeen vartija tarkistamaan kohteen. Vasteajan (15min) noudattamista ja riittävyyttä testataan kerran vuodessa.

KATAKRI	Liite
F301.0	
F305.0	
F307.0	

16.10 Kassakaapit

Suojattavaa tietoaineistoa ja muuta materiaalia varten kassakaapit ovat sijoitettuna turvallisuuspäällikön tiloissa ja suojaustason III tiloissa.

KATAKRI	Liite
F208.0	

16.11 Vartiointi

Laitoksen vartioinnista vastaa Securitas Oy, jonka piirivartija käy tarkistamassa kohteen päivittäin ja asettamassa hälytykset päälle. Piirivartija käy kiertämässä kiinteistössä sovitut pisteet ja raportoi mahdollisista poikkeamista laitoksen yhteyshenkilölle. Piirivartijalla ei ole kulkuoikeuksia suojaustason III tiloihin. Tarkemmat yhteystiedot löytyvät pelastussuunnitelmasta (liite x).

16.12 Kulunvalvonta

Laitoksella kulkuoikeuksia jaetaan vain henkilöstölle ja hankekohtaisille vierailijoille. Kulkuoikeuksia jakaa hallintoyksikössä hallintosihteeri, mutta suojattuihin tiloihin kulkuoikeudet määrittää turvallisuuspäällikkö projektipäällikön esityksestä. Kulunvalvontajärjestelmään on liitetty pääsääntöisesti kaikki toimitilojen kuorella sijaitsevat ovet, kriittiset tilat sekä suojatut tilat. Henkilöiden kulkemisista on saatavilla jälkeenpäin kulkuraportit tarpeen vaatiessa. Henkilökunta ja vieraat pitävät laitoksen tiloissa ollessaan selvästi näkyvillä henkilö-/ vierailijakorttia. Laitoksen vierailukäytäntö ohjeistetaan erillisellä dokumentilla, joka löytyy liitteestä X.

KATAKRI	Liite
F302.0	
F306.0	

16.13 Muutokset kulunvalvontaan

Muutokset kulunvalvontaan tehdään tarpeen vaatiessa henkilöstöhallinnon henkilön toimesta hänen saadessaan käskyn hoitaa se. Henkilökohtaisten kulkuoikeuksien uudelleen määrittäminen tehdään työtehtävä ja projektikohtaisesti. Kulunvalvontajärjestelmään saadaan liitettyä myös uusia ovia tarpeen tullen.

(152)

16.14 Kameravalvonta

Kiinteistössä on kameravalvontajärjestelmä, joka kuvaa toimitiloihin sisään johtavia reittejä. Kameroiden tallenteet säilytetään X ajan, jonka jälkeen niiden päälle aloitetaan tallentamaan uusinta kuvamateriaalia. Palvelintilaan johtavalla ovella on kamera valvomassa kulkua.

KATAKRI	Liite
F104.0	
F303.0	
F304.0	

16.15 Huoltotoimenpiteet

Laitoksella kiinteistöhuollosta vastaa Coor- huoltoliike. Laitoksella on myös oma vahtimestari ja siivooja, sillä se on ollut helpompi toteuttaa kuin ostamalla palvelu ulkopuoliselta tarjoajalta. Suojattuihin tiloihin kohdistuvat huolto-, asennus- ja siivoustoimenpiteet tapahtuvat hankkeeseen hyväksytyn henkilön valvonnassa alusta loppuun.

KATAKRI	Liite
F215.0	
F216.0	
F308.0	

16.16 Rakenteet

Laitoksen toimitilat on rakennettu vuonna 1995. Toimitilojen seinät ja muut rakenteet ovat pääosin teräsbetonia ja suojattujen tilojen rakenteita on muutettu vaatimusten mukaisiksi. Tarkemmat tiedot pelastussuunnitelmassa (liite x). Luokitellut tilat on remontoitu 2013.

KATAKRI	Liite
F201.0	

(152)

16.16.1 Palo-osastointi ja paloturvallisuus

Laitoksen palo- osastointi on kuvattu toimitilojen pohjapiirustuksessa ja rakennuksen paloluokka on palonkestävä P1. Tiloissa on palovaroitin- ja – ilmoitinjärjestelmä sekä tarvittava alkusammutusvälineistö, jota osataan käyttää ja joka on asianmukaisesti huollettu. Automaattista sammutusjärjestelmää ei ole. Alkusammutuskaluston ja ensiapuvälineistön kartta on liitteessä x.

16.16.2 Lämpösuojaus

Tietoteknisissä laitetiloissa huolehditaan jäähdytys- ja ilmastointilaitteistolla lämpötilan pysymisestä laitevalmistajien ilmoittamien ohjearvojen sisällä.

16.16.3 Savusuojaus

Savun kulkeutuminen ilmanvaihtojärjestelmän kautta palo-osastosta toiseen estetään. Toimitiloissa on 6 savunpoistoluukkua, joista 2 toimii mekaanisesti sekä 4 elektronisesti.

16.16.4 Vesivahinkosuojaus

Tietoteknisissä laitetiloissa ei ole vesijohto-, lämmitys-, viemäri- tms. putkistoja, joista voisi aiheutua vesivahinkoa. Laitteistot sijoitetaan laitetilassa alapohjan päälle joko omille jalustoille tai laitetelineisiin. Alapohjan alle sijoitetaan kosteusilmaisimet.

16.16.5 Pölysuojaus ja puhtaus

Tietoteknisissä laitetiloissa käytetään pintamateriaaleja, jotka eivät muodosta pölyä. Tiloissa ei tehdä pölyä aiheuttavia toimintoja. Tuloilmasta suodatetaan epäpuhtaudet ja tilat siivotaan säännöllisesti laitoksen oman siivoajan toimesta. Suojattuihin tiloihin kohdistuvat huolto-, asennus- ja siivoustoimenpiteet tapahtuvat hankkeeseen hyväksytyn henkilön valvonnassa alusta loppuun.

16.16.6 Sähkön syötön ja laadun varmistaminen

Palvelintiloissa on UPS- järjestelmä. Kohteessa varavoima toteutetaan vain varauloskäyntien valoissa akkuvarmistuksella.

(152)

KATAKRI	Liite
F218.0	

16.16.7 Laitteistojen sijoitus

Tietotekniset laitteistot sijoitetaan ja suojataan siten, että luvattoman pääsyn ja olosuhdevahinkojen aiheuttamat riskit ovat hallinnassa. Sijoituksessa otetaan huomioon suojaustasoluokitus.

16.16.8 Ulkoisiin häiriöihin varautuminen

Ulkoisia häiriötilanteita (mm. pommiuhkaus, tiloihin tunkeutuminen, ryöstö, häiritsevä tai uhkaileva asiakas) varten laaditaan ja koulutetaan henkilöstön toimintaohjeet.

16.17 Aukot rakenteissa

Laitoksen toimitiloissa ei ole valvomattomia tai suojaamattomia aukkoja.

KATAKRI	Liite
F204.0	

16.18 Ovet

Laitoksella on pääosin umpinaisia ovia tai profiiliovia, jotka toimivat riittävästi äänieristeenä. Suojaustason III tilan ovet täyttävät vaatimukset.

KATAKRI	Liite
F205.0	
F206.0	

16.19 Laite- ja palvelintilojen valvonta

Laite- ja palvelintiloihin pääsee vain pääsyoikeuden saaneet henkilöt. Tiloihin johtaviin oviin on asennettu kulunvalvontajärjestelmä. Tiloihin johtaville ovilla on myös sijoitettu valvontakamera, jotta voidaan varmistaa oikean henkilön käyttäneen omaa tunnistettaan. Laitetilojen laitteista ja ohjelmistoista pidetään rekisteriä. Tilat tarkistetaan ylimääräisten laitteiden varalta säännöllisesti.

KATAKRI	Liite
I508.0	

16.20 Tilojen äänieristys

Suojausluokiteltuihin tiloihin on asennettu putkistoihin ja muihin aukkoihin äänieristeet, jotta äänet eivät pääse kulkeutumaan suojattujen tilojen ulkopuolelle.

KATAKRI	Liite
F207.0	

16.21 Varautuminen hajasäteilyyn ja salakuunteluun

Suojatuissa tiloissa on äänieristeet (ks. Edellinen kappale), tilan ovet pidetään suljettuina aina ja tiloissa ei käytetä ylimääräisiä elektronisia laitteita.

KATAKRI	Liite
F217.0	

16.22 Toimitilojen pohjapiirrokset

Toimitilojen pohjapiirrokset löytyvät liitteestä X.

17 Henkilöstöturvallisuus

Henkilöstöturvallisuuden tarkoituksena on suojata henkilöstöä uhkilta ja vaaroilta.

17.1 Henkilöstöluettelo ja muutokset henkilöstössä

Henkilöstöluettelo on henkilöstöhallinnossa ja on myös nähtävissä Intranetissä yhteystietoluettelona. Muutokset henkilöstössä menevät henkilöstöhallinnon kautta. Hankkeisiin osallistuvista henkilöistä tehdään erillinen luettelo, joka sisältää henkilön nimen, henkilötunnuksen, työtehtävän ja osaston tai organisaation. Turvallisuuspäällikkö määrittelee ja hallinnoi hankkeissa tapahtuvat muutokset projektipäällikön esityksestä.

KATAKRI	Liite
P101.0	
P102.0	

17.2 Rekrytointivaiheeseen liittyvät turvallisuusjärjestelyt

Uuden työntekijän henkilöllisyys tarkistetaan passista, ajokortista tai viranomaisen myöntämästä henkilöllisyystodistuksesta. Haastattelussa tarkistetaan taustatietojen, suosituksien, koulutuksen ja työhistorian oikeellisuus. Huumausainetesti suoritetaan tarvittaessa. Lisäksi haastattelussa varmennetaan henkilön kyky toimia laitoksen arvojen mukaisesti ja minkälaisia luottamustehtäviä on tehnyt aikaisemmin. Voidaan tehdä myös henkilö- ja soveltuvuusarviointitesti. Työsuhteen alussa pidetään koeaika. Laitokselle tulevat henkilöt kuitenkin tunnetaan pääsääntöisesti entuudestaan työn tai harjoittelun puolesta.

Turvallisuusselvitys teetetään määritellyistä tehtävistä, joihin kuuluvat ainakin tehtävät, joihin sisältyy merkittävää päätösvaltaa, merkittäviä hankintoja, maksuliikenteen hoitoa, laajaa pääsyä kriittisiin tietojärjestelmiin ja suojattaviin tietoihin, hallintaoikeuksia tietotekniikan perusinfrastruktuuriin tai hallintaoikeuksia turvajärjestelmiin. Katso myös luku 17.5. Turvallisuuteen liittyvät koko henkilöstölle tarkoitetut ohjeet ja määräykset jaetaan tai pidetään muuten koko henkilöstön saatavilla.

KATAKRI	Liite
P105.0	
P202.0	
P301.0	

(152)

P302.0	
P303.0	
P402.0	
P403.0	
P406.0	

17.3 Toimenkuva

Työtehtävistä on laadittu työjärjestys, josta ilmenee työhön liittyvät tehtävät, vastuut, oikeudet ja velvollisuudet. Työjärjestys löytyy Intranetistä. Rekrytoitaessa varmistetaan henkilön osaaminen työtehtävän osalta.

KATAKRI	Liite
P501.0	

17.4 Työtehtävien eriyttäminen

Työjärjestyksessä on eriytettynä tehtävät ja vastuualueet niin, että pystytään vähentämään suojattavien kohteiden luvattoman tai tahattoman muuntelua tai väärinkäyttöä. Vaarallisia työyhdistelmiä vältetään, mutta niiden varalle on menettelyohje. Kriittisimmät toimenpiteet vaativat kahden henkilön hyväksynnän.

KATKARI	Liite
I709.0	

17.5 Turvallisuusselvitykset

Turvallisuusselvityksiä tehdään tarpeen mukaan. Henkilöstö suostuu etukäteisesti työsopimusta tehdessään mahdollisen turvallisuusselvityksen tekemiseen, sillä pääpaino tutkimuslaitoksella on projekteissa, joiden vaatimukset vaihtelevat. Muuten selvitykset haetaan hanke- tai tehtäväkohtaisesti.

KATAKRI	Liite
P404.0	
P405.0	

17.6 Vaitiolo- ja salassapitositoumus

Perehdytys- ja koulutustilaisuuksissa tuodaan henkilöstölle esille salassapitoon liittyvät säädökselliset velvoitteet. Laajempia velvoitteita ja seuraamuksia asetettaessa tai muuten asian merkitystä korostettaessa vaaditaan erillisen salassapitositoumuksen allekirjoittamista. Ulkoisilta sidosryhmiltä vaaditaan aina salassapitositoumus, jos palvelua toimitettaessa on mahdollisuus päästä laitoksen tai sen hallinnassa oleviin tietoihin. Päästäkseen käsittelemään suojattavaa tietoa, kaikki työntekijät, kumppanit ja sidosryhmäläiset allekirjoittavat salassapito- tai vaitiolositoumuksen.

KATAKRI	Liite
P401.0	
P407.0	

17.7 Perehdyttäminen

Jokainen työntekijä osallistuu turvallisuusosuuden sisältävään tulokasinfoon. Tarvittaessa myös sidosryhmäläiset perehdytetään laitoksen turvallisuuskäytäntöihin ennen varsinaisten työtehtävien aloittamista. Tämän lisäksi jokaiselle työntekijälle nimetään perehdytyksestä vastaava henkilö. Perehdyttäjän turvallisuuden muistilista löytyy Intranetistä turvallisuusosiosta. Hankekohtainen perehdytys suoritetaan erikseen.

KATAKRI	Liite
P503.0	

17.8 Osaamispääoman hallinta

Laitoksella tehdään turvallisuuden osaamiskartoitus joka toinen vuosi. Tämän lisäksi esimies ja alainen käyvät vuosittain keskustelun turvallisuusvastuista sekä osaamisen kehittämisen tarpeista.

Hankkeeseen osallistuvalla henkilöstöllä tulee olla riittävä osaaminen työtehtäviinsä. Työntekijöiltä vaaditaan rekrytoinnin yhteydessä opinto- ja työhistoria, nimikirjainote, suositukset ja todistukset. Nämä varmistetaan haastattelussa, kuten kappaleessa 17.2 mainittu.

KATKARI	Liite
P103.0	
P201.0	
P203.0	

17.9 Turvallisuuskoulutus

Kaikille laitoksen työntekijöille annetaan asianmukaista koulutusta, jotta heillä on riittävä tietoisuus turvallisuutta uhkaavista tekijöistä ja edellytykset huolehtia omalta osaltaan turvallisuusvelvoitteista. Laitoksella järjestetään säännöllisesti vuosikellon mukaisesti turvallisuusseminaareja, jossa käsitellään ajankohtaisia turvallisuusasioita. Koulutusohjelma löytyy Intranetistä nimellä ”Turvallisuuden koulutusohjelma” tarkennettuna kevät-/-syysmerkinnällä sekä vuosiluvulla.

KATAKRI	Liite
P502.0	
P504.0	

17.10 Jaksaminen ja työkyky

Työssä jaksamista ja työkykyä seurataan säännöllisesti. Työntekijän toiminnan äkillisestä muutoksesta menetellään ohjeistuksen mukaan. Toimintavastuu tästä on esimiehillä.

KATAKRI	Liite
P602.0	
P603.0	
P604.0	

17.11 Turvallisuuden ohjeistus ja turvalliset käytännöt

Muuttuneista turvallisuusohjeista ja – käytännöistä tiedotetaan Intranetin kautta ja sen lisäksi sähköpostitse. Sääntöjen noudattamista valvotaan erityisesti esimiesten toimesta ja poikkeamiin puututaan. Turvallisuusmääräysten ja -ohjeiden sanktiomenettely on kuvattu Intranetissä ja tiedotettu kaikille laitoksella työskenteleville. Työntekijöiden tekninen valvonta on käsitelty YT- menettelyn mukaisesti (Laki yksityisyyden suojasta työelämässä, 21§, 1.)

17.12 Avainhenkilöiden kartoitus ja varahenkilöjärjestelyt

Laitoksen toiminnan kannalta kriittiset tehtävät ja avainhenkilöt on tunnistettu ja on luotu kattava varahenkilöjärjestelmä ja varahenkilöt koulutetaan tehtäviinsä. Ylimmän johdon tehtävien osalta huolehditaan, että laitoksella on vähintään kaksi osaajaa.

KATAKRI	Liite
P408.0	

17.13 VAP- varaukset

VAP- varauksista on tehty sijaisuusohjelma, jota päivitetään ja ylläpidetään.

KATAKRI	Liite
P601.0	

17.14 Kolmas osapuoli ja tukihenkilöstö

Ulkoisille palveluille ja toiminnoille nimetään laitoksesta vastuuhenkilö, joka huolehtii tarvittavasta ohjauksesta ja valvonnasta. Laitoksen vahtimestari ohjaa ja valvoo tarvittaessa ulkopuolisia.

17.15 Palvelussuhteen päättymiseen liittyvät turvallisuusjärjestelyt

Laitoksella huolehditaan siitä, että käyttö- ja pääsyoikeudet puretaan, avaimet ja henkilö- ja kulkukortit sekä tietoaineistot ja muu laitoksen omaisuus kerätään pois ja poislähtemisestä informoidaan tarvittavassa laajuudessa muuta henkilöstöä ja mahdollisesti myös sidosryhmiä. Organisaatiossa on menettelyohje työsuhteen päättämiselle. (menettelyohje tekeillä)

KATAKRI	Liite
P605.0	

17.16 Sanktiomenettelyt

Laitoksella puututaan turvallisuuspolitiikan ja – ohjeistuksen rikkomuksiin. Sanktiomenettelyt määritellään asianmukaisiksi ja rikkeet käsitellään yhtenevästi määritellyn menettelytavan mukaisesti. Suojaustason III turvallisuusrikkomuksissa toimivaltainen viranomainen tutkii rikkeet.

KATAKRI	Liite
A803.1	

18 Riskienhallinta ja jatkuvuuden varmistaminen

Kokonaisvaltaisen turvallisuusjohtamisen prosessi sisältää riskienarviointien perusteella tehtävää päätöksentekoa ja tehokkuuden arviointia. Laitoksella on riskienhallintapolitiikka, joka ohjaa riskienhallintaa ja priorisoi turvallisuustoiminnan painopisteitä. Laitos arvioi koko toimintaan kohdistuvat riskit ja riskien arviointi ohjaa turvallisuustoimintaa. Riskienarviointia suoritetaan ja päivitetään säännöllisesti vuosikellon mukaan ja tulokset dokumentoidaan.

Riskienarvioinnin avulla on tunnistettu suojattavat kohteet, niihin kohdistuvat uhat ja kohteille on nimetty vastuuhenkilö. Riskienhallintaprosessi on kuvattuna riskienhallintapolitiikassa (liite x). Riskienarvioinnin tuloksena riskit luokitellaan ja asetetaan tärkeysjärjestykseen.

Riskienhallinta on systemaattista ja jatkuvaa toimintaa, jonka avulla pyritään tunnistamaan, arvioimaan ja hallitsemaan toimintaa uhkaavia riskejä, arvioimaan niiden todennäköisyyttä ja merkitystä sekä hallitsemaan niitä tehokkaasti. Riskienhallinnan avulla pyritään varmistamaan organisaation toimintojen jatkuvuus.

KATAKRI	Liite
A401.0	
A402.0	
A403.0	
A405.0	
A406.0	
A407.0	
A606.0	

18.1 Riskienhallinnan menettelyt

Laitos tunnistaa ja arvioi toimintaansa kohdistuvia riskejä jatkuvasti. Lisäksi organisaatio arvioi vuosikellon mukaan säännöllisesti niitä tekijöitä, jotka voivat estää toiminta-ajatuksen toteutumisen tai tulostavoitteiden saavuttamisen. Riskianalyysin perusteella kohdennetaan resursseja tärkeimpiin toimintoihin ja valvonta kohdistetaan esille nousseihin suurimpiin riskeihin.

Laitoksella arvioidaan suojattavien kohteiden osalta riskit ja määritellään tarvittavat hallintatoimenpiteet. Riskien arviointiin sisältyy uhkien tunnistaminen, nykyisten hallintatoimenpiteiden selvittäminen, uhkien toteutumisen todennäköisyyden ja seurausten vakavuuden analysointi, nykytilanteen riskiluokitus, tavoitetilanteen riskiluokitus ja tavoitetilanteeseen pääsemiseksi tarvittavat toimenpiteet. Arviointi dokumentoidaan ja laitoksen johto tekee päätökset riskienkäsittelysuunnitelmasta ja hyväksyttävästä jäännösriskistä.

Turvallisuusriskejä arvioidaan ydintoimintojen ja – järjestelmien osalta vuosittain ja suurten muutosten yhteydessä. Vähimmäisvaatimuksena on riskien dokumentointi tärkeistä toiminnoista. Dokumentaatiota päivitetään vuosittain.

Merkittävistä riskeistä tehdään tarkempi arvio ja laaditaan toimenpiteet sen osalta. Toimenpidedokumenttiin merkitään päätös riskienhallintatoimenpiteistä. Projektoitavat riskienhallintatoimenpiteet kirjataan riskienhallinnan dokumentaaatioon.

KATAKRI	Liite
A401.2	

(152)

18.2 Toiminnan jatkuvuuden varmistaminen ja ennaltaehkäisevä toiminta

Laitoksella on jatkuvuus- ja toipumissuunnitelma ICT: n osalta, jossa on tunnistettu toimintaa uhkaavat tekijät sekä tärkeimmät toiminnot ja järjestelmät (liite x). Resurssien tarve on määriteltynä suunnitelmassa. Toimintaa uhkaavia häiriöitä seurataan ja arvioidaan samalla tavalla kuin itse jatkuvuuden hallinnan toteutumista. Riskienhallinnan avulla varmistetaan toiminnan jatkuvuus ennaltaehkäisevin toimin.

KATAKRI	Liite
I701.0	
A601.0	

18.2.1 Toimintojen kriittisyyden selvittäminen

Laitoksella seurataan turvallisuustoimenpiteiden vaikutusta toimintaan ja tulokset dokumentoidaan tulevaa analyysia varten. Analyysi suoritetaan vähintään kerran vuodessa turvallisuusryhmän kokouksessa. Analyysin tavoitteena on eri toimintojen kriittisyyden selvittäminen ja niihin kohdistuvien turvallisuustoimenpiteiden vaikutusten selvittäminen.

Kriittisien toimintojen keskeytysvaikutusanalyysillä selvitetään erilaisten häiriö- ja keskeytystilanteiden vaikutukset suhteessa käyttökatkon pituuteen. Keskeytysvaikutusten ja käytettävyystarpeiden pohjalta päätetään varsinaisista käytettävyysvaatimuksista ja järjestelmien välisestä priorisoinnista. Tietoja hyödynnetään jatkuvuus- ja toipumissuunnitelmien laatimisessa ja palvelutaso- sekä huolto- ja ylläpitosopimusten tekemisessä.

ICT- järjestelmien omistajat on velvoitettu tunnistamaan ICT- varautumiseen liittyvät vastuunsa ja toiminta on organisoitu ja vastuutettu sen mukaisesti. Järjestelmistä on tehty järjestelmäkohtainen tietokortti, josta ilmenee vastuut ja toimenpiteet. (Liite x)

18.2.2 Toipumis-, jatkuvuus- ja valmiussuunnitelmat

Laitoksen kokonaisvaltaisesta toipumis-, jatkuvuus- ja valmiussuunnittelusta vastaa turvallisuuspäällikkö turvallisuusryhmän kanssa. Laitoksen tietojenkäsittelyn toipumis- ja jatkuvuussuunnittelusta vastaa turvallisuuspäällikkö ja tietohallinto. Toipumissuunnitelmassa on johdon hyväksymä tärkeysjärjestys ICT- palveluille. Suunnitelmia ylläpidetään ja säilytetään tietohallinnon tiloissa. Suunnitelmien päivitykses-

tä ja katselmoinnista vastaa turvallisuuspäällikkö. Järjestelmien häiriöistä ja niiden syistä pidetään kirjaa järjestelmäkohtaisissa tietokorteissa (liite x). Tietoa käytetään hyväksi riskienhallinnassa ja sopimusten teossa.

Jatkuvuussuunnittelulla varmistetaan, että varsinainen toiminta saadaan ylläpidettyä ja palautettua riittävän nopeasti. Suunnittelu kattaa niin tekniset kuin fyysisetkin näkökohdat. Häiriö- ja keskeytystilanteita varten määritellään toimintaryhmä, ennaltaehkäisevät järjestelyt, ongelman paikallistaminen ja korjaavat toimenpiteet sekä tarvittava koulutus, testaus ja ylläpito.

Poikkeusoloihin ja vakaviin normaaliolojenkin häiriöihin varaudutaan valmiussuunnittelulla. Lähtökohtana on, että laitoksen normaaliolojen toimintoja pyritään ylläpitämään mahdollisimman pitkään ja että poikkeusolojen mahdolliset uudet tai muuttuneet tehtävät hoidettua. Ääritilanteessa järjestelmät on ajettava hallitusti alas siten, että myös niiden myöhempi uudelleen käynnistäminen on hallittua.

18.2.3 Harjoitukset ja testaaminen

Laitoksella on tunnistettu keskeiset turvallisuusriskit poikkeamatilanteisiin ja toimintaohjeet ovat kuvattuna pelastussuunnitemassa ja jatkuvuus- ja toipumissuunnitelmassa (liite x). Toimintamalleja harjoitellaan tarpeen mukaan. Suojattujen tilojen hanke- ja projektikohtaisia jatkuvuusharjoituksia tehdään tarvittaessa.

KATAKRI	Liite
A803.0	

18.2.4 Turvallisuuspoikkeamien käsittely

Henkilöstön ohje poikkeamatilanteissa toimimiseen on kuvattu Intranetissä. Vakavista poikkeamatilanteista raportoidaan johdolle ja turvallisuuspäällikölle viivytyksettä ja ne dokumentoidaan tilastointia ja tarkempaa analysointia varten. Laitoksen henkilöstöllä on velvoite ja kanavat ilmoittaa havaitsemistaan turvallisuuteen liittyvistä heikkouksista, puutteista, vahingoista, väärinkäytöksistä ja niiden epäilyistä esimiehelle ja turvallisuuspäällikölle, joiden velvollisuutena on ryhtyä tarvittaviin toimenpiteisiin. Vakavat ja muuten merkittävät tapahtumat raportoidaan myös laitoksen johdolle.

Turvallisuuteen liittyvien poikkeamien, ongelmatilanteiden ja rikkomusten hallintaan ylläpidetään menettelyä, jolla tilanteet voidaan havaita, korjata ja raportoida, jotta tapahtumista voidaan oppia. Menettely sisältää valtuuksien määrittelyn ja viestintäkeinot myös pikaisiin ja laajavaikutteisiin toimiin.

Turvallisuuspoikkeamien selvityksestä ja tiedottamisesta vastaa turvallisuuspäällikkö. Turvallisuuspoikkeamien selvitystyötä koordinoi tarvittaessa suojelupäällikkö. Vi-

ranomaiskontakteista vastaa turvallisuuspäällikkö. Kriisiviestintä tapahtuu viestintästrategien mukaisesti yhteistyössä viestintäjohtajan kanssa. Turvallisuuspoikkeamien toteutuminen jatkossa pyritään ennalta ehkäiseviin toimenpiteisiin. Turvallisuuspoikkeamista tehdään vuosittain yhteenveto turvallisuusryhmän kokouksessa. Turvallisuuspoikkeamat, jotka ovat yhteisiä muiden organisaatioiden kanssa, käsitellään tarvittaessa yhteistyöryhmissä.

Laitoksen tietohallinto vastaa siitä, että sähköisten viestien, sähköpostien, tunnistamistietojen sekä paikkatietojen luottamuksellisuudesta ja oikeasta käsittelystä huolehditaan myös turvallisuuspoikkeamatilanteita selvitettäessä. Alempana on turvallisuuspoikkeamien merkitsemiseen tarkoitettu perustaulukko.

Ajankohta	
Poikkeama	
Syyt ja seuraukset	
Vaikutukset	
Korjaavat toimenpiteet	
Status	

KATAKRI
A607.0

18.2.5 Turvallisuuspoikkeamia selvittävä sisäinen ryhmä

Laitoksella turvallisuuspoikkeamien selvitystä varten on turvallisuusryhmä. Turvallisuusryhmän kokoonpanossa on tehtävään riittävä koulutus tehtävien suorittamiseen. Turvallisuusryhmäryhmä harjoittelee turvallisuuspäällikön johdolla turvallisuuspoikkeamatilanteiden hallintaa säännöllisesti vuosikellon mukaan.

18.2.6 Yhteistyö palvelutoimittajan kanssa turvallisuuspoikkeamatilanteessa

Palveluntuottajalta hankituissa palveluissa turvallisuuspoikkeamatilannetta koordinoi palvelutoimittajan turvallisuuspäällikkö yhteistyössä asiakkuuspäällikön kanssa. Laitoksen yhteyshenkilöinä toimivat palvelusopimuksessa nimetyt henkilöt.

(152)

Turvallisuuden valvonnasta ja poikkeamien kirjaamisesta sekä raportoinnista vastaa laitoksen turvallisuuspäällikkö. Palvelutoimittaja on velvollinen ilmoittamaan turvallisuuspoikkeamista välittömästi ja aloittamaan korjaavat toimenpiteet. Poikkeamasta ja sen syystä valmistuu kirjallinen raportti. Tietoa poikkeamien syistä käytetään sopimusten ja toiminnan parantamiseen.

18.2.7 Korjaavat ja ehkäisevät toimenpiteet

Turvallisuuspoikkeamien syyt selvitetään ja tietoja käytetään paitsi yksittäisen tilanteen korjaamiseen, myös vastaavien ongelmien ennalta ehkäisemiseen. Toimintaa, palveluita ja järjestelmiä kehitettäessä otetaan ennakolta huomioon turvallisuustarpeet ja määritellään turvallisuusvaatimukset turvallisuuspoikkeamien ehkäisemiseksi.

18.2.8 Varmuus- ja suojakopiointi

Varmuus- ja suojakopiot otetaan säännöllisesti ja säilytetään turvallisesti tietokonelaitteistosta erillään siten, etteivät kaikki kopiot voi tuhoutua samassa fyysisessä vahingossa. Kriittisimmät varmuus- ja suojakopiot säilytetään palosuojatussa kassakaapissa eri rakennuksessa. Myös kopioiden siirto järjestetään turvallisesti. Projektihenkilöstö vastaa varmuuskopioiden tekemisestä projekteissa käsiteltävistä tietoaineistosta. Varmuuskopioihin pääsee käsiksi vain valtuutettu käyttäjä. Suojatussa tilassa käsiteltävän materiaalin varmuuskopiot kryptataan AES- 256- menetelmällä.

18.2.9 Palvelutasosopimukset

Palvelutasosopimuksissa määritellään haluttu palvelutaso siten, että sen saavuttaminen voidaan mitata ja sovitun tason alittaminen sanktioida. Toteutumaa seurataan säännöllisesti ja tarvittaessa sovitaan korjaavista ja parantavista toimenpiteistä.

18.2.10 Huolto- ja ylläpitosopimukset

Huoltosopimuksilla sovitaan vasteajoista, varaosien saatavuudesta, huoltopalvelun henkilöresursseista sekä normaaliolojen häiriötilanteiden että tarvittaessa myös poikkeusolojen varalle. Huoltojärjestelyt ovat osa jatkuvuuteen liittyvää suunnittelua.

19 Dokumentaatio

(152)

Laitoksen turvallisuustoiminnan hallintaprosessit, turvallisuusmekanismit ja menettelytavat dokumentoidaan siten, että asiat ovat tarkistettavissa ja koulutettavissa. Tässä turvallisuuskäsikirjassa on koottuna liitteisiin tai linkitetty Intranetiin kaikki turvallisuuteen liittyvä dokumentaatio samaan paikkaan.

Turvallisuuden hallintaan liittyvät asiakirjat yksilöidään ja niille määritellään vastuuhenkilö, tarkistamis- ja hyväksymismenettely, muutoshallinta ja jakelu. Voimassa olevat versiot pidetään turvallisuusryhmän, henkilöstön ja tarvittaessa muiden sidosryhmien saatavilla.

Turvallisuustoiminnan toimivuudesta ja turvallisuustapahtumista kerätään ja ylläpidetään tarvittavia tallenteita. Tarvittavat tallenteet yksilöidään ja niille määritellään vastuuhenkilö, käsittelijät, käyttötarkoitus, suojaustapa, säilytysaika ja hävittäminen. Tallenteiden määrittelyssä ja käsittelyssä otetaan erityisesti huomioon yksityisyyden suojaan liittyvät vaatimukset.

Osa-alue	Julkisuus	Tallennuspaikka
Jatkuvuuden varmistavat tai poikkeustilanteiden hallintaa ohjaavat dokumentit		
Järjestelmäselosteet	Salassa pidettävä ST IV	
Riskienhallinta		
Turvallisuuskoulutus		
Ohjeet, menettelyt ja periaatteet		
Hankinta ja sopimustenhallinta		
Suojattavien kohteiden/tietojenkäsittely-ympäristön ja toimintaympäristön dokumentointi		

(152)

Muut		

20 Liitteet

Liite 1

Geodeettisen laitoksen turvallisuuspolitiikka

Turvallisuustoiminnan päämäärä ja tavoitteet

Laitoksen turvallisuustoiminnan päämääränä on suojata henkilöstö, tieto, maine, omaisuus ja ympäristö onnettomuuksilta ja vaaroilta, jotta voidaan taata toiminnan häiriötön jatkuvuus. Keskeisimpänä tavoitteena on kehittää ja ylläpitää tavoiteltua turvallisuuden tasoa sekä vähentää erilaisten riskien toteutumista. Luotettava ja turvallinen toimintaympäristö on tärkeä sekä omalle henkilöstölle että sidosryhmien henkilöstölle.

Riskienhallinta

Ylijohtaja on vastuussa riskienhallinnan järjestämisestä ja sen riittävyydestä. Riskienhallintapolitiikassa on määriteltynä kokonaisvaltaisen riskienhallinnan periaatteet ja riskienhallintaprosessi sekä riskienhallintaan liittyvät vastuut. Laitos tunnistaa ja arvioi toimintaansa kohdistuvia riskejä säännöllisesti vuosittain.

Turvallisuustoiminnan organisointi ja vastuut

Ylimmän johdon vastuulla on turvallisuustoiminnan organisointi, riskienhallinnan ja halutun riskitason ylläpitäminen, resursointi, päätös henkilöstön kouluttamisesta turvallisuusasioihin sekä erilaisten politiikkojen, ohjeiden ja strategioiden hyväksyminen. Turvallisuuspäällikön ja turvallisuusryhmän vastuulla on toteuttaa turvallisuustoimintaa, seurata turvallisuustoimintaa koskeva lainsäädäntö ja kouluttaa henkilöstö turvallisuusasioihin. Viime kädessä jokainen laitoksen työntekijä on kuitenkin vastuussa turvallisuudesta ja sen parantamisesta omalta osaltaan.

Dokumentointi

Turvallisuustoimintaa koskeva dokumentaatio on kerätty turvallisuuskäsikirjaan, joka sisältää tieto-, henkilöstö- ja toimitilaturvallisuuden osa- alueet sekä turvallisuuden hallinnoimisen.

Koulutus

Turvallisuusryhmän, johdon ja esimiesten vastuulla on uuden henkilöstön perehdyttäminen turvallisuusasioihin. Koko henkilöstölle järjestetään vuosittain toimintaan liittyvien turvallisuusasioiden koulutusta. Turvallisuusohjeistusta ja muuta turvallisuusmateriaalia löytyy Intranetistä. Koulutuksista ilmoitetaan henkilöstölle sähköpostilla ja Intranetissä.

Viestintä

Turvallisuusviestinnän tavoitteena on ylläpitää ja parantaa turvallisuustietoisuutta ja turvallisuustoimintaa laitoksen sisällä ja sidosryhmien kanssa.

Valvonta

Turvallisuustoiminnan tason kehittäminen ja ylläpito vaatii jatkuvaa valvontaa ja siitä tehdään arviointia vuosittain sekä siitä raportoidaan johdolle säännöllisesti. Turvallisuuskartoituksia järjestetään ainakin kerran vuodessa ja tulokset dokumentoidaan sekä suoritetaan toimenpiteet poikkeamien korjaamiseksi. Havaituista turvallisuuteen liittyvistä puutteista tai poikkeamista on ilmoitettava turvallisuuspäällikölle tai turvallisuusryhmälle. Turvallisuuspäällikkö johtaa valvontaa ja raportoi tuloksista laitoksen johdolle.

Voimaantulo

Tämä turvallisuuspolitiikka tulee voimaan 22.04.2013.

Hyväksynyt 22.04.2013: Tutkimusjohtaja, ylijohtajan sijainen

Liite 2

Geodeettisen laitoksen riskienhallintapolitiikka

Riskienhallintapolitiikassa määritellään viraston/organisaation/tms. kokonaisvaltaisen riskienhallinnan peruskäsitteet, riskienhallinnan tavoitteet, toimintaperiaatteet sekä vastuut. Riskienhallintapolitiikka sisältää toimintaperiaatteet riskienhallinnasta osana viraston/organisaation/tms. strategiaprosessia, sekä vuositason toiminnan ja talouden suunnittelua ja seurantaa.

Riskienhallintapolitiikan tarkoituksena on selkeyttää riskienhallinnan tavoitteita, organisointia, periaatteita, vastuita ja toimintatapoja. Näin varmistetaan, että riskienhallinnan toimintamalli on yhtenäinen läpi koko organisaation ja että johdolla on riittävästi tietoa riskeistä päätöksentekoaan varten.

Riskienhallinnassa toimitaan ottaen huomioon yleisesti hyväksytyt kansainväliset standardit ja menetelmät.

1 § Riskienhallinnan määritelmä

Riskin määritelmä

Riski on mahdollinen tulevaisuuden tapahtuma, joka voi vaikuttaa tavoitteiden saavuttamiseen.

Riskienhallinnan määritelmä

Riskienhallinta on systemaattista ja jatkuvaa toimintaa, jonka avulla pyritään tunnistamaan, arvioimaan ja hallitsemaan toimintaa uhkaavia riskejä, arvioimaan niiden todennäköisyyttä ja merkitystä sekä hallitsemaan niitä tehokkaasti.

Kuva 1: Esimerkki organisaation riskienhallinnasta

2 § Riskienhallinnan tavoitteet

Toimiva riskienhallinta sisäisen valvonnan kanssa varmistaa organisaation talouden ja toiminnan laillisuuden ja tuloksellisuuden, varojen ja omaisuuden turvaamisen ja oikeat ja riittävät tiedot organisaation toiminnasta ja taloudesta.

Toimiva ja tehokas sisäinen valvonta ja riskienhallinta tukevat suunnittelua ja päätöksentekoa ja parantavat siten organisaation tuloksia ja tavoitteiden saavuttamisen mahdollisuuksia.

Tunnistamalla riskit ja kuvaamalla niiden merkittävyys, syyt ja seuraukset yhtenäisellä ja vertailtavalla tavalla mahdollistetaan tehokkaat riskienhallintatoimenpiteet ja hyvän hallintotavan edellyttämä läpinäkyvyys.

Riskinhallinnan keinoina käytetään riskin välttämistä, minimoimista, siirtämistä, sen todennäköisyyden pienentämistä, taikka sen vaikutusten rajaamista tai pienentämistä. Myös riskin hyväksyminen tai riskin ottaminen voivat olla tietyillä riskialueilla tarkoituksenmukaisia menettelyitä. Riskienhallinnalla pyritään varmistamaan myös toimintojen jatkuvuus riskien realisoituessa.

Aktiivisella ja oikea-aikaisella viestinnällä on keskeinen rooli riskienhallinnassa.

Riskienhallinta perustuu eri riskien yhtenäiseen tunnistamiseen, arviointiin ja raportointiin. Riskejä tulee hallita ennakoivasti hyväksyttyjen periaatteiden mukaisesti ja järjestelmällisesti osastoissa, prosesseissa ja projekteissa.

3 § Riskienhallinnan vastuut

Talousarvioasetuksen 69 §:n mukaan laitoksen johdon on huolehdittava siitä, että virastossa ja laitoksessa toteutetaan sen talouden ja toiminnan laajuuteen ja sisältöön sekä niihin liittyviin riskeihin nähden asianmukaiset menettelyt. Kunkin ryhmän johtaja vastaa sisäisestä valvonnasta ja riskienhallinnasta siinä toiminnassa, josta työjärjestyksen mukaan on vastuussa. Jokaisella työntekijällä on vastuu oman tehtäväalueensa tietoturvallisuudesta ja riskienhallinnasta.

Ylijohtaja vastaa riskienhallinnan järjestämisestä ja sen asianmukaisuudesta ja riittävyydestä.

4 § Riskien luokittelu

Riskit voidaan luokitella seuraavasti:

Strategiset riskit

Varoja ja omaisuutta koskevat riskit

Henkilöstö- ja osaamisriskit

Laillisuusriskit ja hyvän hallinnon vajeet

Tieto- ja IT-riskit

Toiminnan ohjauksen ja päätöksentekoinformaation riskit

Riskien jakaminen luokkiin auttaa ymmärtämään niiden luonnetta ja mahdollisia hallintakeinoja sekä auttaa ottamaan laajemmin huomioon erityyppiset riskit riskienhallintaprosessissa.

5 § Riskienhallintaprosessi

Riskienhallinta on olennainen osa toiminnan suunnittelua. Kokonaisvaltaista riskienhallintaa tehdään toiminnalle asetettujen tavoitteiden lähtökohdista. Tavoitteita asetettaessa riskienhallinnan avulla varmistetaan, että tavoitteet ovat tasapainossa riskinottokyvyn- ja halun kanssa.

Kokonaisvaltainen riskienhallinta koostuu kuudesta osatekijästä:

Riskienhallintapolitiikka

Riskien tunnistaminen

Riskien itsearviointi

Vuosittain tehtävä

Huomioidaan toimintaympäristön muutokset

Riskien arviointi

Riskien tunnistamisen yhteydessä

Arvioidaan todennäköisyyttä ja vaikuttavuutta asteikolla 1-5

Riskeihin vastaaminen

Riskien priorisointi

Toimenpiteiden valinta

Riskiraportointi

Seuranta ja kehittäminen

6 § Riskienhallintapolitiikka

Riskienhallintapolitiikassa määritellään kokonaisvaltaisesti riskienhallinnan periaatteet sekä riskienhallintaprosessi ja siihen liittyvät vastuut. Riskienhallintapolitiikkaa päivitetään tarvittaessa ja päivittämisestä vastaa riskienhallinnan vastuuhenkilö.

7 § Riskien tunnistaminen ja arviointi

Riskejä tunnistetaan itsearvioinnin tuloksena ja projektien suunnitteluvaiheessa. Lisäksi riskejä voidaan tunnistaa ja havaita päivittäisjohtamisessa ja vuosittain tehtävässä kyselyssä.

Riskin arvioinnilla määritetään riskien olennaisuus, joka lasketaan numeerisesti vaikuttavuuden ja todennäköisyyden tulona. Vaikuttavuutta arvioidaan asteikolla 1-5 ja sen arviointikriteereinä ovat riskin realisoitumisen taloudellinen vaikutus, vaikutus ihmisten/eläinten/kasvien terveyteen, vaikutus julkisuuskuvaan tai juridinen vaikutus. Vaikuttavuuden arvioinnissa käytetään sitä arviointikriteeriä, jossa riskin vaikutukset ovat suurimmat. Vaikuttavuutta mitataan asteikolla 1-5, jossa:

1 = riskin vaikutukset ovat erittäin vähäiset,

2 = riskin vaikutukset ovat vähäiset,

3 = riskin vaikutukset ovat huomattavat,

4 = riskin vaikutukset ovat merkittävä, ja

5 = riskin vaikutukset ovat erittäin merkittävä

Todennäköisyyttä mitataan asteikolla 1-5, jossa:

1 = riskin realisoituminen on epätodennäköistä,

2 = riskin realisoituminen se on harvinaista,

3 = riskin realisoituminen on kohtalaista,

4 = riskin realisoituminen on todennäköistä, ja

5 = riskin realisoituminen on lähes varmaa.

8 § Riskeihin vastaaminen

Riskeihin vastaamisessa on kolme vaihetta:

Riskikartan luominen, riskien priorisointi ja niihin liittyvien toimenpiteiden määrittely;

Riski-informaation ja kehittämistoimenpiteiden vieminen strategiaprosesseihin;

Riskienhallinnan tavoitteiden jalkauttaminen osastojen ja yksiköiden tulossopimuksiin

Riskien tunnistamisen ja arvioinnin jälkeen luodaan saaduista tiedoista riskikartta. Kriittisille riskeille valitaan tai määritellään hallintatoimenpiteet, joilla riskejä pyritään hallitsemaan. Olennaisimpia riskienhallintakeinoja ovat:

Riskin välttäminen tarkoittaa sellaisen toiminnan välttämistä, jossa kyseiselle riskille altistuttaisiin. Tämä tarkoittaa myös mahdollisen riskin ottamisesta saatavan hyödyn menettämistä, tavoitteista tai toiminnasta luopumista.

Riskin pienentämisellä pyritään pienentämään riskin toteutumistodennäköisyyttä tai vähentämään vaikutusta riskin sen toteutuessa.

Riski voidaan siirtää sopimusten avulla toisen osapuolen kannettavaksi, joko osittain tai kokonaan. Tyypillisin riskin siirtämiskeino on vakuuttaminen, mutta riskiä voidaan siirtää myös esim. toiminnassa tehtävien sopimusten kautta.

Riski voidaan pitää myös omalla vastuulla, sillä riskin ottamiseen voi sisältyä myös mahdollisuus saatavasta hyödystä. Riskin ottamiseen liittyvät päätökset tehdään pääasiallisesti strategisen johtamisen prosessin yhteydessä ylimmän johdon toimesta.

Riskinottokyky tarkoittaa sitä määrää riskiä, joka voidaan hyväksyä saavuttaakseen tavoitteensa. Riskin ottamisen on aina tapahduttava

tietoisen päätöksen seurauksena, hyvää päätöksentekotapaa ja huolellisuutta noudattaen. Päätöksenteossa on huomioitava myös riskin

toteutuessaan aiheuttamat vaikutukset. Riskin ottaminen ja siihen liittyvä päätöksenteko tulee aina dokumentoida huolellisesti.

9 § Menettelyt ja toimintatavat

Organisaatio tunnistaa ja arvioi toimintaansa kohdistuvia riskejä jatkuvasti ja erityisesti toiminnan suunnittelun yhteydessä. Lisäksi organisaatio arvioi säännöllisesti niitä tekijöitä, jotka voivat estää toiminta-ajatuksen toteutumisen tai tulostavoitteiden saavuttamisen. Riskianalyysin perusteella kohdennetaan resursseja toimintoihin ja valvonta kohdistetaan riskianalyysissä valikoituneisiin toimintoihin.

Organisaatio pyrkii turvautumaan tietojärjestelmiensä ja muun tietotekniikan käyttöönotossa vikasietoisiin ratkaisuihin. Uusia tietotekniikkaratkaisuja suunnitellessa arvioidaan ratkaisuihin liittyviä riskejä.

Toimitila- ja turvaratkaisuja toteutettaessa arvioidaan niiden riskit myös kumppaneiden ja henkilöstön turvallisuuden kannalta.

Henkilöstöä koulutetaan tunnistamaan vastuualueellaan toimintaa uhkaavia riskejä ja ilmoittamaan niistä vastuuhenkilölle.

10 § Riskiraportointi

Riskienhallinnan tila on pystyttävä raportoimaan vuosittain.

10 § Valvonta

Seurannan ja sisäisen valvonnan menetelmät sovitetaan riskitekijöiden seuraamiseksi ja niiden vaikutuksen vähentämiseksi. Myös organisaation toiminnan kehittämistä koskevissa suunnitelmissa kuvataan tavoiteltavat hyödyt ja arvioidaan niiden toteutumista uhkaavat riskit.

Organisaation sisäinen tarkastus arvioi sisäisen valvonnan ja riskienhallinnan riittävyyttä ja asianmukaisuutta. Sisäistä valvontaa suoritetaan lisäksi auditoinnin 3-vuotissuunnitelman mukaan.

11 § Voimaantulo

Tämä riskienhallintapolitiikka tulee voimaan 04.12.2012

Ylijohtaja

Liite 3

GEODEETTISEN LAITOKSEN TIETOTURVAPOLITIIKKA

1 Tavoitteet

Tiedon turvaaminen on oleellinen osa laitoksen toiminnan ja palveluiden laatua, kokonaisturvallisuutta ja laitoksessa tapahtuvaa päivittäistä tietojen käsittelyä. Tietoturvallisuuden hyvä hallinta edellyttää kaiken toiminnan jatkuvaa seurantaa, pitkäjänteistä suunnittelua ja resursointia, varautumista erilaisiin uhkatilanteisiin, sovittujen toimintatapojen noudattamista, ohjeita, koulutusta ja viestintää. Tavoitteena on luoda ja ylläpitää luotettava ja turvallinen ympäristö niin laitoksen omien kuin sen piirissä käsiteltävien sidosryhmienkin tietojen käsittelyyn. Normaaliajan toiminnan tietojenkäsittelyn turvaamisen lisäksi varaudutaan toiminnan keskeyttäviin uhkatilanteisiin, ja niistä toipumiseen.

Hallinnollisten, teknisten ja muiden toimenpiteiden avulla laitoksen tiedot, tietojenkäsittelyjärjestelmät ja – palvelut pidetään asianmukaisesti suojattuina sekä normaali-, että poikkeusoloissa.

Laitoksen tavoitteena on, että tietoturvajärjestelyt ovat hyvää kansallista ja kansainvälistä tasoa. Lisäksi tavoitteena on, että tietoturvallisuuden perustaso kattaa laitoksen kaiken tietojenkäsittelyn, ottaen huomioon yksiköiden perusluonteen, ja mahdollisen tarpeen tietoturvan tehostamiseen. Laitoksen tavoitteena on turvata riittävällä ja tarkoituksenmukaisella tasolla toiminnalleen tärkeiden tietojen, tietojärjestelmien, palveluiden ja tietoverkkojen toiminta, estää niiden valtuudeton käyttö sekä tahaton tai tahallinen tiedon tuhoutuminen ja vääristyminen.

Vastuu Geodeettisen laitoksen toiminnoista on sen ylimmällä johdolla. Laitoksen toiminta ja palvelut ovat hyvin riippuvaisia tietotekniikkapalveluiden keskeytyksettömästä ja turvallisesta toiminnasta. Tietotekniikan hyödyntäminen ja sekä tietotekniikan että yleisempäänkin tietoturvallisuuteen panostaminen ovat johdon strategisia päätöksiä, joilla vaikutetaan laitoksen toimintakykyyn merkittävällä tavalla. Geodeettinen laitos vastaa maa- ja metsätalousministeriölle tietoturvallisuudesta osana tulosohjausta. Laitoksen tietoturvallisuuden varmentaminen tapahtuu kansallisten ja kansainvälisten säädösten ja suositusten pohjalta, sekä valtionhallinnon tietoturvallisuudesta annettuja ohjeita ja suosituksia noudattaen.

2 Tietoturvallisuus

Tietoturvallisuus koostuu tiedon luottamuksellisuudesta, eheydestä ja käytettävyydestä sekä soveltuvilta osin pääsynvalvonnasta ja kiistämättömyydestä

Luottamuksellisuus tarkoittaa, että tiedot ovat sovituilla tavoilla ja sovittuun aikaan vain niiden käyttöön oikeutettujen saatavissa, ja ettei tietoja paljasteta tai muutoin saateta sivullisten tietoon.

Eheys tarkoittaa, että tiedot ja tietojenkäsittelyjärjestelmät ovat luotettavia, oikeellisia ja ajantasaisia eivätkä ole muuttuneet tai vahingoittuneet laitteisto- tai ohjelmistovikojen, luonnontapahtumien tai oikeudettoman inhimillisen toiminnan seurauksena.

Käytettävyys tarkoittaa, että tiedot ja tietojenkäsittelyjärjestelmät ovat toiminnan kannalta hyväksyttävän ajan kuluessa käytettävissä ja käyttökelpoisia valtuutetuille käyttäjille.

Pääsynvalvonta tarkoittaa, että tietoa ja tietojärjestelmää ei voi käyttää ilman lupaa.

Kiistämättömyys tarkoittaa todisteiden luomista sen varmistamiseksi, ettei yksikään tietojen käsittelyn, tai siirron osapuoli voi jälkikäteen kiistää osuuttaan siihen.

3 Tietoturvan organisointi ja vastuut

Tietoturvallisuutta johtaa laitoksen ylijohtaja, joka päättää kokonaisturvallisuuden eri osa-alueiden kehittämistoiminnan tavoitteista, organisoinnista, resursseista ja toimintavaltuuksista. Apunaan hänellä on tietohallinnosta vastuulliseksi määrätty tietoturvapäällikkö.

Jokainen laitoksen tietoja käsittelevä, tietojärjestelmien tai tietoverkkojen ylläpitäjä ja käyttäjä on viime kädessä vastuussa tietoturvallisuuden toteuttamisesta omalta osaltaan. Kukin laitoksen tietojärjestelmien, ja niiden sisältämien tietojen omistaja vastaa tietojensa ja tietojärjestelmiensä suojaamisesta.

Poikkeusoloihin varautumisesta vastaa ylijohtaja.

4 Toteutuskeinot

Tietoturvallisuuden ylläpito ja kehittäminen on jatkuvaa toimintaa, joka tapahtuu hallinnollisten, fyysisten ja tietoteknisten ratkaisujen avulla. Käyttäjien toimintaa ohjataan niihin sisältyvillä käyttöpolitiikoilla, säännöillä ja toimintaohjeilla sekä tietojen turvallisen käsittelyn koulutuksella ja tiedotuksella. Tietoturvapolitiikan pohjalta laaditaan laitoksen tietoturvasuunnitelma.

Laitoksessa otetaan käyttöön tietojen ja tietojärjestelmien turvallisuusluokitus. Kullekin turvallisuusluokalle on määritelty vaadittava tietoturvallisuustaso, ja sen mukaiset tietoturvatoimenpiteet.

Jokaisella tietojärjestelmällä, tai sen osalla on oltava yksikäsitteinen omistaja. Tietoturvallisuuden toteuttamista ohjaavat dokumentit ovat vahvistettuja, ja asianomaisten kohderyhmien saatavissa.

5 Viestintä

Tietoturvallisuudesta tiedottamisen tulee olla informoivaa, ohjaavaa ja ohjeistavaa ja sen perustarkoituksena on edistää tietoturvatietoisuutta.

Henkilökunnalle jaetaan heidän työskentelyssään tarvitsemansa tietoturvaohjeet.

6 Tietoturvallisuuden seuranta

Tietoturvallisuuden ylläpito edellyttää jatkuvaa seurantaa, johon kuuluvat tietoturvallisuuden valvonta sekä sen tason ja poikkeamien raportointi. Seurannassa käytetään johdon hyväksymiä mittareita. Seuranta on osa esimiesvastuuta. Tietoturvapäällikkö koordinoi tietoturvallisuuden seurantaa ja raportoi tietoturvallisuudesta laitoksen johdolle.

Tietoturvapäälliköllä on ylimmän johdon antama valtuutus ja velvollisuus tehdä laitoksen tietoturvallisuuteen liittyviä kartoituksia ja käynnistää toimenpiteet havaittujen puutteiden korjaamiseksi.

Käyttäjien ja ylläpitäjien tulee ilmoittaa havaitsemistaan tietoturvallisuuden puutteista, tietoturvallisuuteen liittyvistä väärinkäytöksistä tai epäilemistään tietoturvarikkomuksista tietoturvapäällikölle.

Hyväksynyt 19.9.2012: Ylijohtaja

Liite 4

Kansallisen turvallisuusauditointikriteeristön soveltaminen (versio 2, 2011)

Vaatimus-tunnus		**Kriteerin pääasiallinen sisältö**	**Luku**
A	**101.0**	Johdon määrittelemä ja hyväksymä turvallisuuspolitiikka	3.4
A	**102.0**	Turvallisuuspolitiikan ja/tai turvallisuusjohtaminen sisältää ainakin tila-, tieto- ja henkilöstöturvallisuuden	2.1
A	**103.0**	Vastaako turvallisuusdokumentaatio riskeihin	3.4
A	**104.0**	Toimiiko koko organisaatio turvallisuuspolitiikan mukaisesti	8
A	**105.0**	Lainsäädännön ja paikallisten turvallisuusmääräysten huomioiminen turvallisuuspolitiikassa	3.4
A	**105.1**	Lakisääteinen toiminta	3.4
A	**106.0**	Turvallisuuspolitiikan tiedottaminen henkilöstölle.	3.4
A	**107.0**	Turvallisuuspolitiikassa on vaatimus kaikkien työntekijöiden sitoutumiselle.	3.4
A	**108.0**	Keskeisten turvallisuustavoitteiden ilmaiseminen turvallisuuspolitiikassa	3.4
A	**201.0**	Dokumentoitu toimintaohjelma turvallisuuden johtamisen ja turvallisuustyön tavoitteiden saavuttamiseksi.	3.5
A	**202.0**	Menetelmien, vastuiden ja aikataulujen erittely toimintaohjelmassa.	3.5
A	**203.0**	Toimintaohjelman säännöllinen tarkistaminen	3.5
A	**204.0**	Dokumentoitu ohjelma tietoturvallisuuden johtamiseksi	2.1
A	**301.0**	Turvallisuustyön tavoitteiden asettaminen turvallisuuspolitiikan mukaisesti	2.1
A	**302.0**	Turvallisuustavoitteiden asettaminen eri hierarkiatasoille ja toiminnoille	2.1
A	**303.0**	Tavoitteiden mitattavuuden varmistaminen	2.1
A	**304.0**	Tavoitteiden saavuttamisen aikataulutus	2.1
A	**305.0**	Tavoitteiden asettaminen riskit, vaatimukset, mahdollisuudet ja rajoitukset huomioiden	2.1
A	**306.0**	Suojattavan tiedon käsittely- ympäristön suojaaminen	11
A	**401.0**	Menetelmä turvallisuusriskien tunnistamiseen ja arviointiin	18

A	**401.1**	Toiminnalle tärkeät suojattavat kohteet tunnistettu	3.4
A	**401.2**	Suojattavien kohteiden riskienarviointi	18.1
A	**402.0**	Riskienarvioinnin riittävä kattavuus (normaalioiminta, erityistilanteet, onnettomuudet ja hätätapaukset)	18
A	**403.0**	Riskienarvioinnin tulosten dokumentointi ja päivittäminen	18
A	**404.0**	Riskienarvioinnin huomiointi turvallisuustoiminnan tavoitteiden asettamisessa	2.1
A	**405.0**	Riskienarvioinnin tulosten perusteella tehtävä priorisointi	18
A	**406.0**	Riskienarvioinnin käyttö turvallisuuskoulutuksen suunnittelussa	18
A	**407.0**	Riskienhallintatoimenpiteiden toteuttaminen ja tehokkuus	18
A	**408.0**	Tietoturvallisuuden arviointi	10
A	**409.0**	Tietoturvallisuuden hallinta hankinnoissa ja muussa yhteistyössä	10
A	**410.0**	Toiminta tietoturvapoikkeamatilanteissa	10
A	**501.0**	Turvallisuustyön vastuiden ja organisoinnin riittävyys organisaation eri tasoilla	2
A	**501.1**	Johon tuki ja sen näkyminen tietoturvallisuudessa	10
A	**502.0**	Turvallisuuden organisoinnista tiedottaminen tarvittaville osapuolille	2
A	**503.0**	Turvallisuustyön riittävän resursoinnin varmistaminen	2
A	**504.0**	Turvallisuudesta vastaava henkilö ja turvallisuustyön kattavuus	2.3
A	**505.0**	Turvallisuustyöstä vastaavan vastuun ja valtuuden riittävyys	2.3
A	**506.0**	Johdon sitoutuminen turvallisuustavoitteisiin ja niiden saavuttamiseen sekä turvallisuuden jatkuvaan parantamiseen	2
A	**601.0**	Jatkuvuudenhallintamenettely	18.2
A	**602.0**	Onnettomuuksien, vaaratilanteiden ja turvallisuuspoikkeamien käsittelyn organisointi	2.3
A	**603.0**	Vastuiden määritteleminen kriisitilanteiden, onnettomuuksien, vaaratilanteiden ja turvallisuuspoikkeamien vaikutusten ennalta pienentämiseksi.	2.3
A	**604.0**	Menetelmät turvallisuuspoikkeamien havaitsemiseksi ja suojaavien että korjaavien toimenpiteiden tekemiseksi	6
A	**605.0**	Toimenpiteiden tehokkuuden ja oikean kohdistamisen varmistaminen	2
A	**606.0**	Kontrolleihin tehtävien muutosten riskien arviointi	18

A	**607.0**	Turvallisuustoimenpiteiden vaikutusten analysointi.	18.2.4
A	**608.0**	Tietojenkäsittelyyn liittyvä muutoshallintamenettely	10
A	**701.0**	Toimintajärjestelmä dokumentointiin	10.16
A	**702.0**	Turvallisuustavoitteiden saavuttamisen dokumentointi	2
A	**703.0**	Turvallisuuskoulutusten rekisteröinti	3.4
A	**704.0**	Turvallisuuskoulutuksen riittävän tason varmistaminen	2
A	**801.0**	Turvallisuusvaatimusten tärkeyden ja oikeiden toimintatapojen kouluttaminen	3.4, 7.1
A	**802.0**	Henkilöstön oman työhön liittyvien turvallisuusriskien tunnistaminen	7.1
A	**803**	Henkilöstön riittävän osaamisen varmistaminen eri tilanteissa, joissa turvallisuus on vaarantunut	18.2.3
A	**803.1**	Tietoturvaohjeiden noudattamisen valvonta	17.16
A	**804.0**	Tasovaatimukset turvallisuuskoulutukselle	7.1
A	**805.0**	Työntekijöiden sopivuuden, koulutuksen ja perehtymisen varmistaminen työtehtäviin liittyen	7
A	**806.0**	Ohjeistuksien, koulutuksen ja tiedotuksen kattavuus	7
A	**807.0**	Tietoon ja tietojenkäsittelyyn hyväksyttävän käytön ohjeet	11
A	**901.0**	Turvallisuudesta vastaavan henkilön raportointi ylimmälle johdolle	6.1
A	**902.0**	Johdon säännöllinen turvallisuusjärjestelmän toimivuuden tarkastaminen	8
A	**903.0**	Johdon tekemä turvallisuusjärjestelmän soveltuvuuden, resurssien riittävyyden ja toiminnan tehokkuuden arviointi	6
A	**904.0**	Seurantatarkastusten dokumentointi	8
A	**905.0**	Seurantatarkastusten tulosten käyttö jatkuvaan parantamiseen	8
P	**101.0**	Luettelo hankkeeseen osallistuvista henkilöistä	17.1
P	**102.0**	Menettelytapaohje henkilöstössä tapahtuvien muutosten ilmoittamiseksi ja yhteyshenkilön yhteystietojen ajantasaisuus	17.1
P	**103.0**	Koulutusdokumentaatio saadusta koulutuksesta (hankkeeseen osallistuvat)	17.8
P	**104.0**	Vierailijaluettelon ylläpito	7.2
P	**105.0**	Vaatimusten noudattaminen suojaustason ja turvallisuusluokituksen mukaisesti	17.2

P	**201.0**	Työntekijän osaamisen todentaminen keskeisten dokumenttien avulla	17.8
P	**202.0**	Työhaastattelussa saatujen tietojen oikeellisuuden varmistaminen	17.2
P	**203.0**	Työnhakijan osaamisen varmentaminen asiantuntevilla kysymyksillä	17.8
P	**301.0**	Yrityksen arvojen mukaiseen toimintaan sitoutumisen varmistaminen työhaastattelutilanteessa	17.2
P	**302.0**	Huumausainetestauksen käytön arviointi ja käyttömahdollisuus	17.2
P	**303.0**	Luotettavuuden varmistaminen erityistä luotettavuutta vaativissa tehtävissä	17.2
P	**401.0**	Salassapito- ja vaitiolositoumusmenettely	17.6
P	**402.0**	Koeaikamenettely	17.2
P	**403.0**	Vastuuhenkilötietojen ja yrityskytkentöjen selvittäminen	17.2
P	**404.0**	Suppean turvallisuusselvityksen tekeminen	17.5
P	**405.0**	Perusmuotoisen turvallisuusselvityksen hakumahdollisuuden selvittäminen projektin tai tehtävän osalta	17.5
P	**406.0**	Henkilöiden luottotietojen hakeminen	17.2
P	**407.0**	Salassapito- ja vaitiolosopimukset vastaavat tietojen suojaustarpeita	17.6
P	**408.0**	Avainhenkilöiden tunnistaminen ja varahenkilöjärjestely	17.12
P	**501.0**	Työntekijän tehtävistä, vastuista, oikeuksista sekä velvollisuuksista sopiminen, etenkin tietojen suojaamisessa	17.3
P	**502.0**	Työntekijän perehdyttäminen yhtiön turvallisuusmääräyksiin	17.9
P	**503.0**	Uuden henkilön perehdyttäminen tehtäviin ja yrityksen toimintaan	17.7
P	**504.0**	Tietoturvakoulutuksen järjestäminen	17.9
P	**505.0**	Prosessikuvaukset valtuuttamisesta ja pääsyoikeuksien antamisesta tietoon ja tiloihin	10.4
P	**601.0**	Sijaisuusjärjestelyihin ja avainhenkilöihin liittyvien ohjeistusten järjestäminen	17.13
P	**602.0**	Työtyytyväisyydestä ja työmotivaation ylläpidosta huolehtiminen	17.10
P	**603.0**	Työssä jaksamisen ja työkyvyn seurannan järjestäminen	17.10

P	**604.0**	Toimiminen ja vastuut työntekijän käyttäytymisen muuttuessa	17.10
P	**605.0**	Menettelyohje työsuhteen päättämisestä	17.15
P	**606.0**	Vierailumenettely	7.2
F	**101.0**	Suojautuminen elektroniselta tiedustelulta pysäköintijärjestelyjen avulla	16.3
F	**102.0**	Suojautuminen elektroniselta tiedustelulta lastaus- ja purkualueella	16.3
F	**103.0**	Kiinteistön alueella tapahtuvan liikkumisen rajoittaminen	16.3
F	**104.0**	Alueen videovalvonta	16.14
F	**201.0**	Kuoren rakennemateriaalit	16.16
F	**202.0**	Ikkunoiden sijainti maantasoon nähden	16.8
F	**203.0**	Kattoikkunoiden suojaus	16.8
F	**204.0**	Kuoren aukkojen suojaaminen	16.17
F	**205.0**	Ovien murtosuojaus	16.18
F	**206.0**	Suurten ovien suojaus	16.18
F	**207.0**	Tilojen äänieristys	16.20
F	**208.0**	Kassakaapit ja holvit	16.10
F	**209.0**	Tilojen pääsyoikeuksien hallinta	16.4
F	**209.1**	Pääsy- ja käyttöoikeuksien hallinta	16.4
F	**209.2**	Ulkopuolisten henkilöiden ja vieraiden tunnistaminen	7.2
F	**210.0**	Tilojen lukitus	16.5
F	**211.0**	Mekaanisten avainten hallinta	16.7
F	**212.0**	Suojattavien tilojen avainhallinta	16.7
F	**213.0**	Yleisavaimen pääsyrajoitukset	16.6
F	**214.0**	Vartiointi- ja kiinteistönhoitohenkilöstön avaintenhallinta	16.7
F	**215.0**	Huoltotoimenpiteiden järjestäminen	16.15
F	**216.0**	Laitetilan ja sen laitteistojen huolto-, asennus- ja siivoustoimenpiteiden valvonta	16.15
F	**217.0**	Varautuminen salakuunteluun, hajasäteilyyn ja vastaaviin uhkiin	16.21
F	**218.0**	LVIS- järjestelyjen varmistaminen	16.16.6
F	**219.0**	Näyttöpäätteiden asettaminen	10.8
F	**301.0**	Rikosilmoitinjärjestelmä	16.9
F	**302.0**	Kulunvalvontajärjestelmä	16.12

F	**303.0**	Kameravalvontajärjestelmä	16.14
F	**304.0**	Palvelintilan kameravalvontajärjestelmä	16.14
F	**305.0**	Rikosilmoitinjärjestelmän toiminnan testaus	16.9
F	**306.0**	Kulunvalvontajärjestelmän hallinnointi	16.12
F	**307.0**	Rikosilmoitinjärjestelmän hallinnointi	16.9
F	**308.0**	LVI-automaation hallinta	16.15
I	**401.0**	Tietoliikenneverkon rakenteen turvallisuus	12
I	**402.0**	Palomuurien ja vastaavien liikennettä suodattavien laitteiden säännöstöjen laatu	12.4
I	**403.0**	Liikennettä suodattavien tai valvovien järjestelmien oikean toiminnan varmistaminen	12.4
I	**404.0**	Hallintayhteyksien suojaus	10.10
I	**405.0**	Verkon aktiivilaitteiden koventaminen	10.1.1
I	**406.0**	Langattomien verkkojen perussuojaus	12.4
I	**407.0**	Sisäverkon rakenteen näkymisen estäminen Internetiin	12.4
I	**408.0**	Verkon, järjestelmien ja niiden käytön valvonta	10.1
I	**409.0**	IPv6: n erityispiirteiden huomiointi	12.4
I	**410.0**	Reitityksen turvallisuus	10.1
I	**501.0**	Käyttäjien tunnistaminen ennen pääsyn sallimista organisaation tietoverkkoon ja -järjestelmiin	10.5
I	**502.0**	Menettelytapa uusien järjestelmien turvalliseen asentamiseen	12.3
I	**503.0**	Suojautuminen haittaohjelmia vastaan	12.4
I	**504.0**	Lokimenettelyjen toteuttaminen	12.4
I	**505.0**	Suojattavien tietojen turvallinen säilyttäminen tietojärjestel-missä	10.1
I	**506.0**	Liikuteltavien tietovälineiden suojaaminen luvatonta pääsyä vastaan	10.1
I	**507.0**	Salassa pidettävien tietojen suojaaminen huoltotoimenpiteiden ja käytöstä poiston yhteydessä	12.3
I	**508.0**	Verkon luvattomien laitteiden ja järjestelmien estäminen	16.19
I	**509.0**	Salausratkaisujen riittävän turvallisuuden varmistaminen	10.13
I	**510.0**	Salausavainten hallinta	10.13
I	**511.0**	Istunnonhallinnan turvallinen toteuttaminen	10.6
I	**512.0**	Autentikaatiodatan suojaaminen tietojärjestelmissä	11.1

I	**513.0**	Ajettavan koodin turvallisuuden varmistaminen	12.2
I	**514.0**	Hankittavien laitteiden tietoturvallisuuden varmistaminen	12.3
I	**601.0**	Tiedon luokittelumenettely	10.2
I	**602.0**	Salassa pidettävien manuaalisten tai siirrettävillä tietovälineillä olevien tietojen turvallinen säilyttäminen	11.1
I	**603.0**	Luottamuksellisen tietoaineiston turvallinen hävittäminen	11.6
I	**604.0**	Salassa pidettävän tietoaineiston turvallinen kopiointi ja tulostus	10.1.2
I	**605.0**	Salassa pidettävän aineiston turvallinen sähköinen välitys	11.3
I	**606.0**	Salassa pidettävän aineiston turvallinen välitys postilla ja/tai kuriirilla	11.3
I	**607.0**	Salassa pidettävien aineistojen välityksen seuranta	11.4
I	**701.0**	Jatkuvuuden varmistavat suunnitelmat	18.2
I	**702.0**	Toipumisen varmistaminen organisaation dokumentaation avulla	10.1
I	**703.0**	Ohjelmistojen, tietoliikenneyhteyksien ja oheislaitteiden asentamiseen liittyvät periaatteet	12.2
I	**704.0**	Periaatteet ja mekanismit etä- ja matkatöiden riskien hallitsemiseksi	7.3
I	**705.0**	Kehitys-/testaus- ja tuotantojärjestelmien erottaminen	10.10
I	**706.0**	Tunnettujen haavoittuvuuksien estäminen verkoissa ja sen palveluissa	10.1
I	**707.0**	Laitteiden suojaus työskentelytauoilla	10.8
I	**708.0**	Puhtaan pöydän ja näytön politiikka	10.8
I	**709.0**	Vaarallisten työyhdistelmien välttäminen	17.4
I	**710.0**	Riittävästä varmuuskopioinnista huolehtiminen	10.14

Liite 5

VAHTI 2/2010 Soveltaminen

Vaatimus		
1.1. Johtajuudelle asetettavat vaatimukset		
1.1.1 Strateginen ohjaus		Käsikirjan asiaa käsittelevä kohta
1.1.1.1. Perustaso	Organisaation toimintaa koskevan lainsäädännön asettamien vaatimusten tunnistaminen ja niistä henkilöstölle tiedottaminen on organisoitu ja vastuutettu.	luku 3.4
1.1.1.2. Perustaso	Organisaation ydintoiminnot ja -prosessit on tunnistettu sekä organisoitu ja vastuutettu.	luku 9
1.1.1.3. Perustaso	Organisaatiolla on kirjallinen johdon hyväksymä tietoturvapolitiikka.	luku 2
1.1.1.4. Korotettu taso	Organisaatiolla on strategiatason kirjallinen suunnitelma, josta mm. käy ilmi, miten tietoturvatyö vastuutetaan ja organisoidaan ydintavoitteiden saavuttamiseksi.	luku 3.5
1.1.1.5. Korkea taso	*Organisaatiolla on vuosittainen tietoturvallisuuden kehittämissuunnitelma.*	luku 5.2
1.1.1.6. Korkea taso	*Tulosohjauksessa käytetään myös tietoturvallisuuteen liittyviä osuuksia.*	luku 3.5, luku 5.1
1.1.2 Resursointi ja organisointi		
1.1.2.1. Perustaso	Organisaatioon on nimitetty tietoturvavastaava, jonka työnkuvassa on mainittu tietoturvavastuut.	luku 2.2
1.1.2.2. Perustaso	Tietoturvavastaavalla on aikaa tietoturvavastuidensa suorittamiseen.	luku 6.1

1.1.2.3. Korotettu taso	Kaikkien tietoturvavastuita omaavien työnkuvissa vastuu on mainittu.	luku 2.2
1.1.2.4. Korotettu taso	Organisaatiossa on sen kokoon ja tavoitteisiin nähden riittävästi tietoturvahenkilöstöä.	luku 6.1
1.1.2.5. Korotettu taso	Tietoturvallisuuden resursointi on huomioitu organisaation toiminta- ja taloussuunnittelussa tai budjetissa ja toteutumista seurataan.	luku 5.2
1.1.2.6. Korkea taso	*Tietoturvavastaava on päätoiminen.*	*Ei sovelleta.*
1.1.3 Yhteistyön koordinointi		
1.1.3.1. Perustaso	Organisaation johto ja tietoturvallisuuden eri osa-alueiden vastuuhenkilöt keskustelevat säännöllisesti.	luku 4.1
1.1.3.2. Perustaso	Organisaatiossa on säännöllisesti kokoontuva tietoturva-asioita käsittelevä yhteistyöryhmä.	luku 4.1
1.1.3.3. Korotettu taso	Johdon tapaamiset ovat vähintään kerran vuodessa.	luku 4.1
1.1.3.4. Korotettu taso	Tietoturva-asioita käsittelevä yhteistyöryhmä kokoontuu vähintään kaksi kertaa vuodessa	luku 4.1
1.1.3.5. Korkea taso	*Tapaamisissa käsitellään mm. havaittuja riskejä, asetettuja tietoturvatavoitteita, niiden saavuttamista ja tulevaisuuden tarpeista aiheutuvia muutoksia.*	*luku 4.1*
1.1.3.6. Korkea taso	*Tapaamisista pidetään pöytäkirjaa ja sovittujen toimenpiteiden toteutumista seurataan.*	*luku 4.1*
1.1.4 Raportointi ja viestintä sidosryhmille		
1.1.4.1. Perustaso	Sidosryhmät, joille organisaatio on vastuussa tietoturvallisuudesta, ja niiden kontaktipisteet on tunnistet-	luku 4.2

	tu.	
1.1.4.2. Perustaso	Johto on organisoinut ja vastuuttanut sidosryhmiin vaikuttavista tietoturva- asioista raportoinnin sekä tietoturvapoikkeamista tiedottamisen.	luku 4.2
1.1.4.3. Korotettu taso	Sidosryhmille raportoidaan tietoturvallisuudesta vuosittain tai johdon määrittelemällä tavalla.	luku 4.2
1.1.4.4. Korotettu taso	Sidosryhmäraportilla on mallipohja	luku 6.2
1.1.4.5. Korkea taso	*Jos muuta ei sovita, raportin sisältöön kuuluu mittaustietoa vaatimuksenmukaisuudesta, tietoturvatavoitteiden saavuttamisesta, poikkeamista, poikkeamien johdosta tehdyt toimenpiteet sekä muut merkittävimmät tietoturvamuutokset.*	luku 6.2
1.1.4.6. Korkea taso	*Raportointia kehitetään sidosryhmien palautteen perusteella*	luku 6.2
Johtaminen erityistilanteessa 1.1.5		
1.1.5.1. Perustaso	Tietoturvapoikkeamien käsittely on organisoitu ja vastuutettu.	luku 18.2.4
1.1.5.2. Perustaso	Vakavista tietoturvapoikkeamista kerrotaan johdolle viivytyksettä ja niistä pidetään kirjaa.	luku 18.2.4
1.1.5.3. Korotettu taso	Organisaatiossa on kirjallinen malli tietoturvapoikkeamien käsittelyyn. Ohjeessa on määritelty roolitasolla kuka selvittää tapahtunutta kenen määräyksestä ja kuka päättää viranomaiskontakteista (esim. esitutkintapyynnön teosta) ja tiedottamisesta.	luku 18.2.4

1.1.5.4. Korotettu taso	Tietoturvapoikkeamista tehdään jälkikäteisanalyysi ja käynnistetään tarvittavat korjaavat toimenpiteet tapahtuman uusiutumisen ehkäisemiseksi.	luku 18.2.4
1.1.5.5. Korkea taso	*Havaituista tietoturvapoikkeamista tehdään vuosittain yhteenveto.*	luku 18.2.4
1.1.5.6. Korkea taso	*Tietoturvapoikkeamista vaihdetaan tietoja kumppanien kanssa ja kumppanien kokemuksia käytetään hyväksi.*	luku 18.2.4
1.1.6 Raportointi johdolle		
1.1.6.1. Perustaso	Tietoturvallisuudesta raportointi on vastuutettu ja organisoitu.	luku 4.2, luku 6.1
1.1.6.2. Perustaso	Tietoturva-asioista raportoidaan organisaation johdolle säännöllisesti.	luku 6.1
1.1.6.3. Korotettu taso	Raportointimenettely on kuvattu kirjallisesti.	luku 6.1
1.1.6.4. Korotettu taso	Tietoturva-asioista raportoidaan organisaation johdolle vähintään vuosittain	luku 6.1
1.1.6.5. Korkea taso	*Jatkuva raportointi perustuu päätettyihin toiminnan mittareihin.*	luku 6.1
1.1.6.6. Korkea taso	*Raportin sisältöön kuuluu mittaustietoa resurssien käytöstä, tietoturvatavoitteiden saavuttamisesta, poikkeamista, poikkeamien johdosta tehdyt toimenpiteet sekä muut merkittävimmät tietoturvamuutokset.*	luku 6.1
1.2 Toiminnan suunnittelulle asetettavat vaatimukset		
1.2.1 Toimintaympäristön vaikutus		
1.2.1.1. Perustaso	Erilliset tietojen käsittelyn toimintaympäristöt ja niihin kuuluvat jär-	luku 9

	jestelmät ja toiminnot on tunnistettu.	
1.2.1.2. Perustaso	Kunkin toimintaympäristön erityisvaatimukset ja tavoitteet tietoturvallisuuden osalta on tunnistettu	luku 9
1.2.1.3. Korotettu taso	Toimintaympäristöt ja niihin kuuluvat järjestelmät on dokumentoitu.	luku 9
1.2.1.4. Korotettu taso	Ympäristö- ja järjestelmälistaukset katselmoidaan ja tarvittaessa päivitetään vähintään vuosittain	luku 12.1
1.2.1.5. Korkea taso	*Ympäristöjen elinkaaren vaiheet on dokumentoitu ja dokumentissa on kriteerit milloin ja miten ympäristö siirtyy vaiheesta toiseen.*	luku ??
1.2.1.6. Korkea taso	*Kunkin elinkaaren vaiheen erityisvaatimukset tietoturvallisuuden osalta on määritelty ja dokumentoitu.*	luku ??
1.2.2 Tavoitteiden määrittely		
1.2.2.1. Perustaso	Kunkin ydintoiminnon ja -prosessin tietoturvallisuuden kannalta suojattavat kohteet on tunnistettu ja luokiteltu vaadittavan tietoturvallisuuden tason mukaisesti.	luku 9
1.2.2.2. Perustaso	Ydintoimintojen tai -prosessien tavoitteisiin on liitetty myös tietoturvatavoitteita.	luku 9
1.2.2.3. Korotettu taso	Tietoturvatavoitteiden määrittelyssä on otettu huomioon sekä luottamuksellisuus, eheys että saatavuus.	luku 9
1.2.2.4. Korotettu taso	Ydintoiminnoista ja -prosesseista on karkean tason toiminta- tai prosessikuvaukset.	luku 9
1.2.2.5. Korkea taso	*Toiminto- tai prosessikuvauksiin on liitetty tietoturvallisuuden kannalta oleelliset tietoturvaprosessit tai toimet tai ne on dokumentoitu*	luku 9

	erikseen.	
1.2.2.6. Korkea taso	*Toimintojen tietoturvatavoitteisiin on liitetty suoriutumista kuvaavia mittareita.*	luku 9
1.2.3 Toiminnan kehittäminen riskien arvioinnilla		
1.2.3.1. Perustaso	Organisaatiossa tehdään säännöllisesti tietoturvallisuuteen liittyvien riskien arviointia.	luku 18.1
1.2.3.2. Perustaso	Riskien arvioinnin perusteella parannetaan tietoturvallisuutta liian suurten riskien osalta johdon päättämillä toimenpiteillä.	luku 18.1
1.2.3.3. Korotettu taso	Organisaatiossa tehdään ydintoimintojen tietoturvariskien arviointia vähintään vuosittain.	luku 18.1
1.2.3.4. Korotettu taso	Organisaatiolla on riskien arvioinnin menetelmä ja ohjeistus.	luku 18.1
1.2.3.5. Korotettu taso	Organisaatiolla on kirjallinen tietoturvasuunnitelma, joka määrittelee mitä teknisiä ja hallinnollisia toimia ja prosesseja organisaatiossa käytetään havaittujen tietoturvariskien hallitsemiseksi.	luku 18.1
1.2.3.6. Korkea taso	*Organisaatiossa tehdään tietoturvariskien arviointia myös suurten muutosten yhteydessä*	luku 18.1
1.2.3.7. Korkea taso	*Organisaatiolla on riskienhallintapolitiikka.*	Liite 2
1.2.3.8. Korkea taso	*Suurimmista riskeistä pidetään koko organisaation tasolla kirjaa ja riskienhallintatoimenpiteiden toteutumista seurataan.*	luku 18.1
1.2.4 Toimintaverkoston hallinta		

1.2.4.1. Perustaso	Organisaatiossa on tiedossa, missä toimintaverkostoissa organisaatio on mukana sekä mitä alihankkijoita ja yhteistyökumppaneita sen tietojen kanssa toimii missäkin roolissa.	luku 4.2
1.2.4.2. Korotettu taso	Organisaatiolla on kirjallinen dokumentti, jossa kuvataan sen osallistumista ja roolia erilaisissa alihankinta- ja yhteistyöverkostoissa sekä osallistumisen yleisiä tietoturvavaatimuksia.	luku 4.2
1.2.4.3. Korkea taso	*Toimintoverkostot on luokiteltu tietoturvatason mukaan ja kullakin luokalla on omat tietoturvavaatimuksensa.*	luku 4.2
1.2.4.4. Korkea taso	*Palveluntarjoajaksi voidaan valita vain sellainen palveluntarjoaja, jolla on mahdollisuus suojata asiakirjojen luottamuksellisuus ja tarvittaessa selvittää luottamuksellisuuden loukkaukset sähköisen viestinnän tietosuojalain (516/2004) 13 a - 13k §.ssä tarkoitetulla tavalla.*	luku 4.3
Erityistilanteiden hallinta 1.2.5		
1.2.5.1. Suomen erityisvaateet	Organisaation johto on tiedostanut mitä yhteiskunnan elintärkeiden toimintojen turvaamiseen (YETT) liittyviä vastuita organisaatiolla on.	Ei sovelleta
1.2.5.2. Perustaso	Organisaatiolla on jatkuvuussuunnitelma tai -suunnitelmia.	luku 18.2.2
1.2.5.3. Korotettu taso	Jatkuvuussuunnitelmien päivitys ja katselmointi on vastuutettu ja organisoitu.	luku 18.2.2
1.2.5.4. Korotettu taso	Jatkuvuussuunnitelmien toimivuutta testataan, harjoitellaan ja arvioidaan säännöllisesti.	luku 18.2.2
1.2.5.5. Korkea taso	*Jatkuvuussuunnitelmien toimivuutta harjoitellaan keskeisten yhteis-*	luku 18

	työkumppanien kanssa.	
1.3 Henkilöstölle asetettavat vaatimukset		
1.3.1 Osaamisen ja tietoisuuden kehittäminen sekä sanktiot		
1.3.1.1. Suomen erityisvaateet	Työntekijöiden tekninen valvonta on käsitelty YT-menettelyn mukaisesti (Laki yksityisyyden suojasta työelämässä, 21§).	luku 17.11.
1.3.1.2. Perustaso	Organisaatiossa järjestetään säännöllisesti tietoturvakoulutusta henkilöstölle ja muille avainryhmille. Tietoturvahenkilöstön osaamista kehitetään ja ylläpidetään.	luku 17.9
1.3.1.3. Perustaso	Perehdyttämistilanteessa käsitellään myös tietoturva-asioita.	luku 17.7
1.3.1.4. Perustaso	Muuttuneista tietoturvaohjeista ja -käytännöistä tiedotetaan kaikille organisaatiossa toimiville.	luku 17.11
1.3.1.5. Perustaso	Sääntöjen noudattamista seurataan ja poikkeamiin puututaan.	luku 17.11
1.3.1.6. Korotettu taso	Organisaatiossa on kirjallinen tietoturvallisuuden koulutussuunnitelma.	luku 17.9
1.3.1.7. Korotettu taso	Perehdyttäjällä on kirjallinen lista käsiteltävistä tietoturva-asioista.	luku 17.7
1.3.1.8. Korotettu taso	Henkilöstön osallistumista koulutuksiin seurataan.	luku 17.9
1.3.1.9. Korotettu taso	Tietoturvamääräysten ja -ohjeiden rikkomisen seuraukset on kuvattu organisaatiossa ja tiedotettu kaikille organisaatiossa työskenteleville.	luku 17.11
1.3.1.10. Korotettu taso	Esimies ja alainen käyvät vuosittain keskustelun työn tietoturvavastuista ja osaamisen kehittämisen tarpeista.	luku 17.8

1.3.1.11. Korotettu taso	Henkilöstön tietoturvaosaamisesta varmistutaan.	luku 17.8
1.3.1.12. Korkea taso	*Tietoturvakoulutuksessa otetaan huomioon organisaatiossa ja lähiympäristössä tapahtuneet muutokset ja tietoturvapoikkeamat.*	luku 17.9 Sovelletaan tarvittaessa järjestämällä koulutusta.
1.3.1.13. Korkea taso	*Hyvistä tietoturvateoista annetaan positiivista huomiota.*	Ei sovelleta
1.3.2 Henkilöresurssien ja tehtävien hallinta		
1.3.2.1. Perustaso	Toteutettavaksi valitut tietoturvatoimenpiteet ja -prosessit on organisoitu ja vastuutettu.	luku 5.2, luku 18.1
1.3.2.2. Perustaso	Tietoturvallisuuden avainroolit on tunnistettu ja niille on nimetty varahenkilö tai -henkilöt.	luku 2.3
1.3.2.3. Korotettu taso	Toteutettavaksi valituista tietoturvaprosesseista tai -toimenpiteistä ja niiden vastuuhenkilöistä on luettelo.	luku 2.3
1.3.2.4. Korotettu taso	Tietoturvallisuuden varahenkilöt on koulutettu tehtäväänsä	luku 2.3
1.3.2.5. Korkea taso	*Organisaatiossa on määritelty tehtävät tai roolit, joiden hakijasta tehdään turvallisuusselvitys, ja selvityksen hakuprosessi on dokumentoitu.*	luku ??
1.3.2.6. Korkea taso	*Organisaatiossa on tehty tietoturvallisuuden osaamiskartoitus*	Luku 7
1.3.3 Erityistilanteissa toimiminen		
1.3.3.1. Suomen erityisvaateet	Sähköisten viestien, sähköpostien, tunnistamistietojen sekä paikkatietojen luottamuksellisuudesta ja oikeasta käsittelystä huolehditaan myös tietoturvapoikkeamatilanteita	luku 18.2.4

	selvitettäessä (Sähköisen viestinnän tietosuojalaki 4§ ja 5§ sekä Laki yksityisyyden suojasta työelämässä 6. luku).	
1.3.3.2. Perustaso	Henkilöstö tietää, kenelle tietoturvapoikkeamista ja -tapahtumista tai niiden uhkista tulee ilmoittaa.	luku 18.2.4
1.3.3.3. Korotettu taso	Tietoturvapoikkeamia selvittävät henkilöt on koulutettu tehtäväänsä.	luku 18.2.5
1.3.3.4. Korkea taso	*Organisaatiossa on tietoturvapoikkeamien selvittämiseen koulutettu ryhmä, joka harjoittelee säännöllisesti.*	luku 18.2.5
1.4 Kumppanuuksille ja resurssien hallinnalle asetettavat vaatimukset		
Sopimusten hallinta 1.4.1		
1.4.1.1. Perustaso	Kumppanuus- ja hankintatoiminta on vastuutettu ja organisoitu.	luku 4.3
1.4.1.2. Perustaso	Kumppanin kanssa tehdään kirjallinen sopimus, jossa määritellään yhteistyön tai hankinnan kohteen tietoturvavaatimukset sekä miten tietoturvallisuuden valvonta, seuranta, auditointi ja raportointi tapahtuu.	luku 4.3
1.4.1.3. Korotettu taso	Kumppanille asetetaan tarvittavat tietoturvavaatimukset jo tarjouspyyntö- tai kumppanuusneuvotteluvaiheessa.	luku 4.3
1.4.1.4. Korotettu taso	Kumppanuussopimuksessa määritellään mitä tietoturvallisuustasoa kumppanin ja mahdollisen kumppanin alihankintaverkoston on kohteen luonteen huomioon ottaen noudatettava.	luku 4.3

1.4.1.5. Korkea taso	*Ennen sopimuksen solmimista organisaatio auditoi tai pyytää kirjallisen selvityksen kumppanin yhteistyön kohteeseen liittyvistä tietoturvamenettelyistä.*	luku 4.3
1.4.1.6. Korkea taso	*Sopimuksessa on määritelty sanktiot tietoturvapoikkeamista ja -loukkauksista.*	luku 17.6
1.4.2 Toiminnan varmistaminen erityistilanteessa		
1.4.2.1. Perustaso	Tietoturvallisuuden valvonta sekä poikkeamien kirjaaminen ja raportointi on organisoitu ja vastuutettu yhteistyön kohteeseen liittyen.	luku 18.2.6
1.4.2.2. Perustaso	Havaituista kumppania koskevista tietoturvapoikkeamista tiedotetaan kumppanille välittömästi ja poikkeaman korjaustoimet aloitetaan sovitusti.	luku 18.2.6
1.4.2.3. Korotettu taso	Tietoturvapoikkeaman käsittelystä yhteistyössä on kirjalliset ohjeet.	luku 7
1.4.2.4. Korotettu taso	Poikkeamasta ja sen syystä valmistuu kirjallinen raportti	Luku 7
1.4.2.5. Korotettu taso	Organisaatiokohtaisia jatkuvuusharjoituksia toteutetaan säännöllisesti	luku 18.2.3
1.4.2.6. Korkea taso	*Yhteistoimintaa erityistilanteessa harjoitellaan kumppanin kanssa.*	luku ??
1.4.2.7. Korkea taso	*Tietoa poikkeamien syistä käytetään sopimusten ja toiminnan parantamiseen.*	luku 18.2.6
1.5 Prosessit		
1.5.1 Tietoaineistojen hallinta		
1.5.1.1. Suomen erityisvaateet	Organisaatiolla on arkistonmuodostussuunnitelma (Arkistolaki 8§), josta käytetään usein myös nimitystä	luku 10.2

	tiedonhallinta- tai tiedonohjaus-suunnitelma.	
1.5.1.2. Suomen erityisvaateet	Organisaatio pitää luetteloa organisaatioon käsiteltäviksi tulleista ja käsitellyistä asioista (Julkisuuslaki 18§).	luku 10.2
1.5.1.3. Perustaso	Työntekijät tietävät miten tietoaineistoja organisaatiossa käsitellään.	luku 10.2
1.5.1.4. Perustaso	Organisaation tuottamasta kirjallisesta asiakirjasta käy ilmi kuka sen on laatinut ja milloin sekä sen hyväksymisen tila.	luku 10.2
1.5.1.5. Perustaso	Hävitettäväksi tarkoitettavat asiakirjat on tuhottava niin, että luottamuksellisuus ja tietosuoja on varmistettu.	luku 10.2
1.5.1.6. Korotettu taso	Organisaatiossa on tietoaineistojen käsittelyn kirjallinen ohje, jossa kerrotaan, miten asiakirjat hyväksytään, katselmoidaan ja mikä organisaation aineisto on salassa pidettävää tai muun vaitiolovelvollisuuden alaista	luku 10.2
1.5.1.7. Korkea taso	*Organisaatiossa käytössä olevat tietoaineistojen hallinnan välineet tukevat aineistojen luokittelua ja arkistointia.*	luku 10.2
1.6 Toiminnan arvioinnille ja todentamiselle asetettavat vaatimukset		
1.6.1 Toiminnan arviointi ja todentaminen		
1.6.1.1. Perustaso	Organisaatiossa tehdään säännöllisesti tietoturvallisuuden auditointeja tai arviointeja.	luku 8
1.6.1.2. Perustaso	Auditoinnit tai arvioinnit ovat suunniteltuja ja johdon hyväksymiä.	luku 8
1.6.1.3. Perustaso	Auditoinnin tai arvioinnin tulokset raportoidaan toiminnon tai kohteen	luku 8

	omistajalle.	
1.6.1.4. Perustaso	Auditointien tai arviointien suosituksista pidetään koko organisaation tasolla kirjaa ja parannustoimenpiteiden toteutumista seurataan.	luku 8
1.6.1.5. Korotettu taso	Tietoturva-auditointeja tai arviointeja tehdään joka vuosi.	luku 8
1.6.1.6. Korotettu taso	Organisaatiossa on kirjallinen johdon hyväksymä auditointi- tai arviointiprosessi, jossa on mm. määritelty auditoijien tai arvioijien pätevyysvaatimukset.	luku 8
1.6.1.7. Korotettu taso	Raportin pohjalta toiminnon tai kohteen omistaja määrittelee ja vastuuttaa parannustoimenpiteet, joilla havaitut riskit saadaan hyväksyttävälle tasolle.	luku 8
1.6.1.8. Korkea taso	*Auditoinnit tai arvioinnit käyvät läpi organisaation avaintoiminnot 5 vuoden aikajaksolla.*	luku 8
1.6.1.9. Korkea taso	*Tietoturva-auditoinneissa tai arvioinneissa käytetään myös ulkopuolisia resursseja.*	luku 8

2 Tietojärjestelmien hallinnan vaatimukset		Soveltaminen
2.1. Raportointi tietoturvavastaavalle		
2.1.1. Perustaso	Säännöllinen raportointi IT-järjestelmien ja niiden hallinnan tietoturvallisuuden tilasta tietoturvavastaavalle on organisoitu ja vastuutettu.	luku 6.3

2.1.2. Perustaso	Vakavista tietoturvatapahtumista kerrotaan tietoturvavastaavalle viivytyksettä.	luku 6.3
2.1.3 Korotettu taso	Raportointi on kirjallinen.	luku 6.3
2.1.4. Korkea taso	Raportointi perustuu sovittuihin tietoturvatavoitteisiin ja niiden mittareihin.	luku 6.3
2.2. Omaisuuden hallinta		
2.2.1. Suomen erityisvaateet	Organisaation omistamista henkilörekistereistä on Henkilötietolain 10§ mukainen rekisteriseloste ja se on asetettu rekisteröityjen nähtäville.	10.16
2.2.2. Suomen erityisvaateet	Kustakin tietojärjestelmästä on Julkisuuslain 18§ mukainen tietojärjestelmäkuvaus.	12.1
2.2.3. Perustaso	Organisaatiossa on luettelot organisaation omistamista ja käyttämistä fyysisistä tai virtuaalisista laitteista, tietojärjestelmistä, palveluista sekä ohjelmistoista ja lisensseistä.	luvut 12.1 ja 12.3
2.2.4. Perustaso	Laitteiden, rekistereiden ja tietojärjestelmien omistajuus on organisoitu ja vastuutettu.	luku 14, 15
2.2.5. Perustaso	Laite-, tietojärjestelmä-, palvelu- ja ohjelmistoluettelojen sekä lain mukaisten selosteiden ja kuvausten päivitys on organisoitu ja vastuutettu.	luku 10
2.2.6. Korotettu taso	Omistaja on dokumentoinut laitteiden, tietojärjestelmien ja rekistereiden tietosisällön.	luku 10

2.2.7. Korotettu taso	Omistaja on luokitellut omaisuuden tarvittavan tietoturvallisuustason mukaisesti.	Käsitellään tietoturvakortissa.
2.2.8. Korotettu taso	Omistajat katselmoivat laite-, rekisteri-, palvelu- ja ohjelmistoluetteloiden sekä lain mukaisten selosteiden ja kuvausten sisällön säännöllisesti.	luku 10
2.3 Tietojenkäsittely-ympäristöjen käyttöönotto ja poisto		
2.3.1. Perustaso	Tietojärjestelmän ja työasemien käyttöönottoasennuksessa ja käytöstä poistamisessa otetaan huomioon järjestelmän tietosisällön tietoturvavaatimukset.	luku 10.18, 13
2.3.2. Perustaso	Tietojärjestelmien ja työasemien käyttöönottoon ja käytöstä poistamiseen liittyvät toimenpiteet on vastuutettu ja organisoitu.	luvut 13
2.3.3. Korotettu taso	Tietojärjestelmien ja työasemien ensiasennuksesta ja käytöstä poistosta on kirjallinen ohjeisto, jossa kerrotaan mm. eri turvatasoilla käytettävät tietoturva-asetukset sekä laitteiden käsittelyn ja massamuistien tyhjennyksen menettelyt silloin kun ne siirtyvät ympäristöstä toiseen tai kun ne poistuvat organisaation hallinnasta.	luku 13
2.3.4. Korotettu taso	Ohjeiden päivitys on vastuutettu ja organisoitu.	luku 13
2.3.5. Korkea taso	Korkean tietoturvallisuustason tietojärjestelmät ja työasemat kovennetaan.	luku 13

2.3.6. Korkea taso	Tietojärjestelmät ja työasemat huolletaan niin, että massamuisteilla olevat tiedot eivät joudu ulkopuolisten haltuun.	luku 13
2.4 Tietojenkäsittely-ympäristöjen päivitys ja muutoshallinta		
2.4.1 Perustaso	Laitteiden ja tietojärjestelmien päivitysten tarpeen seuranta, päivityspäätösten teko ja päivitysten asennus on vastuutettu ja organisoitu erityisesti tietoturvapäivitysten osalta.	luku 12.3
2.4.2. Perustaso	Laitteiden ja tietojärjestelmien muutostarpeen seuranta, muutospäätösten teko ja muutosten toteutus on vastuutettu ja organisoitu.	luku 13
2.4.3. Perustaso	Organisaatiolla on periaatteet, jotka kertovat, millaiset päivitykset tai muutokset asennetaan välittömästi ja millaisiin päivityksiin ja muutoksiin käytetään riskitason huomioon ottavaa tarveharkintaa.	luku 12.3
2.4.4. Korotettu taso	Muut kuin päivitys- ja muutoshallintaperiaatteiden perusteella kiireellisinä toteutettavat päivitykset tai muutokset tehdään vain etukäteen sovittuna aikana (ns. huoltoikkuna).	luku 12.3
2.4.5. Korotettu taso	Tietojärjestelmään saadaan asentaa tai liittää vain järjestelmän omistajan hyväksymiä ohjelmia ja laitteita.	luku 12.3

2.4.6. Korotettu taso	Organisaation päivitys- ja muutosperiaatteet ovat kirjalliset.	luku 12.3
2.4.7. Korkea taso	Päivitysten ajantasaisuutta ja onnistumista mitataan ja seurataan.	luku 12.3
2.4.8. Korkea taso	Päivitykset ja muutokset testataan ennen kuin ne otetaan tuotantokäyttöön.	luku 12.3
2.4.9. Korkea taso	Organisaatiossa osallistutaan tietoturvatilanteen seuranta- tai yhteistyöryhmiin.	luku 4.1
2.5 Turva-alueiden muodostus ja niiden välinen suodatus		
2.5.1 Perustaso	Organisaatiossa on tunnistettu ja eriytetty tietoverkon eri suojaustasoa vaativat osat ja eri suojaustason verkkojen välistä liikennettä rajoitetaan ja suodatetaan.	luku 12.4
2.5.2. Perustaso	Organisaatiossa on vastuutettu ja organisoitu palomuurien ja muiden tietoliikennelaitteiden sääntöjen lisääminen, muuttaminen ja poistaminen.	luku 12.4
2.5.3. Perustaso	Palomuurien tai muiden suodatuslaitteiden suodatussäännöt on dokumentoitu.	luku 12.4
2.5.4. Perustaso	Julkisesta verkosta organisaatioon sisäänpäin tulevaa liikennettä rajoitetaan ja suodatetaan ”kaikki liikenne on kielletty ellei erikseen sallittu” -periaatteella. Myös organisaatiosta julkiseen verkkoon lähtevää liikennettä suodatetaan.	luku 12.4

2.5.5. Perustaso	Organisaatiossa on etäkäyttöperiaatteet.	luku 12.4
2.5.6. Korotettu taso	Organisaatiossa on kirjallinen palomuuri- ja liikenteensuodatuspolitiikka sekä kirjallinen sääntöjen päivitysprosessi.	luku 12.4
2.5.7. Korotettu taso	Palomuurien tai muiden suodatuslaitteiden säännöstöjen ajantasaisuutta katselmoidaan säännöllisesti.	luku 12.4
2.5.8 Korotettu taso	Tietoverkkoihin saadaan liittää vain verkon omistajan hyväksymiä laitteita.	luku 12.4
2.5.9. Korotettu taso	Etäkäyttöperiaatteet ovat kirjalliset. Periaatteissa kerrotaan minkälaisilla laitteilla ja mistä verkoista yhteyttä voidaan ottaa sekä mitä järjestelmiä käyttää ja ylläpitää.	luku 12.4
2.5.10 Korkea taso	Tietoverkkoja valvotaan tietoturvapoikkeamien ja -loukkausten varalta ja havaittuihin poikkeamiin reagoidaan.	luvut 12.4 ja 16.2.4
2.6 Pääsynvalvonta		
2.6.1. Perustaso	Tietojärjestelmän omistaja hyväksyy kuinka luotettavaa identiteettiä ja vahvaa tunnistamista järjestelmän sisältämien tietojen käyttöön tarvitaan.	luku 10.10
2.6.2. Perustaso	Sekä onnistuneet että epäonnistuneet sisäänkirjautumiset kirjoitetaan lokiin niin, että yksittäisen	luku 10.1.9

	käyttäjän kirjautumiset järjestelmään voidaan selvittää ja yhdistää hänen henkilöllisyyteensä luotettavasti.	
2.6.3. Perustaso	Huonolaatuisten salasanojen käyttöä estetään.	luku 10.4
2.6.4 Korotettu taso	Organisaatiossa on kirjallinen pääsynvalvontapolitiikka, jossa kerrotaan mm. eri turvatasoilla hyväksyttävät tekniset tunnistusmenetelmät, tunnusten lukitus- ja avausperiaatteet sekä salasanan tai muiden tunnisteiden laatuvaatimukset ja vaihtoperiaatteet.	luku 10.4
2.6.5. Korotettu taso	Pääsynvalvontalokit säilytetään niin, että niitä ei päästä jälkikäteen muuttamaan.	luku 10.5
2.6.6. Korotettu taso	Tunnistuksen epäonnistuminen liian monta kertaa peräkkäin tärkeimpiin järjestelmiin tai palveluihin aiheuttaa tunnuksen lukittumisen.	luku 10.5
2.6.7. Korkea taso	Varmenteiden myöntämisestä, käytöstä ja uusimisesta on kirjallinen ohjeisto ja käytössä olevista varmenteista ajantasainen lista.	luku 10.7
2.6.8. Korkea taso	Korkean tason järjestelmissä pääsynvalvontalokeja ja kirjausketjuja tuotetaan myös järjestelmän sisällä toimimisesta toiminnan vaatimusten mukaisesti.	Ei sovelleta
2.6.9. Korkea taso	Tunnistuksen epäonnistumista sekä muita valtuuksien puutteeseen kariutuvia toimenpideyrityk-	Ei sovelleta

	siä tilastoidaan.	
2.7 Käyttäjien ja käyttövaltuuksien hallinta		
2.7.1. Perustaso	Organisaatiossa on sovittu käyttövaltuuksien hallintaperiaatteet. Tunnusten ja valtuuksien myöntö, muuttaminen ja poisto on organisoitu ja vastuutettu periaatteiden mukaisesti.	luku 10.7
2.7.2. Perustaso	Käyttövaltuudet ovat henkilö- tai roolikohtaisia.	luku 10.4
2.7.3. Perustaso	Käyttövaltuudet perustuvat palvelussuhteeseen tai muuhun kirjalliseen sopimukseen ja järjestelmien käyttö estetään teknisesti ilman tarpeetonta viivytystä perusteen päätyttyä.	luku 10.7
2.7.4. Perustaso	Yksittäisen käyttäjän käyttövaltuudet voidaan selvittää.	luku 10.7
2.7.5. Perustaso	Uuden henkilön tullessa organisaatioon ensimmäinen tunnistus tehdään valokuvallisesta henkilöllisyystodistuksesta tai sähköiseen palveluun rekisteröitymisen osalta käyttäen samantasoista todennusmenetelmää.	luku 10.5, 10.7
2.7.6. Korotettu taso	Organisaatiossa on kirjallinen käyttövaltuuspolitiikka ja hallintaprosessi.	luku 10.7
2.7.7. Korotettu taso	Jokaisella käyttövaltuudella on omistaja.	luku 10.7

2.7.8. Korotettu taso	Järjestelmien käyttövaltuudet katselmoidaan vähintään kerran vuodessa ja tarpeettomat tunnukset, roolit ja valtuudet suljetaan tai poistetaan.	luku 10.7
2.7.9. Korotettu taso	Myöntöprosessista jää jälki, millä perusteella käyttäjälle on myönnetty käyttövaltuus.	luku 10.7
2.7.10 Korotettu taso	Kielletyt työ- ja rooliyhdistelmät on dokumentoitu ja valtuuksia myönnettäessä tai muutettaessa kiellettyjen yhdistelmien syntymistä seurataan ja estetään.	luku 10.4
2.7.11. Korkea taso	Ylläpito- ja pääkäyttäjäoikeuksien määrää seurataan ja tilastoidaan.	10.7.
2.7.12. Korkea taso	Käyttövaltuuksien poistoon kuluvaa aikaa seurataan ja tilastoidaan.	Ei sovelleta
2.7.13. Korkea taso	Organisaatiossa on dokumentoitu menettely käyttäjätunnuksen tai käyttövaltuuksien välittömään poistoon tai passivointiin.	luku 10.7.
2.8.1. Perustaso	Organisaatiossa suodatetaan haittaohjelmia sekä työasematasolla että kaikissa sähköpostin ja www-liikenteen sisääntulo- ja ulosmenopisteissä.	luku 12.4
2.8.2. Perustaso	Haittaohjelmakuvaukset päivittyvät säännöllisesti ja automaattisesti.	luku 12.4
2.8.3. Korotettu taso	Käyttäjiä on ohjeistettu, miten haittaohjelmia levittäviä sähköposteja voidaan yrittää tunnistaa ja mitä tehdä haittaohjelmaepäi-	luku 12.4

	lytilanteessa.	
2.8.4. Korotettu taso	Haittaohjelmistokuvausten ajantasaisuutta valvotaan.	luku 12.4
2.8.5. Korkea taso	Työasema ei saa kytkeytyä korkean tietoturvallisuustason verkkoihin, ellei ole varmistettu että se on puhdas haittaohjelmista.	luku 10.4
2.8.6. Korkea taso	Haittaohjelmasuodatuksen kattavuutta mitataan ja seurataan.	luku 10.4
2.9. Fyysisen ympäristön suojaus		
2.9.1. Perustaso	Organisaatiossa on tunnistettu omien tilojen tarvitsema suojausluokka ja eriytetty eri suojausluokkaa vaativat osat rajoittamalla kulkua tilojen välillä.	luku 16.1
2.9.2. Perustaso	Organisaatiossa on sovittu henkilö- tai roolitasolla, kenellä on pääsy IT-laitetiloihin ja kulunvalvonta on organisoitu tämän mukaisesti.	luku 16.1
2.9.3. Korotettu taso	Tilojen eriytys eri suojausluokkiin on dokumentoitu.	luku 16.1
2.9.4. Korotettu taso	Tietoliikennelaitteiden, -yhteyksien ja kytkentäpisteiden sijainti on otettu huomioon suojausluokittelussa.	luku 16.16.7
2.9.5. Korkea taso	Tiloja ja niissä kulkua valvotaan automaattisesti ja valvontamenettely on dokumentoitu.	luku 16.1
2.9.6. Korkea taso	Ulkopuolisten toimintaa IT-laitetiloissa valvotaan.	luku 16.1
2.10. Varmuuskopiointi		

2.10.1. Perustaso	Organisaatiossa on vastuutettu ja organisoitu varmuuskopioiden ottaminen.	luku 10.14
2.10.2. Perustaso	Organisaatiossa on tunnistettu varmuuskopioinnin kannalta olennaiset suojattavat kohteet ja niistä otetaan varmuuskopioita suunnitelman mukaisesti. Myös varmuuskopioiden palauttaminen on suunniteltu.	luku 10.14
2.10.3. Korotettu taso	Organisaatiossa on kirjallinen varmuuskopiointipolitiikka ja -prosessi, jotka on muodostettu ottaen huomioon toiminnan vaatimukset ja joissa ohjeistetaan varmuus- ja suojakopioiden käsittely siirron ja varastoinnin aikana.	luku 10.14
2.10.4. Korotettu taso	Organisaatiossa otetaan tärkeimmistä järjestelmistä suojakopioita, joita säilytetään eri palotilassa kun varsinaisia varmuuskopioita.	luku 10.14
2.10.5. Korkea taso	Eri järjestelmien varmuuskopioiden palautusta testataan säännöllisesti.	luku 10.14
2.10.6. Korkea taso	Varmuuskopioilta palautettavien tietojen määrää ja palautuksen syitä tilastoidaan.	Ei sovelleta
2.11 Tietoturvapoikkeamien valvonta		
2.11.1. Suomen erityisvaateet	Sähköisten viestien, tunnistamistietojen sekä paikkatietojen luottamuksellisuudesta ja oikeasta käsittelystä huolehditaan myös lokitietojen käsittelyssä (Sähköi-	luku 12.4

	sen viestinnän tietosuojalaki 4§ ja 5§).	
2.11.2. Perustaso	Laitteet, ohjelmistot sekä tietojärjestelmät tekevät riittäviä lokeja ja kirjausketjuja toiminnastaan.	luku 12.4
2.11.3. Korotettu taso	Organisaatiossa on kirjallinen lokienkeräys-, hälytys- ja seurantapolitiikka, joka on muodostettu ottaen huomioon toiminnan vaatimukset.	luku 12.4
2.11.4. Korkea taso	Lokien seurannan perusteella muodostetaan tilannekuvaa ja havaitaan tietoturvapoikkeamia sekä kehitetään toimintaa.	luku 12.4
2.12 Tietojärjestelmien toipuminen häiriöistä		
2.12.1. Suomen erityisvaateet	ICT- järjestelmien omistajat tietävät ICT- varautumiseen liittyvät vastuunsa ja toiminta on organisoitu ja vastuutettu sen mukaisesti.	luku 18.2.1
2.12.2. Perustaso	ICT-järjestelmien häiriöiden selvitys ja niistä toipuminen on organisoitu ja vastuutettu.	luku 18.2.4
2.12.3. Perustaso	Organisaatiossa on yleinen toipumisstrategia ja suunnitelma tärkeimpien omien järjestelmien häiriöille, jossa on mm. johdon hyväksymä tärkeysjärjestys ICT-palveluille.	luku 18.2.2
2.12.4. Korotettu taso	Organisaatiolla on tärkeimmistä järjestelmistä kirjalliset toipumissuunnitelmat.	luku 18.2.2
2.12.5. Korkea taso	Järjestelmien häiriöistä ja niiden syistä pidetään kirjaa. Tietoa käytetään hyväksi riskianalyyseissä ja palvelutasosopimusten teos-	luku 18.2.2

	sa.	
2.13 Tietojärjestelmäkehityksen ja sovellusylläpidon hallinta		
2.13.1. Perustaso	Järjestelmän omistaja hyväksyy, mitä tietoturvallisuustasoa järjestelmän tulee valmiina tai muutosten jälkeen noudattaa.	luku 13
2.13.2. Perustaso	Järjestelmään kohdistetaan riskianalyysi, jolla pyritään löytämään tietoturvavaatimukset tarjouspyyntöön, vaatimusmäärittelyyn tai uuden version asennuksen projektisuunnitelmaan.	luku 13
2.13.3. Perustaso	Hankkivalla organisaatiolla on tietoturvavaatimuksia sisältävä tietojärjestelmien arkkitehtuurilinjaus, jonka mukaisia hankittavien tai kehitettävien järjestelmien tulee olla.	luku ??
2.13.4. Korotettu taso	Järjestelmän toimivuus testataan ennen tuotantokäyttöön ottamista.	luku 13
2.13.5. Korotettu taso	Jos organisaatio hankkii räätälöityjä tietojärjestelmiä tai kehittää niitä itse, organisaatiolla on dokumentoitu tietojärjestelmän kehitysprosessi, jonka eri vaiheissa on otettu tietoturvallisuus huomioon.	luku ??
2.13.6. Korotettu taso	Osana hankinta- tai kehitysprojektia järjestelmästä valmistuu kirjallinen turvallisuussuunnitelma ja käyttäjän ohje, joissa kerrotaan miten järjestelmä suoja-	luku 13

	taan tuotantokäytössä ja millaiset ovat käyttäjiltä vaadittavat tietoturvatoimenpiteet.	
2.13.7. Korotettu taso	Järjestelmän määritykset ja toteutukset on auditoitu tietoturvallisuuden osalta	luku 13
2.13.8. Korkea taso	Tietoturvavastaava tarkastaa järjestelmän tietoturvakuvauksen, -suunnitelman tai -suunnitelmat.	luku 13
2.13.9. Korkea taso	Kehitys- tai räätälöintityön aikana järjestetään katselmointeja tietoturvallisuuden kannalta kriittisiin osiin ja katselmoinneista valmistuu pöytäkirja.	luku 13